SKRUMBLE NETWORK

# ブロックチェーンによる分散型コミュニケーション

## ホワイトペーパー

1. このホワイトペーパーはSkrumble Network White Paperの英語版から翻訳されています。一貫性がない箇所は英語で表示されます。
2. Skrumble Networkは積極的に研究を進めています。本文の新しいバージョンはwww.skrumble.networkにて発表されます。ご意見・ご感想はウェブサイトを通じてお寄せください。

「時々、新しい技術、古い問題、大きなアイデアが革新に変わる。」

Dean Kamen

ディーン・カーメン

# 目録

# 前書き

今、簡単で安全なコミュニケーション手段とデータの所有権がこれまでにないほど必要とされています。コミュニケーションをとる事は不可欠であり、そのコミュニケーションは安全で、個人がデータを所有するべきであります。 Skrumble Networkは、ブロックチェーン技術に基づく分散型で強力、安全、そしてアクセスしやすいコミュニケーションソリューションです。これにより、オープンなコミュニケーションが可能になり、人々が世界中で繋がり、可能な限り安全なプラットフォームで自由に話す機会が生まれます。

現在、ブロックチェーン技術で世界を変えるソリューションを構築する数千の革新者がいます。 フィンテック企業と政府は仮想通貨を探求し、専門的サービス会社はスマートコントラクトを使用し、サプライチェーンの管理者はリアルタイムで在庫を追跡し、そして資産は初めて明白なリアルタイムの所有記録によって保護されています。ブロックチェーンの誕生により、Skrumble Networkは革新を続け、分散型ネットワークがいかにより安全なコミュニケーションを可能にするかを詳細に検討する必要があります。

このホワイトペーパーでは、データ記憶のための集中型サーバーに伴うリスク、インターネットに基いたコミュニケーションシステムに関わるユーザー情報への脅威、そして意味のある接続をオンラインで確立することの難しさについて説明します。これらの問題は、完全に匿名のユニークなエンドツーエンド体験を提供する、統一された安全なネットワークを必要とします。これにより、分散型コミュニケーションネットワークが無限の成長を遂げる機会が生まれます。

Skrumble Networkは、世界規模でのコミュニケーションを真に民主化する可能性を秘めており、これまでになかった新しいアプリケーションの時代を切り開き、先進的かつ比類のない革新と発見に導きます。それは世界中のどこでも誰とでも安全かつ簡単に接続できる機能を備えています。Skrumble Networkは、ブロックチェーン技術と分散型ネットワークプロトコルを使用して、従来のファイアウォールを突破し、ユーザーの匿名性、コンテンツとデータのプライバシーを保証する安全で完全なコミュニケーションエコシステムを構築します。グループやピアツーピアメッセージ、通話、ビデオ、ファイル転送などの機能を含み、一箇所で処理できます。

# 問題

1.セキュリティ：集中型サーバーに基づいたコミュニケーションシステムはデータの安全性が問われます

2. プライバシー＆データの所有権：プラットフォームハプライベートではなく、ブロックされたり侵入される可能性があります

3.　グローバルアルセス：社会の隅に追いやられタコミュニティーは自由で信頼できる繋がりを求めています

## 1. セキュリティ：集中型サーバーに基づいたコミュニケーションシステムはデータの安全性が問われます

インターネットは、私たちがコミュニケーションをとる方法を完全に変えました。今やボタンひとつをクリックするだけでビデオチャットが可能で、企業は国際的に運営、そして提携し、銀行は毎日何十億ドルもの資金の国際移転を行い、ツイッターでつぶやくひとつで一国の大統領と繋がることが可能です。Eコマースでは、広州で製造された商品をニューヨークの会社がシドニーの女性に販売することができます。ソーシャルメディアは、コミュニケーション、ニュース報道、そしてエンターテインメントの姿を変えました。インターネットによりネット上のほぼすべての人が繋がることに成功しましたが、それに伴いプライバシーとデータの安全性に対する懸念も高まっています。

インターネットユーザーはよく、時には無意識のうちに、企業が広告主や政府など他の機関と個人情報を共有することを許可するサービス規約に同意します。たとえばグーグルは、ブラウザの活動や検索履歴などのユーザーデータを共有することで、主要な消費者サービスを無料で提供しています。Facebookはユーザーのデータや投稿などを広告主に販売しています。ソーシャルメディアやEコマースのサイトにアクセスした時、よく上記のデータやオフラインで交わされた会話の内容までもが反映された広告が出てきます。これはデジタル盗聴やユーザーのプライバシーに関する懸念を引き起こします。

コミュニケーションアプリケーションは、大量のデータトラフィックの日常管理に使用されます。メッセージプラットフォームWhatsAppは、1日あたり約550億件のメッセージ、40億枚の写真、そして10億回のビデオ転送を処理しているといわれています。しかし、他のほとんどのインターネットに基づいたコミュニケーションプラットフォームと同様、これらのデータはすべて1つの主要な接触点を持つ集中型サーバーを経由してルーティングされてます。この種の中央集中型システムでは、単一の接触点を突破することは比較的容易であり、悪質な関係者が大量のネットワークデータにアクセスする可能性があります。これにより、ハッカーは情報を盗み、改ざんすることができます。2018年1月、暗号技術者はWhatsAppのセキュリティシステムの裏口を発見し、グループチャットに侵入しました。この大規模なデータ漏洩により、WhatsAppの信憑性が疑われ、チャットツールのエンドツーエンド暗号化が無効となりました（Greenberg、2018）。

今、プライバシーを侵害されずに、またはハッキングの危険にさらされることなく、インターネットを使用することはほぼ不可能です。従って、ユーザーが自分の個人情報が侵害されることを心配することなく安全にコミュニケーションし繋がる事ができる、分散型の侵入不可能なネットワークが必要です。これは、大量の金銭が危機にさらされている仮想通貨の世界では特に不可欠だといえるでしょう。

## 2. プライバシー&データの所有権：プラットフォームハプライベートではなく、ブロックされたり侵入される可能性があります

相互にコミュニケーションをすることになると、一般に人々は情報転送の主要な源としてネットを使います。しかし、ネット上では数多くの情報やディスカッションフォーラムが今日利用されているため、いくつかの異なるコミュニケーションプラットフォームを使用して、ブロックチェーンやその他の課題なトピックについて学び、議論しています。これは、非常に断片化され、切断されたコミュニティー体験につながります。

Facebook、WhatsApp、WeChatなどの異なるプラットフォームを使用した情報の共有では、一貫性と信頼性の高いグローバルスタンダードを得ることが難しくなります。コンテンツを検閲しブロックすることが知られているTelegramのようなプラットフォームでも、既知のVPN　のURLまたはIPアドレスのためデータが収集され、復号化され、アクセスが完全にブロックされることがあります（Russell、2017）。実際、2018年2月1日に、「不適切なコンテンツ」のためApple　App　StoreからTelegramが削除され、内容をフィルタリングするための保護対策が施されていることを確認するよう求められました（Warren、2018）。これらのプラットフォームの中には、特定の国で禁止または抑制されているものがあり、情報の不平等を招いています。 FacebookやWhatsAppは中国では禁止され、最近イランでTelegramの禁止が解除されましたが、Telegramはいまだにインドネシア等複数の国で禁止されています。（Toronto Star、2018 - Toor、2017）

