

メッセージングの未来

ホワイトペーパー v. 1.5.2 ENG

概要	4
ADAMANTのコンセプト	5
データ保護と匿名性	5
プライバシー保護に関する法的側面	7
ADAMANTのメッセージの保存	7
トークン転送システム	8
長期トークンホルダーに対する利息	8
ADAMANT ビジネス	8
競合サービスの評価とその比較	10
技術的な解決策	11
システムアーキテクチャ	11
ADAMANTトークンの特徴	12
独立したブロックチェーン	12
ADAMANTのトランザクション	13
インフラの維持およびADMトークンの生成(マイニング)	14
セキュリティと信頼性	15
データの保存量	16
プロジェクトのステータス	17
ADAMANTメッセンジャー	17
ブロックチェーンエクスプローラ	20
ADAMANTフルノードパッケージ	20
経済的側面	21
トークン価値の適正化	21
トークンの割り当て	21
将来のプロジェクトのための資金調達(ICOキャンペーン)	22
プロジェクトの予算計画	23
ADAMANT Whitepaper, v. 1.5.2 ENG	p. 2 of 32

AMADANTの成長戦略	24
仮想通貨取引所でのADMトークン取り扱いについて	24
マーケットプロモーション	25
ユーザーウォレットの初期付与額	25
パウンティプログラム	26
プロジェクトのロードマップ(2017-2018)	27
ADAMANTテックラボ	28
ADAMANT公式ページ	32

概要

ブロックチェーン上における支払いシステム及びデータやメッセージの転送は、個 人間および ビジネスの場において大きな利益をもたらしている。

個人向けのADAMANT - あらゆるデバイスから利用可能なブロックチェーンメッセンジャーです。

堅牢な匿名性とデータ保護、使いやすさを併せ持つ支払いシステムです。 ADAMANTネットワークインフラを維持するために、ADMトークンは生成されます。 これは内部アカウントに使用されます。

ADAMANT メッセンジャーは既にhttps://msg. adamant. imで利用可能です ADAMANT ビジネス - デジタル署名する機能、および支払いシステムを備えた、 データおよびメッセージ転送を行う企業向けシステムであり、内部取引における費用を削減することができます。

ADAMANTのコンセプト

データ保護と匿名性

今日、企業の電子デバイスと同様に個人ユーザーが扱う電子デバイスにおいて、 データ転送保護が最も高い優先事項となっています。 日々この事実を認識する人は 増えると同時に、BlackBerry、IBM、Google、Apple、Samsung、Facebookなどの 大企業はデータ保護のために独自のソリューションを提供しています。

最新の暗号化は強力なアルゴリズムを使用しており、少量のデータでさえも完璧に解読するためにはスーパーコンピュータを使用して何年もの作業が必要です。また、メッセージの傍受のようなサイバー攻撃に対しても、「公開鍵と秘密鍵」の概念を使用することによってデータ交換のセキュリティはこれまで以上に堅牢です。

現在、暗号化を使用しない現代のメッセンジャーはおそらくありません。しかし、 全てのユーザーが現在の暗号化を信じているわけではありません。

これは、「安全ではない」暗号化メソッドを使用しているからではなく、それら暗 号化メソッドが含む隠れた

ソースコードユーザーの情報を第三者に提供しているからです。

別の大きな問題は、ユーザーの個人情報のアクセスに関してです。 ほぼすべての メッセンジャーは

デバイスのアドレス帳に直接アクセスし、そのデータを(個人情報と一緒に) 自らのサーバーに送信します。サービスの使いやすさを追求するがあまりに、このような挙動を正当化しており、このやり方は情報漏洩や相互接続時の不要なデータ使用が引き起こします。

これには、

ほとんどのメッセンジャーがユーザの識別が必要であり、そのため電話番号、メールアドレス、メッセンジャーのアカウント、SNSアカウントのリンク、ユーザーのブラウザ活動の追跡などを行い、結果、企業側はプライベート写真、メッセージ、場所の詳細、他の人との関係、ユーザーの好みやその他の個人情報を詳細に把握することになります。

このようなデータ収集は、明らかにプライバシーを侵害していますが、登録時に「ユーザーの同意」や「契約条件」において同意を "強制"することで、これら事実を合法的に"隠蔽"しているのです。そして、ほとんどのユーザーはこれらの契約書を読んでおりません。 これらのデータは収集された後、"企業独自の裁量で"使用されることが多く、最悪の場合、この情報は第三者の手に渡ることもあります。

さらに、これらの中央集権化されたメッセージ転送サービスは、ユーザーし、特定の制限を設けたり、企業側の都合でアカウントを閉鎖することさえあります。 一例として、Telegramでは第三者機関からの苦情への対応として、アカウントがいくつか閉鎖されました。

また、ユーザーのIPアドレス公開(中央サーバーまたは Peer-to-Peerに接続する場合)は最近のメッセンジャーサービスを使用するユーザーが抱える別の問題です。 しかし、TorネットワークまたはADAMANTネットワークのようなブロックチェーンインフラを使用することでこの問題を効果的に解決することができます。

ADAMANTはこのような個人情報に関する信用問題に対応するために作られました。

堅牢であるブロックチェーンを基に開発され、かつそのプログラムコードは一般に 公開されています。つまり、 誰もがコードの確認を行うことができ、さらにより良 いシステムを自ら構築することもできます。

Blockchain技術のもう一つの非常に素晴らしい利点は匿名性にあります。中央集権で運営されている他のメッセージ転送システムとは異なりシステムで必要な信用証明書がないため、メッセージ履歴と特定の人物とを関連付けることはできません。ユーザーは、携帯電話番号、電子メール、ソーシャルアカウント、または支払明細などを入力する必要はありません。

