

---

# Roburst Network Whitepaper

---

*Présenté par l'équipe de Roburst Network*



*2018*

Roburst Network

---

Version 1.0b

Avertissement .....	4
Préface .....	8
Introduction .....	9
1. <i>Blockchain</i> , crypto-monnaies et pourquoi ce sont des opportunités.....	9
2. Roburst Network et le Roburst Coin .....	11
3. Le Roburst Trading Bot.....	13
4. Banque numérique et l'avenir du paiement.....	14
5. Aperçu de l'ICO .....	16
6. À lire si vous ne continuez pas la lecture à la section suivante .....	19
Roburst Network .....	21
1. La crypto-monnaie de Roburst (Roburst Coin) .....	21
1.1. Roburst Coin .....	21
1.2. Sécurité .....	21
1.3. Transactions .....	22
1.4. Blocs .....	24
1.5. iDPOS.....	26
1.6. Récompenses du réseau.....	29
1.7. Taux d'inflation .....	30
1.8. Le pool de transactions.....	31
2. Roburst Main Network (Roburst Network) .....	32
2.1. RoburstBridge™ .....	32
2.2. La carte Roburst et le paiement sans espèces .....	33
2.3. Roburst Trading Bot .....	34
2.4. L'équipe Roburst Network .....	35
2.5. Roadmap .....	39
ICO .....	41
1. Roburst Bonus Coin (Bonus ROC).....	41
2. Investisseurs early-bird .....	41
3. L'étape de prévente.....	42
4. Les étapes de l'ICO .....	43
5. Parrainage.....	44
Appendix.....	46

References .....47

# Avertissement

En participant à la prévente et/ou à l'ICO (Initial Coin Offering) de Roburst Network ou en utilisant toute information disponible dans ce whitepaper/sur le site internet de Roburst Network (à l'exception des sites internet de tierce partie utilisant les Roburst Coin en tant que système de paiement) vous acceptez les conditions suivantes :

## AVERTISSEMENT GÉNÉRAL

En utilisant les services fournis par Roburst Network, vous (l'utilisateur), que ce soit en tant que participant à l'ICO (ci-après prévente et/ou ICO ou vente publique) ou client des produits et/ou services de Roburst Network, comprenez entièrement et acceptez les dispositions suivantes :

1. L'utilisateur doit comprendre et accepter que les coins Roburst Network seront fournis par Roburst Network à partir du bloc de génèse. Aucune modification ne peut y être apportée par une tierce partie.
2. L'utilisateur reconnaît que Roburst Network n'engage aucune responsabilité quant à la possibilité de participer à la prévente et/ou l'ICO pour des raisons qui sont hors du contrôle de Roburst Network incluant, sans s'y limiter, la durée de la prévente/de l'ICO, les délais lors des transactions et les problèmes liés aux délégués.
3. L'utilisateur doit comprendre que l'équipe de Roburst Network se concentrera sur la complétion des tâches incluses dans la roadmap afin de les livrer en temps et en heure. En revanche l'équipe Roburst Network n'a aucune obligation d'agir pour ou dans l'intérêt de l'utilisateur lors des étapes de la prévente/de l'ICO.
4. L'utilisateur doit comprendre qu'en transférant de l'argent ou d'autres bien à Roburst Network il prend une décision finale et qu'il n'a aucun droit au remboursement. Seuls deux cas permettent à l'utilisateur de transférer de l'argent ou d'autres bien hors de Roburst Network :
  - Le montant minimale de vente n'est pas atteint, ce qui a pour conséquence que tout argent, ou autres biens, déposés seront renvoyés à l'utilisateur sur le portefeuille de son choix.

- Avant et après les étapes de l'ICO nous autoriserons les utilisateurs à transférer leurs biens hors de Roburst Network. En revanche, si le montant des biens à transférer est supérieur à 25 000 dollars l'utilisateur devra avoir un compte vérifié afin de réaliser le transfert
5. L'utilisateur doit comprendre que la durée de chaque étape de la prévente/de l'ICO peut varier en fonction du nombre restant de coins mis en vente par Roburst Network pour chaque étape. Les étapes de la prévente/de l'ICO peuvent se terminer plus tôt que prévu. L'utilisateur recevra un courrier électronique l'informant de la fin de l'étape de vente.
  6. L'utilisateur reconnaît que toute activité suspecte réalisée depuis son compte peut mener au bannissement de celui-ci. Si besoin Roburst Network fournira les preuves de l'activité suspecte sur le compte de l'utilisateur. L'utilisateur doit demander ces preuves endéans 7 jours. Passé ce délai Roburst Network ne garantit pas la disponibilité de ces preuves.

#### **AVERTISSEMENT LIÉ AUX TAXES**

L'utilisateur doit comprendre que Roburst Network n'agit pas en tant qu'agent fiscal pour l'utilisateur ; L'utilisateur et Roburst Network gèrent leurs obligations fiscales en vertu des lois locales de leur lieu de résidence. Roburst Network n'est pas un agent fiscal et ne doit donc pas fournir d'informations financières sur l'utilisateur à de tierces parties. Ces informations ne seront en aucun cas transmises.

#### **PAS DE GARANTIES**

Toutes les informations dans ce whitepaper sont fournies « telle-quelle » et sans aucunes garanties. Aucunes garanties explicites ou implicites, incluant les garanties de qualité marchande ou d'adéquation à un usage particulier, ne sont faites vis-à-vis l'information ou l'usage de l'information sur ce site ou cette plateforme. Roburst Network ne fait aucune représentation et n'offre aucune garantie quant à la précision et l'exhaustivité des informations contenues dans ce whitepaper ou sur cette plateforme.

#### **EXCLUSION DE RESPONSABILITE**

Roburst Network exclu toute responsabilité en cas de perte ou de dommage subit résultant de l'usage ou du mésusage de toute information ou contenu de ce whitepaper ou du site internet de Roburst Network. Roburst Network exclu toute

responsabilité en cas de perte ou dommage résultant de l'usage, du mésusage ou de la confiance accordée à toute information ou contenu de ce whitepaper ou du site internet de Roburst Network.

En aucun cas Roburst Network ne sera responsable vis-à-vis de l'utilisateur pour tout dommage, particulier, indirect, accessoire, immatériel, dommages et intérêts (incluant la perte de revenus ou de profits et l'incapacité de réaliser les économies attendues découlant de toute demande liée aux services fournis par Roburst Network) que la réclamation soit basée sur la garantie, le contrat, le délit (incluant la négligence ou la responsabilité stricte) ou autre raison similaire.

### **À UTILISER À VOS RISQUES ET PÉRILS**

En participant à la prévente et/ou à l'ICO de ROC, en utilisant la plateforme de Roburst Network ou le site web de Roburst Network, incluant sans s'y limiter les actifs transférés à Roburst Network, l'utilisateur confirme qu'il comprend et assume tous les risques directs ou indirects liés à sa participation à la prévente et/ou à l'ICO et/ou son usage des produits et services de Roburst Network.

### **FORCE MAJEURE**

L'utilisateur comprends que Roburst Network ne saura être tenu responsable pour tout manquement aux présentes, incluant la non livraison ou le délai dans la livraison des services, occasionnés par des causes indépendantes de la volonté de Roburst Network. Cela comprend, sans s'y limiter, la non disponibilité du matériel, les grève, les ralentissement et arrêt de travail, le manque de main-d'œuvre, la fermeture, le feu, les inondations, les tremblements de terre, les tempêtes, la sécheresse, les intempéries, les émeutes, les vols, les accidents, les embargos, la guerre (déclarée ou non) et autres déclenchement d'hostilités, les guerres civiles, les actions gouvernementales, les actions divines, les lois ou règlements gouvernementaux, les ordonnances ou injonctions, ou autres raisons, qu'elles soient similaires ou pas aux précédentes (chacune étant un "cas de force majeure").

### **DERNIERE AVERTISSEMENT**

La participation à la prévente et/ou à l'ICO peut être considérée comme du trading à haut risque. L'achat d'instruments financiers via une prévente et/ou une ICO, ou l'utilisation des services offerts sur le site web peuvent conduire à des pertes importantes voire totales de tous les fonds investis.

1. Aucune informations fournis sur la plateforme ou le site web de Roburst Network ne doit être interprétée comme un conseil d'investissement. Elles ne constituent pas une offre ou une invitation de Roburst Network envers l'utilisateur à acheter ou vendre des jetons ou à investir.
2. L'utilisateur garantit être une personne légalement capable, majeure et répondre aux règles juridiques et aux lois applicables dans la juridiction où il réside.
3. En participant à la prévente et/ou à l'ICO, l'utilisateur confirme avoir lu, compris et accepte de se conformer à toutes les restrictions énoncées ci-dessus.

# Préface

L'apparition d'internet a ouvert une nouvelle ère de la vie numérique qui a vu naître de nombreux nouveaux termes. Vous avez sûrement entendu parler de courrier électronique aussi connu en tant qu'e-mail, de commerce électronique, ou e-commerce, pour faire court. Pourtant il y a un terme dont vous avez sans doute entendu parler et dont l'ampleur peut vous surprendre : crypto-monnaie. Dans les années 2000 les monnaies électroniques (ou monnaies numériques) étaient une telle mode que chaque entreprise voulait sa propre monnaie. Les problèmes arrivèrent lorsque de plus en plus de ces monnaies furent piratées, leur côté centralisé rendant leur sécurité faible. En 2008 le Bitcoin a réinventé les "monnaies numériques" en étant la première monnaie électronique décentralisée. Depuis elle n'a cessé de prendre de l'ampleur jour après jour. Au cours des 5 dernières années la croissance du Bitcoin a été de 100 000 pour cent et ce n'est pas tout. Pour la première fois dans l'histoire une monnaie virtuelle peut atteindre une capitalisation (« market cap ») de presque 1 billion (1 000 milliards) de dollars. Avec Roburst Network et le Roburst Coin nous espérons réaliser le même miracle que le Bitcoin, et, bien sûr, plus rapidement et de plus grande ampleur.



I.

# Introduction

*Un bref résumé sur les crypto-monnaies et Roburst Network*

## 1. **Blockchain, crypto-monnaies et pourquoi ce sont des opportunités**

Les termes « *Blockchain* » et « *Crypto-monnaie* » sont familiers pour presque tout le monde de nos jours. Pour les autres, la blockchain, de manière générale, est une technologie qui empêche la propriété de se retrouver centralisée. À la différence des monnaies électroniques traditionnelles que l'on trouve sur internet, une monnaie utilisant la blockchain est difficile à pirater et personne ne peut réellement en prendre le contrôle. Pour plus de détails techniques sur le fonctionnement de la blockchain veuillez vous référer au point (1).