- Facebook、WhatsApp、およびグーグルは中国本土で禁止されています（India Today、2017）。
- WhatsAppは最近、グループチャットに侵入可能な裏口が存在することが分かりました（Greenberg, 2018）。
- WeChatはユーザー会話を検閲し、複数のデバイス間で同期出来ません（WeChat、2018）。
- Telegramはコンテンツを検閲し、一度イランで禁止されました（Toronto Star、2018）。
- FacebookとGoogleは、広告主とユーザー活動を共有します。（Facebook、2018; Google、2018）

さらに、新技術やその他の話題に関する特定のフォーラムでは、他の形の検閲が存在するかもしれません。例えば、BitcointalkやRedditのスレッドのような仮想通貨に関する議論のためのフォーラムです。仮想通貨に興味を持つ人がこの領域に入る際一番の壁は、仮想通貨取引の合法性に関する情報の欠如です。これらのフォーラムは、多くの場合個人的な意見で構成されているため、検証可能な事実に裏付けられているとは限りません。

また、仮想通貨のエコシステムや他のほとんどすべてに関する情報を知るため、多くの人がYouTubeのような動画共有プラットフォームを利用しています。これらのコンテンツは単方向であり、信頼性に欠け、主に個々の嗜好を反映しているため偏見があり、どのト

ピックについても表面的な見解しかないという問題が存在します。また、これらのコミュニケーションプラットフォームは集中型ネットワークを使用するため、上記のリスク、すなわちハッキング、ソーシャルエンジニアリングなどセキュリティ上の脆弱性に直面しています。

現在のオンラインコミュニティとコミュニケーションプラットフォームは、各システム内部の欠陥や脆弱性が明らかになっています。既存のソリューションは断片化、切断され、信頼性が低く、世界中の信頼と接続性を向上させるための改善の余地があります。グローバルにアクセス可能なオンラインコミュニティのようなソリューションを通じて、統一された安全なコミュニケーションは人々を結集させる機会を増やし、拡大します。

## 3. グローバルアルセス：疎外されたコミュニティーは自由で信頼できる繋がりを求めています

データの安全性についての不安が続く中、人々はどのように持続可能なオンラインコミュニティーを作り、会話の中で意味のある情報を共有すればいいのでしょうか？オンライン活動の課題の1つは、自分のアイデンティティを保護し、快適性、安全性を保ち、実行可能な活動を展開しながら関係を構築することです。人々には、公開フォーラムやプラットフォームへ自由にアクセスし、自由に話し、仲介者や未知の第三者に個人情報を把握される心配から免れる権利があります。

単に共通の関心事を話し合い、ストーリーを共有し、ネットワーキングすることで、人々を結びつけることができます。人々が繋がったとき、彼らは真実で正直なアイデアや個人情報を共有し、意味のある関係を築くのに十分な安心感と快適さを感じます。このような気楽な繋がりよって、信じられないほどの革新が生まれます。

時には疎外されたコミュニティーが自由な議論の場を求める中、新しいアイデアを共有するためのオープンで合理的な媒体を見つけることは難しいかもしれません。接続性とグローバルアクセスを必要とする1つの例は、仮想通貨コミュニティーです。仮想通貨に対する一般的な認識は、その採用と価値の最大の決定要因の1つです。まだ誕生から9年ほどにもかかわらず、仮想通貨は急速な成長と拡大の段階にあり、現在数千もの異なる通貨とアプリケーションが存在します。このような環境の中、ブロックチェーン技術企業が新しいアイデアを紹介し、潜在的なユーザーがより多くの人々とつながり、最新のコミュニティー発展について理解を深めることがますます困難になりつつあります。ブロックチェーンの主張者が潜在的なユーザーや一般人と関わる最良の方法は、直接コミュニケーションをとることです。

安全なコミュニケーションネットワークは、意味のある接続の確立を促進するだけでなく、世界中の誰もがひとつになれる真の媒体を提供することができます。人々は、ハッキングや他人が自分の個人情報に関与していることを心配することなく、自由に話したり、情報を共有したり、データを転送したりすることができます。グローバルなブロックチェーンコミュニティーは、現在のブロックチェーンユーザー、または安全で保護されたネットワークを使用して他人と繋がりたい人のために、世界中のコミュニケーションを改善します。

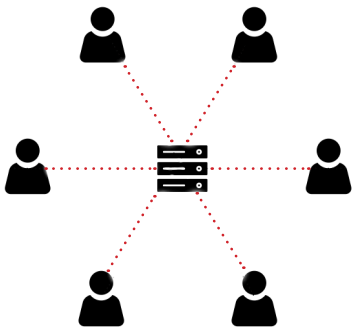
# ソリューションの要件

1.安全性：独自のコミュニケーション技術によるセキュリティ強化

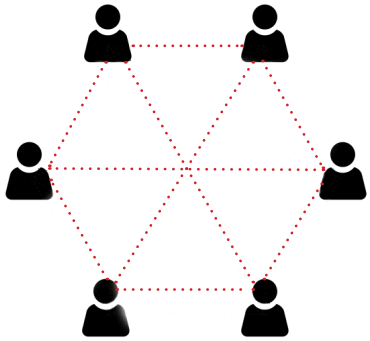
2.分散型：安全なコミュニケーショントランザクションをサポートする分散型ブロックチェーン台帳

## 1. 安全性：独自のコミュニケーション技術によるセキュリティ強化

一般的に、コミュニケーションネットワークは、ユーザー間のすべてのデータトランザクションの情報を記憶した集中型サーバーに依存しています。しかし、ブロックチェーンのような分散型ネットワークでは、ひとつの場所に情報が記憶されていないため、サイバー犯罪者がハックすることはほとんど不可能です。ハッカーやその他のサイバー犯罪者は、世界中のコンピュータセキュリティシステムやネットワーク全体に数時間内で侵入することが出来ます。しかし、情報がブロックチェーンの分散台帳に記録された場合、その瞬間に消去、変更、再配置、または改ざんは不可能となります。 1つの中央型サーバーを攻撃するだけでは、システム全体を制御することはできません。この分散型ネットワークのコンセンサスに基づく不変性は、透明で安全な枠組みを作り出し、大きな可能性を秘めています。



集中型サーブー



分散型ネットワーク

金融部門では、デジタル取引を保護する方法は必要な投資であり、仮想通貨コミュニケーションで使用されるブロックチェーン技術は一番重要な投資対象のひとつです。仮想通貨を研究している経済学者は、資金がすでに物理的形式からデジタル形式に移行し始めており、カナダ、インド、ロシアなどの国の政府は、仮想通貨を組み込む手段を検討し始めていることを確認しています（Sabbin、2018）。ブロックチェーンの固有の不変性は、トランザクションを検証するコストを削減し、その分散型の特質は、取引の過程から仲介役を省くことを可能にします。

分散型ネットワーク上のコミュニケーションソリューションやアイデンティティ管理についても同じことが言えます。ブロックチェーン技術の幅広い応用、およびその応用がもたらす透明性と安全性を考慮すると、これらのサービスを一般人がより利用しやすくするための高度サービスとプラットフォームには、大きな成長の機会があります。