ADAMANTには、次のような特有のセキュリティと匿名機能があります。

- ●すべてのメッセージはブロックチェーンに直接格納されます。
- ●ユーザーのアドレス帳にアクセスすることはできません。
- ●ユーザーの位置情報にアクセスすることはできません。
- ●ユーザー識別情報はなく、完全な匿名性を実現しています。
- ●すべてのメッセージは送信者のデバイスで完全に暗号化され、受信側で解読されます。 誰も (開発者を含む) あなたのメッセージにアクセスできません。併せてメッセージ転送方式もご確認ください。
- ●クライアントアプリは、ユーザーの秘密鍵またはニーモニックフレーズ(パスワード)をいかなる状況においても転送致しません。全ての動作はユーザーデバイスのローカルで行われます。
- ●したがって、ユーザの個人情報は転送されません。
- ●メッセージの履歴はデバイスに保存されることはなく、ブロックチェーン上で直接 読み込まれます。
- ●P2Pメッセンジャーとは異なり、ユーザーのIPアドレスを取得することは不可能です。
- ●ADAMANT メッセンジャーとブロックチェーンのプログラムコードは公開されています。
- ●開発者であってもADAMANTアカウントを閉鎖、ブロック、あるいは制限すること はできません。

プライバシー保護に関する法的側面

ほとんど国において、私生活とそれに関するプライバシーは憲法レベルで保護されています。

例えば、ロシア連邦憲法第23条の抜粋:

1.誰も私生活、個人および家族の秘密が侵害されることなく、その人の名誉と評判が守られる権利を有している。

2.電話の会話、メール、電信、その他の種類のメッセージを含むプライバシーが守られる権利があります。この権利に対する制限は裁判所が決定した場合にのみ許可されます。

もう1つ、イタリア憲法第15条から:

"通信およびその他のすべての形態のコミュニケーションの自由と秘密は侵すことができない。前項に対する制限は、法律で定められた司法当局の理由を付した令状によってだけ行うことができる。"

しかし、政府はしばしばこれらの原則を違反するため、国民は自らの権利を守る新たな方法を見つける必要があります。

ADAMANTはあなたのプライバシーを守るために作られたのです。

ADAMANTのメッセージの保存

すべてのADAMANTメッセージはブロックチェーンに分散され、保存されます。

これにより、

- ●メッセージ履歴の保存容量の確保と高い信頼性。
- ●古いメッセージを遡って変更することができない。
- ●メッセージ送信者とその受信者、そして中間者攻撃に対する認証された信頼性 (この種の攻撃を検出し、送信者識別者を変更する)。
- ●中央集権的ストレージのようにあらゆるデバイスからユーザーメッセージへアクセスが可能。
- ●信頼性の高いブロックチェーンによるメッセージ配信。
- ●次の暗号化方式によって提供される高いセキュリティ: Ed25519 EdDSA、Curve25519、Salsa20、およびPoly1305。

誰もが暗号化されたメッセージにアクセスできるにもかかわらず、最新の暗号化方式では、特定のメッセージの解読は送信者と受信者だけが可能です。ブロックチェーンに基づいたビットコインがこの信頼性を証明しています。ウォレットの残高は公で保存されているにも関わらず、暗号鍵が壊され、ウォレットにアクセスされるような事件は起こりませんでした。

トークン転送システム

現代の世界では、便利で信頼できる転送システムが求められています。特に、自国 通貨がハイパーインフレに陥った地域、あるいは従来の支払い手段が様々な理由で 制限されている地域ではこの問題は深刻です。 ビットコインとブロックチェーンの技術は、すでにこれらの問題を解決する力があることを示してきました。今日では、一般公開される仮想通貨の数が年々増え続けています。 しかし、それらには長所と短所があります。

ADAMANTシステムには、独自のアカウンティングユニットであるADMトークンがあり、これは

- ●メッセージ転送費用、直接転送、あるいはその他ネットワークインフラ全体を維持するために使用されます。
- ●非常に優れたトランザクション速度(5秒のブロック時間)で動作します。
- ●チャット画面からの直接トークン転送するため利便性が高く、使い方も簡単です。
- ●他のサービスやブロックチェーンとは完全に独立しています(ADAMANTは 自給自足型システムで構築されています)。

ADMはADAMANTインフラ内におけるトークンです。これは内部トランザクションシステムや全体のネットワーク稼働の維持に使われます。

長期トークンホルダーに対する利息

資金調達時(プレICOおよびICO)で販売しなかったADMトークンは、既存の所有者(保有者)間で比例配分されます。 これにより、利子(最初の1年か2年)を得るため多くのトークン保有者が長期保有し、売り出し初期現れる投機ムードを鎮静化することができると考えています。

配布プロセスの詳細な計画は、「経済的側面」パートに記載されています。ホワイトペーパーの「ADAMANTの今後の成長」をご確認ください。

ADAMANTビジネス

ADAMANTにはメッセージやファイル転送などの一般的な機能に加えて、移転文書にデジタル署名し、ユーザが条件を確認できるようにする機能があります。

ADAMANTは、機能性に優れた転送システムも備えており、チャット画面内から直接、関連する条件文書(必要な場合)またはファイルとともに、トークンを送ることができます。それら支払いに関連する様々な契約を「上書き」することもできます。そして、そのすべてのデータがブロックチェーン上に保存され、それ以後変更することはできません。

即時支払いも可能です。全てのデータがブロックチェーン上に半永久的に保存されるため、以降偽造される心配はありません。

一方、企業は通常のADAMANTブロックチェーンではなく、パートナー企業と社内 システムで完結するサービスが求められることもあります。この機能は、 ADAMANT ビジネスソリューションによって提供することができます。 多くの地域に跨っている企業がブロックチェーンを使用することにより、内部取引の手数料を劇的に減らすことができます。 特に、年に複数回限られた企業間において多額の送金があり、かつ法定通貨に換金する必要がない場合、大きなメリットがあります。

この場合、ほとんどの会計は会社内で (トークンを使用して) 完結し、資産は必要なときにのみ法定通貨に換金すれば良いのです。

さらに企業にとってブロックチェーンを使用する利点は、社員に対する報酬や貢献の程度、またはボーナス、その他様々な用途として活用することができることです。

ADAMANTプラットフォームは、簡単かつ効率的なビジネスツールになります。

競合サービスの評価とその比較

メッセンジャーは現在最も人気があり便利なコミュニケーション手段です。 様々なメッセンジャーが使用されており、PC あるいはスマートフォンの利用者のほぼ 100%に近い人々が少なくとも1つのメッセンジャーをインストールしています。しかし、中央集権化されたサーバー(またはグループ)から独立し、セキュリティ指向が高くかつ匿名であるメッセンジャーの割合は明らかに低いです。

