Famille Freeman

4 juillet 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

Un système de paiement électronique Peer to Peer

STOCKAGE DE VALEUR + MOYEN D'ÉCHANGE + UNITÉ DE COMPTE

1,7 milliard d'adultes n'ont pas accès au système financier international, tandis que 1,3 milliard d'autres ne sont mal desservis.
Epic Cash libère le potentiel humain en connectant les individus sur le marché international. Rapide, pratiquement gratuit d'utilisation et ouvert à tous.

Version 7.1b **French**

Table des matières

I. Présentation

Epic Cash est le point final dans le voyage vers une véritable monnaie Internet P2P, la pierre angulaire d'un système financier privé. La monnaie Epic vise à devenir la meilleure monnaie digitale au monde en matière de protection de la vie privée. Pour atteindre cet objectif, elle remplit les trois fonctions principales d'une monnaie :

1. **Stockage de valeur** – Peut être conservée, récupérée et échangée à un moment ultérieur, et à une valeur prévisible lorsqu'elle est récupérée ;
2. **Moyen d'échange** – Tout ce qui est accepté comme représentant une valeur standard et échangeable contre des biens ou des services ;
3. **Unité de compte** – l'unité par laquelle la valeur d'une chose est comptabilisée et comparée.

	$ USD	BTC	EPIC
Stockage de valeur	✗	✓	✓
Moyen d'échange	✓	✗	✓
Unité de compte	✓	✗	✓

En 2009, le Bitcoin est apparu comme la première monnaie numérique basée sur une blockchain, et avec elle, trois caractéristiques déterminantes par rapport auxquelles les autres cryptomonnaies sont évaluées:

- **"Sans tiers de confiance"** . personne n'est tenu de faire confiance à une entité centralisée ou à une contrepartie pour que le réseau soit opérationnel ;
- **Immutabilité** – Les transactions ne peuvent pas être annulées
  a. Il devrait être hautement improbable ou difficile de remanier l'histoire de la chaîne ;
  b. Il devrait être impossible pour quiconque autre que le propriétaire d'une clé privée de transférer des fonds associés à cette clé privée ;
  c. Toutes les transactions sont enregistrées dans la blockchain.
- **Décentralisation** – "Les blockchains sont politiquement décentralisées (personne ne les contrôle) et architecturalement décentralisées (aucune faille dans l'infrastructure)... "[1].

Le Bitcoin a ouvert de nouvelles voies sur le plan technologique tout en respectant des principes fondamentaux qui ont fait leurs preuves la structure de sa politique monétaire. Le succès du Bitcoin est fortement lié à son offre limitée combinée à une blockchain fiable, immuable et décentralisée. Epic Cash imite la politique monétaire du Bitcoin qui consiste à réduire l'inflation et l'offre limitée pour s'assurer que la monnaie Epic peut servir de réserve de valeur efficace.

Malgré le succès du Bitcoin, certaines lacunes ont été révélées depuis sa création il y a 10 ans. D'autres projets ont tenté de combler ces lacunes et nous avons étudié les meilleurs d'entre eux pour nous en servir comme point de départ. Nous avons décidé d'utiliser la base du code de Grin et l'excellent travail de plusieurs autres projets pour nous aider à perfectionner les réalisations et découvertes durement accomplies des prédécesseurs d'Epic Cash. Epic Cash possède les qualités essentielles d'une monnaie idéale :

- **Fongibilité** – La valeur d'une unité d'Epic doit toujours être égale à une autre unité d'Epic, tout comme un Yen ou Yuan est toujours égal et substituable par un autre Yen ou Yuan. La concrétisation de la fongibilité dépend en grande partie de la privacité.
- **Mise à l'échelle** – Epic Cash maintient une blockchain efficace, sur laquelle de nouveaux nœuds peuvent être facilement créés sans équipements exigeants en ressources. La blockchain Epic Cash est capable d'au moins deux fois le débit de celle du Bitcoin.
- **Confidentialité** – La blockchain Epic Cash protège l'anonymat des titulaires et utilisateurs d'Epic en protégeant les détails des transactions et est conçue pour être à la fois intraçable et invisible à la surveillance.
- **Vitesse** – Les transactions Epic Cash sont fluides, régulières et sont exécutées beaucoup plus rapidement que sur les générations précédentes de blockchains. Alors que le Bitcoin a besoin de six blocs de 10 minutes pour obtenir une confirmation de transaction complète, les transactions Epic ont lieu dans un seul bloc de confirmation dès qu'un bloc a été miné (1 minute) .

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Confidentialité

L'utilisation contemporaine de l'argent peut être comprise comme le transfert collectif d'unités de compte entre personnes et institutions. Le paysage financier d'un moment donné peut être cartographié en répondant aux questions suivantes :

1. *Qui en possède, et combien en ont-ils ?*
2. *Qui traite avec qui et pour quel montant ?*

Pour les monnaies fiat traditionnelles, ainsi que pour le Bitcoin, nous pouvons répondre à ces questions. Ce faisant, beaucoup de renseignements peuvent être recueillis sur la vie des gens, comme les habitudes de consommation, la possession et les acteurs de la transaction. Il est possible de tirer des conclusions assez précises sur les intérêts et les intentions d'une personne en suivant les transferts de valeur. En l'absence de protection de la vie privée, les données transactionnelles peuvent être des renseignements dangereux entre les mains de tierces parties abusives.

L'utilisation des cryptomonnaies au cours de la dernière décennie montre un continuum de "privacité" dans diverses implémentations blockchain. L'échelle de protection de la vie privée, si l'on en tient compte, va d'ouverte et notoire d'un côté, à anonyme de l'autre. Au fur et à mesure que la privacité disparaît, une pierre angulaire essentielle des cryptomonnaies, l'absence de confiance, se dégrade également. Comme en témoigne le succès des services d'analyse de la blockchain Bitcoin, le Bitcoin se situe davantage vers l'extrémité notoirement transparente du spectre de la confidentialité. Les utilisateurs doivent de plus en plus prendre des mesures pour s'assurer qu'ils ne traitent pas par inadvertance des Bitcoins "**sales**". La solution Epic Cash fait basculer l'aiguille vers l'anonymat et restaure cette propriété essentielle en s'assurant que la confidentialité de l'individu et celle des transactions sont intégrées au système à un niveau fondamental.