Crypto-monnaie est le terme utilisé pour désigner les coins (pièces ou monnaie) utilisant la technologie de la blockchain. Le Bitcoin en est l'exemple le plus marquant par sa popularité et son succès. Le Bitcoin n'est plus uniquement un moyen de paiement mais aussi un bien numérique valant des milliers de dollars. L'utilisation de la technologie de la blockchain rend les transactions en Bitcoin transparentes mais anonymes. La distance n'a plus d'importance lors du transfert d'un pays à l'autre comparé aux monnaies traditionnelles. En revanche la volatilité de son cours rend son usage en tant que moyen de paiement plus compliqué. Il n'y a pas de moyens permettant de garder sa valeur stable, et si c'était le cas personne n'investirait dans ces monnaies. C'est pourquoi nous créons un nouveau moyen de paiement qui peut à la fois être utilisé comme méthode de paiement traditionnel mais aussi un bien que tout le monde veut posséder.

Au fil des ans les gens ont proposé des crypto-monnaies basées sur presque tout. Par exemple l'émission initiale de monnaie (ICO – Initial Coin Offering) ne fait pas référence à la monnaie elle-même mais constitue un moyen de lever des fonds pour une start-up.

Pour vous aider à bien visualiser cela, le graphique ci-dessous montre une comparaison des capitalisations de crypto-monnaies entre elles ainsi que de monnaies traditionnelles.

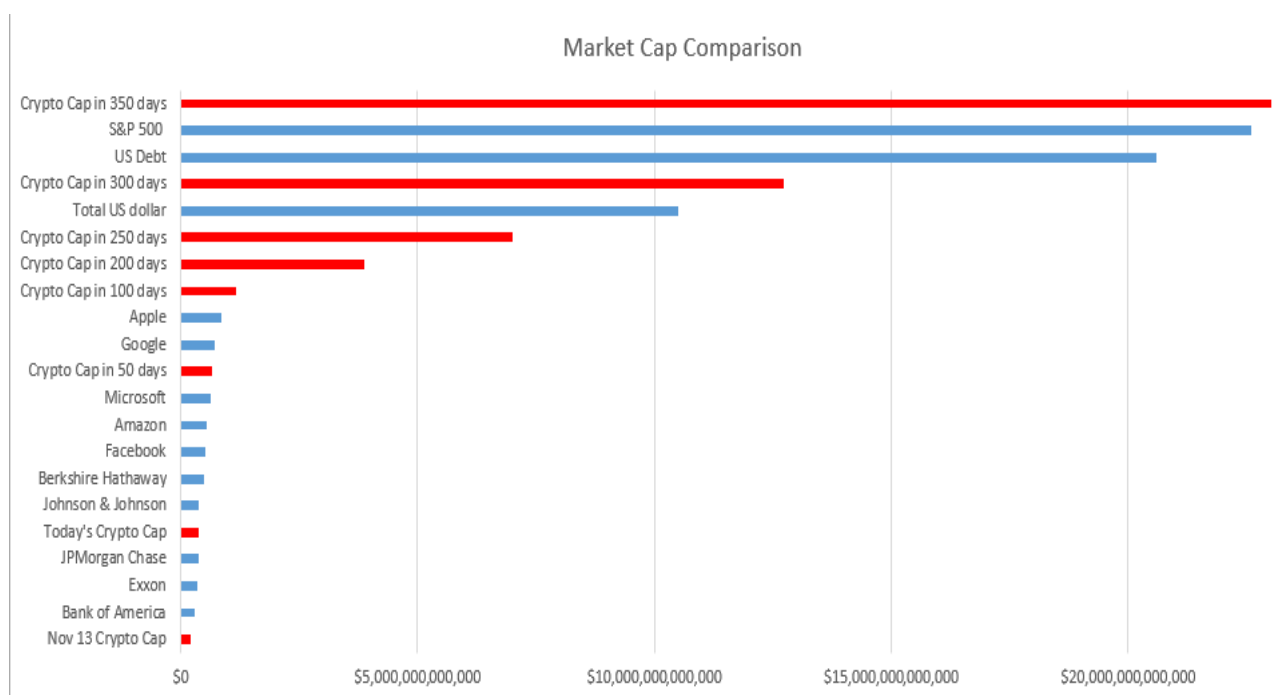


Figure I.1.1: La capitalisation de diverses crypto-monnaies et monnaies traditionnelles

Le graphique montre une augmentation de la capitalisation bien plus forte pour les crypto-monnaies comparées aux autres et la question est : est-ce trop tard pour commencer ? La réponse est non. Dans le monde des technologies tout va si vite que si vous n'arrivez pas à suivre vous êtes vite laissé derrière. C'est pourquoi en introduisant Roburst Network et le Roburst Coin nous sommes convaincus qu'il s'agit d'un investissement prometteur que vous ne voudrez pas manquer.

## **2. Roburst Network et le Roburst Coin**

Le Roburst Coin, en résumé, est comme une crypto-monnaie traditionnelle. Vous pouvez l'envoyer et le recevoir n'importe où, n'importe quand. Le Roburst Coin repose sur le Roburst Network, une série de services qui utilisent le Roburst Coin. Lors de l'introduction du Roburst Coin et du Roburst Network, le premier service à être proposé est le Roburst Trading Bot, un robot qui vous aide à surveiller, prédire le marché des crypto-monnaies pour investir et gagner de l'argent par vous-même, un portefeuille numérique (digital wallet) qui aide les utilisateurs à gérer leurs transactions plus facilement et plus rapidement. Notre vision est d'élargir le réseau à d'autres domaines comme le médical, l'éducation, le commerce électronique, ainsi de suite. Toutes les transactions sur le réseau se feront grâce au Roburst Coin et seront gratuites ce qui signifie qu'il n'y aura pas de frais de transaction quand vous utiliserez un service de notre réseau.

Les développeurs tiers peuvent aussi implémenter la passerelle de paiement Roburst : Roburst Payment Gateway, dans leurs applications et sur leurs sites web, en utilisant l'API fournie par Roburst Network. Le Roburst Payment Gateway sera décrit plus loin dans ce whitepaper. Pour le moment regardons à quoi ressemblera le system de manière simplifiée.

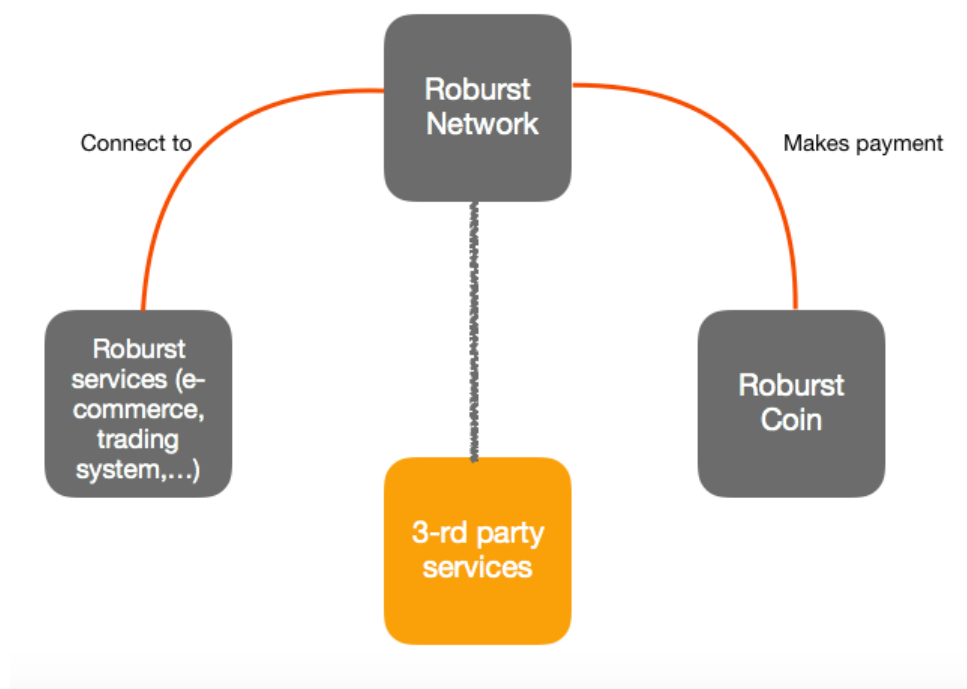


Figure I.2.1: Vue simplifiée du fonctionnement de Roburst Network au sein du système

### 3. Le Roburst Trading Bot

Depuis plusieurs années on constate des avancées significatives au niveau de l'intelligence artificielle : le machine learning et le deep learning. C'est ce que nous avons utilisé dans notre projet pour créer le Roburst Trading Bot (RTB). RTB repose sur TensorFlow, une technologie de deep learning open-source exploitée par Google. Pour le moment RTB est capable de prédire et de trader plusieurs crypto-monnaies, dont les plus populaires : Bitcoin (BTC) et Ethereum (ETH). RTB peut aussi prédire les tendances à la baisse d'une monnaie de sorte à vous donner des stratégies pour de nombreuses situations, bonnes ou mauvaises. Ou vous pouvez laisser RTB choisir la stratégie la plus efficace qu'il aura calculée et réduire vos risques de près de 50%.

Ci-dessous un graphique montrant le retour sur investissement pour l'achat de ces crypto-monnaies entre le 1er Janvier 2017 et le 16 Aout 2017, soit environ 9 mois. Le meilleur retour possible est de 31 620%, soit en achetant pour 1\$ de NEO vous obtiendrez 31620\$ en retour.