## 2.　分散型：安全なコミュニケーショントランザクションをサポートする分散型ブロックチェーン台帳

1998年、暗号の専門家でありスマートコントラクトの考案者であるニック・ザボ氏（Nick　Szabo）氏は、「インターネットでビジネスを行うには、信仰の飛躍が必要だ」と述べました。信用はいつもコミュニケーションと商業の基本的な通貨でありました。毎秒世界中の見知らぬ人の間で行われるオンライン取引は通常第三者を通じて行われ、取引を完了させるためにユーザーとホストの間で信頼関係を構築する必要があります。メッセージを送信する時、または支払いが行われる時に、送信者は仲介者が受信者に安全に送付することを信頼すること以外に選択肢はありません。

しかし分散型ブロックチェーン台帳を使用することで、ユーザーは仲介に頼ることなく、またはプライバシーの侵害を心配することなく、安全かつ直接に相手と繋がり、取引を実行できます。ブロックチェーンと分散型ネットワークは、分散台帳を使用して信頼性の低い環境で自信を持って取引をする方法を提供し、透明性とコンセンサス主導の改ざん防止トランザクションログを作成します。すべてのトランザクションの「ブロック」はネットワーク全体で検証され、その後、チェーンと永遠に連結され、比類ない安全性と責任を保障します。

さらに、ネット上のアイデンティティ管理プロトコルを改善する必要があります。個人の自宅住所、連絡先、財務情報など、今や多くのオンラインアカウントと取引において、身元を確認する必要があります。2017年、アメリカでは最高記録の1540万人がアカウント情報を盗まれ、金融詐欺にさらされました（Pascual、2017）。

分散型台帳は、連絡先の詳細を共有することなく、個人情報をデジタル化し、身元を確認するための強化された方法を提供します。公開鍵と秘密鍵を持つブロックチェーンのデュアル暗号化メカニズムにより、アプリケーションは、公開鍵と秘密鍵を使用する人の身元をデジタルで検証し、偽の鍵伝播やデータ改ざん、そして盗難のリスクを排除します。

この問題の明らかな解決策は、ユーザーを直接接続するブロックチェーンの分散型台帳を利用し、仲介者または未知の当事者に信頼を置く必要をなくすことです。分散型のコミュニケーションネットワークは、ユーザーがプライバシーを心配することなく、安全かつ直接に接続し取引できることを意味します。

# SKRUMBLE NETWORK:
# 完全なグローバルコミュニケーションエコシステム

今、安全で合理化と標準化され、最低限の技術ノウハウで行えるコミュニケーションが必要とされています。ブロックチェーンエコシステムのために設計された、堅牢で安全なフレームワークとユニファイドコミュニケーションの専門技術をを持つSkrumble Networkは、このニーズを満たすために最適だと言えるでしょう。

世界初の分散型ネットワークに基づいた完全なコミュニケーションエコシステムは、Skrumble Technologies Inc.によって構築されます。この類を見ないエコシステムは、オープンなコミュニケーションを介して世界中の誰もが誰とでも接続できる、使いやすく安全なネットワークです。完全に統合されたコミュニケーションにより、Skrumble Networkユーザーは、真に民主化された、安全で、グローバルな分散された環境において、意味のある接続を確立することができます。

独自のコンセンサスに基づいたアルゴリズムと仮名識別手段を使用して、ユーザーは自らユーザー名を設定し、情報、データおよびコミュニケーショントランザクションの所有権を保有します。ユーザーは、完全な安全でプライベートの環境の中多くの人をオンラインコミュニティに集めたり、他のユーザーと1対1の会話が出来ます。このネットワークにより、ユーザーはシームレスなメッセージのやりとり、通話、ビデオ、ファイル転送などをう行うことができ、コミュニケーション、アイデンティティ管理、そして無限の安全なコミュニケーショントランザクションへのユーザーのアクセスを向上させることができます。現在のインターネットに基づいたコミュニケーションシステムの安全リスクを分散型台帳で解決するSkrumble Networkは、独自の斬新なセキュリティ技術を活用しています。

Skrumble Technologies Incは、分散型ネットワークプロトコルのコンセンサスベースの不変性を利用した安全なコミュニケーションエコシステムの必要性を認知し、人間の接続性とアイデンティティ管理の革新の駆動力になる事を目指しています。は、一流のチームの専門知識と経験を活用し、この画期的でユニークなサービスを提供いたします。オープンソースのソフトウェア開発キット（SDK）を使用することで、完全なコミュニケーションエコシステムが構築され、第三者が安全でプライベートな匿名コミュニケーションを必要とする多数のアプリケーションを統合して開発することが容易になります。

世界初のSkrumble Networkはブロックチェーンプロトコルが一般的に応用されている金融取引以外の領域の外で応用されます。コミュニケーション、認証、そしてブロックチェーン技術を世界中のアプリケーションの中でどのように使用できるかについての新しいグローバルスタンダードを設定するために使われます。

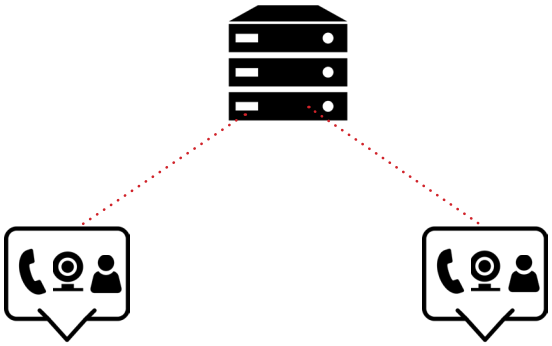
## SKRUMBLE NETWORK コミュニケーション機能

- メッセージ
- オーディオ通話
- ビデオ通話
- ファイル転送
- グループ会議
- 画面共有
- ユーザー制御ストレージ
- スクリーンショットの通知
- 匿名識別
- データ暗号化
- ほぼ全ての機能が最新のブラウザで実現可能
- インコンテキスト送金のためのウォレット

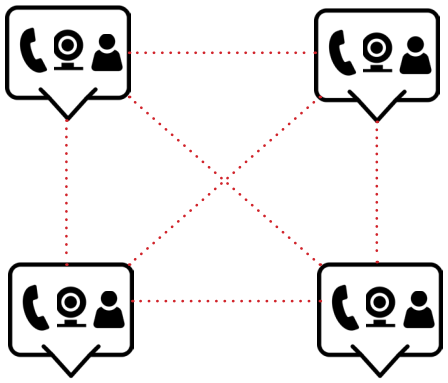
# 技術的コンポーネント：SKRUMBLE NETWORK を支える技術

## はじめに：分散型ネットワークでの安全なコミュニケーション

従来のコミュニケーションネットワークは、集中型サーバーに基づいています。使用されるコミュニケーションプロトコルとは無関係に、それらはすべて本質的に同じように機能しています。すなわち、コミュニケーションのメディアストリームを確立するためのハンドシェイクおよびメタ情報の交換を含む情報パケットを使っています。サーバーは、そのコミュニケーションを確立し、伝達します。Skrumble Networkは、集中型サーバーを完全に切り離すことによってコミュニケーションが行われる方法を革新します。



現在の集中型サーバー



集中型サーバーがなくなった分散型ネットワーク

## SKRUMBLE NETWORKのプロトコルを使用したユニークなセッションIDとデータ管理

Skrumble Networkは、独特なブロックチェーンによって実現された技術エコシステムで、完全な分散型匿名コミュニケーションを可能にします。現代のネットブラウザやSkrumble Networkのネイティブアプリケーション（iOS、Android、PC&Mac）を使用して、ピアツーピア接続上でリアルタイムコミュニケーションプロトコルを活用します。