ADAMANTの主な機能はセキュリティと匿名性であるため、その点を考慮しいくつかの類似サービスと比較してみたいと思います(このため、Kik Messenger、Skype、Googleハングアウトなどのメッセンジャーは比較していません)。

セキュリティ、匿名性、ユーザビリティは、それぞれが矛盾することが多いという点で、今回の比較では利点としてセキュリティと匿名性のみ評価します。例えば、メッセンジャーが既読通知を行っている場合、この挙動は使いやすさの代わりに匿名性を損なってしまいます。

私たちはまた、機能的なプロトタイプがないサービスは比較から除外しました: Echo、Status、Crypviserなどです。 また、メッセンジャーの動作環境がデスクトップのみ(スマートフォンでは動作しません)のものも除外しております: RetroShare、Tox、Bitmessage、Ricochet。

	ADAMANT	WhatsApp	Telegram	Facebook Messenger	Connect.im	Signal	Dust	Ring
Open Source Code for server, application and protocol parts	Yes	No	Closed Source Code for server part and Open Source for protocol and client apps	No	Closed Source Code for server part and Open Source for protocol and client apps	Yes	No	Yes
No centralised storage for any part of the User Data	All User Data is stored in the Blockchain (decentralised)	Operator stores Data of all conversations — including images, video and files	Operator stores all Data, except the one from the "Encrypted" chats	Operator stores data of all conversations — including images, video and files	Peer-to-peer, but there are intermediate servers which store undelivered messages	Operator is able to log all Data on servers	All Data is Stored and Viewed by the operator	Peer-to-peer, but there are intermediat servers which store undelivered message
Developers / Provider is NOT able to block user account	Yes	is Able / Blocking	is Able / Blocking	is Able / Blocking	Is Able	is Able	is Able / Blocking	is Able
o explicit user identification	Yes	Mobile number is used for authorization	Mobile number is used for authorization	Mobile number of Facebook account is used for authorization	Mobile number is used for authorization	Mobile number is used for authorization	Mobile number of Facebook account is used for authorization	User account creation in the Ring Network
End-to-end encryption with inability for developers to read user messages)	Yes	There is a potential ability for operator to read all messages	There is a potential ability for operator to read all messages	There is a potential ability for operator to read all messages	Yes	Yes	There is a potential ability for operator to read all messages	Yes
No access to address book	Yes	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Asks user for access
No access to user location	Yes	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Yes	Asks user for access	Yes
Does NOT transfer user Private Keys over the network	Yes	Source Code is closed for Review	Source Code is closed for Review	Source Code is closed for Review	Stored encrypted on operator's servers	Yes	Source Code is closed for Review	Yes
Does NOT store message history or any other usage information on the user device	Yes	is Storing	is Storing	is Storing	is Storing	is Storing	Is able to delete messages from both end-users' devices.	is Storing
Does NOT disclosure or expose user IP-address	Yes	Exposed to Operator	Exposed to Operator	Exposed to Operator	Exposed to Operator	Exposed to Operator	Exposed to Operator	Directly interacts wit Ring Network
Not able to get statuses like «Message Read» or «User Online»	Yes	Enabled by default	You can hide only the "Last Seen" Status	You can only switch the "Active" Status	Yes	Asks for user Permission	Forced «Message Read" notifications. No Status for user Availability	Yes

比較表は、次のリンクから参照できます。

https://adamant.im/docs/en-adamant-messenger-comparison-table-plain.png

したがって、ADAMANTは機密性とセキュリティの問題を解決するために作られています。

技術的な解決策

システムアーキテクチャ

ADAMANTはDelegated Proof-of Stakeコンセンサス(DPoS)アルゴリズムを基にした、完全に分散されたシステムです。これは、以下の基準を満たすために採用されました。

- ●DPoSにより、5秒間隔で確実に取引を確認することができます。 この間隔は、速いメッセージ送信と支払いの実行には不可欠です。
- ●DPoSにより、システムメンテナンスコストが大幅に削減されます。コンピュータの稼働が以前ほど必要ではなく、それゆえPOWと比較して電気の無駄もありません。
- 取引手数料を固定化できます。
- ●システムのスケーラビリティと信頼性を確保できます。

ADAMANTシステムは、2つのタイプのノードで構成されています。

- 1.ブロックチェーンデータベース全体を含み、新しいブロック生成に参加することができるフルノード:
- 2.ブロックチェーンに転送する前にデータ暗号化を実行するライトユーザー向け ノード。

しかし、すべてのブロックチェーン操作は、フルノードによって実行されます。そのため、ライトユーザーは、すべてのデータをJSON形式で転送する特定のAPIを用い、HTTPSプロトコル(エンド toエンドで暗号化を行う)を介して相互接続する必要があります。

フルノードは、以下の基準を満たしたものです。

- ●OS Linux Server(Ubuntu)。 Dockerアプリケーションパッケージを使用し、他のプラットフォームへのインストールも可能です。
- ●Node.JSアプリケーションサーバー。
- ●ブロックチェーンを格納するPostgreSQLサーバ。

ライトユーザーは、以下の技術を利用します。

- ●Progressive Web App (PWA) 最新のブラウザ用Webアプリケーション。
- ●HTML5、JS、CSS、Vue Web用のプログラム言語とフレームワーク。
- ●特別なAPIプロトコルによってフルノードを活用する。 すべてのネットワークノードは、HTTPSプロトコルを使用してPeer-to-Peer方式を 使用し相互接続します。

ADAMANTトークンの特徴

- ●トークン名: ADAMANT (ADM)
- ●DPoSアルゴリズム (Deleted Proof of Stake)
- ●最大トークン量: 200,000 000 ADM
- ●genesisブロック: 98,000 000 ADM
- ●ブロック時間:5秒(17 280ブロック/日、約6,307,200ブロック/年)
- ●ブロックサイズ:変動(制限なし)
- ●ブロックごとの報酬:
- ○初年度: ブロックあたり0.5 ADM
- ○別の年:毎年0.01 ADMが減少し、1ブロックにつき0.1 ADMまで減少
- ○報酬はブロック番号2,000,000から始まります(約3ヶ月後)
- ●トランザクションごとの報酬(トランザクションコスト):
- ○直接トークンを転送: 0.5 ADM
- ○メッセージ転送: UTF-8で256文字ごとに0.001ADM。