Confidentialité de l'identité

Confidentialité de la transaction

Confidentialité de l'identité

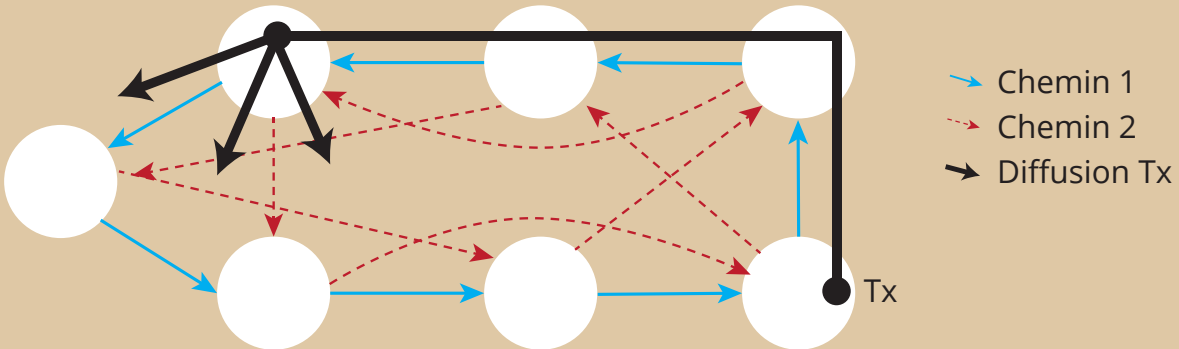
La plupart des cryptomonnaies comme le Bitcoin sont stockées dans des portefeuilles dont les adresses se rapportent à des clés publiques dérivées des clés privées d'un portefeuille. Ces adresses peuvent être considérées comme des balises du coffre-fort privé d'une personne dans le monde digital. La blockchain Epic Cash élimine complètement les adresses et applique à la place une multisignature à partir de laquelle toutes les clés publiques et privées sont générées pour un usage unique.

Parce que les adresses de portefeuille Bitcoin sont la balise d'un coffre-fort dans le monde digital, ce portefeuille peut être relié à l'adresse IP (Internet Protocol) d'un propriétaire, qui le rattache à un ordinateur dans un endroit unique à un moment donné dans le temps. Explication simple : lorsqu'une transaction Bitcoin a lieu, la transaction est diffusée à partir d'un hub de communication appelé " nœud ", puis est diffusée aux autres nœuds appelés " pairs ". Cette information se propage ensuite rapidement aux pairs de chacun de ces nœuds de façon consécutive sur l'ensemble du réseau. Ce processus s'appelle à juste titre le "Gossip Protocol". Chaque Bitcoin a tout simplement une position en ligne visible et un emplacement physique où lui, ou plutôt le propriétaire du Bitcoin, peut être trouvé. Comme l'a souligné la journaliste Grace Caffyn, le Bitcoin n'est " pas plus confidentiel qu'une recherche Google depuis une connexion Internet à domicile ".[2]

En plus d'éliminer les adresses de portefeuille, la blockchain Epic Cash assure la confidentialité de l'identité en s'assurant que les adresses IP ne peuvent pas être tracées. Il le fait grâce à l'intégration du protocole ***Dandelion++***. Le Protocole ***Dandelion++***, qui constitue une amélioration par rapport à son prédécesseur, le Protocole ***Dandelion*** original, est le résultat du travail continu de sept chercheurs pour vaincre la désanonymisation des attaques sur la blockchain. Grâce à ***Dandelion++***, les transactions sont passées sur des trajets entrelacés aléatoires, ou " câbles ", puis soudainement diffusées à un vaste réseau de nœuds, comme les gousses d'une fleur de pissenlit lorsqu'elles sont soufflées depuis leur tige (Figure 1). Il est donc pratiquement impossible de retracer les transactions jusqu'à leur source, et donc leurs adresses IP d'origine.

Figure 1: Anonymisation des transactions avec le protocole *Dandelion++*.

Dandelion++ transmet les messages sur l'un des deux trajets entrelacés d'un graphique à quatre trajectoires régulières, puis les transmet par diffusion. Dans la figure, la transaction se propage sur le chemin solide bleu[3]. Ce processus rend extrêmement difficile le retraçage des transactions jusqu'à leur source, ce qui permet de préserver la confidentialité.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Confidentialité de la transaction

La blockchain Epic Cash assure la confidentialité des transactions en masquant les montants et la relation expéditeur-récepteur d'une transaction. Ceci est possible grâce à l'application d'idées bien connues tirées de ***Confidential Transactions (CT)***[4] et de ***CoinJoin***[5], méthodes en grande partie développées par Gregory Maxwell (développeur Bitcoin Core, co-fondateur et CTO de Blockstream).

CT, créé à l'origine par Adam Back, puis perfectionné par Maxwell, fonctionne en divisant les transactions en plus petites parties grâce au chiffrement homomorphe, une méthode de calcul des informations chiffrées sans décryptage préalable pour préserver leur confidentialité. Une fois divisés, les observateurs ne peuvent pas voir les montants réels des transactions en raison de facteurs opaques, un système qui jette des nombres aléatoires dans le mélange des fragments de transaction pour masquer les valeurs de ces fragments. En fin de compte, seuls les participants (acteurs) d'une transaction connaissent la valeur d'un échange, tandis que la transaction est vérifiée par le réseau par la confirmation que la somme des valeurs de sortie est égale à la somme des valeurs d'entrée et que la somme des facteurs opaques des sorties est égale à la somme des facteurs opaques des entrées.

Pour compliquer davantage la tâche des curieux, toutes les transactions Epic Cash sont masquées par ***CT,*** puis mélangées pour cacher les liens entre les parties à la transaction. Ceci est fait par le deuxième concept de Maxwell, ***CoinJoin***.

Pour illustrer ***CoinJoin*** de manière simple, imaginez que A, B et C envoient des Epic à X, Y et Z, respectivement. Envoyé par le biais de ***CoinJoin***, tout ce que l'on sait, c'est que A, B et C envoient et X, Y et Z reçoivent, tandis que les montants des transactions restent invisibles. Le système ***CoinJoin*** est fondamental pour Epic Cash à travers les signatures combinées à sens unique (OWAS), qui combinent toutes les transactions d'un bloc en une seule transaction.