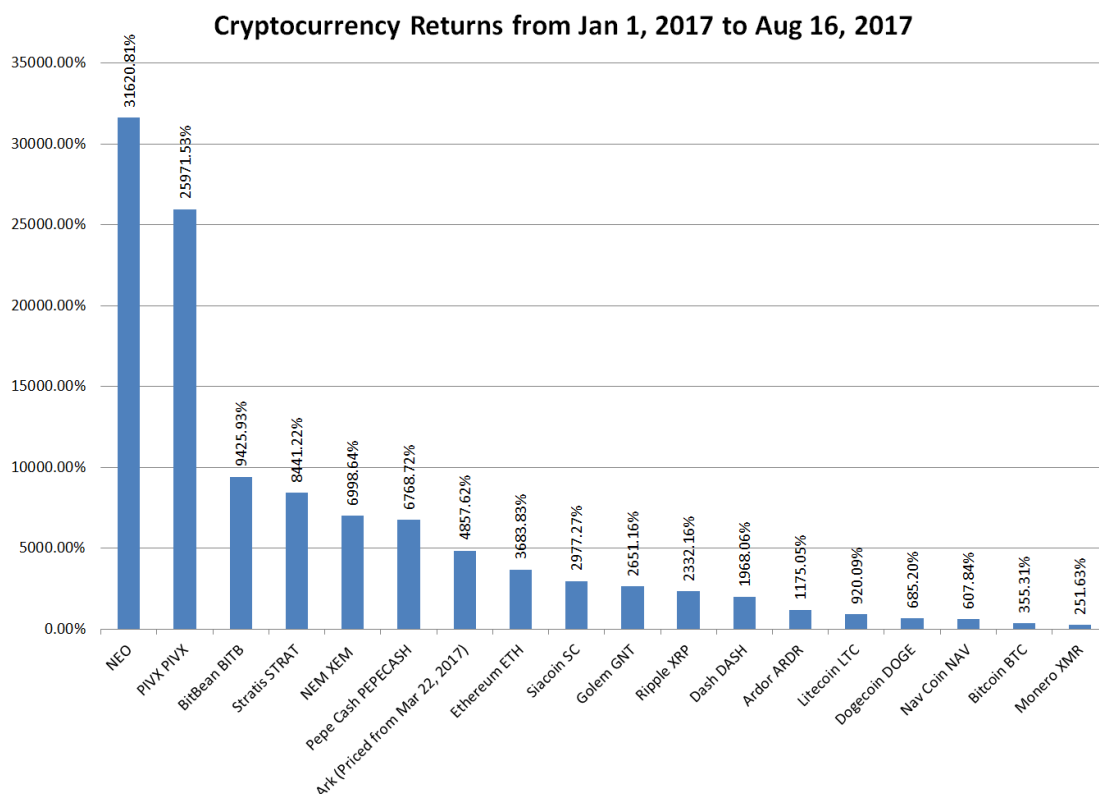


Figure I.3.1: Retour sur investissement pour l'achat de ces crypto-monnaies entre le 1er Janvier 2017 et le 16 Aout 2017, (classée, source CoinMarketCap)

## 4. Banque numérique et l'avenir du paiement

Comme on l'a vu au cours des dernières décennies, le paiement sans espèces est rentré dans la vie de tous. L'explosion d'internet a incité les entreprises à développer de nouvelles méthodes d'achat en ligne. L'une d'entre elles est l'apparition des banques numériques où l'argent liquide devient inutile. Plus personne ne veut d'un sac rempli d'argent qui devient une cible de vol. Avec une simple carte en main on peut payer pour presque tout. La Figure I.4.1 ci-dessous montre qu'en 4 ans, entre 2010 et 2014, l'utilisation du paiement sans espèces a augmenté énormément passant de 311 milliards de dollars à 417 milliards de dollars (d'après une étude du RBR).

Plusieurs technologies se sont suivies pour rendre le paiement sans espèces de plus en plus pratique. Par exemple Samsung Pay et Apple Pay n'utilisent pas de carte mais seulement un téléphone pour réaliser un paiement. L'utilisation du Near-Field Communication (NFC) rend le paiement transparent. L'évolution annuelle prédite de toutes ces méthodes combinées est de 80%, ce qui pourrait porter le volume de paiement via mobile à 4 billions (4 000 milliards) de dollars US en 2020. En 2017 le nombre total d'utilisateurs réguliers, au moins une fois par mois, de solution de paiement sans espèces a atteint les 150 millions à travers le monde.

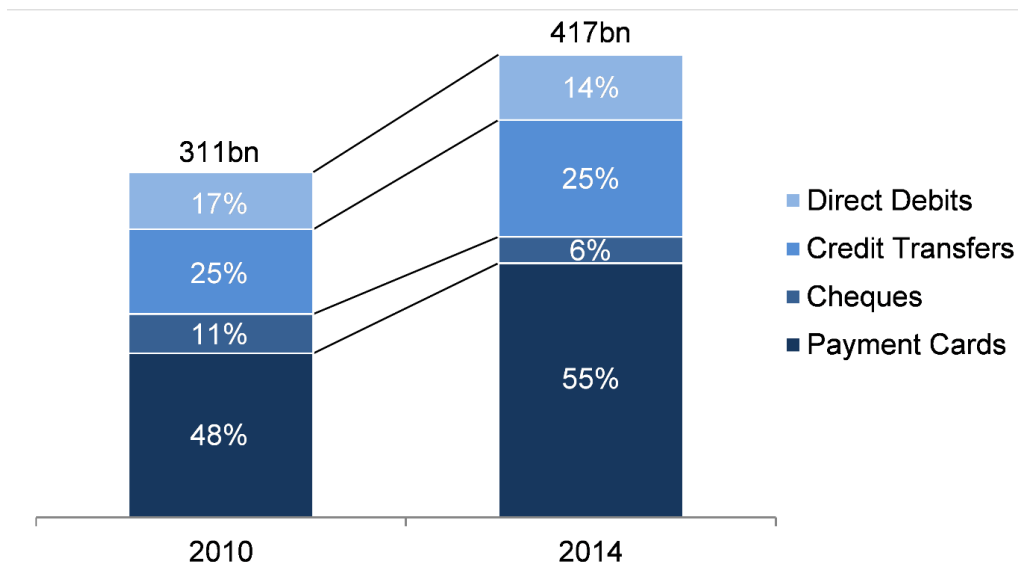


Figure I.4.1: L'augmentation de l'utilisation des méthodes de paiement sans espèces dans le monde de 2010 à 2014

### Number of Apple Pay, Samsung Pay, & Android Pay Contactless Users 2017

	2015	2016	2017
Apple Pay	15	45	86
Samsung Pay	3	18	34
Android Pay	2	12	24

Figure I.4.2: Le nombre d'utilisateurs de méthodes de paiement de proximité (en million, source NFCWorld)

Roburst Network prend place dans ce domaine en émettant la première carte intelligente pour crypto-monnaie (RSC) qui peut vous aider à retirer des espèces avec des frais réduits via n'importe quel distributeur automatique Roburst (Roburst Automatic Teller Machine – RATM) ou directement en payant via les caisses enregistreuses des points de vente Roburst (Roburst Point of Sale – RPOS) sans aucun frais. Toutes ces notions seront décrites dans une prochaine section.

## 5. Aperçu de l'ICO

Afin de faire fonctionner le système et de faciliter le processus transactionnel nous avons décidé de fournir la crypto-monnaie à nos investisseurs early-bird à un prix préférentiel. Le processus démarrera au premier trimestre 2018 et Roburst Network émettra 420 000 000 ROC qui seront distribués au prix initial de 0,00001 Bitcoin (BTC) par ROC.

Pour un aperçu de l'ICO veuillez vous référer au tableau ci-dessous.

Date de début	24 février 2018 – 19h00 CET
Date de fin	25 avril 2018 – 5h00 CET
Durée	60 jours
Nombre de coins en vente <sup>(1)</sup>	315 000 000 ROC
Prix initial par coin <sup>(2)</sup>	0.00001 BTC
Limite technique du nombre de coin <sup>(3)</sup>	Illimité
Hard cap <sup>(4)</sup>	50 million USD
Min cap <sup>(5)</sup>	10 million USD
Date de distribution des coins <sup>(6)</sup>	1 <sup>er</sup> mai 2018 (scenario pessimiste) 25 avril 2018 (scenario optimiste)
Achat minimum	1 ROC
Achat maximum <sup>(7)</sup>	100 000 ROC/compte/jour



Bonus de prévente, appliqué pendant les 30 premiers jours de l'ICO (24 février 2018 – 25 mars 2018)

Bonus alloué	+50% coins	+38% coins	+27% coins	+20% coins
Achat minimum	1 200 000 ROC	500 000 ROC	200 000 ROC	50 000 ROC

Si vous achetez moins de 50 000 ROC vous profiterez d'un bonus early-bird équivalent à 10% du montant acheté.

Pour tout achat à partir de 1 ROC nous avons un bonus de parrainage (8). Pour les détails du fonctionnement de notre système de parrainage veuillez vous référer à la **Section III – ICO**.

(1) : Le nombre de coin en vente inclus les « bounty », les bonus et la prévente.

(2) : Le prix du bitcoin peut varier mais le prix de départ ne varie pas en rapport à la valeur du BTC. Veuillez noter que le prix de vente peut varier, le minimum étant le prix initial.

(3) : Le nombre maximum de ROC que le Roburst Network peut fournir au marché.

(4) : L'ICO prend fin lorsque les ventes atteignent le hard cap. Tous les coins non vendus ou non attribués seront détruits.

(5) : Si l'ICO n'atteint pas le min cap, tous les fonds seront renvoyés vers vos portefeuilles.

(6) : Dans le cas où l'ICO atteint le hard cap avant la date de fin de la vente, nous notifierons tous les investisseurs par e-mail de la nouvelle date de distribution des coins.

(7) : L'achat maximum est le nombre de coins qu'un utilisateur du système peut acheter en un jour. Cette valeur ne s'applique pas lors de la prévente.

(8) : Tous les comptes qui s'enregistrent via votre lien de parrainage seront comptés. Votre portefeuille sera augmenté de 0,1 ROC pour chaque ROC acheté par des comptes parrainés. Pour plus de détails veuillez vous référer à la section Parrainage.

(9) : Les coins de bonus ne peuvent être transféré vers votre portefeuille ou un autre compte durant l'ICO. Après la date de fin les coins de bonus seront automatiquement convertis en coins normaux.

(10) : Un compte actif de parrainage est un compte s'étant enregistré via un lien de parrainage et ayant acheté au moins 0,1 ROC pendant l'ICO.

Pour plus d'information veuillez vous référer à la **Section III - ICO**.

## 6. À lire si vous ne continuez pas la lecture à la section suivante

Si vous comptez lire la section suivant vous pouvez lire ce chapitre à la fin. Autrement, voici une lettre de remerciement de la PDG de Roburst Network, Samantha Wilson.