Skrumble Networkのユニークなセキュリティプロトコルは、Skrumble Networkブロックチェーンを使用して独自のキー派生アルゴリズムによって提供されます。ネットワークに加わると、ユーザーはSkrumble Networkトークンを保持する公開鍵をウォレットに入力するよう、そして安全なパスコードと仮名（個人のユーザー名）を入力するよう求められます。これらの要素の派生物は、個人の独自Skrumble Network ユーザー IDとパブリックIDを生成するために使用されます。そしてユーザーのパブリックSkrumble Network IDを簡単に共有するため、QRコードとリンクが生成されます。

無比の安全性で、会話は、各参加者からの秘密のSkrumble Network ユーザーIDキーの派生物をシード・キーとして暗号化されます。派生アルゴリズムは、関連する参加者に基づいて、セッション内の関連するSkrumbleネットワークキーからランダムに選択するため、2つ同じのキーは存在しません。これにより、全ての会話が異なるキーを使うため、パターンベースの方法でSkunkble Networkの会話を複合化するのは事実上不可能になり、安全性がさらに高まります。例えば、ユーザーAとユーザーBのプライベートSkrumble NetworkユーザーIDキーがランダムに組み合わされ、会話シードキーと会話IDが形成されます。

ユーザー間のコミュニケーションが確立されると、Skrumble Networkブロックチェーンは、従来のコミュニケーションネットワークで発生するハンドシェイクプロトコルを置き換えます。 Skrumble Networkでは、セッション記述プロトコル（SDP）メッセージはブロックチェーンを利用して各セッションを確立し、ハンドシェイクとコミュニケーション開始の信号と、メディア（音声、ビデオ、メッセージなど）の送信を開始するためのリアルタイム転送プロトコル（RTP）ストリームになります。

人々の間で接続が確立されると、ユーザーのIPアドレスは互いにのみ明らかになり、安全なウェブソケット接続が確立され、ユーザーのデバイス間のコミュニケーションセッションを開いて、メッセージ、ファイル転送、および通知のリアルタイムセッションデータを交換します。これにより、データを瞬時に配布して、待ち時間の少ない接続が可能になります。

Skrumble Network上のコミュニケーションは、P2P（Peer-to-Peer、ピアツーピア）であり、より多くの人が参加するオーディオおよびビデオ会議のための特別な高容量リッチコミュニケーションブリッジにアクセスする能力を持っています。

Skrumble Networkは、ほぼ全てのモバイルデバイス（iOSとAndroid）とコンピューター（MacとPC）のスタンドアロンアプリケーションとして機能するだけでなく、最新のブラウザでも動作するように構築されます。スタンドアロンのアプリケーションバージョンは、ブラウザベースのバージョンよりも追加の機能を提供します。

## SKRUMBLE NETWORKコミュニケーション認証ブロックチェーンプロトコル

Skrumble Networkは独自の安全なアドホックコミュニケーションセッションを確立するブロックチェーンを開発します。 Skrumble Networkのブロックチェーンは、アプリケーションのいくつかの側面で利用されます：

1.初期コミュニケーションセッションを確立する。
2.ユーザー仮名をSkrumble NetworkユーザーIDと同期させる。

どちらの機能も、コンセンサスの検証と認証を提供するための採掘（マイニング）を必要とします。 Skrumble Networkは、マスターノードのサーバホスト、およびマイニングコミュニティやパートナーがプロジェクトを積極的にサポートするよう、強力な報酬とアウトリーチプログラムを開発します。 これらのパートナーシップは、Skrumble Networkのコンセンサス解決時間を最適化するのに役立ちます。

## 類を見ない未来のデータ容量とスピード

現在、ユーザーが既存のブロックチェーンに基づいたアプリケーションを使用して活動を行うと、新しいトランザクションとデータが保存され、記憶されます。より多くのトランザクションを保存すると、読み込み時間が長くなります。たとえば、Ethereumの一般的な金融取引では、コンセンサスに達するまでに通常約20秒かかります（Yannik、2017）。コミュニケーショントランザクションの量が増加するにつれて、Skrumble Networkはメッセージ、通話、ビデオ通話、およびファイル転送をすべて個別のトランザクションとみなす必要があるため、各ユーザーのパフォーマンスが低下します。したがって、Skrumble Networkはこの重要な問題を解決するため、プラクティカルビザンチンフォールトトレランス（PBFT）コンセンサスアルゴリズムを利用して、パフォーマンスとスケーラビリティのバランスを取っていきます。リアルタイムでトランザクションを決済するために、Skrumble Networkは、インセンティブに駆使されたマイニングによって10秒以内にコミュニケーション設定を達成することを目指します。

Skrumble Networkは最適な読み込み時間を確保するため、これらのプロトコルはシャーディング技術を使用して開発されます。この技術を利用することにより、大規模なデータベースをより小さく、より速く、より簡単に管理できる部分に分けることができます。データが必要な場合、一度にひとつの記録をロードする代わりに、各断片から情報を引き上げることで、Skrumble Networkはひとつのレイヤードデータベースとしてロードされます。

