

Money, on Your Terms...

ライトペーパー v.1.0

January 30st, 2018

注:この内容は更新中です。予告なく更新されることがありますので、最新バージョンは https://phore.io にてご確認をお願いします。

目次

行動理念	4
Phore の展望	6
歴史と業績	8
Proof of Stake	10
マスターノード	11
ゼロコインプロトコル (zPHR)	13
Phore コミュニティ	15
Phore マーケットプレイス開発	16
マスターノードガバナンス	17
慈善の寄付	19
現在の Phore の統計データ	21
Phore は他の匿名通貨とどのように異なるのか?	22
2018 Phore Roadmap	24
Q1 2018 Milestones	24
Blockchain Technology	24
ウェブウォレット/android ウォレットのリリース	25
ウォレット・コアのアップデート	26
マスターノードセットアップの自動化	26
Phore の予算ガバナンスシステムウェブサイト	26
Phore マーケットプレイスのローンチ	27
Phore 開発者チームの拡大	27
チーム人員募集の継続	27
Q2 2018 Milestone	28
Segregated Witness (Segwit) の統合	28

iOS モバイルウォレット / App	29
Phore 財団の設立	30
Q3 2018 Milestones	30
スマートコントラクト	30
アトミックスワップ統合	34
クリック&コレクト-ベンダー連携プログラム- 位置は未決定	35
Q4 2018 Milestones	35
スマートコントラクト統合	35
モバイルアプリ開発	36
VR/AR マーケットプレイス強化 – β テスト	36
マーケットプレイスへのクリック&コレクトの一部導入	36
Phore ラボによる投資活動	37
2019 Roadmap	37
チーム情報・コミュニティ・リンク	40

注意: Phore ホワイトペーパーの短縮版です。Phore が何か、どのように始まりそして どこへ向かうのかを簡単に記しました。意図的に細部は省いているので、興味のある方はぜひ Twitter @PhoreJapan より日本語版ホワイトペーパーをダウンロードください。

行動理念

これまでの時代の技術の進歩は、歴史上の他の時期とは異なる莫大な富・機会を生み出してきました。人類は今分水嶺にいるのです。ブロックチェーン技術の採用により、コミュニケーション・取引・商品やサービスの支払い方法・アプリケーションなどを再構成するであろうパラダイムシフトが起きつつあります。このような新しい技術には多くのメリットがありますが、コストもかかります。個人情報の収集・追跡・分析・利用は民間・公共の両方に対してより簡単になりました。法人や政府は様々な理由で個人情報を収集しますが、それがもたらす結果はどちらも変わらず、個人のプライバシーの欠如です。

「私は間違ったことがないから、隠すものは何もない」そうおっしゃる方もいるでしょう。しかしこのような考えのままでは、収集されたデータが私たちに与える影響を正しく把握することは出来ません。この情報はターゲットされた広告・検閲・ボイコットに使われ、近年ではこのような例が見られます:

- ソーシャルメディアはコンテンツを禁止し、広告を禁止し、メディア プラットフォームに対して反対的な意見を持つユーザーをバンするた めに利用されています
- ◆ 大規模なクラウドファンディングサイトは政治的な偏見の対象となっており、「地域社会での基準に合致しない」などの理由でプロジェクトが削除されることがあります
- 購買関係の個人情報は広告・検閲・ボイコットなどの目的で企業や政府により利用されており、多くの個人情報が集中的に管理されているため、部分的な盗難・セキュリティ問題が多発します。

Bitcoin のような一般的な暗号通貨は全取引は完全に監視可能であり追跡可能なため、十分な個人情報の保護を提供できません。Phore が行うことのできる解決策の1つは、より改善されたプライバシー志向の暗号通貨となることです。

Phore の通貨としての有用性は、そのエコシステムの要であることです。個人は匿名・公開取引を選択し、即時に行うことが出来ます。これは暗号通貨であるため、法的な実体により通貨が押収されることもありません。米ドルなどの法定通貨以外の交換を利用することの利点は、中央政府による政治的な影響から個人が逃れることができることです。Phore は確立された通貨の運営を行っています。このために個人はセキュリティ問題を気にすることなく意思決定を行えます。Phore の供給の拡大はすべて決められており、それが任意に決まることはあり得ません。そのため、安定した交換媒体を得られます。恣意的な中央銀行の通貨計画による影響は、近年の米国・欧州連合の貨幣史から読みとれます。

- 米国では、大恐慌の最中に金地金の個人所有を禁止し、国民に金を売 却するように要請しました(価格が 50%下落するまで)。
- 2013 年キプロス銀行が 30 億\$の救済措置を IMF と締結しました。これにより、10 万ユーロを越える 47.5%の預金が喪失しました。
- 2014 年、ロシアは政府の資金調達のため、年間で国民の年金退職拠出 金の約80億**\$**を奪っています。
- 様々な見積もりによれば、米ドルは過去 100 年間と比べ購買力は 90% 下がっています 1 。 John Meynard Keynes は「介入主義的経済政策のシステムにより世界の通貨価値が害され、政府は市民の富を秘密裏に

¹"What Has Government Done to Our Money?" by Murray N. Rothbard, Ludvig von Mises Institute, Sept 20th, 2005.

没収できる。彼らは任意に没収することで、多くを貧困にする一方で、一部の人間により多くの富を与えている。」²と述べている。

私たちはコミュニティと個人の権力を重要なものとして考え、自由な討論・商取引の自由は保障されるべき権利であると信じています。商取引には商品・サービスの売買やクラウドファンディングを通じた資金調達・顧客に価値のあるビジネスの運営などの様々な形があります。

ブロックチェーンと分散型技術を使うことで、Phore を個人とコミュニティに権利を取り戻し、個々の目標に対してより効率的に、中央集権的グループによる影響を受けずに行うことができるようにしたいと考えています。

Phore のビジョン

Phore コミュニティのビジョンは、自由で長期間に持続できる分散型の商取引を可能にする基盤としてプライバシーを保護したコミュニティに根差す暗号通貨を提供することです。Phore に組み込まれた技術により皆様に次のような機能を提供します:

- 高速でスケーラブルかつ安全、信頼性の高いトランザクション
- 透明性の高い/匿名性の高いトランザクションを共に実行できる能力
- Phore ネットワークに参加する全員に対し利用可能な報酬(利子のような)

² "The Economic Consequences of the Peace" by John Maynard Keynes, Serenity Publishers, LLC (February 10, 2009)

- 匿名なトランザクションと共に利用できる分散型アプリケーション (dApps)を構築するためのプラットフォームで、この上でお金・個人情報 を管理するような新たな分散型のプライバシーに対応したビジネスモデル が実現されます。
- 広範囲にわたるアクセシビリティ・可用性

