



AVESTA

自由通貨

AVESTA

スケーラブル、高速、セキュア、プライベート

暗号通貨を実生活に用いる、欠けているものを加える、新たなスタンダードを暗号通貨の世界で設定する、個人や企業の方々の財務管理を容易にする、Avesta (AV) がその鍵となります。

目次

エグゼクティブサマリー	4
現在の暗号通貨に関する問題	5
1. ユーザーフレンドリーではない	5
2. 高いハードル	6
3. 機密性とユーザビリティ	6
4. 速度とセキュリティの問題	7
ブロック速度	7
確認	7
二重使用	7
採掘（マイニング）	7
51%攻撃	7
5. 暗号通貨の合法性	8
Avesta はどのように解決するか？	9
ユーザーフレンドリーな Avesta	9
開発者向け Avesta	9
簡単に始める／使う	10
プライバシーとユーザビリティ	11
高速スピードとセキュリティ	11
ブロック速度	11
確認	11
二重使用	12
採掘（マイニング）	12
51%攻撃	12
合法性	12
比較	13
結論	15

市場機会	16
参考文献	17

AVESTA 暗号通貨の新スタンダード



暗号通貨を実生活に用いる、欠けているものを加える、新たなスタンダードを暗号通貨の世界で設定する、個人や企業の方々の財務管理を容易にする、Avesta (AV) がその鍵となります。

エグゼクティブサマリー

Bitcause は暗号通貨の採掘（マイニング）、コンサルティング商社で、暗号通貨の世界で幅広い経験を持っています。

私たちの使命は暗号通貨の使用を容易にし、あらゆる人にとってアクセスし易いオールインワンの体験をしていただくことです。

弊社は世界中で絶え間なく成長しているコミュニティの一員であり、暗号通貨の愛好家、開発者、投資家の支援を受けています。暗号通貨の革命的ともいえる大量採用で、販売活動における暗号通貨の使用環境を作りたいと考えています。

暗号通貨コミュニティの間で憂慮されている点について、過去3年間にわたった情報収集を行い、リストアップしました。そこから暗号通貨の業界におけるハードルを乗り越えるべく、AVESTA プロジェクトを立ち上げることを決定いたしました。

本紙では暗号通貨が現在直面している問題と、AVESTA がそれをどのように解決するかについて説明いたします。将来的には技術基盤についてさらに詳しく説明する、個別のテクニカルペーパーをリリースする予定です。

現在の暗号通貨に関する問題

今日において消費者と鉱夫（マイナー）は暗号通貨の問題に直面しています。弊社では暗号通貨の大量採用の道が開かれるために、取り組まなければならない3つの大きな課題があると考えています。

1. ユーザーフレンドリーではない

暗号通貨コミュニティは着実に成長しましたが、実際このコミュニティはまだ拡張の初期段階にあります。評判の良いメディア・アウトレットは、ビットコインやその他暗号通貨の発展状況について報告を始めています。

世界中で暗号通貨に対する好奇心が高まっています。デジタル通貨の世界は魅力的であり、人々の心をますます引きつけています。ブロックチェーン・プラットフォームが小売業者との簡単な接続や統合を進め、実店舗やオンラインでの決済を可能にしない限り、暗号通貨は大量採用されるようにはなりません。

暗号通貨の現在の決済手順では、通常ある程度の技術的スキルやセキュリティに対する理解、システムへの信頼といったものが必要とされ、これまでの決済方法とは似つかないものです。こういった不便を経験すれば、好奇心旺盛で優れた能力を持つ人々でも、暗号通貨の市場へは背を向けるでしょう。

2. 高いハードル

IT企業や大企業は、ブロックチェーン技術と暗号通貨によって、今後どのように競合他社と差をつけられるかについて、未だはっきりとした考えを持っていません。

通常のユーザーにとっては、ウォレット、トークン、両替といったすべてが難解でうまくいきません。ICOへの参加や採掘の開始などはもちろんのことです。

第一の要因として、規制のない技術の業界へ関与することにより、ビジネスや評判がトラブルに巻き込まれるのではないかという恐れがあります。

第二の要因は、経験豊富なブロックチェーン技術者を募集、訓練、維持することの難しさです。この業界は斬新でビジネスチャンスが多い一方、資格のあるエンジニアの数は不足しています。

