

# EncryptoTel

## Premier PBX Cloud sécurisé

*Autocommutateur téléphonique privé virtuel : Infrastructure de téléphonie par Internet ou soft-phone, avec communications VoIP basées sur la technologie blockchain et cryptage du trafic intégré pour les particuliers et les entreprises*

Roman Nekrasov

[www.encryptotel.com](http://www.encryptotel.com)

## Table des matières

Résumé .....	1
Contexte .....	2
La société de surveillance .....	3
Contenu et métadonnées .....	4
Parcours et projet .....	5
L'opportunité pour EncryptoTel .....	6
Plateforme et technologie .....	8
Multiplateforme, approche unifiée .....	8
Cryptage des appels .....	9
Expérience utilisateur .....	9
Paiements pseudonymes .....	9
Fonctionnalités offertes par EncryptoTel .....	10
Génération de revenus et retour sur investissement.....	11
Abonnement et facturation à la minute .....	12
Droits de vote.....	12
Seuils de financement.....	12
L'équipe EncryptoTel.....	13

## Résumé

L'accroissement rapide de la connectivité via les technologies comme Internet, les réseaux sociaux et les smartphones a totalement révolutionné notre capacité de communiquer. Par la même occasion, les logiciels d'appel audio et vidéo et les services de messagerie instantanée actuels sont aussi

non sécurisés et susceptibles de faire l'objet de placement sous surveillance et d'exploitation par les gouvernements, les grandes sociétés et les tiers malveillants qu'ils sont moins efficaces et moins rentables qu'il aurait été possible de prévoir.

EncryptoTel fera le lien entre les technologies les plus prometteuses et les marchés du secteur des télécommunications, en associant PBX virtuel et cryptage, protocoles blockchain et paiements en cryptomonnaies afin de proposer une amélioration notable des performances, des fonctionnalités et des avantages compétitifs. Nous pensons que cela nous permettra de devenir un leader de l'industrie du PBX disposant d'une plateforme diversifiée parfaitement adaptée aux usagers individuels et aux applications commerciales et bureautiques.

Nous avons déjà développé une version bêta opérationnelle de notre logiciel de base. L'application EncryptoTel sera en définitive une solution multiplateforme permettant aux utilisateurs de se connecter, de passer des appels VoIP à l'aide de n'importe quel dispositif (appareil de bureau ou clients SIP pour Android, Zoiper, 3CXPhone, X-Lite, etc.) et d'avoir accès à leur PBX via des applis de messagerie populaires telles que Telegram Messenger et Facebook Messenger.

Ce livre blanc précise le champ d'action ainsi que la vision d'EncryptoTel en amont de notre crowd-sale qui prendra fin en mai 2017. Dans les mois qui viennent, nous aurons développé, lancé notre produit et fait notre entrée sur le marché mondial du PBX. Le token EncryptoTel (symbole : ETT) désigne la monnaie exclusive dans laquelle seront libellés nos services, nos offres de réduction et autres bonnes affaires, bien qu'il sera aussi possible de payer avec d'autres cryptomonnaies.

## Contexte

Nous jouissons d'un niveau de connectivité sans précédent. Avant l'essor d'Internet, il y a 25 ans, la communication à distance était coûteuse et prenait beaucoup de temps. Même les appels locaux étaient payants, les appels nationaux pouvaient devenir coûteux aux heures de pointe et les appels internationaux, très chers pour la plupart des gens. La communication écrite par voie postale entraînait un temps de distribution d'au moins un jour, et là aussi cela avait un coût. Envoyer une lettre par avion durait le plus souvent un aller-retour de plus d'une semaine.

Il y a vingt ans, alors que de plus en plus de consommateurs accédaient au web, le courrier électronique était considéré comme l'équivalent d'une lettre envoyée à la poste, à cause des coûts d'une connexion à accès commuté. Le débit était limité et relativement cher. Il a fallu attendre l'arrivée du haut débit universel pour vraiment faire pencher la balance. Les appels audio et vidéo sur Internet – la capacité de communiquer en temps réel et à un coût de connexion fixe – étaient devenus possibles et rapidement accessibles pour la première fois, popularisés par les applications comme Skype, fondée en 2003. À côté de ça, les réseaux sociaux se sont rapidement établis, donnant l'opportunité de communiquer à deux ou à plusieurs avec une facilité sans pareille dans toute l'histoire de l'humanité.

L'adoption massive du smartphone, qui a commencé il y a pas plus de dix ans, a fini par compléter le tableau en amenant avec elle ce que nous appelons plus convenablement la culture de la « connexion permanente ». Nous pouvons communiquer avec n'importe qui, n'importe où dans le monde et ce, via un certain nombre de média, y compris les appels vocaux et vidéo, la messagerie et

l'imagerie instantanées, individuellement ou en groupe, en utilisant un bon nombre de dispositifs et essentiellement à coût marginal nul.