アクセシビリティ、使いやすさは Phore のビジョンにおいて重要な部分をなしています。Phore の利用において、高度な技術スキルを持たずとも、特定の言語に縛られずとも製品やサービスの入手・交換が容易になされる必要があります。

Phore のビジョンは通貨としての発展のみにとどまらず、支払いメカニズムとして Phore を中心とした完全に分散型な市場を立ち上げることを目指し準備を行っています。ユーザーは Phore を支払い通貨として(匿名型のトランザクションで送金し)商品を売買することができます。我々はコアチーム・コミュニティの両方により構築される Phore アプリケーションとビジネスによるエコシステムを支援・開発し、関連スタートアップ企業の立ち上げや Phore のビジョンに沿う教育的な研究を支援します。

ビジョンが全て実現されれば、Phore によりセキュアで安全・プライベートかつ完全に分散されたネットワークが実現します。Phore ネットワーク上では、匿

名化された分散型アプリ(dApps), 匿名型の電子商取引、匿名型のビジネスモデルを提供することのできる分散型マーケットプレイスによるエコシステムが展開されます。活動を管理する中央組織は存在しないので、あなたは自由に Phoreやアプリを用いることができます。コアコードの開発や応用はコミュニティによりインセンティブを与えられるでしょう。あなたは、コミュニティへの寄与・活動に対して Phore という形で報われることになります。

コミュニティは我々のビジョンを達成するために最も重要な部分です。コミュニティにより透明性を保った管理をされるように Phore という通貨は出来ており、コミュニティ・コアチームの特定のメンバーが変わったとしても将来を保証できます。8000 人以上の Twitter のフォロワー、4000 人以上の Discord のメンバー、600 人以上の Telegram のメンバーがコミュニティに参加していただいております。チームはコミュニティの皆さまの参加を促すようなフレンドリーな環境を作ろうとしています。

歴史と業績

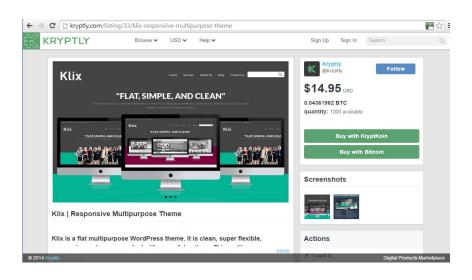
Phore はコアチームの設立・暗号通貨のローンチ・2018 年ロードマップの一部など、2017 年の 9 月にプロジェクトが開始して以降長い道のりを歩んできました。

KryptKoin の起源

hore は 2014/5 にスタートされた KryptKoin(KTK)からアップデート・リブランドされたデジタルな匿名型暗号通貨です。

KryptKoin はプレマインなしで、ステークの有資格者に対して配布されました。500 個のステークが二段階に分かれて配布され、30 日間保持していた人々にボーナスの KTK が与えられました。ICO はなく、開発者へのプレマインもありませんでした。

開発者の Phroshi は他のステークホルダーと同様、1のステークのみ受け取りました。ローンチを通じ、KryptKoin は迅速かつ大胆な開発を実行し、2015 年にはオンラインのマーケットプレイスを導入しました。 Paypal も統合されており、Wordpress のテーマのようなデジタル商品が販売されていました。



これは KTK マーケットのリリースの際の短いプロモーションビデオです。

https://www.youtube.com/watch?v=Sj3f7ucJBlo

コインのスワップ

新たな機能を容易に導入するため、コードの書き換え、更新が必要でした。このために KryptKoin は新たな通貨 Phore へのスワップが必要でした。Phore のコードベースは PIVX プロジェクトからフォークされ、PIVX は Dash から、起源をたどれば、全ては Bitcoin コアからフォークされました。

既存の KTK 保有者が Phore に対して 1:1 でスワップすることが出来、これには二か月間の期間が設けられ、暗号通貨のフォーラム・SNS にて告知がされました。このスワップは 2017/11/18 に終了し、スワップされなかった 700 万枚以上の Phore がバーンされました。現時点での Phore の総供給枚数は 1150 万 PHR 程度です。

Proof of Stake

Proof of Work (PoW) とマイニングをブロックチェーン構築のメカニズムとするビットコインと異なり、Phore ブロックチェーンは Proof of Stake (PoS)を用いています。PoS はネットワークの参加者がどれくらいの金額を保持しているか、Phore の取引・ブロックの検証に参加することに基づき報酬を与えます。分散型ブロックチェーン合意システムを構成するこの方法は、PoW に対して次のような利点を有します:

- Phore ブロックチェーンの保護に必要な計算能力・電力は非常に少ないです。 Ethereum や Bitcoin における PoW マイニングでは、月あたり 100 万ドル以 上の電力と関連費用が発生していると見積もられています。PoS はより持続 可能でエコです。
- ブロックチェーンの保護に参加するインセンティブを提供するために必要なコインが少なくなります。このため、Phore の取引手数料は Bitcoin よりも少なくなります。取引手数料は全てバーンされ、総供給を減少させます。つまり取引量が増加することで、コインの総供給枚数がどんどん減っていくことがありうるということです。

- 上で述べた低コストであることから、Phore ノードは安価なコンピュータでも動作するので、PoS はより分散化を進めることができます。このような分散化の過程で悪意のあるノードによるグループの形成が難しくなります。
- このような PoS の利点は、Phore のネットワークに安全性を提供します。 Phore ネットワーク上のノードは、PoS に参加するには Phore 通貨の保有者 でなければならないため、通貨の価値を保護し向上させる自然なインセンティブを持ちます。

Ethereum は現在、PoW から PoS アルゴリズム(キャスパー)に切り替わるべく 1 月 1 日にテストネットを開始しています。 Phore のウォレットを持つ人は誰でもウォレットをオンラインに保つことで Phore トランザクションの処理と検証を支援し、Phore ブロックチェーンを保護することができます。このサービスを提供し、Phore ネットワークを保護することの報酬として、ステーカーはブロック報酬の一部を受け取ることができます。執筆時点では、ブロックごと(約 60 秒ごと)に 2.8 PHR が与えられます。ブロックを採掘し、ステーキング報酬を得る確率は、全 Phore ノードによってステークされている Phore の数に依存します。 Phore のチームとアドバイザーは、詳細なガイドを作成し、ステークのためにウォレットを設定するユーザーに Discord 上でサポートしています。

マスターノード

Phore ブロックチェーンに追加のサービスとセキュリティを提供する上位のノードであるマスターノードを実装しました。 マスターノードによって提供されているサービスはゼロコイン(zPHR)による匿名型トランザクション(ゼロコインプロトコルを参照)を処理し、Phore の予算案システムを処理することです。Phore の機能が発展するにつれサービスが追加されることがあります。