3. 機密性とユーザビリティ

消費者は購入、売却、または譲渡したものについて、情報を追跡されることを好みません。ほとんどの暗号通貨とブロックチェーンでは、本質的に情報がオープンです。

現時点ではほとんどの匿名暗号通貨が非常に長いハッシュを使用しているか、ユーザーが匿名性を保つために別個の安全な口座を必要としているので、匿名性とユーザビリティは共存しません。

もう一つの問題は、原則として記録が残らない、ということです。ユーザーが自分の口座証明書やプライベートキーなどを紛失したとします。その場合失われた口座を回復する方法はなく、失われたコインは未使用でエコシステム中に残ったままです。

また採掘（マイニング）や暗号通貨を保存するため、ユーザーが異なるウォレットを使用する、またはコインを保管する両替用の口座を必要とすることは、いずれも簡単であるべきです。

4. 速度とセキュリティの問題

ブロック速度

ブロックチェーン技術はブロック上に構築されていますが、ブロックというのは取引の確認のことです。取引を含むブロックが多いほどより安全になります。

そのためブロック速度は非常に重要です。例えばビットコインには平均10分、すなわち600秒のブロック時間があります。つまり確認のために少なくとも10分、さらにより安全な3つの確認をするためには30分も待つ必要があるということです

確認

安全な取引を行うには、ブロック内で取引を確認する必要があります。現在の暗号通貨では時間がかかり、迅速な決済を行うことができません。

二重使用

ブロックチェーン技術では、取引が確認されないと通貨が二重に使用される可能性があります。同じコインがネットワークによって確認されることにより起こりますが、その場合ほとんどのブロックで二重使用が真となって実行されてしまいます。取引手数料は通常、最も高くなることを意味します。

採掘（マイニング）

鉱夫（マイナー）はブロックを解決して確認を行うため、数学的方程式を解くことによって、ブロックチェーンを確保する重要な役割を果たします。鉱夫によって提供される作業は、ハードウェアと電気コストの形式で行われます。これにより分散システムが確保され、51%攻撃が実行困難かつコストがかかるものになります。

51%攻撃

51%攻撃は、現行の暗号通貨におけるプルーフ・オブ・ワークが直面しているリスクの一つです。単一のエンティティまたは当事者が、ブロックのグローバル・ソリューション・レートの51%以上を制御できている状態のことを意味します。理論的には51%攻撃で取引やブロックチェーンを変更または取り消すことは可能です。これは特に大企業が採掘（マイニング）を開始するときの大きなリスクです。

また、ほとんどの鉱夫（マイナー）が同じ採掘プールを使用し始めたとき、その所有者はその特定された暗号通貨に対する権限を乱用する可能性があります。

5. 暗号通貨の合法性

現時点では法律が各国によって異なっており、合法性は解決が困難な問題です。各国の政府が暗号通貨に関する法律や規制の変更を望んでおり、暗号通貨ユーザーにとって確実とできるものはありません。

Avesta はどのように解決するか？

Avesta はオールインワンの暗号通貨とプラットフォームです。ユーザーと鉱夫（マイナー）が直面する多くの問題を解決します。最終的に使用が簡単で登録が迅速な暗号通貨です。

以下に Avesta 開発チームが構築したソリューションの概要を示します。

ユーザーフレンドリー

皆様のための Avesta

Avesta はトークン化されたアドレスの代わりに口座番号を使用します。電話番号や銀行口座番号のような口座番号を導入することで簡単に取引を行い、お気に入りの口座番号のアドレス帳を保持することができます。これによりユーザーは Avesta Instant Messenger (IM) と Voice over IP (VOIP) を使用することもできます。

開発者のための Avesta

Avesta はブロックチェーン上の分散アプリケーション (DAPP) を構築するためのフレームワークを提供します。

Avesta には、開発者およびユーザーが Avesta ウォレットまたは Web プラットフォームからブロックチェーン機能を使用するための、完全な API サポートが付属しています。