Chers investisseurs,

Tout d'abord, je voudrais vous remercier pour le temps consacré à la lecture de ce *Whitepaper*. Je suppose que vous avez lu la section 1 et que vous trouvez ce *Whitepaper* ennuyeux. Vu que c'est la première étape de notre plan, nous avons pu faire des erreurs dans son élaboration. Vous trouvez sûrement les termes de ce document soit trop vagues pour les comprendre soit trop simple et endormant. Nous en sommes sincèrement désolés.

Je dois admettre que je ne suis pas forcément la meilleure personne de mon équipe pour vous transmettre ce message, mais, au fond de mon cœur, je souhaite que vous continuiez votre lecture, que vous souhaitiez investir ou pas. Ce n'est pas une chose que vous devriez ignorer, alors que l'on approche du futur des paiements. Les *crypto-monnaies* et les paiements sans espèces en sont les raisons probables. Dans les prochains mois ou années, vous verrez de plus en plus de mesures favorables venant d'internet, notre vie privée fait l'objet de toutes notre attention lorsque que nous sommes connectés. Pour le moment cela peut paraître étonnant pour certains mais il s'agit potentiellement du plus grand investissement que l'on puisse faire dans le futur.

Enfin, si vous pensez que cela peut être votre deuxième chance après le boom du Bitcoin, mais que vous avez encore peur d'investir dans **Roburst Network** et le **Roburst Coin**, contactez-moi par e-mail : [samantha@roburst.network](mailto:samantha@roburst.network) (en anglais de préférence). Je répondrai à vos questions ou inquiétudes sur Roburst Network dès que possible.

Cordialement,

*Samantha*

Samantha Wilson, PDG de Roburst Network

## II.

# Roburst Network

*Quoi, Comment et Pourquoi Roburst Network*

## 1. La crypto-monnaie de Roburst (Roburst Coin)

**Roburst Coin** est une crypto-monnaie développée par *The Roburst Team* en tant que moyen sécurisé d'échange et de paiement, sur internet en général, et au sein de **Roburst Network** en particulier. À la différence du Bitcoin, Roburst Coin utilise l'algorithme de consensus de preuve de possession déléguée (Delegated Proof of Stake – DPoS), conçu par BitShares. Beaucoup d'autres améliorations ont été apportées à l'algorithme DPoS de Roburst, principalement axées sur le système de vote, la confidentialité et la vitesse de transaction. Nous appelons notre algorithme de consensus « Preuve de Possession Déléguée intelligente », intelligent Delegated Proof of Stake en anglais), ou iDPOS pour faire court.

L'iDPOS se concentre principalement sur le règlement de problèmes qui n'ont pas été traités par la méthode DPoS d'origine, comme la centralisation, ou les votes qui pourraient être obtenus par de puissantes parties prenantes (stakeholder). Nous parlerons plus d'iDPOS dans la dernière section.

### 1.1. Roburst Coin

---

Le coin de base de Roburst Network est appelé Roburst Coin ou ROC en abrégé. Il est divisible en  $10^6$  sous-unités

### 1.2. Sécurité

---

**Roburst Coin** utilise le hashage cryptographique comme toute autre crypto-monnaie sur le marché, mais au lieu d'utiliser le ECDSA qu'on retrouve dans le Bitcoin et beaucoup d'autres, nous utilisons EdDSA pour aller plus vite en étant plus sécurisé.

#### 1.2.1. Key pair

Une paire de clés se compose de deux clés, l'une publique et l'autre privée. La clé publique est dérivée de la clé privée mais il est impossible de retrouver la clé privée

à partir de la clé publique. La clé privée ne doit être connue que de son propriétaire. Le processus de génération de la paire de clés est décrit ci-dessous

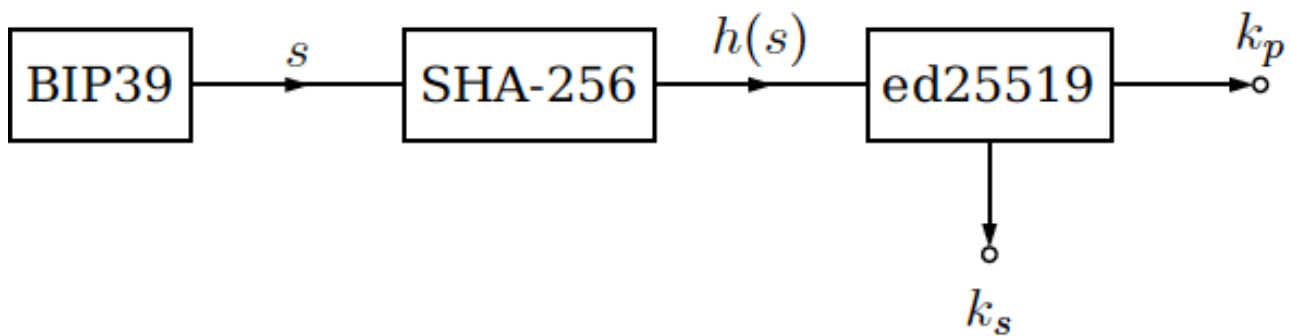


Figure 1.2.1.1: Le processus de génération d'une nouvelle paire de clés

Lorsque l'utilisateur génère une paire de clés, un *BIP39 mnemonics* est créé, puis hashé dans une chaîne de 256 bits. Ce hash est ensuite utilisé comme graine dans ed25519 pour générer une clé privée  $k_s$  et en dériver sa clé publique  $k_p$ .

Avec la paire de clé, l'utilisateur peut utiliser la clé privée pour signer des transactions dans des objets de transaction et les diffuser sur le réseau. Le nœud utilise la clé publique pour vérifier la validité de la signature.

### 1.2.2. Multi-signature

Pour les utilisateurs ayant besoin de sécurité avancée, Roburst Coin offre des comptes à signatures multiples, ce qui signifie que l'utilisateur doit avoir un certain nombre de signatures pour soumettre une transaction. Les utilisateurs qui souhaitent utiliser cette fonctionnalité doivent soumettre un groupe de  $nk_s$  et spécifier le nombre minimum de  $k_s$  requis pour confirmer qu'une transaction est valide. Toute transaction provenant du compte multi-signature doit posséder le nombre minimum de signatures avant d'être traitée.

### 1.2.3. Adresse de portefeuille

L'adresse est dérivée de la clé publique. La clé publique est hashée en une chaîne de 256 bits, puis on prend les 8 premiers octets (soit 64 bits) du hash. L'adresse du portefeuille sera la représentation numérique de ces 8 octets, à laquelle on ajoute la lettre R, qui signifie Roburst.

## 1.3. Transactions

Les transactions en Roburst Coin sont divisées en 5 types représentés dans la table ci-dessous :

Type 0	Transfert de fonds vers une adresse de portefeuille Roburst
Type 1	Enregistrement d'une seconde clé secrète
Type 2	Enregistrement d'un délégué
Type 3	Soumission de vote(s) pour les délégués
Type 4	Enregistrement multi-signature

Figure 1.3.1: Types de transactions dans Roburst Network

Toutes les transactions, quel que soit leur type, doivent être signées avant d'être traitées par le réseau. Le processus de signature d'une transaction est décrit dans la figure ci-dessous :

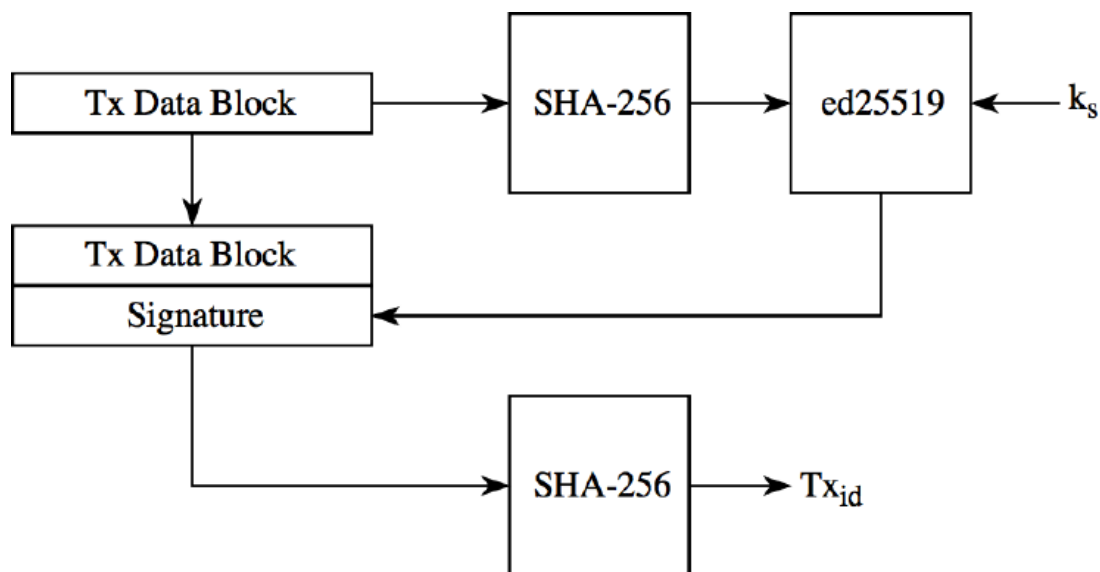


Figure 1.3.2: Le processus de signature d'une transaction à une seule signature

Un bloc de données représentant la transaction doit être généré avec des informations standardisées. Les informations supplémentaires seront différentes selon le type de transaction, mais les champs suivants sont indispensables pour chaque transaction :

- Un entier de 8 bits identifiant le type de transaction

- Un horodatage de 32 bits identifiant l'heure et la date de création de la transaction
- La clé publique de 256 bits de l'émetteur de la transaction
- Un entier de 64 bits représentant la quantité de ROC à transférer

## 1.4. Blocs

Un bloc est composé d'un header (en-tête) et d'une liste de transactions confirmées. Le délégué auquel est attribué un emplacement et dont un nœud est en cours d'exécution génère le bloc suivant et confirme jusqu'à 25 transactions du pool. Ces transactions seront ajoutées à la charge utile du bloc, puis signées dans le bloc.