10,000 Phore を所有する方は 24 時間オンラインで動作しているマスターノードを設定・運用出来ます。マスターノードの所有者は Phore のネットワークを保護し、サービスを提供することに対して大きなインセンティブが用意されます。

マスターノードを実行するには 10,000 の Phore がウォレットの一つのトランザクションで担保としてロックされる必要があり、Virtual Private Server(VPS)上や、自宅のラズベリーパイでも(静的 IP を持っていれば)実行することが出来ます。Phore マスターノードは IPv6 をサポートし、適当な IPv6 対応 VPS で複数のマスターノードを実行できます。追加のプライバシーのために Tor / Onionルーターを実行するよう設定することもできます。マスターノードが一度実行されると、ウォレットを停止しても動作し続けます。



Phore ウォレットのマスターノードタブ

マスターノードの所有者がマスターノードを停止し担保である 10,000 PHR を利用したい場合、いつでもそうすることが可能です。マスターノード保持者はステーカーと同様に各ブロックにおいて報酬の一部として 4.2PHR を得ます。masternode の所有者にとっては新しいビジネスモデルであり、賃貸物件を所有すること似ています。初期に必要な設定作業やメンテナンス、サービスの提供の対価として持続的な報酬が得られます。現時点で、Phore ネットワークでは約450 のマスターノードが動作しています。総量の約38%(450 万の Phore)が担保としてロックされ、流通枚数を約1170 万から約720 万の Phore に減少させています。この条件からマスターノードの所有者に対する収益率は現在約48%の Phore です。この数値はネットワークにマスターノードが追加・削除されたり、ブロック報酬の減少につれ変化します。

Phore チームはマスターノードセットアップの詳細なガイドを開発しました。 Phore チームとコミュニティは、セットアップに対して Discord 上でサポート を提供しています。

ゼロコインプロトコル (zPHR)

Bitcoin のトランザクションはブロックチェーンに記録され、自由に見ることができます。送信者のアドレス・受信者のアドレス・送金量および取引に関連する情報はすべて公開されています。この機能は残高を正確に表示し、二重支出を防止する素晴らしい機能ですが、匿名性はまったくありません。blockchain datacan の分析では、取引情報から同じウォレットに属するアドレスを推測することが可能です。このような情報から他のアドレスを関連づけるためのデータを分析することもでき、米国政府・企業は"匿名"の携帯電話の番号所有者に対して各種情報から特定する手法からブロックチェーンアドレスの所有者の特定について言及しています。

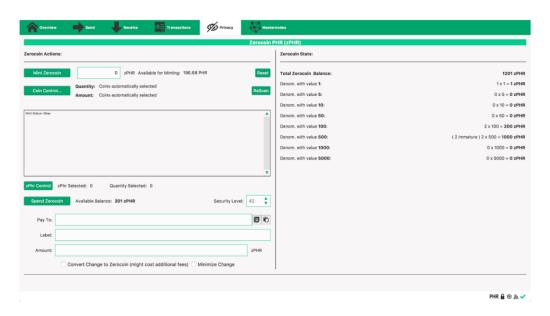
個人は全取引の一部は匿名の状態にしておきたいと考えているはずです。暗号 通貨をもとに給与支払いを受ける場合には、その一切を公に記録されたくないと 思うかもしれません。また地震の個人情報の自動的な集約・分析(および販売)を 受けたくないと考えるでしょう。

Phore は zPHR というカスタムされたゼロコインプロトコルを用いることで 匿名型トランザクションを実装しています。ゼロコインは活発に研究されており、 Johns Hopkins 大学のコンピュータサイエンス学科の発表したゼロコインの論文 を確認できます(注釈 3)。

zPHR は Phore を zPHR に変換("mint")しブロックチェーン上の zPHR アキュームレータプールでコインを混ぜる(ミキシング)技術です。Phore ブロックチェーン上の送金者・受金者を記録せずにトランザクションを検証するため、ユーザーとマスターノード間でゼロ知識証明をしてコインの所有を証明します。このやり取りは RSA-2048 暗号を利用して行うため、開発者を信頼するような設定は必要ありません。この結果、zPHR のトランザクションの身元を明らかにするような情報を知る人間はいません。

ゼロコインプロトコルは、匿名化を効率的に行います。zPHR への変換は 0.5 秒で、zPHR の送金は 2.5 秒で実行されます。またセキュリティレベルとして、 ネットワークで以前に作成された zPHR とあなたのコインを混ぜ合わせる回数 を指定することができます。

マスターノードは zPHR への変換サービスとその際の zPHR アキュームレータとの接続を行います。所有者は、Phore を取引手数料変換される zPHR 当たり 0.01PHR を支払うことで zPHR コインを 1~5,000 Phore の範囲のコインブロック(denominator)で生成できます。 zPHR を生成するためのトランザクション手数料は、計算量の多い動作であるため、スパム行為による攻撃を防ぐために通常のトランザクションより高額になります。他の取引手数料と同様に zPHR 手数料はバーンされ、総供給量は減少します。 ユーザーは zPHR を自分のWallet アドレスに送信するか、他の Phore アドレスへ送金することで、zPHR を PHR へ変換することが可能です。zPHR にはトランザクション手数料はなく、zPHR は匿名で安全なウォレットに保管されます。



PHR を zPHR として保管する他の利点は、アキュームレータ上に保管される zPHR が所有者のアドレスに表示されないことです。これは多くの残高を持つアカウントに対してハッカーの標的になることを防ぐことができる利点があります。 zPHR によって正確な残高を隠すことができるということです。ゼロコインは多くのオプションを持つ匿名化トランザクションを提供する手段の内最も良い方法の一つです。

Phore コミュニティ

コミュニティはプロジェクトの中核です。ローンチ以後、コミュニティの個々人はプロジェクトのアイデアを共有するのみならず、方向性も議論し始めました。コミュニティは Slack チャンネルにいた少数のメンバーから始まりました。ICOやプレマインはないため、初期のメンバーは時間・努力・個人の資金をもとにプロジェクトを普及させました。当初は様々なフォーラムやソーシャルメディアに掲載され、大きく活気のあるコミュニティ作りを目標として取り組んでいました。

初期の活動の結果、Phore に関心を持つ投資家がコミュニティに加わり、最終的にコミュニティの要請に基づき Discord へ移行しました。大規模な Twitter のプロモーターの中にも Phore の価値を理解しフォロワーへ Phore を周知する活動を開始しました。しかし、Phore への投資を選択した理由のほとんどは、コミュニティ自身でした。コミュニティは非常に活発で、チームメンバーがほぼ常にDiscord の中でアクティブであり、サポートを提供し、コミュニティに情報がどこにあるかを指摘するような活動をしています。さらに、私たちのコミュニティには非常にポジティブな雰囲気があります。人々は友好的で、全員がコミュニティな、ひいては Phore をよりよくするための議論をしています。Phore を広めるための初期の活動は、(ほぼ 0 の予算で)十分な成功を収めました。