メッセージ転送コミッションはADMトークンの市場価格上昇に応じ、動的に変動する。

- ○ユーザープロフィール情報の更新: 0.05 ADM
- ○アバターアップロード128x128 px: 0.1 ADM
- ○画像転送(ブロックチェーンに保存せず): 100 KBごとに0.05 ADM
- ○ドキュメント転送(ブロックチェーンに保存): 1 KBごとに10 ADM
- ○文書への電子署名: 100 ADM
- ○デリゲート登録: 3000 ADM
- ○デリゲート投票: 50 ADM
- ●新しく作成されたウォレットの初期トークン額:
- ○ブロック6 300 000 (おそらく最初の年まで) まで0.49 ADM 490メッセージの無料送信に相当
- ○次の125 000ブロックごとに、トークン額は0.01 ADM(最低1年間)の最低値に達するまで0.01 ADMずつ減少。
- ●プログラムコード:オープンソース(GNU GPLv3)
- ●デフォルトのシステムポート: MainNetでは36666、TestNetでは36667になります。

独立したブロックチェーン

残念ながら、EthereumブロックチェーンはADAMANTネットワークを維持するには 最適ではありません これは、比較的高い「ガス」(トランザクション費用)が原因 で、これはEthereumトランザクション上における全てのメッセージ転送に適用され ます。これがADAMANTが独立したブロックチェーン上に構築されている理由であ り、取引コストはネットワーク全体を運営しても安価であり、将来のトークン価格 上昇に柔軟に適応することもできます。

また、Proof if Workは技術的にも適応しません。なぜなら、保守費用が高く、また参加者が増加すると取引手数料が高騰してしまうためです。

これらの理由を考慮し、Liskプロジェクトのプログラムコードをサーバーとブロックチェーンに実装しました。このソースコードは、必要な機能を実装するために使われています。

ADAMANTの構造は、必要に応じて取引手数料を変更できるよう柔軟になっています。

ADAMANTのトランザクション

各ブロックには、さまざまな量のトランザクションが含まれています。 それが承認されるためには、

6~10ブロックの承認が必要です。 しかし、それはトークン取引とドキュメント転送にとってのみ重要であり、メッセージに関しては1度承認されると送信できます。 ここでは、私たちのネットワークのトランザクションタイプの一覧にしました:

- 1.直接トークンの転送
- 2.メッセージ転送
- 3.プロフィールの更新:連絡先やユーザーの設定をブロックチェーンに直接保存する
- 4.プロフィール写真のアップロード
- 5.グループチャットの作成
- 6.特定のチャットを閉じる(チャット履歴を隠す)
- 7.ドキュメント転送(ブロックチェーンに保存)
- 8.文書への署名
- 9.デリゲート登録
- 10.デリゲート投票。

すべての取引実行には支払い(手数料)が必要です。それらの支払いはネットワークのメンテナンスコストとして代表達の間で共有されます。

インフラの維持およびADMトークンの生成(マイニング)

ADAMANTのインフラは、フルノード(ブロックチェーン)による分散型サーバシステムによって処理されます

。 すべてのサーバーのサポート費用は、ADMトークン生成によって賄われます。 1.取引手数料

2.ブロック生成に対する報酬

生成プロセスに参加するには、ノードをネットワークデリゲートとして登録し、ADAMANTユーザーから票を獲得する必要があります。 デリゲート登録料は300ADMです。 別のデリゲートに投票するには、10 ADMを支払う必要があります。

DPoS方式のアルゴリズムは、リアルタイム(ネットワークメンバーの評価を使用して)で進行する投票プロセスに基づき、信頼できるノード(代理人)のリストを作成します。 選出された後、デリゲートはそれらをブロックチェーンに追加し、不正な侵入を防ぐブロックを生成し検証する権利が与えられます。これらのノードは、次々とブロックを生成(作成)します。

デリゲートは、新しいブロックを生成するときにADMトークンを生成(取得または 獲得)します。

このようにして生成されるトークンの量は徐々に増加していきます。初期段階では1ブロックにつき0.1ADM、その後6,307,200ブロック(約1年)ごとに0.01ADMずつ増加していきます。このブロック生成に対する報酬の増加はネットワーク維持・管理を行うデリゲートのモチベーション向上に繋がります。

計算に関して、デリゲートは約46年に渡りの報酬を得ることができます。その後、インフラは取引手数料によって完全に維持されていきます。

ブロック生成に参加するアクティブなデリゲートの数は101つです。それよりも低い場合は、これらの101票は既存のフルノードメンバーに配分されます。ノードの最少数は3つです。ノードの量が増加すると、システム全体はより安定し、信頼性も向上します。

DPoSを使用して新しいブロックを作成(または生成)するには、進行中の101ブロックを作成するために、デリゲートプールから101のデリゲートメンバーを選出する選挙が行われます。

投票はノード(すべてのウォレット所有者)によって、信用度とオンラインの稼働時間に基づき、自動的に実行されます。すべてのデリゲートが選ばれた後、新しいブロックの生成順序が与えられ、101ブロックの列が作成されます。これにはおよそ8分かかります。

しかし、ブロックの生成に対する支払いは、2,000,000のブロックが作成完了した後から始まります。これは、最初のネットワーク参加者は最小限の労力でトークンを取得することはできないことを意味しています。

そして、これは新しいユーザーの関心を常に引きつけ、かつブロックチェーン上の すべてのユーザーを平等な権利を与えることができる。 新しいブロックの情報は5秒間隔で送信されます。 新しいブロックは、全ネットワーク内に素早く行き届けるために送信元ノードから1回送信され、各受信者から2回送信されます。

新たに生成されたブロック内に配置されなかったトランザクションはトランザクション列に並べられる。 この列には、1080ものブロックと最大5000個のトランザクションを含めることができます。

もし特定のトランザクションがブロックに追加されていない場合、 承認(または)許可がされていないとみなされ、ブロックチェーン上に受け入れられず待機リストから削除されます(ウォレットの状態は変更されません)。