Avesta は、ユーザーと開発者がブロックチェーン上でアプリケーションを作成して使用する際の、制限を取り除きます。これにより世界中の産業に新しいアイデアやソリューションがもたらされます。例としては、マイクロペイメント、アプリ内または携帯電話からの購入、サブスクリプションモデル、マーケットプレイス、電子商取引、POS ソリューションなどが挙げられます。

簡単に始める／使う

Avesta は暗号通貨であり、通貨へのアクセスや使用、保存がユーザーの皆様にとって、等しく容易であるよう開発者によって確認されていきます。デスクトップ・ウォレット、モバイル・ウォレット、および Web ウォレットに同じログインを使用します。

これにより難解な暗号通貨へのハードルが取り除かれ、他の暗号通貨や不換通貨を保存して使用するためのアクセスが許可されます。

スマート契約

Avesta を暗号通貨体験の完璧なプラットフォームにする最も重要な機能の 1 つは、スマート契約のユーザーインターフェイスです。Avesta は販売、請求書発行、トークン、その他の機能からなる多様なスマート契約・テンプレートを提供します。数回のタップまたはマウスクリックと同じくらい簡単なものです。

プライバシーとユーザビリティ

プライバシーとユーザビリティはオンラインで、特に暗号通貨で懸念されています。したがって Avesta は取引を保護する最善かつ最も実用的な方法を用いてきており、ユーザーは最善の匿名性ツールが利用可能です。ユーザーの取引は追跡不能かつ匿名であり、難解な取引システムに向き合うこともありません。

パスワードやプライベートキーを紛失するのはよくあることです。そのため Avesta では継承機能が用意されています。実生活上で失われた口座は、口座保有者の「相続人」に引き継がれます。相続人となり得るのは子供、親戚や友人です。暗号通貨の口座保有者に「相続人」が設定されていない場合、その口座は Avesta によって再発行され、口座に保持されているコインは通貨を鉱夫（マイナー）に譲渡することによって返却されます。

強力なスマート契約をブロックチェーンに統合することでこのすべてが行われ、すべてのユーザーが容易にフェイルセーフを持つこととなります。

高い速度とセキュリティ

ブロック速度

迅速な確認かつ安全な取引を実現するため、Avesta は独自の驚異的なブロックチェーンを作成しました。ビットコインよりも 60 倍以上高速なものです。口座間のポイントオブセールによる直接決済や、直接決済が可能になります。

確認

ほとんどの暗号通貨には数分間の確認時間があります。ってポイントオブセールまたは店舗決済の取引を、ブロックチェーン上で直接実行することはできません。

Avesta では、数秒で確認できるブロックチェーンをご用意しています。ほぼテーラーメイドのブロックチェーンを作成し、ポイントオブセールによる取引を可能にしました。

二重使用

Avesta はユーザーとブロックチェーン側において、二重使用をブロックしています。またブロックチェーンは高速で確認もより迅速に実行され、二重使用は不可能です。口座は、ウォレットを介してチェックされ、その後二重使用が発生した場合にノードがチェックされます。

採掘（マイニング）

ノードコンセンサス採掘報酬システムを作成し、Avesta は採掘プールのない画期的な採掘方法を作成しました。すべての鉱夫（マイナー）とプールが競合するのではなく、Avesta は代わりにすべての鉱夫が協力し合う方法を開発しました。すべての鉱夫（マイナー）へ公平に分担が行われます。このような採掘（マイニング）方法は Ethereum ベースの暗号通貨などにおける、いわゆる孤立ブロックまたは Uncle ブロックを防ぎます。これにより通貨の不必要なインフレーションが防止されます。

これらすべてのソリューションは、超高速かつ安全なブロックチェーン・ネットワークの構築をまとめたものです。

51%攻撃

この問題は互いに競合するのではなく、すべての鉱夫（マイナー）が協力して取り組むことにより排除されました。外部のものがネットワークを攻撃し、ブロックチェーンを変更する状況が完全に阻止されています。