Twitter, discord, telegram でコミュニティが拡大してきました。 2017 年 12 月、ガバナンス機能が発動し、チームやコミュニティから提出された提案に基づいて開発資金が提供されました。最初の予算は、プロジェクト開発資金と Phore のコミュニティの普及に重点を置いていました。これらの資金は、ソーシャルメディアキャンペーンを通じてコミュニティを拡大するために使用されました。私たちは現在、テレグラムに 1100 人のメンバー、Discord に 3200 人のメンバー、そして Twitter で 8000 人のフォロワーを持っており、十分な成果を上げたようです。

マスターノード予算管理プロセスに従い、Phore はコミュニティから指針を得ます。私たちチームは積極的にコミュニティに参加し、アイデア・デザインの共有・フィードバックの収集・コミュニティの要望を確認しています。チーム全体

として、常にコミュニティの需要に答え、透明性を確保し、コミュニティに対して正直でありたいと考えています。

Phore マーケットプレイス開発

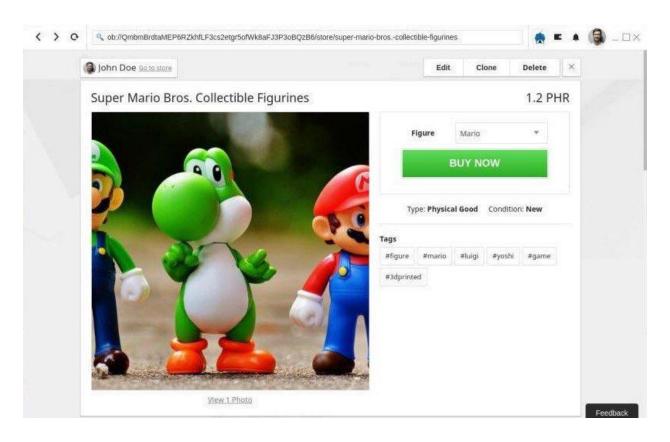
Phore のローンチ以来、コアチームの開発リソースのほとんどは、2018 年第1四半期末までにリリースする予定の Phore マーケットプレイスに集中していました。 Phore マーケットプレイスのベースは OpenBazaar からフォークされましたもので、Phore マーケットプレイスに堅実な基盤を提供し、分散型アプリケーションを目指す Phore の思想と合致します。初期リリース時に利用できるマーケットの機能の詳細については、下記の Q1 2018 を参照してください。開発チームは必要な機能・ユーザーインターフェース・暗号通貨 Phore に基づいた匿名型トランザクションをサポートする完全なマーケットを提供するための開発に取り組んできました。これと並行し、アドバイザーと Phore コミュニティは、最初のベータとローンチに参加してマーケットで利用可能な最初の製品を提供するベンダー・ショップを探しています。

Phore マーケットプレイスは、OpenBazaar プロトコルのフォークです。 エスクローシステムおよび仲裁システムを含む 2 者間の取引は全てプロトコルレベルで処理されます。このため商品の取引をするための完全に分散されたトラストレスなシステムが構築されます。全てのトランザクションはプロトコルレベルで行われるため、マーケット自体は検閲されません。しかし、検索エンジンはPhore マーケットでショップを見つける一つの中央集権的システムとして機能します。

チームは検索エンジンを1つホストし、そのコードをオープンソース化する ことで、誰もが自分の検索エンジンを動かせるようにする予定です。

Phore Marketplace の各ショップには、各々を識別する固有のアドレスがあります。 データを格納するための分散型システムは、IPFS プロトコルのフォークです。 具体的には、集中型サーバーを必要とせずユーザーがストアデータを保

存してアクセスでき、どのショップも店舗の URL を入力することで検索エンジンを使わずにアクセスが可能です。



マーケットプレイスのスクリーンショット

マーケットプレイスはユーザーインターフェース・検索エンジン・Phore ネットワークとの接続と、継続的に開発されています。オープン β は 1 月中旬に、最終リリースは Q1 の後半に行われる予定です。

マスターノードガバナンス

Phore の資金調達とその目的は、Phore コミュニティにより決定され、Phore の長期的な価値を高めるために議論されます。このシステムは Phore のブロッ

クチェーンに直接組み込まれており、担保として 10000PHR をロックしているマスターノード保有者が投票します。

ブロック報酬の 10%がこの開発提案の資金提供のために確保されています。各予算案の提案サイクルは 30 日で、提案にはバーンされる取引手数料 50PHR が必要です。Phore チームは フォーラム https://forum.phore.io を各予算案のための提案・議論のための場として用意しました。各マスターノードホルダーははい/いいえの投票か、棄権できます。承認されるためには、サイクル終了の三日前までに提案を提出し、マスターノードの総数の 10%の賛成を得る必要があります。予算案は 1 度のみの支払いで提出することも、長期プロジェクトへの継続的な資金の調達のために複数回の支払いで提出することも可能です。

```
{
    "Name" : "Jan15Budget",
    "URL" : "https://forum.phore.io/t/january-15-budget/71",
    "Hash" : "ca29a85788ad81cf4712d94354afdf9eaa4345a3e2107e8a14d0bc1da3ad8247",
    "FeeHash" : "42ae927f73484b203a7c4f91a8821c75c88bb855a64179ce6e4cd384d2dd65e0",
    "BlockStart" : 172800,
    "BlockEnd" : 216001,
    "TotalPaymentCount" : 1,
    "RemainingPaymentCount" : 0,
    "PaymentAddress" : "PEQNR5oGqggzRcSQqtgaefcYiYbFhDMoBm",
    "Ratio" : 1.000000000,
    "Yeas" : 82,
    "Nays" : 0,
    "Abstains" : 0,
    "TotalPayment" : 27500.00000000,
    "MonthlyPayment" : 27500.00000000,
    "IsEstablished" : true,
    "IsValid" : true,
    "IsValidReason" : "",
    "fValid" : true
}
```

2018/1 の Phore の予算案提出での JSON 形式の出力

サイクル終了の二日前に投票が終了し、結果が確定します。そして承認されれ

ば予算の確定を行うために別に 50PHR の手数料を支払う必要があります。そしてサイクル終了時に承認された提案に対して予算を配分します。そして次のサイクルの開始ブロックで各提案で指定されたアドレスに予算が提供されます。