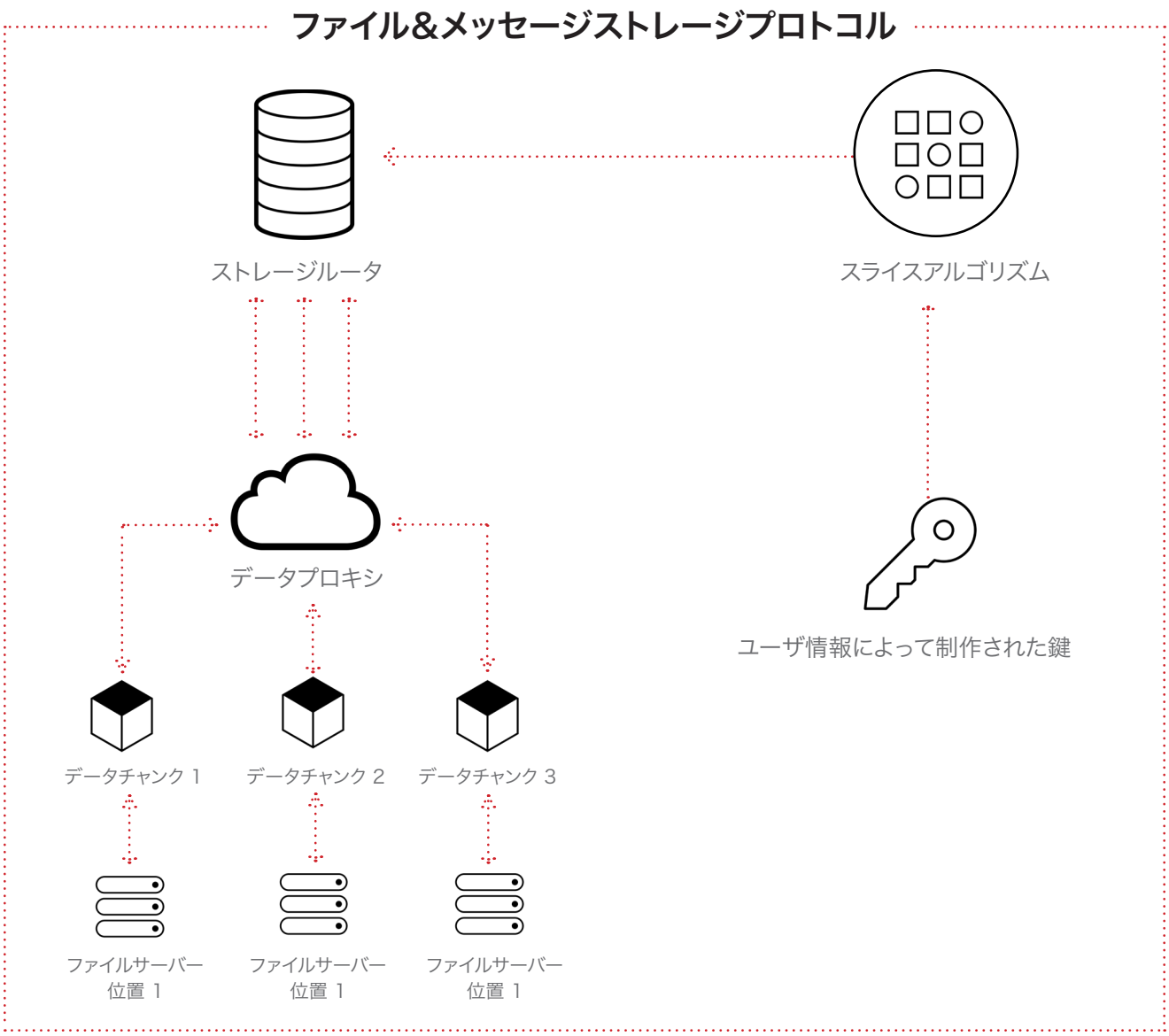
Skrumble Networkチームは、常にコンセンサスとブロックチェーンのロード時間の短縮のより新しく、より早い方法を研究し評価しています。我々は、ユーザーにSkrumble Networkをシームレスに利用していただくため、ネットワークを絶えず改善することに専念します。

## ネットワーク上のファイル保管のための暗号化された排他的なキー

Skrumble Networkは、ファイル情報が暗号化されていることを確認するため、ユーザーごとに唯一のセッションIDとランダム化されたキーデータを使用するアルゴリズムを利用し、真の分散型ファイル保管を実現します。このアルゴリズムにより、ユーザー間の直接ファイル転送を保証し、会話に参加したユーザーのみがアクセスを許可されます。

Skrumble Networkは、新規特許出願中のハイブリッドストレージ戦略を採用します。この方法は2015年にSkrumble Technologies Incによって開発されました。このハイブリッド方法を使用すると、ファイルは唯一のセッションIDとそのシードキーから派生するアルゴリズムを使用して暗号化されます。一旦暗号化されると、個々のファイルはいくつかの断片にスライスされ、異なるサーバーに分散されて保存されます。これらのファイルは、適切なキーのみにより再構成が可能です。したがって、ファイルサーバーが侵害されると、取得されたデータが判読不能になり、すべてのユーザーに安全なデータストレージを保障します。

さらに、保存期間やファイルサイズなどの機能は、ウォレット内のSkrumble Networkトークンの数に基づいてユーザーがアンロックした使用レベルによって決まります。




## 高容量リッチコミュニケーションブリッジ

6人以上の参加者を含むオーディオおよびビデオ会議の場合、匿名のアドホックセッションは、主要な戦略分野にグローバルに配置され、固有のセッションIDと派生キーを使用して認証される専用ブリッジを通じて確立されます。Skrumble Networkはアドレスに IPトンネリングのスキームを使用し、非常に大きなプールからランダムに選択されたものをランダムに変更します。ブリッジに接続するためのプロトコルに従って、ユーザーは接続を確認します。接続が確立されていない場合、次に合意したアドレスに増分します。これらのプロトコルにより、より大規模な音声およびビデオ会議、メッセージ、画面共有、ファイル転送、および通知が可能になります。

多くの参加者を追加する機能や会議時間を延長する機能を使用するには、ウォレット内のSkrumble Networkトークンの数に基づいて、ユーザーが一定のレベルをアンロックする必要があります。

## 業界をリードする機能とユーザー制御ストレージの管理

Skrumble Networkの最大の差別化要因の1つは、グループとピアツーピアメッセージを保存して記憶するオプションです。会話記録は、クラウド内のファイルサーバーにて記憶されます。元の会話に参加した唯一の会話キーを持つユーザーだけが、保存された情報へのアクセスを許可されます。

グループメッセージが作成されると、その会話の管理者に記録を保存するオプションが与えられます。選択機能は、特定のトークン所有金額に基づいてアンロックされます。参加者が会話に参加する前に、管理者が会話を保存すると選択した事が知らされ、参加者は参加か否かを選ぶことができます。2人の参加者との会話に参加する場合は、2者間の同意が必要です。各参加者は、会話が保存されることに同意する必要があります。

さらにSkunkble Networkでは、会話の参加者に基づいて暗号化キーを作成する独自のアルゴリズムなど、あらゆる会話を区別するための機能を打ち出します。世界中の誰とでも接続できるように、ユーザーは大規模なコミュニティグループを簡単に作成できます。Skrumble Networkの匿名プロトコルを維持するために、ユーザーは仮名識別を使用して操作します。そして、他のユーザーが画面共有またはビデオのスクリーンショットを撮ったときに通知を受け取ります。ユーザーは、ライブビデオグループと、暗号化された分散ファイルおよびデータ転送にアクセスできます。

Skrumble NetworkはオープンソースのSDKを公開し、サードパーティの開発者にSkrumble Blockchainのセキュアでプライベートな匿名コミュニケーションエコシステム機能を利用して新しいブロックチェーン技術とアプリケーションを開発するよう促します。

## SKRUMBLE NETWORK：ファイアウォールのないグローバルコミュニケーション

Skrumble Networkの分散型、安全で匿名のコミュニケーションプラットフォームを利用することによる明らかなメリットの中に、特に注目すべき3つの利点があります。

1. Skrumble Networkは従来のファイアウォールではブロックできません。
2. Skrumble Networkにはユーザー制御の記録ストレージがあり、一度削除するとデータは完全に消去されます。
3. すべての会話、メッセージ、およびファイルの優れた暗号化

すべてのユーザーと会話が独特なので、ファイアウォールを使用してブロックする中心的なポイントが存在しません。これにより完全な匿名性が保証され、世界中のどこからでもSkrumble Networkに無制限にアクセスできます。外部のインターネットアクセスがすべてブロックされている管轄区域のみにアクセスが制限されます。

# SKMユーティリティー・トークン・メンバーシップ：SKRUMBLE NETWORKコミュニケーション

SKMは、所有するトークンの数に基づいて特定のクラスのメンバーシップを提供するユーティリティトークンです。これらのメンバーシップ特権により、Skrumble Networkエコシステム上のさまざまな機能やアクションにアクセスできます。最初使用は無料で、トークンはプレミアム機能、メンバーシップレベルをアンロックするためのアクセス手段となります。