*« L'Internet est pour l'humanité l'outil le plus libérateur qui ait été inventé et aussi le meilleur qui soit pour la surveillance. Il ne s'agit pas de l'un ou de l'autre, mais bien des deux à la fois. »*

– John Perry Barlow, militant pour la défense des cyberlibertés

Ces remarquables changements technologiques et culturels ont sérieusement débouché sur des opportunités que peu de gens auraient imaginé possibles dans les générations précédentes : nouveaux méthodes et rythmes de travail, nouvelles structures d'entreprise et évolution des normes sociales. Mais avec tous ces nouveaux avantages, sont venus s'ajouter de nouveaux risques et l'omniprésence de la connexion permanente démontre que nous sommes toujours mal préparés pour reconnaître et réduire ces risques. La connectivité est devenue tellement ancrée dans la vie de tous les jours que nous songeons rarement à la remettre en question.

## ***La société de surveillance***

Dans un tel contexte de connectivité universelle et de communication, les données sont devenues extrêmement précieuses. Des quantités énormes d'informations personnelles sont maintenant systématiquement récoltées par un éventail d'acteurs différents, y compris des organisations soutenues par l'État, des grandes entreprises et des pirates informatiques. Même s'ils ont chacun leurs propres motivations, la ligne qui les sépare est souvent floue. Le piratage parrainé par l'État devient monnaie courante, comme dans le cas du piratage de Sony Pictures orchestré en 2014 par la Corée du Nord, dans lequel des informations personnelles sur les employés, leurs familles et l'entreprise ont été publiées, y compris des e-mails, des informations sur les salaires et même des films non diffusés. Les données détenues par l'État et les grandes entreprises peuvent être piratées ou divulguées par des initiés ou par des tiers externes malveillants et, parfois, diffusées par inadvertance dans le cadre d'une surveillance et à cause d'une incompetence.

*« Soutenir que vous ne vous souciez pas du droit à la vie privée parce que vous n'avez rien à cacher, c'est aussi dire que vous ne vous n'avez rien à faire de la liberté d'expression parce que vous n'avez rien à dire. »*

–Edward Snowden, dénonciateur de la NSA

En 2015, il est devenu public que la télévision intelligente de Samsung pourrait être utilisée comme un dispositif d'écoute<sup>1</sup>. Des documents mis à disposition par Wikileaks ont montré que la CIA avait

---

<sup>1</sup> <https://www.cnet.com/uk/how-to/samsung-smart-tv-spying/>

l'intention d'exploiter cette fonctionnalité pour un certain nombre de dispositifs similaires<sup>2</sup>. Cela a été visiblement exécuté au nom de la sécurité nationale, mais le fait même de la fuite prouve que les données recueillies, quelles qu'elles soient, sont également sujettes aux pertes et aux abus. Des stratégies similaires seront sans doute utilisées par des pirates au fur et à mesure que les nouvelles techniques et les vulnérabilités seront connues. Les piratages spectaculaires de grandes organisations démontrent que les normes de sécurité sont souvent insuffisantes, avec des listes de millions d'emails d'utilisateurs en texte brut, de mots de passe, d'adresses, de numéros de sécurité sociale et plus détruits sur le Web<sup>3</sup>. Des scandales répétés se sont produits, impliquant des photos de célébrités en provenance de services cloud compromis, soit par une mauvaise implémentation ou une erreur d'utilisateur.

La réalité est que dans un monde hyper-connecté, les données ne sont pas sûres. Nous confions aveuglément nos données personnelles aux applications que nous utilisons et aux organisations qui les hébergent et qui les possèdent à leur tour. Nous sommes souvent trop confiants en ce qui concerne notre sécurité personnelle. Réutilisation des mots de passe et des adresses e-mails, négligence quant à l'abonnement à de nouveaux services via les comptes sociaux, manque de compréhension ou méconnaissance de ce qui arrive à nos données : tout cela est normal. Plus important encore, il y a une collusion implicite que nos données personnelles constituent le prix de l'utilisation de plates-formes et d'applications « gratuites ». Les entreprises recueillent des données détaillées sur leurs clients, généralement en dehors de la vigilance ou sans la permission explicite des utilisateurs. Ces informations peuvent être stockées de manière non sécurisée et peuvent être vendues ou mises à la disposition de tiers.