Confidentialité : Résumé

La blockchain Epic Cash protège la confidentialité des individus et de leurs transactions en :

- **Éliminant les adresses de portefeuille - Il n'y a pas d'identificateurs d'emplacement pour les chambres fortes numériques à l'intérieur de la blockchain. Les transactions sont construites directement de personne à personne sur une base portefeuille à portefeuille ;**
- **Transactions confidentielles - diviser les transactions en plusieurs parties et introduire des facteurs d'opacité dans la collection de ces éléments, de sorte que les valeurs des parties et autres paramètres des transactions ne peuvent être connus ;**
- ***Protocole Dandelion++* - opacifie le cheminement numérique d'une transaction de l'adresse IP de l'expéditeur de la transaction ;**
- ***CoinJoin* - combine les transactions en groupes pour masquer les relations entre les participants de la transaction.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Fongibilité

Charlie Lee, le créateur de Litecoin, a déclaré que la fongibilité était la seule propriété d'une monnaie saine manquant dans Bitcoin et Litecoin, admettant que la confidentialité et la fongibilité étaient les prochains terrains de bataille pour ces monnaies[6]. Andreas Antonopoulos, l'un des plus grands experts blockchain mondiaux, a affirmé que "...les monnaies marquées sont destructrices. Si vous brisez la fongibilité et la confidentialité, vous brisez la monnaie."[7]

La fongibilité est la propriété d'un ensemble de biens ou d'actifs qui garantit que les unités individuelles de cet ensemble sont de valeur égale et interchangeables. C'est ce qui différencie les premières formes de monnaie des systèmes de troc précédents. Sans fongibilité, l'argent perd rapidement son utilité. Comme nous le verrons ci-dessous, la fongibilité de la plupart des cryptomonnaies est incertaine, alors que l'architecture de confidentialité d'Epic Cash garantit qu'elle est imperméable à ces menaces.

La plupart des cryptomonnaies similaires au Bitcoin, par la nature des blockchains transparentes sur lesquels elles existent, peuvent être tracées de manière vérifiable à travers chaque portefeuille dans lequel elles étaient conservées. Des tiers privés et des gouvernements surveillent la blockchain Bitcoin avec des moyens de plus en plus sophistiqués pour identifier rapidement les monnaies utilisées dans les activités précédentes. Cela conduit naturellement à craindre qu'un jour les monnaies marquées ne soient interdites de toute transaction, laissant ainsi les détenteurs de bonne foi lésés.

Le 19 mars 2018, l'Office of Foreign Asset Control (OFAC) des États-Unis a annoncé qu'il envisageait d'ajouter les adresses des monnaies numériques à la liste des ressortissants spécialement désignés (SDNs), qui sont des entités avec lesquelles il est interdit pour les personnes ou entreprises américaines de faire des opérations commerciales. Plus troublant encore, l'OFAC n'a pas exclu l'inclusion des adresses détenant actuellement des monnaies marquées sur la liste SDN, ce qui placerait des propriétaires innocents de cryptomonnaies marquées sur une liste noire criminelle en raison de l'affiliation des monnaies qui leur appartiennent à de précédentes activités illégales. C'est ce qui a conduit Andrew Hinkes, professeur de droit à l'Université de New York, à dire " adieu à la fongibilité " et que le public devrait s'attendre à " un surcoût sur les monnaies fraîchement émises, ou sur les monnaies propres marquées... "[8].

Avec ces développements, il n'est pas difficile d'imaginer un bouleversement du marché crypto et la souffrance, voire l'extinction, de nombreuses cryptomonnaies bien établies. Cependant, Epic est l'une des rares cryptomonnaies qui évite entièrement ce problème en raison des fortes caractéristiques de confidentialité décrites précédemment dans cet article. En supprimant le lien entre l'identité et la propriété, et la relation entre les participants de la transaction, Epic ne peut jamais être affiliée à une personne ou à une activité. En tant que tel, la valeur d'Epic reste indépendante de ses utilisateurs et offre des niveaux élevés de confidentialité et de sécurité qui ne peuvent pas être facilement manipulés par des acteurs malveillants dans les domaines criminel, financier ou politique.

> **“...les monnaies marquées sont destructrices. Si vous brisez la fongibilité et la confidentialité, vous brisez la monnaie.”**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Mise à l'échelle

Epic Cash est une implémentation blockchain MimbleWimble qui produit des avancées en matière de mise à l'échelle grâce à une conception peu encombrante qui élimine les données de transaction redondantes. La fonctionnalité Cut-Through qui en est responsable assure que la blockchain devient plus efficace dans le temps, contrairement à la plupart des cryptomonnaies, y compris Bitcoin, et que de nouveaux nœuds peuvent être créés avec un investissement minimal en mémoire et en puissance informatique. En restant peu encombrant, il permet de disposer d'un réseau très dispersé et favorise la décentralisation. De plus, alors que chaque noeud Bitcoin doit stocker toute la chaîne, les noeuds Epic Cash sont capables de contribuer à la sécurité du réseau grâce à un petit sous-ensemble de blocs.

La plupart des cryptomonnaies exigent le stockage indéfini de toutes les données de transaction sur leurs blockchains. La chaîne Bitcoin augmente actuellement de 0,1353 Go chaque jour, tandis que la chaîne Ethereum augmente à un rythme encore plus rapide de 0,2719 Go par jour. Si la chaîne de Bitcoin continue de croître à son rythme actuel, elle atteindra une taille d'environ 6 To d'ici à ce que son dernier bloc soit miné en 2140. L'Ethereum dépassera 10 TB à cette date[9]. Dans la plupart des blockchains sans MimbleWimble, les transactions doivent être vérifiées par des nœuds dans le monde entier. Plus les données augmentent, plus la charge de travail de chaque nœud augmente. Même à seulement 200 Go (la taille approximative de la chaîne Bitcoin actuelle), la synchronisation des données nécessite un réseau stable et une capacité de lecture et d'écriture de disque à grande vitesse.

Par conséquent, le minage est devenue de plus en plus centralisée au sein de grands groupe de minage qui tirent parti de ressources informatiques coûteuses. **Si l'historique complet de la blockchain Bitcoin devait être stocké sur la blockchain Epic Cash, il prendrait presque 90% de place en moins.** Plus petit, c'est plus rapide, car chaque transaction nécessite moins de temps pour être transmise et sécurisée.