SKMユーティリティートークンの使用例：

カナダのユーザーAは、タイのユーザーBとビデオコールをしたいと考えています。ビデオはプレミアム機能です。ユーザーAとユーザーBはビデオコールを実行するために、設定された数のSKMユーティリティートークンを所有している必要があります。

フランスのユーザーAはブラジルのユーザーBにファイルを送信します。ファイルが許可されたファイルサイズを超えています。したがってユーザーAは、特定のトークン量を所有している必要があります。

コロンビアのユーザーAは、オーストラリアのユーザーBとの会話を保存したいと考えています。ユーザー制御の記録保存は、プレミアム機能です。ユーザーBは、保存される会話に参加することを確認しました。次に、両方のユーザは、会話保存のためにトークンを所有していなければなりません。

ドイツのユーザーAが米国のユーザーBにファイルを送信しようとしていますが、ユーザーAはユーザーBにファイルを誰とも共有させたくありません。ユーザーAは一定量のトークンを所有し、もしファイルが第三者に転送されると通知を受け取ります。

フィンランドのユーザーAは、スコットランドのユーザーBのみがファイルにアクセスできるよう、ゲーテッドアクセスキーを使用してユーザーBにファイルを送信します。ユーザーAは一定量のトークンを所有し、ユーザーBにファイルを分割して送信します。ユーザーAからユーザーBに与えられたアクセスキーだけがファイルをアンロックすることができます。

## ユーザー報酬：サプライズ&デライト

・　アクティブなコミュニティーのメンバーは、基準に基づいてサプライズトークンの報酬を受け取ります。たとえば、一定の量の会話を行ったメンバーは、追加のトークンを受け取ることになります。

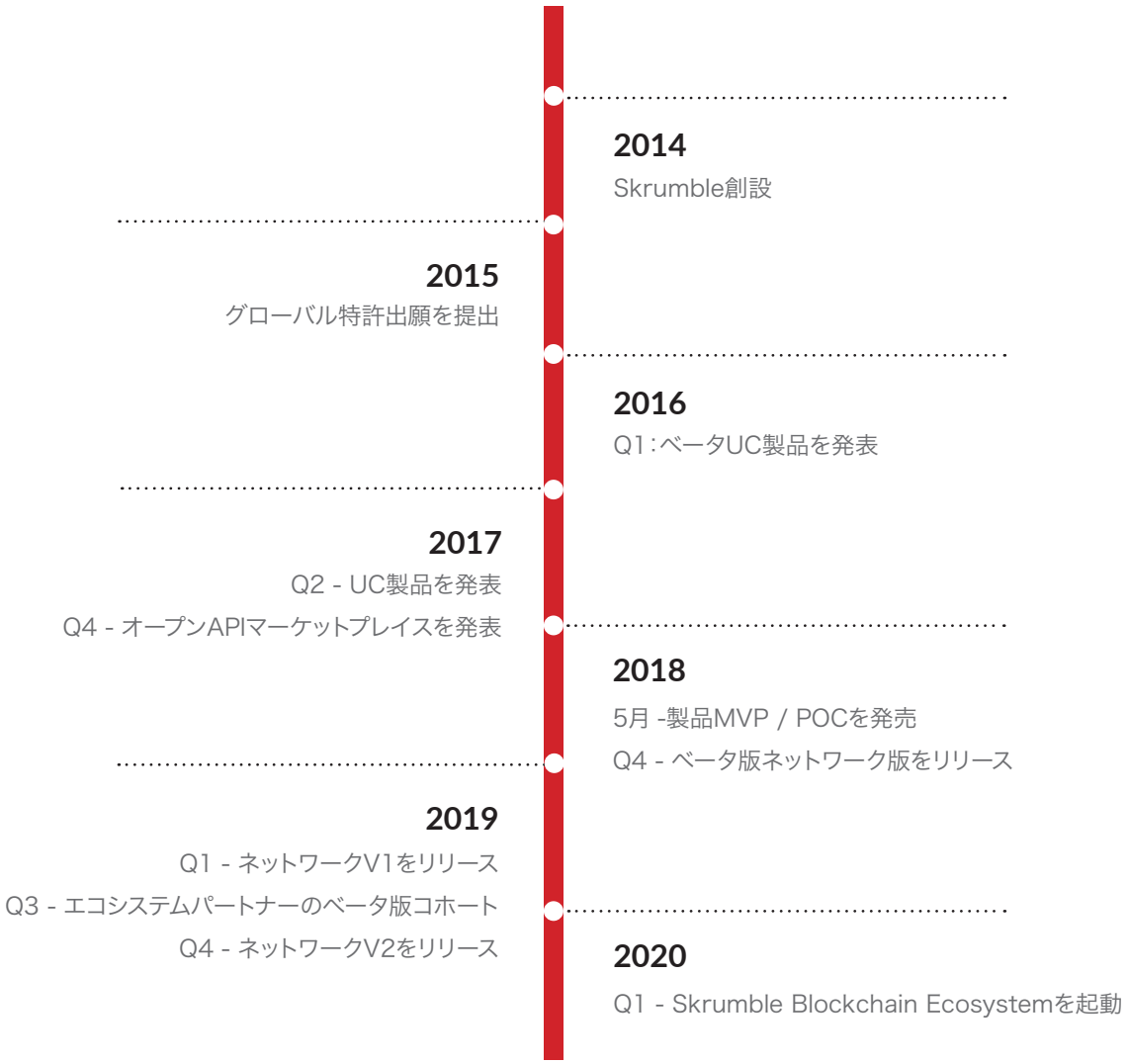
・コミュニティー貢献者を促進するためのランダムな特別報酬があります。

・ネットワークコミュニティを採鉱、認証そして促進したメンバーも、報酬を受け取る機会があります。

## 自己持続可能なエコシステムの構築

- オープンAPI / SDKを提供することで、コミュニティプレイヤー/起業家はSkrumble独自の分散型コミュニケーション技術を活用し、特定の業種にサービスを提供できます。
- このプロセスの第1段階は、Skrumbleラボイニシアチブを通じて、バーチャルショールームやフリーランスマーケットなど、Skrumble Networkに基づいて構築された2-3の初期戦略パートナーを育て、打ち出すことです。
- 第2段階では、独自の製品やサービスを作成するためのAPI / SDKを全ての方に提供します。
- SKMトークンは、Skrumble Networkを介して様々なアプリケーションのユーザーによって消費されます。また、SKMトークンを使用してアプリケーションにインセンティブを与えることもできます。したがって、このエコシステムは、革新的なプラットフォーム開発、コストおよび報酬制度によって持続可能となるでしょう。

# 技術ロードマップ



# SKRUMBLE NETWORKのメリット

プライベート　分散型サーバー　ユーザー制御ストレージ　オープンなAPI

安全　暗号化　安全なファイル転送　追跡不可能

匿名　グローバルに接続　スクリーンショットの通知　ブロック不可能

# SKRUMBLE NETWORKの使用事例

## 1. メッセージの保存と削除

ユーザーがSkrumble Networkを利用してプライベートで安全な匿名の会話をする際、会話履歴を保存して記憶するオプションを提供することが重要です。これには、メッセージ、通話履歴、および記録保存が含まれます。P2P会話の場合、両方のユーザーが会話の保存を承認する必要があります。グループ会話では、会話の管理者は保存するかどうかを選択し、他の参加者は承諾するかどうかを尋ねられます。保存しないことを選択した場合、分散型ネットワークには何も保存されません。保存することを選択した場合、情報はクラウドに保存され、会話の参加者のみがアクセスできます。