Le tableau suivant décrit le header d'un bloc :

0	16	32	48	64
Version		Timestamp		
Previous Block ID				
Number of transactions		Length of payload		
Amount of ROC transferred				
Amount of fee				
Reward of the delegate				
Payload hash				
Delegate's public key				

Figure 1.4.1: Description d'un header de bloc

Le processus de signature d'un header de bloc est similaire à la signature d'une transaction. Le header du bloc est hashé avec SHA-256 puis signé à l'aide de la clé secrète du délégué. Par la suite, le Blockid sera généré en utilisant la même logique



que pour une transaction. La figure ci-dessous décrit le processus de signature d'un header de bloc :

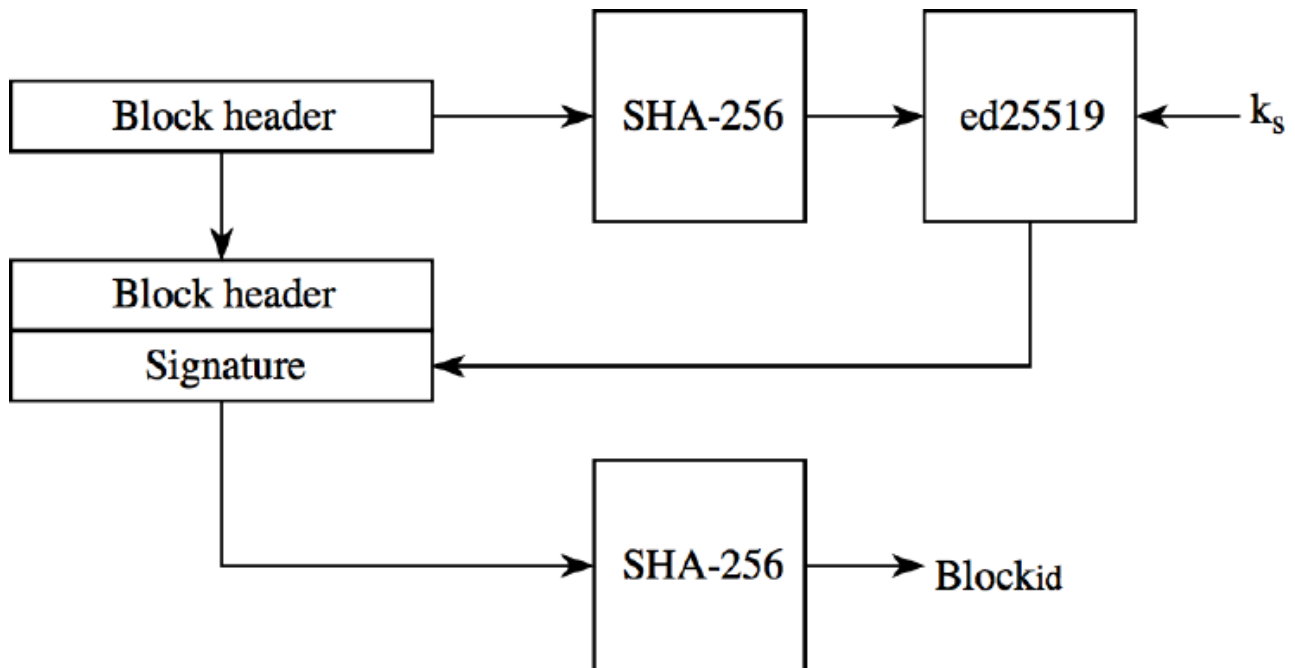


Figure 1.4.2: Le processus de signature d'un header de bloc

La charge utile peut contenir au maximum 25 transactions non confirmées, à condition que la charge utile ne dépasse pas la taille maximum de chaque transaction. Le tableau ci-dessous montre la taille maximum pour chaque type de transaction :

Type de transaction	Taille maximum (octets)
Type 0	220
Type 1	149
Type 2	201
Type 3	2326
Type 4	1223

Figure 1.4.3: La taille maximum de chaque type de transaction

Un bloc est généré toutes les 10 secondes en utilisant le consensus iDPOS. Le processus d'élection sélectionnera un compte pour lui donner le droit de générer le bloc suivant, appelé le délégué. 51% des pairs sont nécessaires pour maintenir

le consensus de broadhash. Le processus de génération sera exécuté lorsque le consensus du broadhash sera établi.

## 1.5. iDPOS

---

L'iDPOS (Intelligent Delegated Proof of Stake) est une méthode améliorée du DPOS original de Bitshares. iDPOS vise à résoudre les problèmes qui existent dans le consensus DPOS actuel ainsi qu'à apporter des améliorations visant la sécurité et la vitesse sur le réseau. Les délégués génèrent tous les blocs du réseau et sont choisis par un système électoral compétitif géré par les parties prenantes (stakeholders). Il y a 101 délégués qui forgent dans le réseau Roburst Coin. Une partie prenante (stakeholder) peut voter pour maximum 101 délégués. Le poids du vote dépend du nombre de Roburst Coin détenu par la partie prenante (stakeholder). Une transaction de vote doit être créée si la partie prenante souhaite voter pour le délégué (Transaction de type 3).

### 1.5.1. Fonctionnalités

#### 1. Les parties prenantes ont le contrôle

Chaque partie prenante (stakeholder) peut voter pour le délégué qui signera le bloc. Ceux gagnant 1% ou plus des votes peuvent rejoindre le conseil. Ils formeront le conseil d'administration et signeront les blocs à tour de rôle. Si l'un d'entre eux rate son tour, les parties prenantes (stakeholder) lui retireront leur vote. Finalement, ces délégués seront éliminés du conseil d'administration et d'autres le rejoindront pour remplir les places vides. Le membre du conseil d'administration recevra une petite quantité de coin pour rémunérer son temps passé à garantir la disponibilité du réseau. iDPOS comporte également un score caché pour chaque membre du conseil d'administration, ce qui signifie qu'ils seront automatiquement renvoyés du conseil d'administration si leur score est inférieur à une valeur prédéfinie. Ce score est calculé en fonction de la disponibilité, la confiance du délégué et de nombreux autres facteurs.

Comme les parties prenantes (stakeholder) gardent le contrôle, le réseau est décentralisé. Aussi imparfait que puisse être le système de vote, lorsqu'il s'agit de partager la propriété d'une entreprise, c'est le seul moyen viable.

## **2. Eco-responsable**

Le processus de minage dans le Roburst Network ne demande presque aucune consommation d'énergie comparé à l'ancienne méthode, preuve de travail (Proof of Work - PoW). Comme de plus en plus de gens minent des crypto-monnaies en utilisant le consensus PoW, l'énergie est gaspillée de manière absurde. L'iDPOS reste décentralisé tout en ne demandant pas d'énergie pour fonctionner.

## **3. Le minage par pool est-il du Proof of Work délégué ?**

Cette question a été posée de nombreuses fois. Quand il s'agit du minage de Bitcoin, l'utilisateur doit choisir un pool, chaque pool pouvant avoir 10% ou plus de la puissance de calcul totale du réseau. Ce processus s'apparente au vote de l'utilisateur pour ses délégués. Au fur et à mesure que le nombre de pools diminue, seulement 5 pools majeurs contrôlent l'ensemble du réseau, le Bitcoin se transforme en une crypto-monnaie centralisée. On essaye de l'empêcher en demandant aux utilisateurs de changer régulièrement de pool. Quand un pool tombe en panne, tout le réseau ralentit et doit attendre que le pool soit réactivé pour revenir à sa vitesse d'origine, ce qui est dangereux comme l'histoire l'a montré.

## **4. Dissuasion vis-à-vis des attaques**

Si un délégué décide de ne pas produire un bloc, ce délégué risque d'être retiré du conseil d'administration et il ne recevra plus aucun profit à l'avenir. Les délégués ne peuvent pas signer de blocs invalides car le bloc doit également être confirmé par les autres délégués.

### *1.5.2. Évolutivité*

En supposant un coût de validation fixe et un prix fixe par transaction, il y a une limite à la décentralisation possible. Si le prix de la transaction est égal au coût de validation, le système est centralisé et ne peut servir qu'un seul validateur. Si le prix de la transaction est 100 fois le coût de validation alors le réseau peut servir jusqu'à 100 validateurs.

Le problème se pose avec le système de consensus Proof of Stake original comme Nxt. Si le système permet à tout le monde d'être validateur le prix des transactions devient excessif. Pour éviter que les couts de transaction n'augmentent, une personne ne peut devenir validateurs que si elle possède 1% ou plus nombre total de coins. Si la chaine considère que 100 validateurs est encore trop centralisé alors il faut augmenter ce nombre à 1 000 ce qui coutera 10 fois plus que iDPOS. Par exemple si la chaine prend de la valeur jusqu'à 10 milliards de dollars alors il faudra posséder 1 million de dollars de coin pour rejoindre le conseil. Pour diminuer ce seuil à seulement 1 000 dollars il faudrait que les frais de transactions soit 10 000 fois plus élevés que ceux d'iDPOS

En conclusion, tout système fonctionnant avec le Proof of Stake traditionnel deviendra centralisé à moins de changer la façon dont le système est exploité. En prenant de la valeur tout système ne supportant pas la délégation deviendra centralisé du fait de ces coûts.

### *1.5.3. Algorithme de vote*

Le système est conçu pour fonctionner uniquement via des votes favorables il n'y a donc pas d'anti-vote dans le système ce qui le rend plus efficace et moins complexe. Les membres du système donnent leur(s) vote(s) à d'autre(s) délégué(s), pendant l'intervalle de maintenance, les votes seront comptés et le résultat prendra effet. L'iDPOS encourage également le vote par procuration (proxy voting), qui désigne le processus de transfert du pouvoir de vote vers quelqu'un d'autre. Ce processus peut être annulé. Le vote par procuration contribue à réduire l'apathie dans le vote et aide les parties prenantes (stakeholder) actives à réagir plus rapidement aux problèmes commerciaux et sécuritaires. De cette façon, les délégués qui se conduisent mal seront virés plus rapidement. Le vote par procuration peut soulever une question sur son côté trop centralisé. Ce processus ressemble au minage par pool du Bitcoin sauf que chaque partie prenante (stakeholder) peut participer et seul le pouvoir de vote est délégué, processus qui, de plus, est réversible. Si les parties prenantes (stakeholder) n'aiment pas le fonctionnement du système, elles peuvent simplement renoncer à leur procuration.

### *1.5.4. Tour de délégué*

Un tour de délégué a exactement N blocs de longueur (avec N actuel est 101, soit le nombre total de délégués actifs qui forgent les blocs). Au début de chaque tour les délégués se verront assigner une position qui indiquera leur ordre dans le processus de génération de bloc. Lors d'un tour chaque délégué forge exactement un bloc. Si un délégué ne parvient pas à forger son bloc alors un autre délégué prendra ce bloc à sa place et le délégué ayant échoué se verra retiré son vote de la part des parties prenantes (stakeholder). Lorsqu'un délégué finit de forger le bloc, le nœud associé au délégué le signera et le diffusera sur le réseau. Une fois cela fait le prochain délégué à forger un bloc sera assigné en fonction de l'ordre prédéfini.