ブロックチェーンの状態の一貫性と関連性を判断するために、ブロードハッシュが 用いられます。これは、ブロックチェーン上の最新の5つのトランザクションをシス テム計算させるチェックサムです。このチェックサムは、すべてのフルノードが特 定の瞬間のブロックチェーンデータベースにおける状態が同一であることを素早く 再確認するために使用されます。

すべての取引手数料の回収は、ブロック生成プロセスに参加したデリゲート間において、101ブロックごとに均等に分配されます。

セキュリティと信頼性

ADAMANTはブロックチェーンに基づいた信頼性の高いシステムであり、以下のコンセプトを基に実装されています。

- ●配布。 ブロックチェーンは、データ保存が可能な不変の分散データベースであり、
- ここではいかなる変更を加えることもできません。 そのため、オープンで安全で信頼性の高いデータストレージとして使用できます。
- ●DPoS技術によって、PoW方式と比較してコンテンツ制作者がブロックチェーンを 今まで以上に管理することができるようになりました。 PoWの場合、強力な処理ユニットと相互接続することによってネットワークを制御します。
- ●Broadhashコンセンサスアルゴリズムにより、最も長いフォークを選択することに よって、その部分との一時的な非同期化がネットワーク全体で可能となります。
- ●ウォレット作成時にBIP39 mnemocodeが生成されます。それはユーザーの秘密鍵をローカルで生成する際に使用されます。 そして、この秘密鍵を使用し、ウォレットアドレスを作成する公開鍵を生成します。 ユーザーはこれら作業が完了した後、システムを使用することができます。 作成可能なウォレットアドレスの数は限りなく無限に違いです。

- ●すべての発信トランザクションは、秘密鍵を使用して署名される、堅牢な暗号アルゴリズムです- Ed25519 EdDSA:
- •すべてのメッセージは、ソース側機器 (Curve25519、Salsa20、иPoly1305) で暗号化され、受信側機器でのみ復号化されます。
- ●クライアントアプリは、ネットワークを通じてパスフレーズまたは秘密鍵を転送することはありません。 すべての暗号化は、ユーザーデバイスにおいて置き換えられます。
- ●対話者のIPアドレス(最も一般的なP2Pメッセンジャーとは異なる)を明らかにすることはありません。

データの保存量

現時点では、ADAMANTノード内に保存されるデータの量を見積もることは困難です。しかし、いくつか考えられる状況を想定することはできます。

1日の推定メッセージ量は初年度でおよそ10,000件のメッセージで、毎年10万人程度増加する見込みです。

1つのメッセージに平均100文字が含まれていると仮定すると、このメッセージのデータ量を安全にブロックチェーンに保存するために必要な数は、100文字×2バイト×暗号化の増加係数1.5で合計サイズ約300バイトとなります。

このようにして、これらのメッセージを初年度に保存するのに必要なスペースは 10,000メッセージ \times 365日 \times 300 = 1 GBであり、毎年10 GB程度増加する見込みです。ADAMANTブロックチェーンは、最初の10年間で50 GB程度成長する可能性があります。

メッセージ送信に対してデリゲートが受け取る手数料は、初年度、 10,000×365×0.005 ADM = 18,250ADMから開始され、翌年から徐々に182,500まで 上昇します。

デリゲートがブロック生成に対しても報酬を受け取ることを考慮すると、ADMトークンの市場価格上昇と安価なデータ保管コストはADAMANTインフラが効果的にサポートされ、デリゲートは常に利益を上げることにつながります。

プロジェクトのステータス

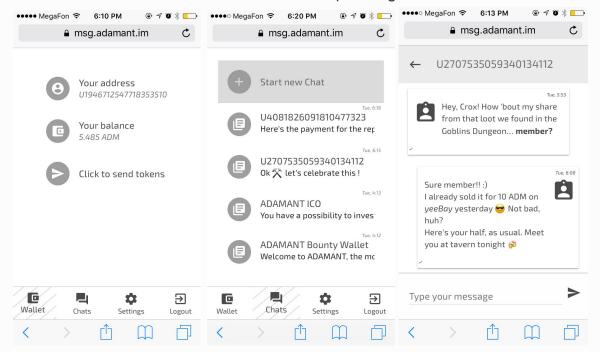
ICOまでに、ADAMANTシステムは、次の機能を実装します。

- ●メッセージ転送(ADAMANT メッセンジャー)。
- ●トークンの保存と転送。
- ・現在のブロックチェーン状態に関する情報調査。

●拡張性の高いフルノードインフラ。

ADAMANTメッセンジャー

ADAMANT メッセンジャーは、次のリンクhttps://msg.adamant.imで使用できます。



ADAMANT メッセンジャーはProgressive Web App (PWA) として実装され、モバイルおよびデスクトップ上で現在の主要なブラウザで動作します。AndroidおよびiOSプラットフォーム用のアプリ開発も現在行われています。

ADAMANT Messengerのシステム要件:

- ●モバイル機器:
- ○Apple iOS 9モバイルオペレーティングシステム以上
- 。Google Android 5.0以降/Chromeブラウザ(バージョン62以降)
- ●PCの場合:
- ○主要ウェブブラウザ全て

ADAMANT メッセンジャーには、ADMトークン(ウォレットアプリ)を保存して送信する機能があります。

ADAMANTメッセンジャーの最新機能:

- 暗号化されたメッセージの転送。
- 会話とチャット履歴のリスト。
- トランザクションリスト。
- すべての支払い取引に関する詳細情報。
- 新しいメッセージ通知。
- 相手方の住所、名前(またはニックネーム)の設定。

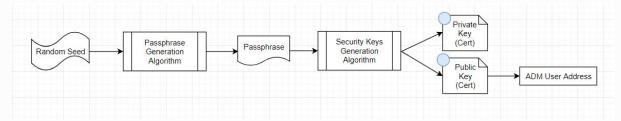
- 絵文字のサポート。
- ▼ークダウンのサポート。

ADAMANT メッセンジャーの実装予定機能:

- (この文書の「ロードマップ」のセクションも確認してください)
- アドレス帳。
- ブロックチェーンに格納されたプロフィールと設定。
- チャット画面内でトークン転送。
- チャット画面内のトークン転送通知。
- 画像転送。
- ブロックチェーンに保存されたドキュメント転送。
- ・ ドキュメントのデジタル署名(承認)。
- チャットやメッセージのお気に入り。
- 連絡先やメッセージの検索。
 - ピンコードを使用し簡易的に行えるログイン。
 - チャットを見えないようにする(クロージャー)。
 - グループチャット。

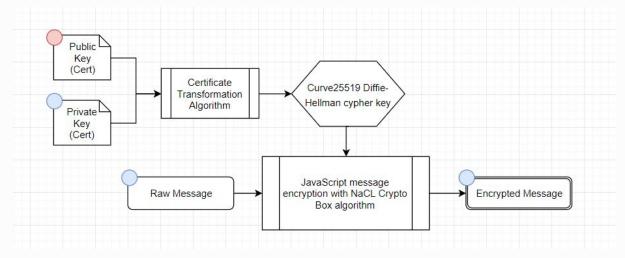
ADAMANT メッセンジャーの利点、特長など詳細についてはこの文書の「ADAMANTのコンセプト」を参照ください。

ADAMANT メッセンジャーのアカウント作成の手順 - ユーザーのデバイス上:



- 1.ランダムシードを生成します
- 2.システムは、このシード値に基づいてユニークなパスフレーズを生成します
- 3.パスフレーズは、公開鍵と秘密鍵を生成するために使用されます
- 4.ユーザーのADMウォレットアドレスが公開鍵から生成されます

ADAMANTメッセンジャーの動作手順 - ユーザーのデバイス上:



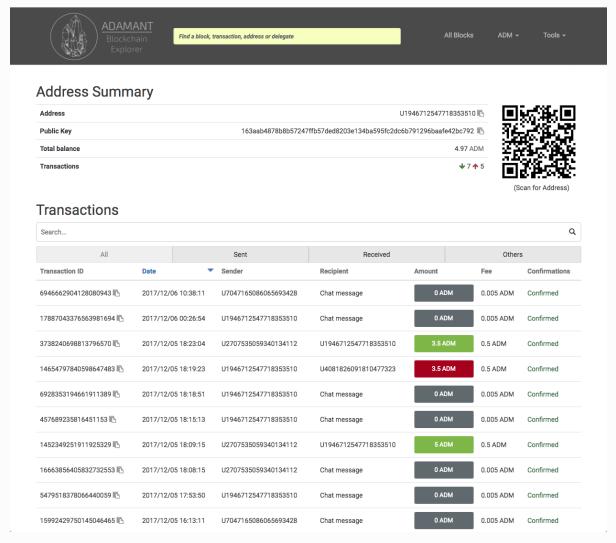
- 1.メッセージは、ユーザーのデバイス上でローカルに暗号化されます(Curve25519、Salsa20、およびPolv1305 cipher アルゴリズム)
- 2.暗号化されたメッセージは、ランダムに選択されたノードを介してブロックチェーンに転送されます

すべてのメッセージはブロックチェーンに送られる前にユーザーのデバイスで暗号化され、メッセージサイズを正確に把握することはできません(メッセージ中に含まれる文字数)。 したがって、転送にかかる手数料は255 UTF-8文字数につき約0.001ADMと計算されます。 メッセージ転送料はADMトークンの実際の市場価格に応じて調整されることもあります。

ADAMANT メッセンジャーは誰でも利用可能です。サービスリリース最初の2年間は新規アカウントに対して少量のADMトークンを付与することでメッセンジャーサービスを多くの方に利用してもらう予定です。

ブロックチェーンエクスプローラ

ブロックチェーンエクスプローラには、ADAMANTブロックチェーンのステータス、ブロックリスト、ネットワークトランザクション、およびそれらに関するすべての情報が含まれています。 また、アクティビティグラフ、デリゲートとネットワークに関する情報も含まれます。



ブロックチェーンエクスプローラはhttps://explorer.adamant.imで利用できます。

ADAMANTフルノードパッケージ

ADAMANTのインフラサポートを行いたい場合、ブロックチェーンノードを実装し、デリゲートメンバーとして登録を行う必要があります。登録完了後、新しいブロックの生成とネットワークトランザクション実行に対する料金受け取りを行うことができるようになります。(注:ユーザーから投票を受け、デリゲート登録を行うために300 ADMを支払う必要があります)。

設定方法についての詳細は、https://adamant.im/devs/をご覧ください。

経済的側面

トークン価値の適正化

ADMはメッセージとデータ転送の料金よって価値が保証されているトークンです。 この支払いは、インフラコストを匿名で安全なデータ伝送に対する需要によって定め、費用を全て賄えるように設計されています。

ADAMANTビジネスサービスには、デジタル文書の署名(承認)機能も含まれています。

また、ICOキャンペーンに割り当てられたが販売されなかった残りのトークンの流通プロセスを通じて発生する付加的なADM価値もあります。

このプロセスを「ADAMANT Grows」と名付け、ICOが終了した後、その翌年から ウォレット残高にあるADMトークンの割合に応じて毎月報酬を与える予定です。 ADMは内部システムにおける使用用途のみに使われるトークンであり、投機やその 他利益を手に入れるために使われることはありません。

トークンの割り当て

ADMANTのメインネット発足当初、9800万ものADMウォレットが作成されました。

初期割り当て分布:

- ●75% (73,500,000 ADM) ICOキャンペーン
- ●4% (3,920,000 ADM) システム開発とインフラ整備のための準備金
- ●4% (3,920,000 ADM) ADAMANTビジネスサービスのマーケティング準備金
- ●9% (8,820,000 ADM) 初期投資家とファウンダーの報酬
- ●8% (7.840,000 ADM) バウンティキャンペーンと初期ユーザーに対する報酬

トークンの最大量(制限付き)は2億ADMです。

したがって、1億200万ものADMトークン(+トランザクション費)がインフラサポートとネットワーク機能の維持に対する報酬としてデリゲートメンバーに支払われます。

ブロック生成報酬についての詳細はホワイトペーパーの"インフラの維持およびADMトークンの生成(マイニング)"部分を参照ください。

将来のプロジェクトのための資金調達(ICOキャンペーン)