## 2. 安全なファイルの転送

Skrumble Networkは、ユーザーに自分のデータを共有し、暗号化された安全なファイルを送信するためのスペースを提供します。ユーザーは、ゲーテッドアクセスキーを使用してファイルを送信することができます。つまり、あるユーザーから別のユーザーにファイルが断片ごとに送信されます。ファイルを受け取ったユーザーには、この内容をアンロックしファイルを元に戻すための秘密のアクセスコードが与えられます。ユーザーは、送信したファイルに通知を送信することもできます。これは、ダウンロードしたり、別の会話に転送したりしたくないファイルが実際にダウンロードまたは転送された場合、ユーザーがすぐに警告を受け取るようにするためです。

# SKRUMBLE NETWORKのエコシステム追加機能

SKMトークンは、Skrumble　Networkを介して様々なアプリケーションのユーザーによって消費されます。また、SKMトークンを使用してアプリケーションにインセンティブを与えることもできます。したがって、このエコシステムは、革新的なプラットフォーム開発、コストおよび報酬制度によって持続可能となるでしょう。 Skrumble、Skrumble ラボインキュベーションプログラム、または他の第三者グループから、以下のアプリケーションの展開を予定しています：

## 1.インテキストと安全なオンライン決済ゲートウェイ

決済ゲートウェイの多くは複雑で、独立した無関係なアプリケーションやフォーマットを設定するために高度な技術的知識を必要とします。Skrumble Networkには、会話の中にエンドツーエンド暗号化決済システムが含まれます。会話内のピアツーピアの送金、ページを離れることなくECによる支払い、またはプライベートメッセージ、通話、ファイルなどのコミュニケーションの際にも決済が可能です。

## 2.フリーマーケット

近年、一定の仕事のためにフリーランサーを雇用し、フリーランサーが要求する賃金を支払うネット上のプラットフォームが増えています。 Skrumble Networkは、スマートコントラクトに基づくフリーランスのマーケットを構築するためのコミュニケーションとトランザクション機能を備えています。各関係者は、フリーランサーを容易に選択し、雇用条件を設定することができ、コントラクトの要件が満たされたときにフリーランサーがそれに応じて支払われます。

## 3. 会話内スマート・コントラクト

スマートコントラクトは、トランザクションやビジネスを遠隔で行うためには不可欠です。Skrumble　Networkは、会話や通信の取引中にユーザーが記入してサインオフするためのスマートコントラクトテンプレートを用意しています。弁護士とクライアントの利用規約の同意、遠隔勤務の従業員への指示、上記のマーケットからのフリーランサーの雇用、または利害関係者の承認を必要とするあらゆるタイプの取引に役立ちます。規約が同意され、会話内でスマートコントラクトが締結され、パートナーシップが達成されると、各当事者は契約上約束された内容を受け取ります。

## 4. バーチャルショールーム

Skrumble Networkは、ビデオ、メッセージング、およびプレゼンテーション機能を利用して、その機能をカスタマイズし、P2Pまたはグループ会話のインタラクションポイントを含めることができます。これらの接触点は、ユーザーがライブビデオを放映し、才能を共有し、会話中に支払いを受け取るためのものです。

## 5. 技術協力

Skrumble Networkエコシステムの機能とサービスをさらに強化するため、Skrumbleはブロックチェーンと仮想通貨業界の主なリーダーと提携します。Aion Networkのエコシステムや決済ソリューションなどの業界で影響力が高い企業と連携することで、Skrumble Networkユーザーの機会を豊かにし、さらにユーティリティートークン保有者にインセンティブを与えることができます。

# 結論：より人間的で連結されたブロックチェーン

ブロックチェーン技術は、多くの深刻な問題を解決します。仮想通貨は、越境の金融機関やトレーディングを大幅な銀行手数料なしで促進します。スマートコントラクトは、提供されたサービスに対してのみ支払いを行い、リアルタイムデータは商品の移動や所有を追跡することができます。その明白なセキュリティ対策、データ管理およびコミュニケーションにより、分散型ネットワークは、より安全なコミュニケーションのための不可欠な触媒です。

ブロックチェーンは、暗号化とユニークなデータ保存と送信、そしてピアツーピアネットワークを組み合わせ、分散型で信頼できるデータベースを作成します。サイバーセキュリティ、データ保存、およびインターネットに基づくのコミュニケーションシステムに関わるユーザー情報への脅威に関する主な懸念は、分散台帳の使用で完全に不要となります。これらの問題を解決する以外に、ブロックチェーンは、革新のための比類なき機会を提供します。インコンテキストのオンライン決済ゲートウェイの新しい方法を発見し、世界中の人々が意味のある接続を確立するための新しい方法を提供するのです。

分散化は革新のための無限の可能性を提示し、エンドツーエンドの暗号化、完全な匿名性とコミュニケーションの機会を可能にする統一された安全なネットワークのソリューションを提供し、世界を接続し、共有させ、成長させます。

Skrumble Networkは、世界のどこからでも誰でも安全かつ簡単に接続することができ、世界中のコミュニケーションを真に民主化する可能性を秘めています。コミュニケーションを確立するために、初めてブロックチェーンを使用することになります。Skrumble Networkは、金融取引を処理するために使用されているブロックチェーン技術の使用をあらゆるアプリケーションの不可欠な要素に変えていきます。容易にアクセス可能で信頼性の高いコミュニケーションにより、世界中の人々は、コンセンサスベースの環境でデータの所有権を取り戻し、セキュリティについて再度心配することなく、異なるコミュニティーに積極的に参加する機会が得られるのです。

# SKRUMBLE TECHNOLOGIES INCについて

Skrumble Technologies Incは2014年に設立され、業界で定評のあるクラウドコミュニケーション会社です。30件以上のグローバル特許を出願したSkrumbleは、Fortune 500企業、ITコンサルティング企業、コールセンター、プロフェッショナルサービス、警察、警備会社、政府、リモートビジネス、開発者などのための信頼できるソリューションを構築するための独占的技術を有しています。40万人以上のユーザーがSkrumbleのさまざまな技術とコミュニケーションソリューションを利用しています。 Skrumbleの使命は、コミュニケーションの方法を革新し、人々が可能な限り安全なプラットフォームでグローバルに繋ぐ機会を創造することです。Skrumbleは2017年の春にユニファイドコミュニケーションプラットフォームを立ち上げ、強い市場反響で企業間のコミュニケーションの仕方を変えました。クラウドプラットフォームの機能を利用して、Skrumbleはリッチプロダクトドキュメンテーションを書いて公開し、開発者がコミュニケーション機能をアプリケーションにプログラムするための強力なオープンAPIをリリースしました。グローバルビジネスにさらに利益をもたらすため、Skrumbleは、医療、法律、コンサルティングなどの企業が独自のテレプラットフォームを持てるよう、コミュニケーションソリューションのホワイトラベリングを始めました。また、Skrumbleは最近開発者がチャット、音声、ビデオを任意のウェブサイトやプラットフォームに直接嵌め込むための新しいウィジェットをリリースしました。さらに、チームのスキルセットと技術知識を活用して、独自のブロックチェーンコミュニケーション経験を構築することで、市場の要求を満たす為に取り組みます。Skrumbleチームの人数は過去1年間で倍以上になり、才能豊かなチームメンバー約40人で構成されています。Skrumbleチームは、引き続き世界中の企業が一緒になって成長するためのコミュニケーションの障壁を打ち破り、ソリューションを革新し続けていきます。Skrumble Technologies Incは、Skrumble Networkをサポートするための開発、ブロックチェーンの専門知識、技術ライセンスを提供します。 Skrumble Networkは、分散型のコミュニケーション技術と、ネットワークコミュニティの構築と育成に注力します。一緒に、次世代コミュニケーションネットワークを構築していきましょう。真の自主性とデータ所有権により、信頼を築き、グローバルネットワークの無限なる未来を切り開くことが出来ると我々は信じています。