MimbleWimble résout ce dilemme de stockage grâce à une méthode innovante de taille de blocs, appelée 'Cut-Through'. Afin de comprendre comment Cut-Through fonctionne, il est préférable d'examiner d'abord comment les transactions et les blocs sont composés dans une blockchain MimbleWimble.

Entrées:

Références à d'anciennes sorties ;

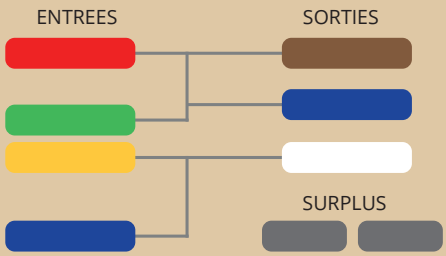
Sorties:

Sorties confidentielles des transactions et preuves de portée (**rangeproofs**) ;

Surplus:

La différence entre les sorties et les entrées, plus les **signatures** (pour l'authentification et pour prouver la non-inflation).

Figure 2:
Parts d'une transaction MimbleWimble



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Tous les blocs Epic Cash contiennent :

Arborescence Merkle des entrées ;

Arborescence Merkle des sorties et des preuve de portée ;

Une liste des valeurs en surplus et des signatures.

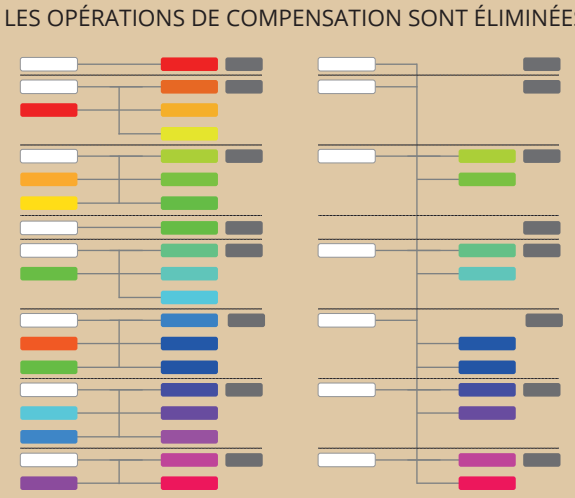
Dans les figures 2 et 3, adaptées des présentations d'Andrew Poelstra[10], nous pouvons voir les Epic **fraîchement** minés **représentés** par les cellules d'entrées blanches. Les cellules de couleur identique représentent les sorties avec les entrées correspondantes. Avec le processus Cut-Through, les entrées et les sorties correspondantes dépensées sont supprimées pour libérer de l'espace à l'intérieur du bloc, ce qui réduit la quantité de données qui doit être stockée sur la blockchain. Bien que les transactions soient omises du registre, les noyaux excédentaires restants (seulement 100 bytes) attestent en permanence que les transactions ont eu lieu.

Au fur et à mesure que les blocs continuent d'être générés, MimbleWimble applique Cut-Through à travers les blocs, de sorte qu'à long terme, il ne reste que les en-têtes de bloc (environ 250 bytes), les transactions non dépensées et les noyaux de transaction (environ 100 bytes). Grin, la deuxième implémentation de MimbleWimble lancée, a montré qu'une chaîne MimbleWimble avec un nombre de transactions similaire à la chaîne Bitcoin représenterait presque 10% de la taille de la chaîne Bitcoin[11]. De plus, la taille d'un nœud sera "de l'ordre de quelques Go pour une chaîne de la taille de celle du Bitcoin, et potentiellement optimisable à quelques centaines de **méga-octets**."[12]

Ceci contraste nettement avec le Bitcoin, où l'ensemble de sa blockchain doit être stockée par chaque nœud. Avec le temps, au fur et à mesure que l'efficacité de la blockchain Epic Cash augmente par rapport à la chaîne Bitcoin, l'efficacité des coûts par rapport à la participation des nœuds dans le réseau Epic Cash augmente également. L'abaissement des obstacles à la participation contribue à assurer une résilience cruciale au niveau des nœuds dans la conception du réseau.

Grâce à l'implémentation de MimbleWimble et à l'application de la réduction de la chaîne avec le processus Cut-Through, la blockchain Epic Cash offre une extensibilité souvent ignorée par la communauté crypto. Elle reflète l'essence même du Bitcoin et de projets similaires : la décentralisation. Indépendamment du nombre de transactions par seconde qu'une monnaie peut traiter, à quoi bon si elle ne peut être soutenue par un réseau large et diversifié ? Si les exigences en matière de mémoire sont telles que la validation finit par s'orienter vers des conglomérats de minages puissants, tous les efforts de la communauté crypto pour créer un écosystème décentralisé sont alors rendus vains. Afin d'assurer un meilleur débit, une implémentation d'une deuxième couche de type Lightning est prévue comme objectif à court terme dans la feuille de route d'Epic Cash.

Figure 3:
Transactions MimbleWimble avant et après le Cut-Through.



[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Politique monétaire

La politique monétaire d'Epic Cash et du Bitcoin est très similaire. L'offre en circulation d'Epic Cash se développe d'abord rapidement et se synchronise ensuite avec l'offre de Bitcoin en 2028. Il augmente ensuite à un rythme décroissant jusqu'à atteindre une offre maximale de 21 millions d'Epic en 2140. Epic Cash a les qualités pour devenir un stockage sûr de valeur à long terme parce que l'approvisionnement en circulation est connu à tout moment de son cycle de vie des émissions et aboutit à un plafond fixe. La politique monétaire Epic Cash se caractérise par les quatre caractéristiques suivantes :

- Émission rapide au cours des neuf premières années de sa durée de vie, au cours desquelles 20 343 750 Epic (96,875 % de l'approvisionnement total) seront minés. Les taux d'émission exacts sont décrits dans la section Calendrier des émissions du présent document ;
- Un approvisionnement maximum de 21 millions d'Epic sera atteint en 2140, à peu près au même moment que lorsque Bitcoin atteindra un approvisionnement maximum de 21 millions d'unités ;
- Les débits d'émission et de circulation d'Epic se synchronisent avec ceux du Bitcoin sur la Singularité Epic vers le 24 mai 2028. Après la singularité, le taux d'émission diminue à un rythme croissant, tandis que l'offre en circulation augmente à un rythme décroissant ;
- Epic est divisible en 8 décimales, de sorte que : 1 Epic est égal à 100 000 000 freemans (tout comme 1 Bitcoin est égal à 100 000 000 satoshis).