このシステムにより継続的な Phore の開発に対して適切に資金を配分する分散型の投票が行われます。マスターノード所有者は、だれがどれくらい支払われ、どのように使われるかを決定します。ICO やプレマインと異なり、このタイプの資金調達方法はアイデアを持つ人が資金を正しく得ることが可能で、Phore が直接的に長期的な開発の資金源を提供するものです。

慈善活動への寄付

暗号通貨という成長ペースの速い業界に進出していくだけではなく、現在の我々がどれだけ幸運なものであるかを理解することは重要なことです。現在の暗号通貨の業界では、常に電気・インターネットを利用できるという点で、誰もが恵まれていると言えます。しかしこの強欲の渦巻く空間でも、助けを求めている人々がいることを忘れてはいけません。Phore では、次のようなことを行うつもりです。

まだ比較的若いプロジェクトであり、ICO やプレマインを行っていないために 資金は多くありませんが、我々は積極的に寄付を行うことを目指しています。こ れまで次の6団体に寄付を行いました:

- Make A Wish Foundation: 危険な病気を患う子供のための"Wish"体験を実現する団体
- Children International: 子供たちが貧困のサイクルから抜け出すのを支援する非営利団体
- Covenant House Tronto: 教育・カウンセリング・医療・雇用支援などのサービスを提供するトロントの若者のためのホームレス避難所
- Life For The World(ハイチ): 持続的な生活プログラムを作り、再就職する孤 児たちにスキルやトレーニングを提供し、孤児院の支援に重点を置く組織。
- American Kidney Fund: 腎臓病を患う 3100 万人のアメリカ人へ支援とリソースを提供している非営利団体。
- カナダ精神保健協会(Canadian Mental Health Association):精神病を患う人々とその 家族にワールドワイドなサービスと支援を提供する組織。

この寄付はコミュニティへの giveaway "All I Want Phore Chirstmas" の際に行われたものです。この慈善的な性質は Phore チームメンバーを反映したもので、それぞれが時折寄付を行っています。技術の進歩は商取引を進展させ、生活の質を向上させるために起きるものです。Phore は世界をより良い場所にするこ

とを約束します。

現在の Phore の統計データ

Phore は PoS とマスターノードを用いてネットワークを保護し、高いセキュリティと匿名性を提供しています。Phore は 1 分という短いブロック時間を持ち、Bitcoin に比べ低いトランザクション手数料です。

全供給量(2017/12/29調べ): 11,526,943 PHR

流通量 (2017/12/29 調べ): 7,316,943 PHR

ブロック時間: 60 seconds

トランザクション手数料: 0.001 PHR

確認: 6

ブロックの成熟: 50

Proof of Stake (PoS) 報酬: 2.8 PHR / ブロック

最小ステーク開始時間: 3時間

マスターノード報酬: 4.2 PHR / ブロック

マスターノードの担保: 10,000 PHR

マスターノードの数 (2017/12/29 調べ): 421

Phore の開発用資金 – ブロック報酬の 10%, 30 日ごとに支払い (43,200 blocks) 次の表のスケジュールに従って、Phore プロジェクトが成長し時間経過とともに インフレーションを制御するためブロック報酬は制御されます。

日付	開始ブロック	終了ブロック	マスターノード報酬	ステーク報酬	開発用基金
現在	現在	250,000	4.2 PHR	2.8 PHR	0.7 PHR
2018/3/9	250,001	518,399	2.7 PHR	1.8 PHR	0.45 PHR
2018/9/11	518,400	1,036,798	2.16 PHR	1.44 PHR	0.36 PHR
2019/9/6	1,036,799	なし	1.62 PHR	1.08 PHR	0.27 PHR

Phore は他の匿名通貨とどのように異なるのか?

Phore は Particl, Monero, Zcash, Dash, PIVX とは異なる特徴を有しています。 それを一挙に見るため、次ページの図をご覧ください。



Phore ロードマップ

Phore は 2018 年のロードマップを発表しました。ロードマップのクリア後、Phore ブロックチェーンは匿名通貨から、匿名かつ分散型のアプリの開発・展開のためのプラットフォームに変わります。また将来的に現在のアーキテクチャを利用して Phore のエコシステムを拡大するための機会が用意されるでしょう。

以下のセクションでは、2018年に行われる中でも重要なマイルストーンについて簡単に説明します。チームは既にマイルストーンを達成してきた実績があります。Phoreコア開発チームと Phoreコミュニティでは、継続して議論・デザインの改良が行われているので、以降に記載されているプランは随時改良・更新されます。フィードバックを元に、一年を通して Phore に他の機能やアップグレードを加える予定です。

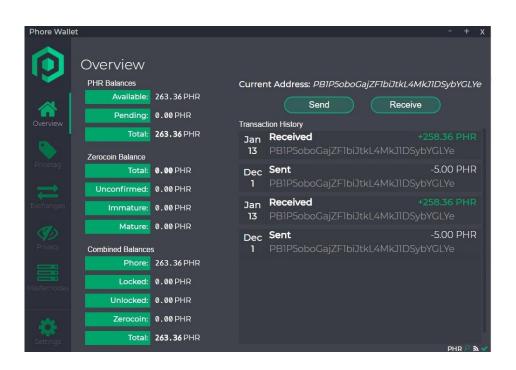
Q1 2018 Milestones

Blockchain Technology

この四半期では Phore のマーケットプレイスへの統合が焦点となります。コアのコードは継続的にレビュー・メンテナンスを行い、次の四半期に行われる Segwit の導入の前に初期テスト・実装テストを行います。

ウェブウォレット/android ウォレットのリリース

Phore のビジョンの一つは、出来る限り多くの人に Phore を利用していただき、より使いやすくすることです。そのため 2018 年第 1 四半期に 2 種類のウォレットをリリースする予定です。 Android ウォレットは、Google Play ストアからダウンロードできるモバイルウォレットで、Phore ブロックチェーンとの安全で素早い同期を提供します。 また二段階認証(2FA)を統合し、Phore デスクトップウォレットの機能を利用してユーザーに Phore を保護するためのセキュリティレイヤーを追加する予定です。 ウェブウォレットは、オンラインにホストされた Phore 財布のプラットフォームを提供します。これにより、人々はPhore ウォレットをラップトップ・モバイルデバイス上で実行せずに Phore を保管することができます。



新しいウォレットの UI のイメージスクリーンショット

ウォレット・コアのアップデート

Phore コア開発チームは、通貨 Phore とウォレットの安全性をより高めるために Phore のコードを継続的に更新およびアップデートします。これは 2018 年を通して継続されます。第 1 四半期中には、将来的なサードパーティによるウォレットの統合をサポートするためのアップデートも行い、ハードウェアウォレットの統合をサポートします。