Nous soutenons que la vie privée est un droit important et fondamental pour chaque personne. La liberté d'expression permet un contrôle essentiel de l'accumulation de pouvoir et la capacité de communiquer librement sans crainte d'être surveillé, que ce soit par l'État, par des entreprises ou par des personnes malveillantes, est une condition préalable à des libertés sociales et personnelles plus grandes. À l'ère de l'information, le savoir est vraiment le pouvoir. Les données peuvent être utilisées de manière courante ou à des fins avantageuses pour les entités dont les valeurs ne sont pas les mêmes que celles de ceux qui fournissent involontairement leurs informations personnelles.

## ***Contenu et métadonnées***

Il est largement admis que le *contenu* des communications non cryptées—le matériel texte, audio et vidéo—est contrôlé massivement par des institutions publiques et d'autres organisations. Dans de nombreux cas, cela restera un processus passif, sauf pour les informations spécifiquement recherchées et les mots déclencheurs. Dans d'autres cas, les autorités s'engageront directement à bloquer l'accès à une plate-forme ou à faire obstacle à une discussion, une stratégie bien connue employée par le gouvernement chinois, qui est censé fausser des centaines de millions de commentaires échangés sur les médias sociaux chaque année<sup>4</sup>.

---

<sup>2</sup> <http://variety.com/2017/digital/news/wikileaks-smart-tv-surveillance-1202003656/>

<sup>3</sup> Voyez par exemple : <https://arstechnica.com/security/2016/09/plaintext-passwords-and-wealth-of-other-data-for-6-6-million-people-go-public/>

<sup>4</sup> [https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?utm\\_term=.09a5c955eb20](https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?utm_term=.09a5c955eb20)

Cependant, au fur et à mesure que le cryptage renforcé devient plus largement disponible et populaire, de nouvelles techniques ont été développées pour permettre une surveillance efficace. Les métadonnées proprement dites deviennent de plus en plus importantes : pas le contenu de la communication, mais les informations relatives à ces communications, telles que la date, l'heure, le type de contact (appel téléphonique, e-mail, publication des médias sociaux, appel vidéo/audio), l'emplacement des participants, la durée des appels et toute autre donnée fournie par les applications au cours de leur utilisation. Dans certains cas, des informations financières pourront être acquises, telles que les données concernant les transactions par carte de crédit.

Bien que les individus puissent se préoccuper à juste titre de la liberté d'expression et de la confidentialité financière, pour les entreprises, la question est encore plus préoccupante. Même si le contenu d'une communication reste privé, les enregistrements financiers peuvent révéler des informations critiques qui peuvent être utilisées par les concurrents dans le cadre de l'espionnage industriel. Les entreprises, les fournisseurs, les employés, les prestataires et les clients sont tous connectés par un réseau complexe de transactions. Toute information divulguée peut (et pourra inévitablement) être utilisée au bénéfice des concurrents et des tiers malveillants.

Au début des années 1990, lorsque le mouvement Cypherpunk (groupe informel de personnes intéressées par la cryptographie) a commencé à préconiser l'utilisation d'un cryptage renforcé dans l'intérêt de la protection de la vie privée, des préoccupations au sujet de la surveillance par l'État et du commerce de l'information, bien peu de gens parmi les critiques dits visionnaires ont compris le volume et l'ampleur des données que nous aurions à transmettre et à protéger un quart de siècle plus tard.

EncryptoTel lancera une suite d'outils qui permettront une communication conviviale et sécurisée, en combinant les applications et les technologies existantes avec d'autres, plus nouvelles et plus personnalisées. La protection de la vie privée est un droit, mais un droit qui doit être exercé de manière active et délibérée

## Parcours et projet

Le projet d'EncryptoTel consiste à réaliser un moyen de communication ouvert, fiable et surtout sécurisé qui puisse être utilisé indépendamment du lieu où se trouvent les utilisateurs. Le produit principal de l'entreprise est un service PBX flexible et complet, c'est-à-dire un réseau privé interne pouvant être partagé par un grand nombre d'utilisateurs, mais également un réseau pouvant s'interfacer avec le réseau de télécommunications externe.

### **PBX et PBX IP**

Un **PBX** (de l'anglais : Private Branch eXchange) est un système de commutation ou d'échange téléphonique interne utilisé dans un seul bureau ou organisation.

Les principaux avantages d'un PBX sont le coût et la commodité. L'utilisation d'un système interne permet aux employés de communiquer directement sans nécessiter l'utilisation et les frais des lignes téléphoniques externes. Les appels sortants d'un grand nombre d'employés peuvent être partagés sur quelques lignes seulement. En même temps, des services supplémentaires peuvent être

intégrés au système de commutation, comme le routage d'appels vers des interphones et d'autres destinations.