## 私たちのオフィス

トロントビジネスオフィス

トロント技術運営オフィス

ラテンアメリカ営業オフィス

# 我们的团队

David Lifson
CEO&社長

Tamir Wolfson
執行副社長

Vivi Herlick
運営担当副社長

Eric Lifson
営業担当副社長

Christine Guo
企業開発担当副社長

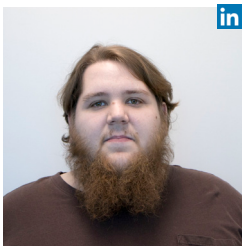
Johnathan Dwek
CFO - CFA

Aleksandra Mihajlovic
プロダクトマネージャー

Michael Dabydeen
フルスタック開発者

Mikhail Khoroshun
フロントエンド開発者

Mikhail Berezovskiy
フルスタック開発者



Daniel Audino
フルスタック開発者

Danyi Lin
フルスタック開発者

Mauricio Bertanha
フルスタック開発者

Matt Mollon
フロントエンド開発者

Leah Williams
フロントエンド開発者

Chantale Barnard
フロントエンド開発者

Eric Eddy
モバイル開発者

Akash Patel
モバイル開発者

Gabriel Hernandez
モバイル開発者

Arnaud Ladoucetter
モバイル開発者

Siv Sathiyaseelan
品質保証アナリスト

Avenson Navalta
UI / UXデサイナー

Shelby Pearce
マーケティング

Wendy Lu
デジタルマーケティング

Wei Chen
ビジネス開発担当者

この免責条項をよくお読みください。取るべき行動について疑問がある場合、ご自身の顧問税理士、公認会計士、弁護士等の専門家にご相談ください。

この文書に記載されている情報は、網羅的ではなく、誓約として解釈されるべきものではありません。予告なく変更または更新される場合があり、専門的なアドバイスを提供するものではありません。Skrumble Network Inc、その子会社および関連会社はこのホワイトペーパーに含まれる資料の正確性、信頼性、または完全性から生じるいかなる法的責任も一切の保証をするものではありません。

SKMトークンは、いかなる管轄区域においても有価証券とみなされる意図を有してはいませんが、特定の管轄区域の規制当局によって有価証券に該当する場合があります。このホワイトペーパーは、勧誘を行うことが違法である管轄区域にてSKMトークン売却の募集・勧誘を意図するものではありません。カナダの居住者および米国の居住者またはグリーンカード保有者は、当地の証券法の適用除外規定以外、SKMトークンの購入対象外とさせていただきます。SKMトークンに関する提案・勧誘は、機密扱いの覚書および該当するすべての有価証券およびその他法律の条項に従ってのみ行われます。

Skrumble Technologies Inc.、その子会社および関連会社は、SKMトークンの購入、販売またはその他の流通に関する意見を提供しておらず、本ホワイトペーパーは、契約の締結又は投資判断の根拠として使われるべきではありません。

# 参考文献


Cendrowski, Scott (April 14, 2017). Fortune Magazine. China's WeChat is a censorship juggernaut. Retrieved on January 26, 2018 from http://fortune.com/2017/04/14/china-wechat-tencent-censorship-709-crackdown/

Coin Market Cap (2018). Cryptocurrency Market Capitalizations. Retrieved on January 21, 2018 from https://coinmarketcap.com/all/views/all/

CyberScout (December 27, 2017). Identity Theft Resource Center. Data Breach Reports. Retrieved on January 24, 2017 from https://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

Facebook (2018). Making ads better and giving your more control. Retrieved on January 26, 2018 from https://www.facebook.com/help/585318558251813?ref=notif&notif_t=oba

Google (2018). How Ads Work. Retrieved on January 26, 2018 from https://privacy.google.com/how-ads-work.html

Greenberg, Andy (January 10, 2018). Wired. WhatsApp security flaws could allow snoops to slide into group chats. Retrieved on January 25, 2018 from https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/

Hollerith, David (November 6, 2017). Bitcoin Magazine. Survey polls American awareness of cryptocurrencies and ICOs. Retrieved on January 20, 2018 from https://bitcoinmagazine.com/articles/survey-polls-american-awareness-cryptocurrencies-and-icos/

Martin, Ellen (October 2017). The Next Web. Why more people will use blockchain-based payment platforms over banks in the future. Retrieved on January 18, 2018 from https://thenextweb.com/contributors/2017/09/07/blockchain-vs-banks/

Pascual, Al, Marchini, Kyle & Miller, Sarah (February 1, 2017). 2017 Identity Fraud: Securing the Connected Life. Retrieved on January 20, 2018 from https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

Perlroth, Nicole & Haag, Matthew (April 29, 2017). The New York Times. Hacker leaks episodes from Netflix show and threatens other networks. Retrieved on January 24, 2018 from https://www.nytimes.com/2017/04/29/business/media/netflix-hack-orange-is-the-new-black.html

Pullen, John Patrick (November 21, 2017). Fortune Magazine. Jennifer Lawrence reveals why she didn't sue Apple over her nude photo leak. Retrieved on January 24, 2017 from http://fortune.com/2017/11/21/jennifer-lawrence-apple-lawsuit-nude-photo-leak/

Sabin, Dyani (January 3, 2018). Futurism. Everything you need to know about cryptocurrency and why it's the future of money. Retrieved on January 17, 2018 from https://futurism.com/cryptocurrency-future-money-bitcoin/

Sethi, Rahul (September 26, 2017). After Google and Facebook, WhatsApp banned in China. Retrieved on January 26, 2018 from https://www.indiatoday.in/technology/news/story/after-google-and-facebook-whatsapp-banned-in-china-1052534-2017-09-26

Toronto Star (January 13, 2018). World News. As protests wane, Iran lifts ban on messaging app Telegram. Retrieved on January 24, 2018 from https://www.thestar.com/news/world/2018/01/13/as-protests-wane-iran-lifts-ban-on-messaging-app-telegram.html

WeChat (2018). WeChat Help Center. Why doesn't my prior chat log appear when I log in to WeChat from a new device? Retrieved on January 26, 2018 from https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?t=help_center/topic_detail&opcode=2&id=1208117b2mai1410242meeYj&lang=en&plat=android&Channel=helpcenter

Yannik (June 26, 2017). Updated January 9, 2018. How long do Ethereum transactions take? Retrieved on February 1, 2018 from https://support.metalpay.com/hc/en-us/articles/115000373814-How-long-do-Ethereum-transactions-take-