La politique monétaire d'Epic Cash s'inspire de celle du Bitcoin pour les raisons suivantes :

- Accord avec les fondamentaux économiques du Bitcoin, à savoir que la rareté et la prévisibilité de l'offre en circulation sous-tendent sa forte capacité de stockage de la valeur ;
- Le public connaît déjà le modèle du Bitcoin et ses résultats éprouvés au cours des dix dernières années depuis sa création. En se synchronisant approximativement avec la réserve en circulation du Bitcoin, et en reflétant la réserve maximale et la structure de divisibilité du Bitcoin, Epic prend le chemin de la moindre résistance vers une adoption massive.

VI. Calendrier d'émission

Epic Cash a un total de 33 périodes de minage, chacune définie par des diminutions des récompenses de blocs, par rapport à leur **période** précédente. Le Genesis d'Epic, la date à laquelle le bloc #1 d'Epic est miné, a lieu le août 2019. Les blocs sont produits à raison d'un par minute. Les cinq premières époques produisent près de 97% de l'offre maximale d'Epic, ce qui correspond à 20 ans d'émissions de Bitcoin en environ neuf ans. Cela peut être considéré comme une opportunité de " revenir en arrière " pour ceux qui ont raté l'ascension spectaculaire du Bitcoin.

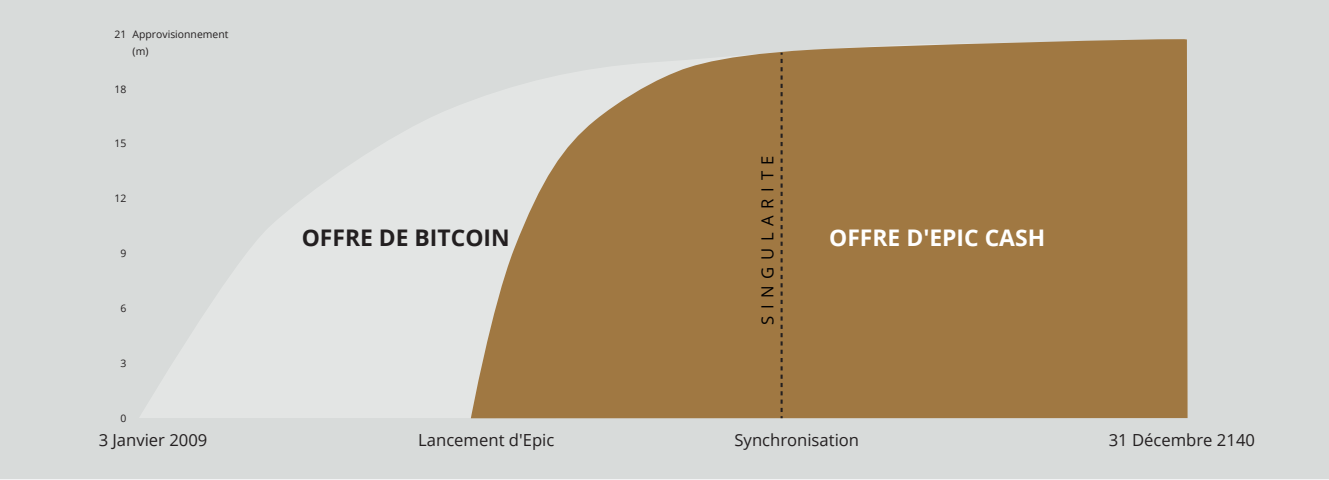
Le tableau 1 indique les dates de début et de fin des sept premières périodes de minage, les récompenses de blocs correspondantes et les quantités en circulation qui en découlent pour chaque époque. Les époques 8 à 33 ne sont pas incluses dans le tableau par souci de concision. Pour ces époques, il devrait suffire de comprendre que chaque ère suivante aura une récompense en bloc égale à la moitié de la récompense de l'ère précédente, exactement comme pour le Bitcoin. La quantité d'Epic émise à chacune de ces époques sera la somme des récompenses de bloc sur une période de 4 ans (environ 1460 jours).

Au niveau de la singularité d'Epic (2028), l'offre en circulation d'Epic croise la quantité en circulation de Bitcoin, à ce moment, Epic Cash adopte la récompense de bloc Bitcoin et le modèle de halving, qui voit les primes de bloc diminuer de moitié tous les 4 ans. La seule exception est que les blocs Epic continuent d'être minés à raison d'un par minute, contre un bloc toutes les dix minutes pour le Bitcoin. Ce faisant, la circulation d'Epic maintient une parité approximative avec la circulation de Bitcoins pour le reste de leur existence.

Tableau 1 : Calendrier des émissions pour les sept premières périodes de minage. Les dates sont approximatives.

Période	1	2	3	4	5	SINGULARITE	6	7
Récompense de bloc	16	8	4	2	1		0.15625	0.078125
Date de début	1er Août 2019	29 Juin 2020	11 Oct 2021	3 Juin 2023	10 Août 2025		24 Mai 2028	22 Mai 2032
Date de fin	29 Juin 2020	11 Oct 2021	3 Juin 2023	10 Août 2025	24 Mai 2028		22 Mai 2032	20 Mai 2036
Durée (en jours)	334	470	601	800	1019		1460	1460
Approvisionnement de départ	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Approvisionnement de fin	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% du total	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Figure 4 : Calendriers des émissions d'Epic et de Bitcoin.



VII. Minage

La blockchain Epic Cash va dans le sens de la décentralisation en accueillant une grande variété de matériel de calcul. Le minage d'Epic est initialement disponible pour les CPU, GPU et ASIC, en utilisant trois algorithmes de hachage respectifs : RandomX, ProgPow et CuckATOO31+. Les algorithmes peuvent être trivialement commutés sans compromettre l'intégrité de la chaîne.