Une certaine forme de PBX est maintenant la norme pour les entreprises, en particulier dans les grandes organisations, où il est inutile et inefficace de louer de nombreuses lignes externes. Les systèmes **PBX IP** (PBX utilisant le protocole Internet) adoptent la même approche que le PBX traditionnel plus ancien, avec la différence qu'ils utilisent les ordinateurs et l'infrastructure Internet existante pour acheminer les appels au sein d'une organisation. Cela permet une efficacité et une polyvalence accrues, puisque les installations numériques peuvent être intégrées au système téléphonique, y compris le stockage et la connexion des messages aux services voix sur IP (VoIP), tout en utilisant un nombre limité de lignes pour interagir avec le réseau téléphonique externe. Étant donné que presque toutes les entreprises sont connectées à Internet et utilisent une infrastructure haut débit ultra-rapide, le PBX IP offre des avantages substantiels à faible coût par rapport aux systèmes de télécommunications existants.

EncryptoTel offrira un PBX IP virtuel, ainsi qu'une intégration facile de la VoIP cryptée dans les réseaux PBX IP existants.

Nous voulons proposer ce service, que nos clients représentent ou non un seul individu ou une grande entreprise avec plusieurs milliers d'employés. Notre logiciel et l'infrastructure blockchain sous-jacente nous permettent de répondre aux besoins de quiconque, quel que soit l'échelle, grâce aux économies qu'il offre en termes de micro-transactions et d'opérations de décentralisation. Sans la technologie blockchain, la proposition d'EncryptoTel ne serait tout simplement pas économiquement viable.

L'idée derrière la création d'EncryptoTel est enracinée dans les expériences qu'a eu l'équipe de développement de travailler pour une entreprise de télécommunications. La connaissance de l'infrastructure traditionnelle de télécommunications et de la technologie blockchain a permis de créer un produit supérieur à tout ce qui se trouve actuellement sur le marché. L'équipe a travaillé à temps plein sur le projet pendant plusieurs mois et a une application en bêta publique. Un crowdsale fournira les fonds pour augmenter la qualité du produit et le commercialiser correctement.