## 1.6. Récompenses du réseau

---

Un nœud de Roburst Network peut bénéficier de nombreuses incitations pour continuer à fonctionner. La première récompense est attribuée lors de la génération de blocs, l'autre récompense est attribuée pour avoir sécurisé le réseau en tant que délégué actif dans le tour de délégué.

Roburst Coin récompense ceux ayant généré des blocs d'une récompense fixe par bloc accepté par le réseau. Tous les délégués actifs dans le réseau recevront la récompense de bloc. Au fur et à mesure que le nombre de blocs générés augmente, la récompense diminue. Cela incitera le délégué à rester actif dans le réseau. La récompense de bloc sera réduite linéairement tous les 3 000 000 blocs, commençant à 5 ROC par tour de forge.

En plus de la récompense de bloc les délégués actifs se partagent également les frais de transactions générés durant le tour. À la fin du tour tous les frais de transactions seront divisés entre tous les délégués actifs. Ces frais peuvent donner aux participants une quantité importante de coins, qui pourrait être supérieure à la récompense de bloc. Si un membre du conseil échoue à forger un bloc alors le membre qui a forgé le bloc à sa place aura le double de la récompense. Il ne pourra plus remplacer d'autres membres échouant à forger leur bloc immédiatement. Ce membre sera qualifié pour remplacer à nouveau un membre échouant à forger son bloc seulement après N tour (N étant le nombre de membres dans le conseil). Le tableau ci-dessous représente les frais de transaction dans le réseau.

Type	Frais
Type 0	0.1 ROC
Type 1	1 ROC
Type 2	20 ROC
Type 3	1 ROC
Type 4	1 ROC/signature

Figure 1.6.1: Les frais de transactions varient par type au sein de Roburst Network

Veillez noter que les frais de transactions pour les transactions de type 0 au sein du Roburst Network ne seront pas imputés au compte effectuant la transaction mais seront sponsorisés. Le membre du conseil recevra quand même les frais de transaction correspondant au type 0.

## 1.7. Taux d'inflation

Du fait de l'existence de la récompense de forge de bloc le taux d'inflation est aussi une préoccupation dans le réseau. En effet en plus de la récompense correspondant aux frais de transaction, les délégués reçoivent également un montant fixe par tour appelé récompense de forge ("forging reward"). Pour s'assurer que le taux d'inflation reste faible la récompense de forge sera réduite chaque 3 000 000 de blocs, soit environ 1 fois par an, jusqu'au minimum qui est de 1 ROC et sera atteint après 4 ans de fonctionnement. Le taux d'inflation attendu est présenté dans le graphique ci-dessous :

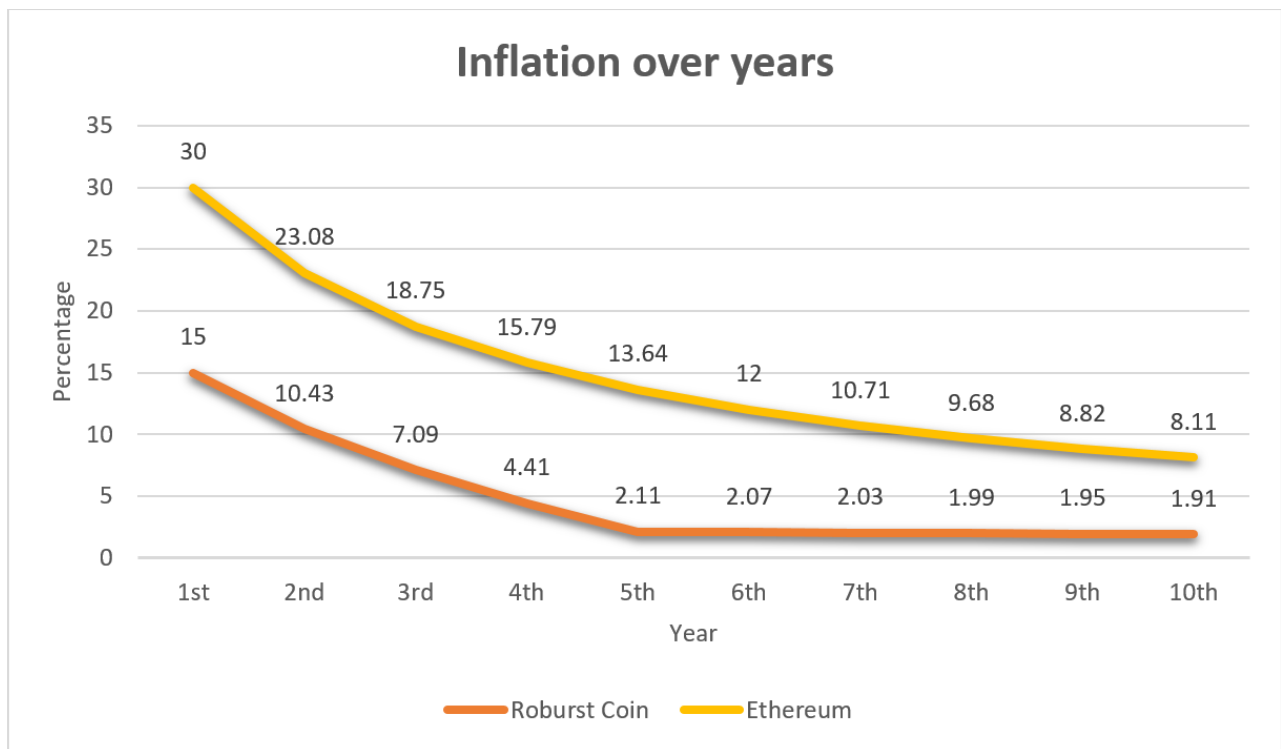


Figure 1.7.1: Taux d'inflation par année comparé à Ethereum

## 1.8. Le pool de transactions

Avec l'évolution du réseau la capacité de 25 transactions par bloc pourrait ne plus suffire à traiter le nombre de transactions simultanées. C'est pourquoi nous avons créé le Roburst Transaction Pool qui conservera les transactions non-confirmées en trop pour les intégrer au prochain bloc. Ce pool servira de maison aux transactions en attente de signature. De cette manière les transactions multi-signatures, dont au moins une signature manque, peuvent attendre d'être complétées sans affecter le processus de génération de blocs. Afin de garder le pool de transactions en ordre, les transactions en attente ont une durée de vie au sein du pool. Dans ce cas il sera de 3h ou 10 800 secondes. Cela signifie que si une transaction en attente ne peut être traitée endéans 1 080 blocs elle sera marquée comme échouée (failed) et sera supprimée.

L'autre utilité du pool de transactions est de servir de mécanisme de propagation des transactions. Le nœud qui prépare le bloc récupère 25 transactions en attente du pool et effectue la validation du bloc. Ensuite ce bloc sera diffusé aux autres nœuds du réseau.

## 2. Roburst Main Network (Roburst Network)

Le réseau principal de Roburst (Roburst Main Network) ou Roburst Network est le lien entre les services utilisant le Roburst Coin en tant que monnaie. Roburst Network fournit plusieurs utilitaires qui aident les utilisateurs mais qui peuvent aussi servir aux développeurs qui bénéficient ainsi de moyens simplifiés d'intégrer Roburst Coin au sein de leurs applications.

### 2.1. RoburstBridge™

---

Puisque Roburst Coin ne supporte pas de méthodes permettant le "sidechain" ou les bases de données d'application distribuée (DApp Database) nous avons développé RoburstBridge™ comme une méthode permettant à n'importe quelle blockchain de recevoir ou d'envoyer des informations, ou de déclencher des fonctions à travers Roburst Network.

RoburstBridge™ va créer un pont entre les blockchains aidant les gens au sein de Roburst Network à communiquer avec d'autres blockchains. Par exemple en créant un service de prêt dans lequel une personne au sein de Roburst Network peut demander un micro crédit et le notifier sur une autre chaîne, comme par exemple Ethereum, et attendre d'être contacté par d'autres personnes au sein de notre réseau. Cette méthode est traitée par un Encoded Listener (service d'écoute encodé) d'abord introduit par ARK puis amélioré par Roburst Network.

Une blockchain existante peut appliquer cette méthode au sein de son réseau en quelques étapes simples fournies par Roburst Network. Le travail de RoburstBridge™ peut être illustré par le graphique ci-dessous :



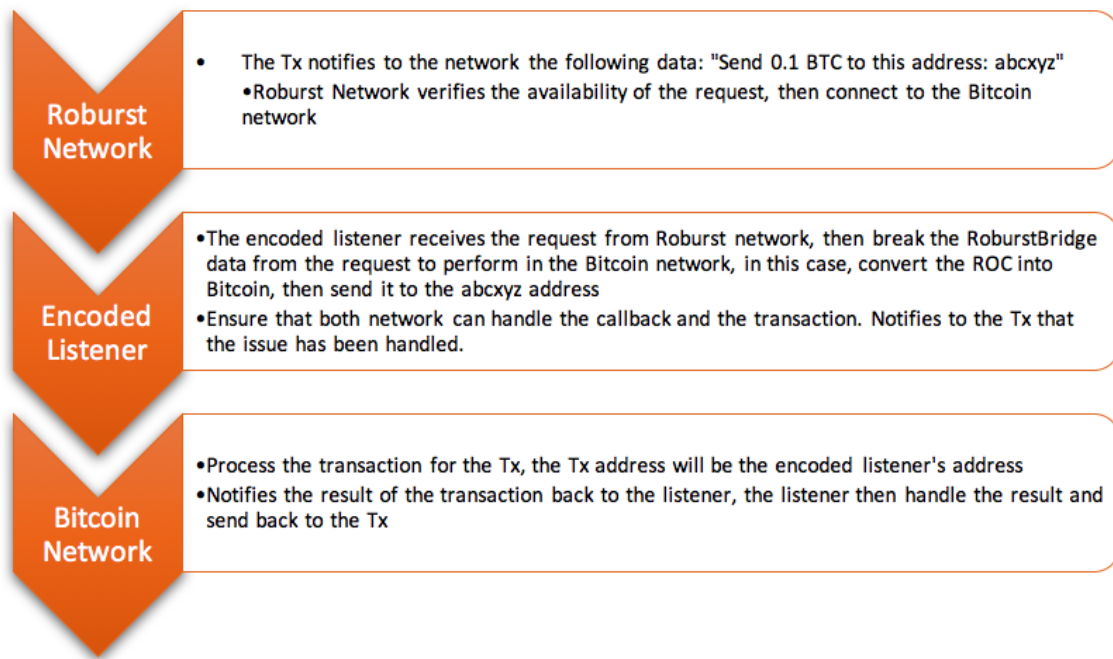


Figure 2.1.1: Le flux de fonctionnement de RoburstBridge™ dans un cas spécifique

Toutes transactions effectuées avec le RoburstBridge™ sont marquées en fonction du type défini par le développeur. Par exemple si vous voulez envoyer 1 BTC à un autre compte en utilisant des Roburst Coin vous devrez payer les frais de transaction de type 0 (transfert de ROC vers un autre compte) et serez facturé des frais de transaction entre le BTC et le ROC. En passant par le Roburst Trading Bot, les frais de transaction de type 0 ne vous seront pas facturés car il s'agit d'un service de Roburst Main Network et qu'ils sont sponsorisés par le réseau lui-même.