プレICOおよびICOキャンペーンを通じて、genesisブロックからADMトークンを販売することは、さらなる開発プロセスに必要な資金を集め、ADAMANTシステム全体に成長をもたらすことを目的に計画されました。

ICO時に配布するトークン量は73,500,000 ADMに過ぎません。

ADMはADAMANTインフラ、トランザクションシステムの機能を維持するために作られたトークンです。ADMトークンを入手することはどの国の方でも可能であり、 違法性はありません。

販売されなかったトークンは、"ADAMANTの成長戦略"でも言及しましたが、口座残高に応じてユーザーに割り当てられます。

プレICOは 2017年12月14日から2018年1月25日の期間で実施されました。 ICOによる資金調達については2018年1月30日から2018年6月30日の期間で実施します。

- ●参加方法: https://adamant.im/ico/から自動交換システムを通じて購入できます。
- ●ADMトークンの受け取り方:支払い処理が確認された後、パートナーのウォレットに自動転送されます。
- ●受け入れ可能な仮想通貨: ETH、BTC、BCH、DASH、DOGE、LTC、XMR、ETC、ZEC、LSK
- ●トークン価格: 1ADM につき0.0002 ETHから0.0004 ETH。他仮想通貨に対するADMトークンの正確な価格は、購入日の実際のETH価格に基づいて計算されます。
- ●最小参加可能額:下限なし
- ●ICO運用フェーズ:
 - ○第1期:
 - ■2018年1月30日から2018年2月14日
 - ■トークン価格: 1 ADM = 0.0002 ETH
 - ○第2期:
 - ■2018年2月15日から2018年2月28日
 - ■トークン価格: 1 ADM = 0.0003 ETH
 - ○第3期:
 - ■2018年3月1日から2018年6月30日
 - ■トークン価格: 1 ADM = 0.0004 ETH
- ●参加報酬(全フェーズで同じ):
 - ○20~30 ETH: ADM購入量から+20%
 - ○30~50 ETH: ADM購入量から+30%
 - ○50~90 ETH: ADM購入量から+ 40%
 - ○90以上ETH: ADM購入量から+ 50%

プロジェクトの予算計画

ICOで調達された資金はすべて、ADAMANTの開発、サポートなどに使われます。

ソフトキャップ - \$ 500,000 ハードキャップ - \$ 8,000,000

ソフトキャップは、メッセンジャーの主要機能の開発ととインフラ全体のサポートのために必要なリソースに割り当てられます。より多くの資金を調達できれば、その分開発速度を上げ、ADAMANTのアクティブユーザー増加に向け力を傾けることができます。

調達した資金の今後2年間の予算計画:

- ●インフラサポート 10%
 - oサーバー
 - ○スタッフ給与
- ●開発 30%
 - ○スタッフ給与
 - ○オフィススペースの賃貸と維持
 - ○技術機器とそのサポート
 - ○仮想交換取引所(市場)の上場費用
 - ○コンサルタント費用
- ●外部セキュリティおよびコードオーディション(レビュー) 10%
- ●ユーザーとのコミュニケーション 50%
 - ○オフラインプロモーションキャンペーンやカンファレンスへの参加
 - ○スタッフ給与
 - ○コンテクスト広告
 - ○仮想通貨の広告
 - ○関連テーマに関する記事や投稿の作成と公開

AMADANTの成長戦略

ADMトークンの価値を高めるため、ICO用に準備されたが販売されなかったトークンはADM所有者間に分配され、ICO後1年間、ADM所有者のウォレット残高が毎月5%ずつ増加する予定です。

ADMトークンはネットワークインフラを維持するために使用され、ADAMANTの成長はシステム維持を伴うものであり、利益のみを追求していくものではありません。

この分配はICO用トークンがなくなるまで続きます。

したがって、早期にADAMANTをサポートすることでトークンの所有期間が長くなり、結果毎月増加するボーナスを手に入れる期間も長くなります。

●配信開始:2018年4月11日

●配布時期:毎月 ●成長率:5%

●配布終了時期:ICO用トークンがなくなるまで。

以下のウォレットはトークン配布キャンペーンには参加できません。

1.初期のシステムウォレット(ICO、投資家の報酬、予備ウォレットなど)。 2.ウォレット残高が10 ADMトークン未満の財布。

各配布時期の詳細情報は公開されており(公式サイトでも公開されます)、グローストランザクションはADAMANTエクスプローラーで確認することができます。

仮想通貨取引所でのADMトークン取り扱いについて

ICOキャンペーン終了後、ADAMANTトークン(ADM)は以下の仮想通貨取引所において無料で取引されます: Livecoin, Yobit, Liqui, Bittrex。

マーケットプロモーション

現在のメッセンジャーサービスは便利なコミュニケーション手段となりました。日常生活でメッセンジャーを使用する人々の割合は常に増え続け、すぐに100%に達するでしょう。

ADAMANT メッセンジャーは、メッセージの高いセキュリティ性や便利なトークン 転送手段を求めているユーザーをターゲットにしています。

ユーザー数の急激な増加は、近年リリースされたメッセージサービスの主な特徴の1つです。

新規ユーザー数は初期段階では緩やかに増加していきますが、しばらくすると、アクティブユーザーが友人や親戚を招待し始め、ユーザーの数は指数関数的に増加し始めます。

ADAMANTプロジェクトでは、アクティブユーザーベースの成長戦略に関して以下 の施策を行います。

- ●仮想通貨コミュニティに属する人々を惹きつけるICOキャンペーン。
- ・バウンティキャンペーン。
- リーシャルネットワーク広告キャンペーン。
- ●広告キャンペーンとコマーシャル(オンラインとオフライン)。
- カンファレンスへの出席。
- ●新規ユーザーウォレットへのトークン付与。
- ●企業向けADAMANTビジネスサービス。

ユーザーウォレットの初期付与額

ブロックチェーン内のトランザクションは、一定の手数料が必要となります。これは、ネットワークインフラを維持するために必要な費用です。

そこで、多くのユーザーにADAMANTの機能を試してもらうため、ウォレット作成 プロセス時に少額のトークンを付与致します:

- ●ブロック番号6,300,000まで0.49 ADMを付与します (これを達成するまで1年程度 かかります)
- メッセージ490通分
- ●その後、この付与額が0.01 ADMまで達するまで、125,000ブロックごとに0.01 ADM(推定ではさらに1年)ずつ減額されます