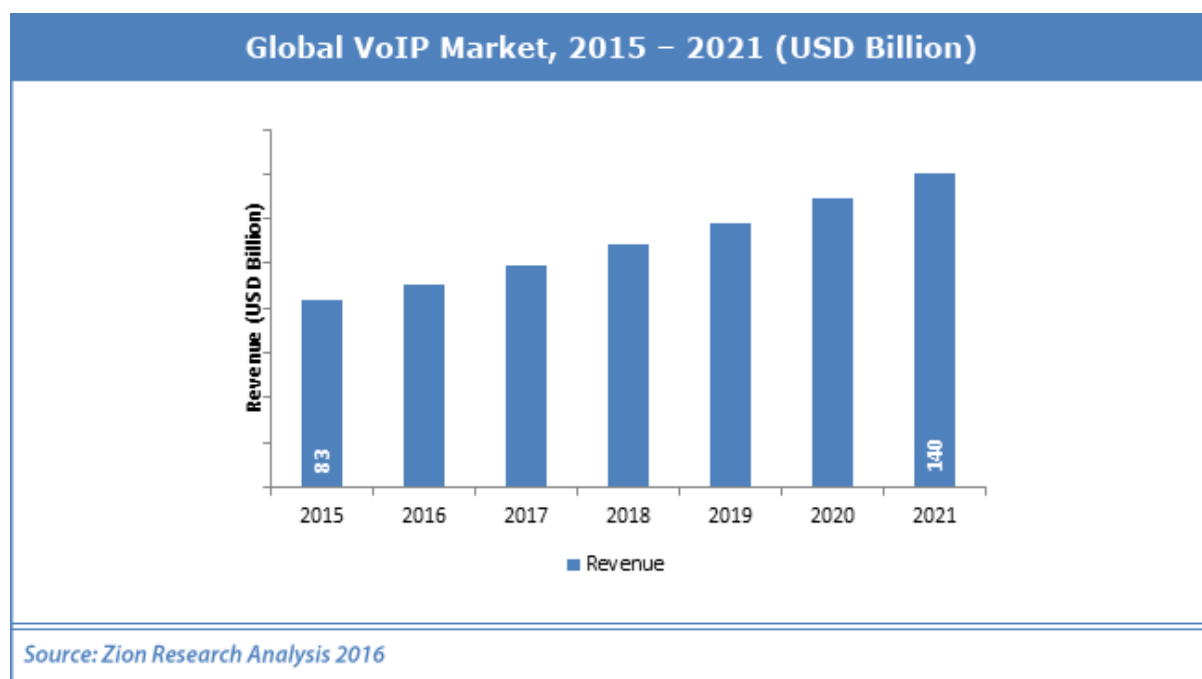
## **L'opportunité pour EncryptoTel**

Le marché des télécommunications est actuellement l'un des secteurs les plus dynamiques de l'économie. Alors que le système téléphonique traditionnel connaît une réduction de son utilisation, les nouvelles technologies basées sur Internet se développent rapidement, offrant des avantages significatifs en termes de coût et de commodité par rapport aux anciennes approches. Il est maintenant possible de communiquer par chat vidéo via Skype, Facebook Messenger et de nombreuses autres plates-formes au moyen d'un simple smartphone et sans autre coût que celui de la connexion Internet.

« Le secteur des télécoms continue d’être une force indispensable pour la croissance, l’innovation et le changement dans de nombreuses industries technologiques. »

–Deloitte<sup>5</sup>

« La demande mondiale pour le marché des services VoIP a été évaluée à plus de 83 milliards de dollars en 2015, devrait atteindre plus de 140 milliards de dollars en 2021 et devrait croître à un taux supérieur à 9,1% entre 2016 et 2021<sup>6</sup>. » En raison de leur efficacité et de l’utilisation désormais omniprésente de l’infrastructure haut débit, les services VoIP ont le potentiel de rendre obsolète les appels traditionnels effectués à partir des téléphones fixes et des téléphones mobiles.



**Marché mondial de la VoIP, 2015 -2021 (en milliards de dollars)**

EncryptoTel est plus comparable à un fournisseur de PBX virtuel qui vend des numéros de téléphone aux utilisateurs partout dans le monde. Les entreprises qui le font actuellement doivent collecter et divulguer des informations sur leurs clients lorsque les autorités réglementaires l'exigent. En outre, aucune entreprise de PBX n'accepte les paiements en cryptomonnaies ni n'exploite la technologie blockchain au niveau de leur infrastructure de base. À l'heure actuelle, cela signifie qu'EncryptoTel n'a pas de concurrents directs et offre une approche unique et un ensemble de services plus diversifiés.

Après avoir travaillé dans le secteur du PBX, l'équipe d'EncryptoTel est familière avec les produits existant sur le marché, a mené des recherches approfondies et a recueilli des commentaires de

<sup>5</sup> <https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/telecommunications-industry-outlook.html>

<sup>6</sup> <http://www.marketresearchstore.com/news/global-voip-services-market-is-expected-to-reach-above-231>

clients sur les principaux problèmes liés aux systèmes PBX actuels. L'expérience combinée de l'équipe sera appliquée à la création d'un nouveau produit plus souple et plus vaste que tout ce qui est actuellement disponible, contournant ou résolvant les inconvénients qui existent dans les systèmes de télécommunications traditionnels et offrant un grand nombre de fonctionnalités nouvelles. Le résultat du travail à ce jour est une application qui permet :

- Une communication privée
- Le déploiement rapide d'un PBX complet
- Une réduction du coût des appels sortants
- Une communication absolument gratuite et sécurisée à travers tout le réseau
- La possibilité de payer en cryptomonnaies
- Une transparence additionnelle au niveau du contrôle et du monitoring grâce à la technologie blockchain.

L'approche d'EncryptoTel évite tous les inconvénients rencontrés par les systèmes PBX virtuels traditionnels et ajoute des fonctionnalités nouvelles uniques. En termes de paiement, l'utilisation des cryptomonnaies offre pour la première fois un véritable accès anonyme au service. À la suite de cet ensemble de fonctionnalités, EncryptoTel se démarque de tout service PBX virtuel traditionnel, détient plusieurs avantages concurrentiels et a le potentiel pour occuper une fraction importante du marché.

## **Plateforme et technologie**

En tant que PBX virtuel, EncryptoTel est conçu pour être très accessible à ses clients. Il ne nécessitera aucune infrastructure de télécommunications en plus d'un périphérique connecté à Internet (smartphone, tablette, ordinateur portable, ordinateur de bureau). Les équipements de bureau tels que les téléphones ne sont pas nécessaires, bien qu'ils puissent être connectés au service via une passerelle VoIP si désiré. Tout ordinateur moderne peut répondre à cet objectif, car il s'agit simplement d'interconnecter le réseau IP avec le réseau téléphonique ordinaire.