RoburstBridge™ est au cœur de notre prochain system dans lequel le trading entre crypto-monnaies est simplifié et ses frais réduits. Les développeurs peuvent créer leur propre application tournant sur RoburstBridge™, émettre leur propre crypto-monnaie qui pourrait facilement interagir avec un réseau comme les Smart Contract d'Ethereum, mais de manière plus efficace et sans consommer d'énergie pour fonctionner. Pour plus de détails sur le développement via RoburstBridge™ veuillez vous référer à la roadmap.

## 2.2. La carte Roburst et le paiement sans espèces

Quiconque utilisant l'application mobile Roburst Coin peut créer une carte spécifique permettant de réaliser des paiements dans le monde réel. Il s'agit d'une carte virtuelle permettant de payer dans n'importe quel point de vente supportant le paiement NFC. Ce mécanisme utilise le RoburstBridge™ pour convertir les ROC en monnaie locale via Paypal ou un autre service similaire. Si le magasin supporte le ROC comme moyen de paiement alors le client peut scanner un simple QR code pour réaliser son paiement et ne paiera aucun frais.

### 2.3. Roburst Trading Bot

---

Roburst Trading Bot (RTB) sera l'un des premiers services disponibles sur Roburst Network. RTB fournit un service de trading automatique pour ceux qui sont trop occupés et veulent juste un revenu sans rien faire. Grâce à l'apprentissage profond (deep learning), RTB représente un choix d'investissement sûr dans les crypto-monnaies pour celui qui n'a pas de connaissances de trading. RTB possède deux modes de fonctionnement : trading entièrement automatique ou manuel. Le mode entièrement automatique est créé comme un système de prêt avec beaucoup d'options, comme une visibilité détaillée au jour le jour. Vous pouvez voir combien de profits vous avez réalisé et le pourcentage de risque que vous prenez. Le mode manuel vous laisse les commandes, mais vous bénéficiez d'un système de conseils. Chaque heure le robot vous donnera une nouvelle prédiction de prix, pour les 24h à venir, basée sur les nouvelles informations, les réseaux sociaux, les prédictions précédentes et les cours réels des crypto-monnaies. Nous supportons l'envoi des prédictions via Telegram et Whatsapp afin que vous restiez informé en permanence sans avoir à retourner sur notre site chaque heure. Veuillez noter que le trading se fera uniquement via le site Roburst Trading, notre robot de trading ne supporte pas d'autres sites de trading. Cette fonctionnalité nécessite un montant fixe de Roburst Coin dans votre portefeuille. Si vous possédez moins de ROC que le montant minimum le service sera désactivé. Les coins de bonus ne comptent pas pour ce service.



Figure 2.3.1: Pr vision de Roburst Trading Bot pour Ethereum sur les prochaines 24h

## 2.4. L quipe Roburst Network

Nous sommes fiers de nous pr senter comme une  quipe capable de relever des d fis, de d passer les obstacles que nous avons rencontr  sur notre route vers le produit final que vous voyez ici.



**Samantha Wilson**

**PDG, Co-fondatrice**

*Ph.D of Economics, University of California*

Samantha est une personne tr s ambitieuse et poss dant de larges connaissances dans les domaines financiers et  conomiques. Elle s'int resse aux crypto-monnaies et   la blockchain et vise   les populariser aupr s du public.



## **Daniel Lee**

### **Directeur technique, Co-fondateur**

*Master of Computation for Design and Optimization, Massachusetts Institute of Technology*

Daniel est l'une des personnes les plus exceptionnelles que nous ayons rencontré. Il travaille dur sur le terrain pour en apprendre plus dans le domaine des crypto-monnaies. Ses recherches sur le protocole actuel de Roburst sont stupéfiantes.



## **Justin Wilkerson**

### **Directeur opérationnel**

*Bachelor of Business Administration, University of Chicago*

Justin est très talentueux pour gérer des plans stratégiques et marketing important. Grâce à lui notre projet est une encore plus grande réussite.



## **Ronald Raji**

### **Directeur financier**

*Master of Finance, University of Minnesota*

Ronald est un analyste financier expérimenté de chez F.N.B. Corporation. Le fait que ses connaissances en crypto-monnaies soient étonnamment bonnes, combiné avec son expérience est vraiment incroyable.

**“...les paiements sans espèces seront la prochaine génération de paiement que rien ne pourra remplacer...”**

**- Samantha Wilson**

## Conseillers



**David Jones**

*MBA, Co-Fondateur  
de EAZL*



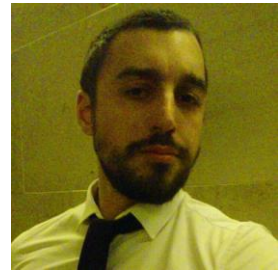
**Michael Suppo**

*Youtuber crypto-  
monnaies*



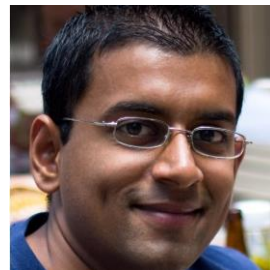
**Marshall Hand**

*Analyste et écrivain  
Blockchain & Crypto-  
monnaie – Avocat de la  
Blockchain*



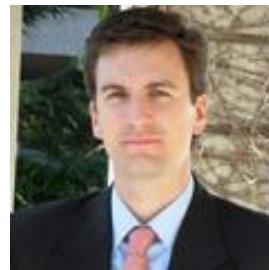
**Samy Mkacher**

*Conseiller Blockchain*



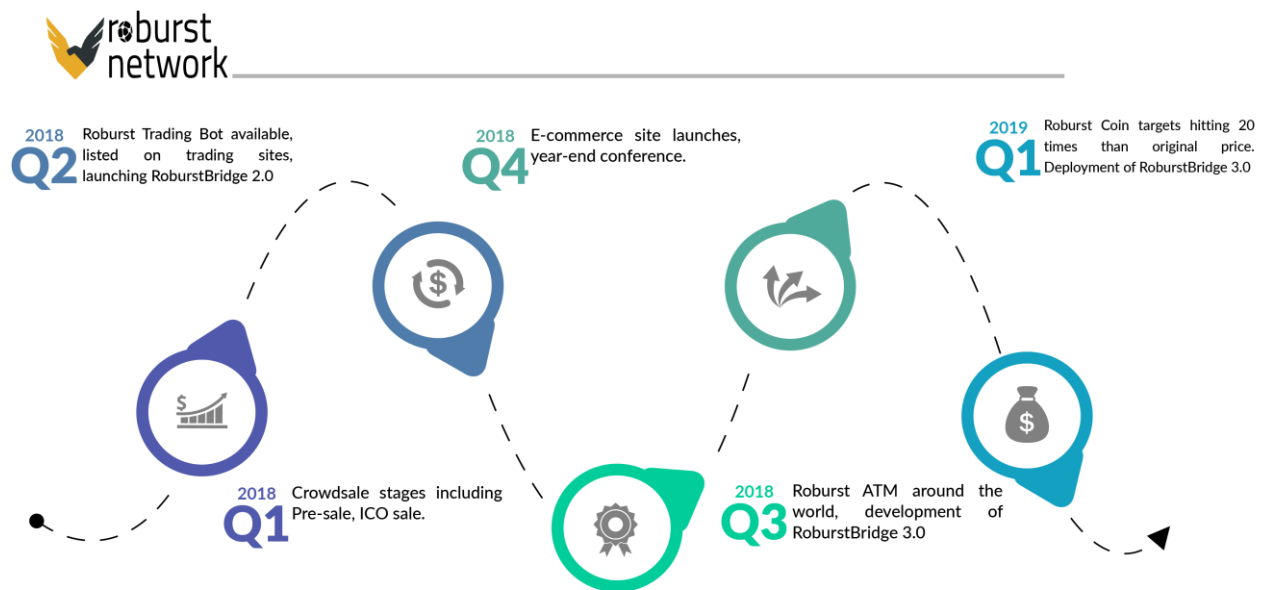
**Arvind Narayanan**

*Assistant professeur en  
sciences informatique à  
Princeton.*



**Marc Badia**

*Assistant Professeur de  
comptabilité et de  
contrôle à IESE school*



## 2.5. Roadmap

Voici la feuille de route (roadmap) simplifiée des plans de Roburst Network. Il s'agit d'un plan à 1 an et pourrait varier en fonction des ventes à venir. Ci-dessous vous trouverez notre plan détaillé. Veuillez noter que les date peuvent évoluer.

### Début de la prévente

**24 février 2018**

La prévente est ouverte. Pour rejoindre la prévente les investisseurs doivent s'enregistrer sur la whitelist fournie par Roburst Network.

### Fin de la prévente et début de l'ICO

**25 mars 2018**

Résumé de la prévente et début de la prochaine étape : l'ICO

### Fin de l'ICO

**24 avril 2018**

Fin de l'ICO. Résumé de toutes les étapes avec les ventes et les coins non vendus.

### Date de distribution des Coins

**1er mai 2018**

Lancement du réseau principale (mainnet) et distribution des coins dans les portefeuilles des investisseurs.

### Listing sur les sites de trading

*5 mai 2018*

Roburst Coin est maintenant disponible sur les sites de trading (au moins 5 sites incluant le site interne de trading : Roburst Trading Bot).

Déploiement de RoburstBridge 2.0

*15 juin 2018*

Premier déploiement de RoburstBridge 2.0 avec la possibilité de créer des sidechains, de faire des transferts entre chaînes et implémentation d'améliorations au niveau de la sécurité, de la vitesse, de la stabilité et plus.