マスターノードセットアップの自動化

Phore はマスターノードのセットアップ・実行をするユーザーに対してガイド・テクニカルサポートを提供していますが、セットアップのプロセスはより簡略化出来ることを理解しています。そのためマスターノードをセットアップするより自動化された方法を開発します。

Phore の予算ガバナンスシステムウェブサイト

透明性のため、Phore ブロックチェーンと連携し予算案・投票状況・予算配分のステータスを表示するサイトをホストします。これにより容易に予算案の状況を確認でき、使いやすさが向上します。

Phore マーケットプレイスのローンチ

オープン β は Q1 の初 \sim 中期に行われ、リリースは Q1 の終盤に向け行われます。

Phore 開発者チームの拡大

このロードマップを確実に達成するため、Phore コアチームの一員として Phore コアブロックチェーン技術・製品・サービスの開発専門の開発経験豊富な 開発者を加え、Phore コミュニティ内の開発者を増やす予定です。我々は Phore チームに参加することについていくつかの有能な開発者とすでに議論を開始して おり、これは 2018 年第 1 四半期ずっと継続されます。

この拡大の一環として、世界中の大学からブロックチェーン技術系の卒業生を 育成し誘致するための給料有りのインターンシップを開始する予定です。

チーム人員募集の継続

更に専門家を Phore チームへ募集します。特に開発スキルに焦点を当て、スマートコントラクトの統合、Phore ラボのマイクロレンディング・投資家の採用を行います。

Q2 2018 Milestone

Segregated Witness (Segwit) の統合

Segregated Witness によりトランザクションの形式を変更します。具体的には scriptSig や scriptPubKey などの署名データをトランザクション ID で表されるトランザクションデータと別のものとして分離して扱います。 Segwit を行わなければ、ネットワーク上のノードにより署名データをわずかに書き換えられたり、署名者が署名を変更することがあります。同量のコインが同アドレスへ支払われますが、トランザクション ID が変更されます。

Txid により表されるデータから署名データを分離することで、トランザクションに展性を持たせるのを防ぎ、次の利点をもたらします:

- ウォレットのコードが簡約化されます。ウォレットが支払いトランザクションを追跡する最も良い方法の一つはトランザクション ID から参照することであり、トランザクション ID を変更することができる場合、ウォレットにはその可能性に対処したコードを別に書く必要がありました。
- 未確認取引による支払いトランザクションの信頼性が向上します。例えば、トランザクション A で支払いをし、トランザクション B でそれを利用して支払いをした場合、A の署名データが変更されたときにトランザクションの順序が入れ替わりトランザクション B が無効になることがありました。SegWit はこのような事例を起こらなくします。

- トランザクションのスループット・スケーリングが向上しました。現在のPhore は 60 秒のブロック時間・2MB のブロックサイズを持ち、トランザクションの処理において非常に高速かつ効率的です。SegWit は署名データを実際のサイズの 1/4 として計算し、ブロックにより多くのトランザクションを埋め込み、スケーラビリティとパフォーマンスを向上させます。
- トランザクションの展性の問題を解決すると、Lightning Network に類似し たサイドチェーンを追加することで、書き込みが簡単にし、ブロックチェー ンデータの使用効率が向上させることが出来ます。
- スマートコントラクトの設計・レビュー・監視を容易にします。

最後の2つの利点は、Phore のビジョンにとって非常に重要です。2018年後半に Phore 上でスマートコントラクトを導入し、スマートコントラクトアーキテクチャの一部としてサイドチェーンを使用する予定があるためです。SegWitのアクティベーションにより、この新たなプラットフォームに必要な用意が行われます。

iOS モバイルウォレット / App

暗号通貨への関心の高まりに伴い、Phore は iPhone と iPad 用のモバイルウ ォレットを導入することが重要です。iOS を利用する多くの Phore ホルダーに よる利用を容易にし、Android と同等の性能を発揮します。 Apple Store でアプ リを作成して配布するプロセスは Google Play よりも複雑です。そのためリリースの時間が長くかかる予定です。

Phore 財団の設立

Phore 内に長期的な電子商取引ソリューション・投資・パートナーシップを構築するための研究所が設立します。その目的は Phore を持続的に発展させることで、様々な課題に迅速に対応し、要として働くことです。 Phore 財団の一部である Phore ラボは世界中の個人、大学、新興企業、および協同組合による最先端のデジタルサービス・製品を特定するインキュベーター/初期投資家として働きます。

Q3 2018 Milestones

スマートコントラクトの統合

スマートコントラクトは Phore をまったく新しいレベルの能力に導きます。 そのとき Phore はもはや単なる暗号通貨ではなくなり、Phore ユーザーは、ブロックチェーン上で実行され、ブロックチェーンと統合された分散型アプリケーション(dApp)を作成・コンパイル・実行することができます。

ユースケースとして考えられる単純なものは、Phore マーケットプレイスにおいて Phore スマートコントラクトがエスクローや購入をサポートします。これによりマーケットはより安全になり、契約の不履行を減らすことができるように

なります。マーケットはリリース時から仲裁の能力を持ちますが、スマートコントラクトは仲裁人を不要にするかもしれません。他にもクラウドファンディングの場合、収集された資金の回収・エスクローを管理するスマートコントラクトを作成し、所定の期間内に十分な資金調達レベルに達したときに自動で配布を行うことや、必要条件が満たさなかった場合 Phore を自動的に払い戻すことができます。

Phore Smart Contract プラットフォームは、非常に強力で、より高度なユースケースとして、Phore のブロックチェーン上で実行されるスマートコントラクトを用いた新しい分散型ビジネスモデルが含まれる可能性があります。 分散型暗号通貨取引所・トラストレスな予測市場・ホームシェアリングのアプリなど・小さなアプリケーションから数え切れないほどのさまざまなサービスにおいて分散化された Phore アーキテクチャ・プログラム制御・匿名性・セキュリティを用いることが出来ます。

スマートコントラクトをサポートするための最初のアーキテクチャアップグレードは、サイドチェーンをサポートすることです。 これによりスマートコントラクト機能を Phore メインブロックチェーン(メインチェーン)に直接追加するより多くの利点があります。 Satoshi Nakamoto が Bitcoin を作成したとき、あるユースケースに対してコインを最適化することで、異なるユースケースへ最適化する能力を失うこと、つまり高速かつ匿名・スケーラブルなブロックチェーンと非常に柔軟かつ堅牢なスマートコントラクトチェーンはその目的に対して最適化された意思決定を持つために同ーチェーンではなしえないことに気付いたのです。 そのため、 Phore ではメインチェーンからスマートコントラクトのためのサイドチェーンへ移動し、後にメインチェーンへ戻ることでこの制限を取り除きました。こうすることで各チェーンはその目的のために最適化することが出来、何かを犠牲にする必要はなくなります。この手法は 2017 年に起きた DAO, パリティの悪用などの Ethereum スマートコントラクトの初期段階で起きた問題を解決するのにも役立ちます。