### ***Multiplateforme, approche unifiée***

EncryptoTel prend une approche multiplateforme et peut être utilisé avec Windows, Linux, iOS et Android. Il prend en charge les appels vidéo et audio, ainsi que la messagerie instantanée. De nombreuses applications gratuites peuvent être utilisées avec EncryptoTel, telles que Zoiper, X-Lite et 3CXphone. Ce sont également des applis «softphone» multiplateformes facilitant des appels audio et vidéo sur Internet sans exiger de matériel dédié. L'objectif est de rendre EncryptoTel aussi polyvalent et accessible que possible, ce qui réduit les frictions pour démarrer le service à un niveau presque nul. En temps voulu, nous intégrerons EncryptoTel à d'autres applications de messagerie populaires, notamment Facebook Messenger et Skype



## ***Cryptage des appels***

La version bêta d'EncryptoTel propose déjà un cryptage du trafic basé sur les technologies SIP/TLS. Cela garantit qu'un niveau de cryptage basique est mis en place lorsqu'une connexion client-serveur est établie afin d'éviter l'interception et l'accès non autorisé.

EncryptoTel travaille actuellement sur le développement de son propre réseau de connexion sécurisé, basé sur deux contours de réseau (internes et externes) et qui comprend plusieurs éléments, y compris l'autorité de certification, l'organisation de VPN, le système de fichiers chiffrés distribués, le serveur HTTPS, etc. L'entreprise mettra en œuvre ses propres protocoles de sécurité à l'aide du cryptage des certificats basé sur les protocoles blockchain.

## ***Expérience utilisateur***

En raison de son intégration avec les applications de softphone traditionnelles, l'expérience utilisateur d'EncryptoTel sera transparente. Les clients qui utilisent des applications populaires comme Zoiper continueront à les utiliser de la même manière, avec pour seule différence que les applications seront intégrées au logiciel EncryptoTel qui cryptera l'ensemble des appels passés en leur sein.

## ***Paiements pseudonymes***

Comme expliqué ci-dessus, maintenir la confidentialité n'est pas seulement une question de cryptage du contenu d'un appel ou d'un autre type de communication. Si des métadonnées sont disponibles, alors elles peuvent être utilisées pour recueillir de précieuses informations sur la nature, le but et les participants d'un appel. Les transactions financières sont particulièrement précieuses à cet égard, puisqu'elles sont généralement liées à une carte de crédit ou à un compte bancaire, offrant des données personnelles étendues. Les paiements en cryptomonnaies traiteront ce défaut qu'on retrouve dans les systèmes PBX actuels.

La plupart des cryptomonnaies ne sont pas strictement anonymes, mais pseudonymes. Les adresses sont essentiellement des chaînes aléatoires de caractères alphanumériques. La blockchain est transparente et il est possible de voir où se déplace l'argent, retraçant les transactions à leur source. Cependant, sans informations supplémentaires, il est impossible de voir avec qui sont associées ces adresses.

En réalité, un défaut de vigilance de la part des utilisateurs peut provoquer des fuites, ce qui signifie qu'il est souvent possible de recueillir des données sur la personne à l'origine d'une transaction. Néanmoins, il est tout à fait possible d'assurer la protection des renseignements personnels en mettant en pratique les meilleures méthodes. D'autres services tels que les brouilleurs augmentent radicalement la complexité et le coût des transactions de traçage. Les altcoins centrés sur l'anonymat, tels que Dash et Monero, offrent encore d'autres facilités pour la protection des identités des détenteurs de cryptomonnaies.

EncryptoTel facilitera aux utilisateurs le paiement de ses services par cryptomonnaie, de sorte que non seulement il sera impossible de savoir ce qui est communiqué, mais aussi celui qui communique. Pour les habitués des cryptomonnaies, il y aura un plug-in externe qui permettra de passer des appels directement à partir du client Waves Lite et d'effectuer les paiements plus facilement.

## Fonctionnalités offertes par EncryptoTel

Les services suivants et d'autres encore seront proposés par EncryptoTel. Ceux-ci seront facturés sur la base d'un abonnement ou par appel, avec des réductions offertes pour les paiements effectués avec le token EncryptoTel (ETT).