システムの直接振込手数料が0.5ADMであるため、初期残高をかき集め搾取することは不可能です。この付与は、新しいウォレットを作成し最初の数分以内にウォレット配布用トークン(7.840.000 ADM)から

配布されます。したがって、この方法でシステムをテストできるユーザ数は約700 から1400万です。

バウンティプログラム

バウンティキャンペーンでは、ユーザーがADAMANTプロモーションに貢献すると 報酬としてADMトークンを受け取れます。

このキャンペーンは2017年12月14日から2018年6月30日の間に開催され、

- ●Bitcointalk.org上の活動。
- ●ソーシャルネットワーク上での活動。
- ウェブサイトやドキュメントの翻訳。
- ●Bitcointalk.orgとBounty Bitcointalkなどの主要スレッドの翻訳とサポート。
- ●ADAMANT メッセンジャーアプリの翻訳。
- ホワイトペーパーの翻訳。
- ●ブログやウェブサイトの記事のプロモーション。
- ウェブサイト上のバナーのホスティング。

バウンティキャンペーンに関する追加情報は、以下URLで確認できます。 https://adamant.im/bounty/

プロジェクトのロードマップ(2017-2018)

✓ 2017年第2四半期

- ✓ ADAMANTのコンセプト設計
- ✓専門家との打ち合わせ
- ✓ ADAMANTテストネットの運用

✓ 2017年第3四半期

✓ Progressive Web Appの開発(ADAMANT ウォレットとメッセンジャー) ✓ホワイトペーパーの作成

2017年第4四半期

- ✓ ウェブサイトの開発
- ✓ ADAMANTメインネットの運用開始
- ✓ フルノードの配布パッケージ作成
- ✓ ADAMANTブロックチェーンエクスプローラの作成
- ✓マーケティング準備(ソーシャルネットワーク、フォーラム、ブログ)
- ✓バウンティキャンペーン開始
- ✓内部セキュリティ監査
- ✓プレICO開始(2017年12月14日)

2018年第1四半期

- ✓プレICO終了(2018年1月25日)
- ✓ICOの開始(2018年1月30日)
- ●ADAMANTメッセンジャープロモーション詳細の確定
- ●コンテンツ言語の追加と翻訳
 - ●ADAMANTメッセンジャーの機能拡張(ユーザープロフィールを基に行う 簡易ログインとチャット画面からファイル/トークンを処理、送信する)

2018年第2四半期

- ●iOS用のADAMANTアプリのリリース
- ●仮想通貨取引所へのADMトークン上場
- ●インフラ設備全体の拡張
- ●ADAMANTメッセンジャー機能の拡張(アドレス帳、グループチャットルームの 追加、メッセージ検索、チャットルームを閉じる方法)
- ●ICO終了(2018年6月30日)

2018年第3四半期

- ●仮想通貨取引所へのADMトークンの上場
- ●ADAMANTビジネスサービスの展開(ブロックチェーン上でのドキュメント保存とデジタル署名機能)
- ●Android用のADAMANTメッセンジャーアプリのリリース
- ▼マーケティングキャンペーン

2018年第4四半期

- ●独立したセキュリティ監査
- ●パートナー企業向けにADAMANTビジネスサービスを実施
- ▼マーケティングキャンペーン

ADAMANTテックラボ

ADAMANTチームには20人以上のメンバーがいます。

(主要メンバーは以下の通りです)



CEO — Pavel Evgenov

ITおよび金融プロジェクトの経歴を持つ経営者であり、イノベーター。MBA。

Graduate of Government and Municipal Management (IMEI) 。

モスクワ青少年コミュニティ区幹事

http://vk.com/p.evgenov



Lead Developer — Alexey Lebedev

IBM認定ソリューションデザイナー - ラショナル統一プロセス ブロックチェーン愛好家。

ITプロジェクトの管理/開発において15年以上の実務経験があります。InfoResheniyaとirソフトウェアのリーダー。

<u>lebedevau@gmail.com</u>



Lead Developer — Dmitriy Soloduhin
ウラジミール州立大学情報システム学科の理学修士。
様々な情報システムの開発およびシステム設計者(
ブロックチェーン含む)。IT専門家。興味:レゴ、写真。
https://www.linkedin.com/in/dmitriy-soloduhin



Lead Designer — Maxim Pikhtovnikov

Graduate of the faculty of Micro-units and technical cybernetics (MIET) 。

デザイナーおよびマーケッターとして国際企業での仕事経験を持つ。 1999年からコンピュータネットワークと情報セキュリティに没頭。 ITアドバイザー、エグゼクティブ、コーチ。



Product manager — Artem Vorobev

Graduate of the faculty of Micro-units and technical cybernetics (MIET) — 卒業. 10年以上のITプロジェクト経験。 IT起業家との7年以上の実務経験。 幅広いITに関する知識がある。

art.vorobev@gmail.com



Public relations— Sergey Lebedev

Graduate of the Architecture and Construction Department of Vladimir State University.

Chief project engineer, entrepreneur.

チーフプロジェクトエンジニア、起業家。 彼のリーダーシップの下、建設設計分野に関する50以上 のプロジェクトが行われました。

https://vk.com/id405481034



IOS Developer — Pavel Anokhov Moscow Institute of Management

テクニカルサポートから高負荷のバックエンドアプリケーションまで、ITに関して12年間従事。 興味: プログラミング、スノーボード、ポータル2

https://vk.com/realbonus

ADAMANT公式ページ

- ●ウェブサイト: https://adamant.im
- ●メッセンジャー: https://msg.<u>adamant.im</u>
- ●ブロックエクスプローラ: https://explorer.<u>adamant.im</u>
- •Githubのソースコード: https://github.com/Adamant-im
- •Twitter: https://twitter.com/adamant im
- Facebook : https://www.facebook.com/adamant.im
- •Vkontakte : https://vk.com/adamant_im
- •slack : https://adamant-im.slack.com
- •telegram : https://t.me/adamant_im
- ●Bitcointalk.org ADAMANT Messengerスレッド: https://bitcointalk.org/index.php?topic=2635564.0