Premier distributeur automatique (ATM) à Los Angeles

*20 juin 2018*

Avec l'aide de RoburstBridge 2.0 le premier distributeur de billet Roburst Coin sera disponible à Los Angeles, Californie.

Développement de RoburstBridge 3.0

*4 juillet 2018*

Début du développement de la prochaine version de RoburstBridge 3.0, incluant l'implémentation du Lightning Network.

Déploiement mondial des distributeurs automatiques Roburst Coin

*5 Septembre 2018*

Notre objectif est de déployer 300 distributeurs dans le monde, d'abord dans les grandes villes mondiales.

Autorisation pour la création de sidechains publiques.

*1er octobre 2018*

Tout le monde peut maintenant créer sa propre crypto-monnaie basée sur Roburst Network.

Lancement du site web Roburst E-commerce

*11 novembre 2018*

Site web de e-commerce de Roburst Network n'acceptant que les Roburst Coins.

Evènement planétaire de Roburst Network

*12 décembre 2018*

Premier évènement planétaire tenu par Roburst Network qui résumera un an de travail pour Roburst Network.



## III.

## ICO

*Une offre initiale de coins (initial coin offering - ICO) est un moyen de financement participatif centré autour d'une crypto-monnaie (Wikipedia)*

## 1. Roburst Bonus Coin (Bonus ROC)

Roburst Bonus Coin est un coin émis par Roburst Network. Roburst Bonus Coin **EST** un Roburst Coin avec les limitations suivantes :

1. **NE PEUT** être transféré vers un autre compte durant les périodes de prévente et d'ICO.
2. **NE PEUT** être tradé durant les périodes de prévente et d'ICO.
3. **NE PEUT** être retiré durant les périodes de prévente et d'ICO.

À la fin des périodes de prévente et d'ICO les **ROBURST BONUS COINS SERONT AUTOMATIQUEMENT CONVERTIS EN ROBURST COINS**. Vos Bonus ROC seront ajoutés à votre portefeuille principal de ROC et pourront dès lors être retirés, tradés et transférés.

Le nombre de Roburst Bonus Coin est limité à 84 000 000 de Bonus ROC. Ils sont distribués à travers le Roburst Community Program, le Bounty Hunter Program et la Campagne Marketing. Quand le nombre de Bonus ROC est épuisé le programme de parrainage et le bonus de prévente s'arrêtent. Nous en informerons les investisseurs par e-mail.

## 2. Investisseurs early-bird

Les investisseurs early-bird sont les investisseurs qui prennent part à la prévente et achètent au moins 50 000 ROC.

Voici les bénéfices associés au statut d'investisseur early-bird durant la prévente :

- Accès au Roburst Trading Bot Beta (dès la fin de l'ICO)
- Accès au Roburst Trading Bot pour générer une prédiction à 24h



- Aucun frais de transferts au sein du réseau (pour les services fournis par Roburst Network uniquement)
- Pas de frais de trading avec Roburst Trading Bot
- Chaîne Telegram dédiée
- Support d'urgence (réponse en moins de 20 minutes)
- Ticket VIP pour l'événement Roburst Network
- Accès prioritaire à nos nouveaux services

### 3. L'étape de prévente

Roburst Network offre aux investisseurs early-bird des Roburst Coins à prix avantageux, incluant un bonus sur leurs achats. Les investisseurs recevront des Bonus Roburst Coins en tant que récompense pour leurs achats, le montant de cette récompense varie en fonction du nombre de Roburst Coin acheté par l'investisseur. L'étape de prévente se conforme aux standards du KYC (Know Your Customer - Connaitre Vos Clients) c'est pourquoi les investisseurs venant de pays interdisant les ventes d'ICO ne seront pas autorisés à participer à la prévente. Roburst Network exige des investisseurs de soumettre leur carte nationale d'identité / permis de conduire / passeport ou autre document officiel pour confirmer leur identité. Nous exigeons aussi un selfie de l'investisseur pour prévenir les vols d'identité.

Les investisseurs qui ne fourniront pas toutes les informations requises ne pourront pas participer à la prévente. Les investisseurs ne peuvent demander de remboursement pendant la période de prévente. Les investisseurs qui veulent acheter plus de 2 000 000 ROC bénéficieront d'avantages supplémentaires. Participer à la prévente en achetant plus de 50 000 ROC fera de vous un investisseur early-bird. Le nombre de coins en vente pendant la prévente est limité à 63 000 000, soit 20% du total de coins générés pour la vente publique. Une fois ce nombre atteint l'étape de prévente prend fin.

Le tableau suivant résume l'étape de prévente :

Date de début 24 fév. 2018 19h00 (CET)

Date de fin 26 mar. 2018 à 7h00 (CET)

Durée 30 jours

Nombre de coins en vente 63 000 000 ROC

Prix par coin 0.00001 BTC

Date de distribution des coins 1er mai 2018 (pire scenario)

25 avril 2018 (meilleurs scenario)

Achat minimum 10 000 ROC

Achat maximum 10 000 000 ROC/compte

## 4. Les étapes de l'ICO

La vente publique est divisée en 3 étapes, chacune ayant un prix de départ différent qui démarre à 0,00001 BTC par ROC. En fonction de la demande, le Roburst Trading Bot déterminera un prix spécifique pour chaque étape. Les investisseurs peuvent participer à l'ICO sans avoir besoin de participer à la whitelist. Chaque étape dure 10 jours. Les coins non vendus durant la précédente seront transférés dans la première étape d'ICO. Le prix de l'étape suivante sera notifié à tous les membres de Roburst Network 3 jours avant le début de l'étape. Le programme d'investisseur early-bird Roburst ne s'applique pas pendant l'ICO.

Le tableau suivant résume les étapes de l'ICO :

Date de début 26 mar. 2018 à 8h00 (CET)

Date de fin	25 avr. 2018 à 7h00 (CET)
Durée	30 jours
Nombre de coins en vente	252 000 000 ROC + ROC non vendus durant la prévente
Prix par coin	> 0.00001 BTC
Date de distribution des coins	1er mai 2018 (pire scenario) 25 avril 2018 (meilleurs scenario)
Achat minimum	1 ROC
Achat mac	100 000 ROC/compte/jour

## 5. Parrainage

Dans le cadre de notre campagne marketing, nous offrons 21 000 000 ROC aux investisseurs qui recommandent Roburst Network à leurs amis. Toutefois afin de prémunir la fraude pendant la campagne, la récompense sera calculée sur base du nombre de ROC achetés par le parrainé. De plus si votre parrainé recommande Roburst Network à ses amis vous obtiendrez un bonus également. La formule ci-dessous permet de calculer les Bonus Coin de la campagne de parrainage :

Considérons un client qui achète  $C$  coins au niveau  $n$ . Le système récompense les niveaux supérieurs d'un montant  $a$  de Bonus Coins.  $a$  peut être déterminé par :

$$0 \leq a \leq C \lim_{n \rightarrow \infty} \sum_{i=0}^n 5\% \left(\frac{1}{2}\right)^i$$

$$0 \leq a \leq C \frac{5\%}{1-\frac{1}{2}}$$

$a$  est minimum quand  $n = 0$  et atteint le maximum quand  $n$  tend vers l'infini.

Par exemple si votre réseau à 3 niveaux, ce qui signifie que vous parrainez un ami A qui parraine un ami B, si l'ami A achète 1 000 ROC vous recevrez 5% de 1 000 soit 50 ROC. Si l'ami B achète 1 000 ROC alors l'ami A recevra 5% de 1 000 soit 50 ROC et vous recevrez 2,5% de 1 000 soit 25 ROC. Ainsi vous pouvez gagner plus de Bonus Coins en parrainant plus de gens dans votre réseau.

# Appendix

## *Qu'est-ce que EdDSA ?*

EdDSA combine les choix les plus sûres disponibles. EdDSA est comme Schnorr et à la différence de ECDSA il diversifie les hash en entrée, ajoutant de la résistance contre la collision de hash, il évite les inversions, simplifie et accélère les implémentations. EdDSA diffère de Schnorr par l'utilisation d'une fonction de hash de taille double réduisant encore le risque de problèmes avec les fonctions de hash ; en nécessitant des courbes de Edwards, simplifiant et accélérant encore l'implémentation ; et en incluant la clé publique en tant qu'entrée supplémentaire de la fonction de hash, diminuant les inquiétudes concernant des attaques visant plusieurs clés à la fois. EdDSA se passe également d'un mécanisme de compression mineur ; le mécanisme de compression étant publique il ne peut améliorer la sécurité et l'éviter est essentiel pour accélérer la vérification par lots d'EdDSA. Enfin EdDSA génère des nonces secrets par message en hashant chaque message avec un secret à long terme plutôt que d'avoir recourt à une fonction aléatoire à chaque message.

### *BIP39 mnemonic code*

Ce BIP décrit l'implémentation d'un code mnémotechnique ou d'une phrase mnémotechniques -- un groupe de mots facile à retenir -- pour la génération de portefeuilles déterministes. Il est composé de deux parties : génération de l'élément mnémotechnique et sa conversion en "graine" binaire. Cette graine peut ensuite être utilisée pour générer des portefeuilles déterministes en utilisant BIP-0032 ou d'autre méthodes similaires.

# References

Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <http://bitcoin.org>.

Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov (2017). *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*. Retrieved from <https://iacr.org>.

Internet Research Task Force (2017). *Edwards-Curve Digital Signature Algorithm (EdDSA)*. Retrieved from <https://scholar.google.com>.

Larry Ren (2014). *Proof of Stake Velocity: Building the Social Currency of The Digital Age*. Retrieved from <https://coss.io>.

Sunny King, Scott Nadal (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. Retrieved from <http://peerco.in>.

Jae Kwon (2012). *Tendermint: Consensus without Mining*. Retrieved from <https://relayto.com>.

Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, Robbert van Renesse (2016). *Bitcoin-NG: A Scalable Blockchain Protocol*. Retrieved from <https://usenix.com>.

*The Lisk Protocol*. Retrieved from <https://lisk.io>.

Young Bin Kim, Jun Gi Kim, Took Kim, Jae Ho Im, Tae Hyeong Kim, Shin Jin Kang, Chang Hun Kim (2016). *Predicting Fluctuations in Cryptocurrency Transactions based on User Comments and Replies*. Retrieved from <http://plos.org>.