- **Renvoi d'appel.** Possibilité de rediriger un appel entrant vers un autre numéro de téléphone. **Exemple :** L'utilisateur peut rediriger les appels vers un numéro local, ou vers plusieurs numéros locaux en fonction de qui appelle et de l'heure d'appel.
- **Authentification à deux facteurs (2FA).** Une couche additionnelle de protection sera proposée pour des services tels que les échanges et les portefeuilles de cryptomonnaies. **Exemple :** En plus des coordonnées, nom d'utilisateur-mot de passe, les utilisateurs recevront un appel, un SMS ou d'autres détails d'authentification avant que l'accès leur soit accordé.
- **Cryptage et protection du trafic.** Le trafic est hautement crypté et protégé avec les tout derniers protocoles de cryptage. **Exemple :** Pour des cas tels que les négociations commerciales importantes ou pour les personnes soucieuses de leur vie privée pour quelque raison que ce soit, cette fonctionnalité protégera les données contre l'interception audio et des attaques dites de l'homme du milieu (MITM).
- **Communication gratuite.** Chaque abonné recevra un numéro interne gratuit pour le réseau. **Exemple :** Parler au sein d'un réseau, en tête à tête ou en groupe et ce, gratuitement.
- **Masquer un numéro de téléphone.** Les numéros de téléphone utilisés pour les appels sortants seront masqués lors de leur détection par un dispositif de réception. **Exemple :** Conduire des déclarations et d'autres communications sans révéler votre propre numéro d'abonné.
- **Scénario d'exécution.** Cela permet de créer des scénarios exécutés via SMS/MMS et les appels. **Exemple :** Les utilisateurs peuvent transférer des cryptomonnaies à une adresse prédéterminée en appelant un numéro désigné et en saisissant un code PIN via le clavier de leur téléphone.
- **Fonctionnement multiplateforme.** EncryptoTel peut être utilisé sur tous les systèmes d'exploitation, les téléphones IP et les passerelles. **Exemple :** Les utilisateurs auront accès au déploiement et au contrôle de leur PBX via n'importe quel dispositif : terminal mobile, poste de travail, tablette, etc.
- **Enregistrement des conversations et stockage des données.** Les enregistrements de conversations ou d'autres données importantes peuvent être stockés en toute sécurité. **Exemple :** Activer l'option de stockage pour toutes les négociations et tous les fichiers. Ces données stockées ne peuvent être déchiffrées que par le propriétaire utilisant la technologie blockchain intégrée à EncryptoTel.

- **Suivi des appels.** Gérer les ressources liées au trafic. **Exemple :** Il est possible de créer un numéro unique pour chaque élément de publicité. Les statistiques peuvent être téléchargées et les progrès suivis à partir du compte de l'utilisateur.
- **SVI (Serveur vocal interactif).** Options de reconnaissance vocale. **Exemple :** Créer des instructions préenregistrées pour les personnes qui vous appellent afin d'optimiser le traitement des appels entrants.
- **Appels vidéo.** Appel en direct. **Exemple :** Appeler quelqu'un en utilisant une caméra ou commencer une conversation live en vidéo.
- **Aide-mémoires.** Synchronisez votre application avec votre agenda. **Exemple :** Lancer le système de rappel des événements importants par appel ou par SMS.
- **API.** Interagissez avec le service EncryptoTel en arrière-plan. **Exemple :** Intégrez votre GRC ou un autre système avec le PBX d'EncryptoTel et accédez à tous ses services, avec la possibilité de créer de nouvelles applications au-dessus de celui-ci.
- **Intelligence artificielle et interaction texte.** Effectuez une configuration et un contrôle de base pour les messagers populaires en utilisant le robot intelligent d'EncryptoTel. **Exemple :** Initialisez un appel via Telegram, le client XMPP/Jabber à l'aide d'un message simple, tel que «Appelle numéro +1 ... 1 du code pays États-Unis, puis appelle-moi sur le numéro +1 ... 2.»

## Génération de revenus et retour sur investissement

EncryptoTel facturera de certains services aux utilisateurs sur la base d'un abonnement ou à la carte, selon les préférences du client. Les statistiques relatives aux ventes et aux revenus pourront être clairement visualisées grâce à la transparence de la blockchain.

Nous occuperons le marché des télécommunications parmi les entreprises de crypto monnaies et de blockchain dans un délai d'un an et attirerons un grand nombre d'utilisateurs individuels au moyen de tarifs bas, de fonctionnalités étendues et d'une politique de publicité agressive. Après avoir établi une telle présence, nous consoliderons et élargirons cela auprès des utilisateurs réguliers et des grandes entreprises.

Les jetons ETT seront vendus lors du financement participatif d'EncryptoTel. Même si différentes cryptomonnaies seront également utilisées, ETT sera la seule pour laquelle des réductions seront possibles, ce qui augmentera sa demande en tant que monnaie utilitaire. La hausse de la demande de la part des utilisateurs finaux augmentera sa valeur en définitive.

## ***Abonnement et facturation à la minute***

Nous voulons faire d'EncryptoTel un service flexible qui permet aux clients de payer comme ils le souhaitent. Nous proposerons d'abord deux structures de paiement.