1 RandomX et CPUs

RandomX est un algorithme de preuve de travail (PoW) optimisé pour les CPU tout usage. Il utilise des exécutions de programmes aléatoires avec plusieurs techniques à difficulté de mémoire pour atteindre les objectifs suivants :

- Prévention du développement des ASIC monopuce ;
- Minimiser l'avantage de l'efficacité du matériel spécialisé par rapport aux processeurs tout usage

Le Minage d'Epic avec CPU nécessite une allocation contiguë de 2 Go de RAM physique, 16 Ko de cache L1, 256 Ko de cache L2, et 2 Mo de cache L3 par thread de minage[13]. Les périphériques Windows 10 nécessitent 8 Go de RAM ou plus. Il n'est pas inconcevable qu'un jour, dans un avenir proche, les téléphones mobiles puissent devenir des nœuds de minage viables. L'intégration précoce du CPU dans le réseau minier d'Epic Cash est une excellente opportunité pour beaucoup de personnes ne disposant que de moyens informatiques modestes pour obtenir des récompenses de bloc tout en sécurisant le réseau Epic Cash.

2 ProgPow et GPUs

La preuve programmatique du travail (ProgPow) est un algorithme qui dépend de la bande passante mémoire et du calcul de base de séquences mathématiques aléatoires, qui tirent parti de nombreuses fonctions de calcul d'un GPU et exploitent ainsi efficacement le coût énergétique total du matériel. Comme le ProgPow est spécifiquement conçu pour tirer pleinement parti des GPU standards, il est à la fois difficile et coûteux de réaliser des gains d'efficacité significativement plus élevés grâce à du matériel spécialisé. En tant que tel, l'algorithme ProgPow atténue les incitations pour les grands groupes ASIC à faire concurrence aux GPU, comme on le voit souvent avec de nombreux autres algorithmes PoW, tels que le SHA-256 du Bitcoin. Les GPU, bien que moins répandus que les CPU, sont encore couramment disponibles. Grâce au développement technologique mené par les sociétés de production de matériel, Nvidia et AMD, les GPU sont capables de traiter en parallèle beaucoup plus de puissance de minage que les CPU. C'est grâce à cette combinaison d'ubiquité et de puissance de traitement élevée que les GPU constitueront l'épine dorsale d'une grande partie de l'activité de minage au cours des premières périodes, comme indiqué au tableau 2.

3 CuckATOO+31 et ASICs

CuckATOO31+ est une permutation ASIC de l'algorithme Cuckoo Cycle développé par l'informaticien néerlandais John Tromp. Un parent du CuckAROO29 résistant à l'ASIC, CuckATOO31+ génère des graphes bipartites aléatoires et astreint les mineurs à trouver une boucle de longueur donnée 'N' passant par ses points.

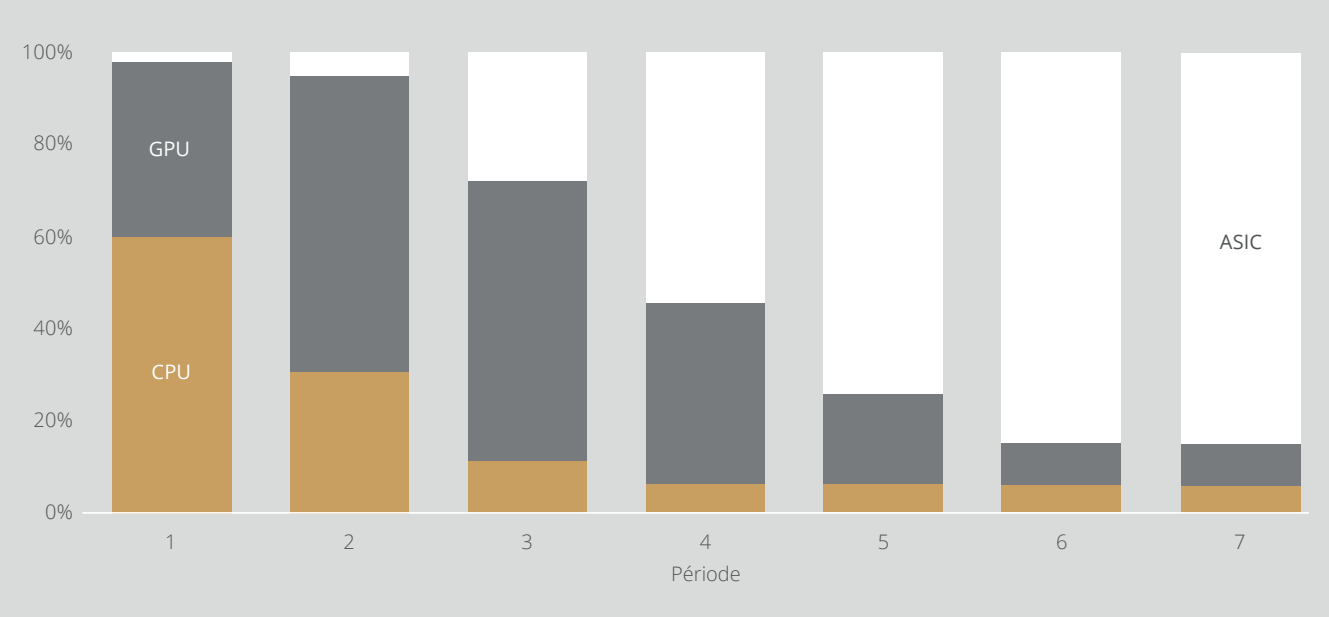
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Il s'agit d'une tâche liée à la mémoire, ce qui signifie que le temps de résolution est lié à la largeur de bande mémoire plutôt qu'à la vitesse du processeur brut ou du GPU. Par conséquent, les algorithmes du cycle Cuckoo produisent moins de chaleur et consomment beaucoup moins d'énergie que les algorithmes PoW traditionnels. Le CuckAToo31+ compatible ASIC permet d'améliorer l'efficacité par rapport aux GPU en utilisant des centaines de Mo de SRAM tout en restant congestionné par des I/O de mémoire[14]. En fin de compte, les ASIC offrent les plus grandes économies d'échelle potentielles des trois options de minage. Toutefois, dans un souci d'inclusion, bien qu'ils se voient attribuer une petite partie des récompenses de minage par rapport aux CPU et GPU dès le début, les ASIC finiront par prendre une participation majoritaire dans les récompenses des blocs minés, en supposant qu'il y aura un écosystème concurrentiel de fabricants de dispositifs pour CuckAToo31+.