合法性

Avesta は世界中の法人と提携することにより、ブロックチェーン技術と決済ソリューションの幅広い採用のための、法的枠組みの開発を開始します。

比較

Avesta は他の暗号通貨と比較して、優れたユーザーエクスペリエンスと優れたユーザー機能を提供します。以下の表は、Avesta と他のテクノロジーを比較したものです。

暗号通貨の比較表

	ビットコイン	Ethereum	Zcash	Avesta
採掘 (マイニング)	✓	✓	✓	✓
匿名性			✓	✓
スマート契約		✓	✓	✓
口座番号				✓
コインの継承				✓
平均確認時間 (少ないほど良い)	600s	14s	150s	10s
トランザクション/秒 (約)	20-30	30-40	20-30	1000+
コイン制限ハードキャップ	21.000.000	POS ? 100.000.000+	21.000.000	ICO+採掘 200.000.000

製品開発ロードマップ



発足

Avesta 発足日は
2018年1月5日

- 以下含む
- ウォレット
 - プラットフォーム
 - 採掘

E-決済

Web ショップと
E-決済モジュール

ウォレットがスマート
請求書発行、スマ
ート契約ユーザーイ
ンターフェースによ
り更新

デビットカード

KYC 承認口座所有者向け
Avesta デビットカード

Avesta 携帯アプリ向け
VOIP と IM の統合



ICO

2017/11/12
13:00 UTC ICO 開始

2017/12/20
13:00 UTC ICO 終了

12/24 公開テストネッ
ト 4th DEC

会計

会計モジュールと
Avesta ウォレット
を会計 API へ統合

ハードウェア

ポイントオブセール・
ハードウェアとソフト
ウェアの統合

Avesta グローバル展開
への準備

結論

暗号通貨の主要な問題のうち、いくつかは Avesta によって解決されています。高速、安全で使いやすく、追跡も不可能な暗号通貨が生み出されました。それが超高速確認とセキュリティです。

Avesta は、あらゆる方々にご利用いただき、利益が得られるような、新しいブロックチェーン技術を開発しました。暗号通貨に対する考え方に革命を起こし、暗号通貨が採用されるための大きな流れとなる道が開かれるでしょう。弊社の採掘（マイニング）ビジョンにより、暗号通貨ネットワークを維持する報酬の、より公正な分配へも、新しいアプローチへの道が開かれるでしょう。

ブロックチェーン技術で Avesta の真の可能性が明らかになります。

市場機会

暗号通貨の世界が真に成長する可能性を持つことは、事実を観察すると明らかに理解できるでしょう。ケンブリッジ大学の研究では「暗号通貨ウォレットの固有アクティブユーザー数は現在 290 から 580 万人」で、世界人口の 1% に満たないと推定されています。暗号通貨市場には十分な潜在的成長力があり、この白書の作成時点ではほとんどが未開拓であるものの、コイン・マーケットキャップによるすべての暗号通貨の総株式時価総額は、およそ 141,253,369,650 ドル（約 1,410 億ドル）という、非常に印象的な数字となっています。

参考文献

https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-04-20-global-cryptocurrency-benchmarking-study.pdf

<https://cryptolization.com>

https://www.reddit.com/r/Bitcoin/comments/5rlzon/with_4mb_block_size_and_segwit_what_is_the_max/

<https://docs.google.com/spreadsheets/d/150B9eytmjZ642tYD0jSdFZQHldmk7VG5Wm3KVctydpY/pubhtml>

https://www.reddit.com/r/zec/comments/662iq4/noob_question_whats_zcash_network_transactions/ <https://monero.stackexchange.com/questions/405/how-many-transactions-per-second-can-the-monero-network-handle>

チャート

https://docs.google.com/a/bitcause.org/spreadsheets/d/1fVwGE_TkmkkONt12yPUSFEa8qrX9ERm0sSJXShzRGIA/edit?usp=sharing

<https://www.reuters.com/article/us-microsoft-accenture-digitalid/accenture-microsoft-team-up-on-blockchain-based-digital-id-network-idUSKBN19A22B>