1. **Tarif prépayé.** Ce sera un montant mensuel fixe adapté aux clients, tels que les entreprises qui font de gros volumes d'appels chaque mois. Cela peut être accompagné d'une réduction sur un numéro direct et des options supplémentaires telles que SVI, répondeur, suivi des appels, etc.
2. **Tarif à la carte.** Cela entraînera des appels au prix standard, à condition que votre compte dispose d'un solde suffisant. Les clients pourront toujours passer des appels sécurisés dans leur réseau PBX gratuitement.

En plus d'une pression à la hausse sur l'achat direct du token exclusif ETT comme moyen d'obtenir des services à prix réduit, les revenus des autres paiements seront distribués régulièrement aux investisseurs. La façon la plus simple d'y parvenir serait au moins d'un dividende régulier, mais une telle méthode entraînerait des complications réglementaires. Une manière semblable pour atteindre cet objectif est d'effectuer un rachat périodique du token ETT sur le marché, puis supprimer le montant racheté de la masse monétaire totale, ce qui aura pour effet de réduire l'offre disponible et d'augmenter la valeur du token.

## ***Droits de vote***

En plus d'offrir une réduction sur les autres méthodes de paiement, ETT permettra aux détenteurs d'avoir une voix dans l'exécution de l'entreprise. Les détenteurs pourront voter par rapport aux principales décisions stratégiques, même si ce sera fait d'une manière consultative au lieu d'une manière juridiquement contraignante.

## ***Seuils de financement***

EncryptoTel en est déjà à une version bêta fonctionnelle de son produit (allez sur [www.EncryptoTel.com](http://www.EncryptoTel.com)), avec plusieurs de ses fonctionnalités principales mises en œuvre. Un financement supplémentaire est nécessaire pour terminer le développement et commercialiser son résultat. EncryptoTel a défini une série de budgets que nous pensons nous permettra de réaliser différents scénarios :

1. **\$100,000+.** Cela nous permettrait de créer un produit commercial entièrement fonctionnel qui pourrait concurrencer le marché mondial des PBX. Les fonds recueillis au-dessus de ce seuil seront consacrés à l'amélioration de la stabilité, à la mise en œuvre de nouvelles méthodes de cryptage et à la redéfinition de l'expérience utilisateur pour une plus grande accessibilité.

2. **\$250,000+**. Réalisation du protocole de cryptage du trafic d'EncryptoTel basé sur la technologie blockchain. Cela inclurait la publication d'applications mobiles pour Android et iOS pour une communication sûre et simple au moyen d'un PBX.
3. **\$1,000,000+**. Cela permettrait à EncryptoTel de pénétrer le marché international avec une politique d'expansion agressive, ce qui nous permettrait aussi d'occuper une fraction plus importante de l'industrie des télécommunications, y compris l'entrée dans des modèles PBX déjà configurés et personnalisés pour les tâches les plus communes des secteurs B2B, B2C et B2G. Cela nous permettrait enfin d'acquérir les licences nécessaires afin de fournir aux clients les services de télécommunications appropriés et de leur attribuer nous-mêmes les numéros.

## L'équipe EncryptoTel

L'équipe EncryptoTel possède une vaste expérience dans les domaines de la technologie blockchain, de la téléphonie SIP et du développement du service PBX via le cloud.

Tous les membres de l'équipe ont travaillé dans le secteur des télécommunications et celui des technologies associées pendant au moins six ans et ont participé ensemble à des projets de grande envergure, y compris la création de systèmes d'information en partant de rien. Ils sont des experts dans tous les aspects du monde de la monnaie digitale, du minage à l'intégration de la blockchain. L'équipe travaillait ensemble pour la même entreprise de télécommunications et ses membres se connaissaient depuis plus de cinq ans. C'est pendant le temps passé à travailler ensemble qu'ils ont réalisé qu'ils pouvaient révolutionner le marché numérique des systèmes PBX IP.

EncryptoTel a déjà construit un produit en bêta opérationnelle qui peut être testé par des clients potentiels et des investisseurs. L'équipe a précédemment participé à la réalisation d'un certain nombre de projets dans les domaines requis pour la mise en œuvre et le lancement réussis d'EncryptoTel, y compris la création de systèmes de facturation, de softphones et de systèmes ERP multifonctionnels. En outre, ils ont une solide expérience dans l'intégration de ces systèmes dans le processus commercial.

EncryptoTel a déjà consacré beaucoup de temps et de ressources à la conception de son produit de base et à la réalisation d'une bêta fonctionnelle. L'expérience de l'équipe les aidera à résoudre tout problème qui se pose au cours du processus de mise en œuvre, et ils ont les antécédents nécessaires pour réussir un projet aussi compliqué.

Pour obtenir plus de renseignements, rendez-vous sur [www.EncryptoTel.com](http://www.EncryptoTel.com)