Tableau 2 : Attributions de récompenses de minage. Sous réserve de modifications. Les affectations seront orientées de manière à assurer une décentralisation maximale et conforme aux intérêts à long terme du réseau.

Période	1	2	3	4	5	6	7
Jours	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

Figure 5 : Attributions de récompenses de minage pour chaque période selon le tableau 2. Sous réserve de modifications.



[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Contributions de minage

A partir du Genesis Epic (2019) et jusqu'à la singularité Epic (2028), pendant le processus de minage, il y a une allocation d'Epic qui est redirigée, comme contributions de minage, vers la Fondation EPIC Blockchain.

La Fondation EPIC Blockchain se consacre au développement technique et à la promotion de la notoriété et de l'utilité du projet Epic Cash au cours des premières années de sa création, en créant des activités de marketing et en développant des partenariats dans le secteur des technologies financières.

Après la Singularité, le rôle de la Fondation EPIC sera assumé par l'EPIC Distributed Autonomous Corporation (EDAC), qui sera développée par la Fondation avant le transfert.

La Fondation EPIC Blockchain est financée par un pourcentage des récompenses de minage, déduit des récompenses de bloc, selon les barèmes annuels suivants :

Tableau 3 : Barème annuel des contributions de minage de la Fondation en pourcentage des récompenses de minage.

Année	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% des récompenses de minage	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Conclusion

Epic vise à être reconnu comme 'argent digital décentralisé', un moyen d'échange équivalent à la position reconnue du Bitcoin comme or digital décentralisé. En réintroduisant la fongibilité perdue sur une dorsale matérielle beaucoup plus économe en énergie et écologique, Epic Cash fait pencher la balance du pouvoir en faveur des utilisateurs individuels, en contraste flagrant avec les récentes tendances centralisatrices. La combinaison du modèle économique du Bitcoin, de la théorie des jeux et de la formule éprouvée de preuve du travail avec le meilleur de la technologie contemporaine de la blockchain permet d'obtenir une monnaie ne nécessitant pas de tiers de confiance, immuable et décentralisée (Epic) qui est évolutive, fongible et qui protège la confidentialité de ses utilisateurs. La blockchain Epic Cash est ouverte, publique, sans frontières et résistante à la censure. Elle préserve la confidentialité et la fortune de ses utilisateurs et récompense ceux qui emploient leur matériel pour contribuer au réseau par le minage. Chaque Epic est miné par la preuve de travail. L'approvisionnement commence à zéro et le réseau est considéré comme lancé équitablement, avec un réseau test fonctionnel en fonctionnement.

Faits essentiels sur Epic Cash :

- **Le minage débute le août 2019.**
- **La blockchain Epic Cash est basée sur MimbleWimble.**

  Les caractéristiques qui définissent le protocole sont :

  1. **Cut-Through** – la suppression des informations redondantes de la blockchain afin de promouvoir l'efficacité, d'encourager une participation à grande échelle à la validation du réseau et de gérer la décentralisation ;
  2. ***CoinJoin*** – le regroupement des transactions au sein d'un bloc pour assurer la fongibilité de la cryptomonnaie Epic ;
  3. ***Dandelion++ Protocol*** – la propagation des transactions par la communication sur des canaux imbriqués et la diffusion sur un large réseau de nœuds, rompant ainsi les liens entre les transactions et leur origine ;
  4. **No Wallet Addresses** – l'utilisation d'une grande multisignature pour générer des clés privées à usage unique pour les participants à la transaction, éliminant complètement le besoin d'adresses de portefeuille.

- **La politique monétaire d'Epic Cash** est conçue pour synchroniser le nombre total d'Epic en circulation avec le nombre de Bitcoins en circulation dans environ neuf ans, et atteindre le même total maximal de 21 millions d'unités en même temps que le Bitcoin, en l'an 2140. Cette politique, de moins en moins inflationniste, garantit la transparence, la prévisibilité de l'offre et la rareté, favorisant ainsi la sécurité du stockage de la valeur à long terme.

- **Minage** qui intègre des CPU, GPU et ASIC via les algorithmes RandomX, ProgPow et CuckATOO31+ correspondants, pour faciliter l'adoption massive et l'efficacité du réseau.

IX. Caractéristiques Techniques

Nom du projet : Epic Cash
Nom de la monnaie : Epic
Temps de bloc : 60 secondes
Taille de bloc : 1 MB
Approvisionnement de départ : 0
Approvisionnement final : 21 000 000
Bloc Genesis : août 2019
Consensus : RandomX (CPU), ProgPow (GPU) et CuckATOO31+ (ASIC)

Liens :

www.epic.tech

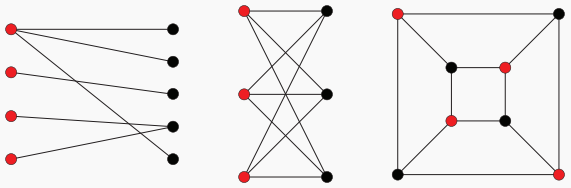
t.me/EpicCash – Telegram

t.me/EpicCashFrancais

X. Lexique

ASIC Application Specific Integrated Circuits ; puces spécialisée dans l'exécution une tâche unique.

Graphe Bipartite un ensemble de graphes décomposés en deux ensembles disjoints de sorte qu'aucun des deux sommets d'un même ensemble ne soit adjacent.



Facteur d'opacité un élément aléatoire introduit dans un message numérique pour faciliter le chiffrage ; un secret partagé entre les deux parties qui chiffre les entrées et sorties de cette transaction spécifique ainsi que les clés publiques et privées des parties à la transaction[16].

Récompense de bloc le nouvel Epic distribué par le réseau comme récompense pour les calculs effectués pour vérifier les transactions dans un nouveau bloc.

Cache un composant matériel ou logiciel qui stocke les données afin que les demandes futures de ces données puissent être traitées plus rapidement.

Approvisionnement en circulation la quantité d'Epic existant à un moment donné.

CPU Central Processing Unit : composant informatique responsable de l'interprétation et de l'exécution de la plupart des commandes provenant des autres matériels et logiciels de l'ordinateur.