サイドチェーンのサポートは、Phore が他のユースケースに最適化された他のサイドチェーンを追加できるようにすることも出来ることは重要です(最初にスマートコントラクトに対して最適化します)。

Phore では、メインチェーンから双方向に Phore スマートコントラクトサイドチェーンに移行し、スマートコントラクトに資金を提供できます。メインチェーンでは、資金が Phore スマートコントラクトチェーンのマイナーの持つ特別な住所に送られ(デポジットされ)るように見えるので、Phore のメインチェーンから見ると通常の Phore のトランザクションとして表示されます。1年に数回スマートコントラクトサイドチェーンから Phore のメインチェーンへ引き戻すことができます。長期間の予告期間があり、各引出しの承認は投票により決まります。

この不規則な引き出しのスケジュールは、スマートコントラクトチェーンのマイナーがスマートコントラクトを悪用する際にそれを阻止し、何が起こっているかを調べ、対処するのに時間を必要とするからです。悪用が成功させる唯一の方法は、スマートコントラクトブロックチェーンの大部分のマイナーを手に入れることです。

このような引き出しスケジュールは、スマートコントラクトを使用して Phore コインを自由に利用したいと思う人にとっては非常に不便に見えるかもしれませんが、我々が提案するアーキテクチャは、スマートコントラクトのサイドチェーンとメインチェーンです。これがアトミックスワップのサポートを構築しようと考える理由の 1 つです。

Phore サイドチェーンの実装の詳細については、後にリリースされる予定です。 技術的な内容を知りたい方は、Drivechain Project と Blockstream の共同設立 者の次の参考文献に記載されている拡張機能のほとんどが説明されています:

https://blockstream.com/sidechains.pdf

https://github.com/drivechain-project/docs/blob/master/bip1-hashrate-escrow.md

https://github.com/drivechain-project/docs/blob/master/bip2-blind-merged-mining.md

サイドチェーンを利用できるようにした後、最初の Phore サイドチェーンとして Phore スマートコントラクトブロックチェーンを構築します。

Phore スマートコントラクトプラットフォームにより、ユーザーはプログラミング機能・状態変数・外部データを含む複雑なトランザクションをスマートコントラクトとして記述できます。これにはマーケットプレイスでのエスクローやクラウドファンディングでのクライアントインターフェースも含まれており、スムーズなユーザーエクスペリエンスを提供します(例: 資金を売り手に開放したり、問題があれば買い手に戻す)。Phore スマートコントラクトプラットフォーム上で最初に作られるスマートコントラクトはマーケットプレイス・クラウドファンディングアプリの機能を強化・保護するものになります。ユーザーは他のアプリ・ビジネスを可能にするために独自のスマートコントラクトを作成・コンパイルできます。

スマートコントラクト機能を実装し既存のスマートコントラクトの機能を構築・強化するためのコアコンポーネントをいくつか構築していきます。そのほとんどは Ethereum のフォークから始まるもので、これらのコンポーネントは次のようなものです:

- ●ツールやインタフェース:
 - ➤ GUI(ウォレット・ブラウザ)
 - ▶ クライアント
 - ➤ JSON RPC 接続
 - ➤ dApp の枠組み
 - Compilers
- ●スマートコントラクトプロトコルは次のものをサポートするでしょう:
 - ▶ P2P ネットワーク
 - ▶ ノードの検索
 - ▶ 暗号化された相互通信
 - ▶ 仮想マシンのコンテナ
 - ▶ スマートコントラクトブロックチェーン(マイニング, コントラクト, トランザクション, アカウント)

- ●分散型ストレージ
- ●分散型メッセージング

アルファ・ベータ版テストにおいてスマートコントラクト機能の最小限実行可能な製品(MVP)を提供し、起動時にプラットフォームで見る特定の機能について、Phore コミュニティでフィードバックを収集することに集中していきます。可能な限り、zk-SNARKSのゼロ知識証明を活用し匿名型スマートコントラクトをサポートするなどのプライバシー保護機能をさらに強化し、Phore に既に組み込まれている匿名化機能へ統合する予定です。

サイドチェーンと同様に、私たちは開発を進めつつ Phore での実装を説明したより詳細なテクニカルホワイトペーパーを執筆します。第3四半期には、第4四半期の正式リリースを目指してアルファ・ベータ版のテストを実施する予定です。

アトミックスワップの統合

Phore はまず、スマートコントラクトサイドチェーンのサポートに必要なコア機能の1つとして、アトミックスワップの統合を実施する予定です。また、Phore と他の主要な暗号通貨との間の直接的なアトミックスワップをサポートし、Phore をより使いやすく利用できるようにする方法を模索する予定です。

分散型クラウドファンディング

最近では大規模なクラウドファンディングサイトがキャンペーンを審査する際に政治的な偏見を持っているという嫌疑を受け、停止することが起きています。この種の問題は中央集権的なクラウドファンディング会社において起きうる評判の危険性を表しており、この問題が分散型のクラウドファンディングに人を呼び込む際の糸口になると考えています。このプラットフォームでは企業による許可や政治的な検閲は必要ありません。貢献度に関係なく支援を行いたいと考える人にも大きなメリットになると我々は考えています。

Phore クラウドファンディングは完全に分散化され、Phore の匿名性で守られ、Phore マーケットプレイスに直接統合されます。資金調達を探しているプロジェクトは、自分のプロジェクトを記述する情報やオプションを追加して、Phore マーケットプレイスに公開することができます。ユーザーはキャンペーンを閲覧し、必要に応じて zPHR のプライバシー機能を利用して資金提供を匿名化し、必要に応じてプロジェクトが製品を送信するために必要な情報のみを共有することが出来ます(情報を必要とするキャンペーンにのみ用意)。ハッキングされたり、他の人に情報が漏洩したりする可能性のあるプラットフォームではありません。全ては分散化されるため、Phore クラウドファンディングのキャンペーンに伴う料金が大幅に減ります。

クリック&コレクト-ベンダー連携プログラム

1 か月からの長期のプロジェクトとして、購入者がオンラインマーケットプレイスで商品を注文し、自分の都合に合わせ都市のベンダーで直接商品を回収することが出来ます。

Q4 2018 Milestones

スマートコントラクト統合

ロードマップの第3四半期で説明したように、第4四半期には Phore スマートコントラクトプラットフォームを開始します。 このロードマップは、Phore マーケットプレイスと Phore クラウドファンディングでのオプションとユーザ

ーエクスペリエンスを強化するスマートコントラクトの初期実装を含みます。また全ての Phore ユーザーにスマートコントラクトの使用方法が公開されます。

モバイルアプリ開発

iOS/Android のウォレットをより洗練したものにします。Phore プラットフォームの開発で実装された高度な機能への対応のため、モバイルウォレットも利用できる機能を拡大します。

VR/AR マーケットプレイス強化 – βテスト

VR/AR を用いたパラレルなマーケットプレイスの実証実験をオープンに行います。これはヘッドセットなしで実施され、究極的な購買体験を提供します。

マーケットプレイスへのクリック&コレクトの一部導入

第3四半期に試験的に導入したサービスの導入により、オンライン市場での 購入後の物品をオフラインのショップでの持ち出しを可能にします。当初の展開 は3~5都市を目標とし、2019年にはより広範囲での対応が予定されていま す。

Phore ラボによる投資活動

10 個までのデジタル製品・サービスに対して投資を行います。Phore の通貨で投資を行い、最初期は Phore のマーケットプレイスでの独占販売権を取得し、一定期間後にオープンに販売できるようにします。この商品の売却による利益を用いてラボラトリープロジェクトに再投資し、様々な商品の市場への到達を助けます。

2019の目標

モバイルウォレットの更なる機能追加・VR/AR機能のフルリリース・Phore ラボプロジェクト・個人、企業とのパートナーシッププロジェクトや更なるサイ ドチェーンなどの 2019 年以降の Phore の向かう先のアイデアを考えています。

しかしチームは過去の経験からコミュニティによるフィードバックは、コミュニティのニーズを満たすような製品のビジョンを導くことを理解しております。 そのうえで我々は Phore の価値を最大限高める機能に対して取り組んでいきたいと考えています。

Phore コアチーム

2017年10月のローンチ以来、チームは多くの分野において急速な成長を遂げました。Phore は KTK のリブランドとして開始され、Phroshi と計 5 人のアドバイザー(あくまで名称で、実際の役割は異なります)がチームでした。しかしこれでは不十分だったので、将来目標のためにチームを拡大する必要がありました。そして3か月ほどが経ち、チームはいま大きく成長しました。現在は25人以上の公式メンバーを保持しています。この人数は Phore の進歩を助けると思われる人々を見つけるにつれさらに増えていくでしょう。

現在のチーム:

Co-CEO:

Anthony Alleyne – Ubermaster(UK)

Thomas Ambler – Sage(UK)

CTO:

(匿名)-Moonshot(US):フルスタックエンジニア

Head of Operations:

Shant Kel Khatcherian – Shanto(CA)

開発者:

(匿名)-Phroshi(UK)-設立者兼開発リーダー

Julian Meyer (US):コア開発者

(匿名) - Jacob (US): 期間有開発者

(匿名): Iced (NL) - 期間有開発者

アドバイザー:

Shunsuke Kurita - Liray-Unendlich (JPN)

Harrison Fischberg (US)

(匿名) - Toby (CA)

(匿名) - King (US)

(匿名) - Hman (US)

法対応:

(匿名) - Willich (UK)

(匿名) - Margo (US)

マーケティング:

Pamela Paige - ThePinkCrypto (US) - マーケティングリーダー

Ramon Freriks - Ramon (NL) - マーケティング / フロントエンド開発者

llies Graffion - La_Moque_e (FR) - グラフィック

Snatch (GER) - ソーシャルメディア管理

Milky (GER) - ソーシャルメディア管理

調整 / プロジェクト進度管理:

Flipster (UK)

ブランディング・連携:

Crypto_NL (NL)

ビデオコンテンツ制作:

Zak.R (UK)

ベンダー関連:

CryptoJoe (US)

研究:

Keyser (US)

コミュニティ管理:

Jesse (US)

チームに関する詳細は https://phore.io/team をご覧ください。Phore はチームを強化するためにより多くのスタッフ・開発者の雇用を積極的に検討しており、日々拡大・発展していきます。

Phore のコミュニティへ参加してください

私たちはすでに通貨 Phore とコミュニティを構築しています。その反応は信じられないほどのもので、毎日のように多くの人々がコミュニティに加わり貢献しています。2018 年は Phore が最も開発が進み、強力なアプリケーション・サービスのエコシステムを持った安全で柔軟性の高い匿名型暗号通貨になる年であることを期待します。

Phore はビジョンを達成するためのロードマップを既に決めており、皆様のコミュニティへの参加を心より歓迎します。もし Phore をよりよくする方法についてアイデアがあれば、いつでも教えてください。開発・ユーザーインターフェースの設計・Phore のロードマップ・予算・設計の方向性について議論することでコミュニティ全員の寄与を我々チームは期待します。

あなたのお金を中央集権から取り戻しましょう。ウェブサイトから Phore ウォレットをダウンロードし、Discord に加入し、我々のコミュニティへ参加してください。

リンク

Official Website

phore.io

Discord

https://discordapp.com/invite/Aucncz5

Bitcointalk

公式

https://bitcointalk.org/index.php?topic=2307909.0

日本公式

https://bitcointalk.org/index.php?topic=2242113

Slack

https://phore-project.herokuapp.com

Twitter 公式 https://twitter.com/phorecrypto 日本公式 https://twitter.com/PhoreJapan Facebook https://www.facebook.com/Phore-1996158580662988/ Github https://github.com/phoreproject/Phore Block Explorer https://chainz.cryptoid.info/phr/# サードパーティのマスターノードシェアサービス https://www.hostmns.net/phore-pool

取引所・統計データ

https://www.cryptopia.co.nz/Exchange/?market=PHR_BTC

https://coinsmarkets.com/trade-BTC-PHR.htm

https://coinmarketcap.com/currencies/phore/

https://www.coingecko.com/en/coins/phore#panel

https://bitcointalk.org/index.php?topic=2307909.200

https://scrypto.io/s/mns-phore/

Forum

https://forum.phore.io

Ask Me Anything - Nov 11th, 2017

https://medium.com/@fishfish313/phore-ama-ask-me-anything-on-

november-11th-2017-f69eccb91eb1

Facebook Fan Group

https://m.facebook.com/groups/249350618927881/

Bitcointalk Fan Page

https://bitcointalk.org/index.php?topic=2461070.0

Telegram

https://t.me/joinchat/F0zLDwzFC8r91eem6x_cBQ

Crypto Delver

https://cryptodelver.com/coin/phore

Masternodes.online

https://masternodes.online/currencies/PHR/

Masternodes Pro

https://masternodes.pro/stats/phr



(c) Phore 2018