Cut-Through un processus de la blockchain MimbleWimble par lequel les entrées et les sorties dépensées correspondantes sont supprimées pour libérer de l'espace à l'intérieur du bloc, réduisant ainsi la quantité de données nécessaires pour être stockées sur la blockchain.

Décentralisation l'état de dispersion des opérations et de la gouvernance d'un réseau.

Émission la création de nouveaux Epic gagnés par les mineurs en récompenses de bloc. Un Epic est créé toutes les 60 secondes lorsque les transactions sont confirmées dans la blockchain.

Singularité Epic le point auquel le total en circulation d'Epic se synchronisera avec le total en circulation du Bitcoin (mai 2028).

Excess (MimbleWimble) la différence entre les sorties et les entrées, plus les signatures (pour l'authentification et pour prouver la non-inflation).

Fongibilité la propriété d'un bien ou d'une marchandise par laquelle des unités individuelles sont interchangeables, et chacune de ses parties ne peut être distinguée d'une autre partie.

Genesis le minage du premier bloc Epic et la création officielle de la blockchain.

GPU Graphics Processing Unit : Unité contenant une puce logique programmable (processeur) spécialisée dans les fonctions d'affichage. Les GPU grand public peuvent être bien adaptés au minage de cryptomonnaie.

Halving (Bitcoin) a lieu tous les 4 ans. Le taux d'approvisionnement diminue de 50 % après chaque halving.

Hash une valeur calculée à partir d'un numéro d'entrée de base à l'aide d'une fonction de hachage.

Algorithme de Hachage (fonction) algorithme mathématique qui associe des données de taille arbitraire à un hachage de taille fixe utilisé pour générer et vérifier des signatures numériques, des codes d'authentification de messages (MACs) et d'autres formes d'authentification.

Chiffrement homomorphe une méthode permettant d'effectuer des calculs sur des informations chiffrées sans les décrypter.

Immutabilité (en programmation) l'état dans lequel un objet ne peut être modifié après sa création.

Entrée (MimbleWimble) le composant d'une transaction MimbleWimble représentant la partie émettrice de la transaction ; créé à partir des sorties des transactions précédentes.

I/O input/output; la communication entre un système de traitement de l'information, tel qu'un ordinateur, et le monde extérieur, éventuellement un système de traitement de l'information humain ou autre.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Approvisionnement maximum	la quantité d'Epic à atteindre à partir de laquelle l'approvisionnement en circulation n'augmentera plus par la suite (21.000.000 Epic).
Difficulté de mémoire	l'utilisation d'une grande quantité de RAM pour éviter que des connexions simultanées n'exécutent des tentatives en parallèle. Les fonctions de mémoire difficiles sont des algorithmes dont les temps de calcul sont principalement déterminés par la mémoire disponible pour contenir les données.
Arborescence Merkle	une structure de données utilisée dans les applications informatiques. Dans les blockchains, les arborescence Merkle permettent une vérification efficace et sécurisée des contenus de grandes structures de données.
MimbleWimble	un protocole proposé par un contributeur pseudonyme, surnommé Tom Elvis Jedusor, dans un Chat de développeurs Bitcoin.
Multisignature	un système de signature digitale qui permet à un groupe d'utilisateurs de signer un seul document. Habituellement, un algorithme à signatures multiples produit une signature conjointe qui est plus compacte qu'une collection de signatures distinctes de tous les utilisateurs.[17].
Nœud	un ordinateur qui se connecte à un réseau blockchain et se branche à d'autres nœuds du réseau pour distribuer des informations sur les transactions et les blocs, en peer-to-peer.
One Way Aggregate Signature (OWAS)	une signature de transaction composée de plusieurs signatures qui est chiffrée de telle sorte qu'il est très difficile de calculer les signatures individuelles qui font partie de l'ensemble.
Sortie (MimbleWimble)	la composante d'une transaction MimbleWimble représentant la réception de la transaction ; utilisée comme entrée pour les transactions ultérieures.
Schéma d'engagement de Pedersen	une primitive cryptographique qui permet à un prouveur de s'engager sur une valeur choisie sans révéler aucune information à son sujet et sans que le prouveur ne soit en mesure de se rétracter.
Private Key	une clé privée est un petit morceau de code qui est jumelé à une clé publique pour déclencher des algorithmes de chiffrement et de déchiffrement de texte. Il est créé dans le cadre de la cryptographie à clé publique au cours du chiffrement à clé asymétrique et utilisé pour déchiffrer et transformer un message dans un format lisible.
Proof of Work (PoW)	une donnée difficile à produire (coûteuse et chronophage), mais facile à vérifier pour les autres et qui répond à certaines exigences. Les preuves de travail sont souvent utilisées dans la génération de blocs crypto.
Public Key	une clé publique est créée dans la cryptographie utilisant un algorithme de cryptage basé sur les clés de chiffrage asymétriques. Cette clé sert à crypter un message dans un format illisible.
RAM (Random Access Memory)	puces de stockage de données à accès rapide dans un dispositif informatique où le système d'exploitation (OS), les programmes d'application et les données en cours d'utilisation sont conservés afin qu'ils puissent être rapidement accessibles par le processeur de l'appareil.
Rangeproof	un contrôle des engagements qui vérifie que la somme des entrées de la transaction est supérieure à la somme des sorties de la transaction et que toutes les valeurs de la transaction sont positives. Les preuves de portée permettent de s'assurer que le total monétaire en circulation n'a pas été trafiqué.
(Digitale) Signature	une composante standard d'un protocole blockchain, principalement utilisée pour sécuriser les transactions et les blocs de transactions, le transfert d'informations, la gestion des contrats et tout autre cas où la détection et la prévention de toute manipulation externe est importante. Ils offrent trois avantages pour le stockage et le transfert d'informations sur la blockchain : • Ils révèlent si les données envoyées ont été trafiquées ; • Vérifie la participation d'une partie particulière à la transaction ; • Prouve l'engagement de ses signataires;
SRAM (Static Random Access Memory)	Random Access Memory (RAM) qui conserve les bits de données dans sa mémoire tant que l'alimentation est fournie.
Débit	la mesure des transactions par seconde qui peuvent être effectuées par un protocole de cryptomonnaie donné.
Sans tiers de confiance	caractéristique d'un réseau ne nécessitant pas l'intervention d'une autorité centrale (tiers de confiance) pour que les règles du protocole soient respectées.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH