皆様、こんにちは。IOHK の CEO、チャールス・ホスキンソンです。
このレコーディングの目的は、現在進行中のカルダノ・プロジェクトについて話す事と、発生したいくつかの遅れについて説明することです。私たちは間もなく、多くの情報をテキストの形式で公開する予定です。

カルダノ・プロジェクトについて

はじめに、私たちは Testnet の 5 番目のバージョンを準備中です。これは大幅なアップデートになります。Ed25519 カーブ（楕円曲線）を使って HD ウォレットを作成したのはすべての人にとって初めてのことです。また、TLS(トランスポート・レイヤー・セキュリティ)、いくつかの新しいトランザクションフォーマット及び hood 下の他の機能一式を実行し、Daedalus ウォレットとカルダノプラットフォーム自体はより緊密な統合が出来ます。**この Testnet リリースの目的は、Testnet をできるだけメインネットに近づけることです。**そうすることで、メインネットを準備しローンチするためのプロセスを開始できるのです。

Ed25519 は、ツイストしたエドワーズ曲線を用いたエドワーズ曲線電子署名アルゴリズムの実装の一つである。
https://ja.wikipedia.org/wiki/%E3%82%A8%E3%83%89%E3%83%AF%E3%83%BC%E3%82%BA%E6%9B%B2%E7%B7%9A%E3%83%87%E3%82%B8%E3%82%BF%E3%83%AB%E7%BD%B2%E5%90%8D%E3%82%A2%E3%83%AB%E3%82%B4%E3%83%AA%E3%82%BA%E3%83%A0

スケジュールについて

現在、私たちは**メインネットのローンチを"Byron"と呼んでおり、7 月から 8 月の間にメインネットのローンチを望んでいます**。 これは、現在の開発リソースを使った場合の最善の推定値です。

私たちは予定より遅れてしまいました。私はこの録音で過去の数ヶ月間に何が起こったのかを説明したいのです。良いこともあればあまり良くないこともありましたが、すべてを克服することができました。

最初に、カルダノ財団の監査した上でアテインコーポレーションが行ったカルダノセールは大成功でした。KYC と AML を通過したユニーク人数は約 1 万人で、14,000 件以上のセールがありました。
売上がありました。そのプロセスを経て、膨大な量のデータが生成されたため、全ての情報を保持していたデータベースは、正確性や重複したアカウントや不正確な情報などのチェックを受ける必要がありました。

プレセールの終了は一月下旬で、そして 2 月いっぱいかけて終了処理や監査を行いました。私たちは 3 月に実際の自動ベンディングに移行しました。

それでは、ベンディングは何か？ ベンディングは、私たちが暗号化を開始したプロセスで、このケースでは RScoin でした。実際に暗号資産に接続された差引残高.を保つためにトークンを発行するために使用しました。

通常、これは ERC20 のようなイーサリアムトークンで行われますが、カルダノを提案したときにイーサリアムはまだローンチされていないので、この独自の目的のために構築されたより小さなブロックチェーンを使用することでした。

だから私たちは RScoin を実行しました。 私たちは 3 月上旬にそれを稼動させることができました。そして、3 月の大半の時間は皆のベンディングを行いました。
交換者の約 93%が自身でベンディングを行っており、残りの 7%が自身で作業をしない強制ベンディングも行いました。ここで、代理店が証明書を作成して送付しました。

私たちは開発ライフサイクルを考えていたところから 8 週間ほど遅れています。
我々はもともと、カルダノのメインネットを 3 月頃に出来上がると最初の見込みでした。

遅れていた要因の第一点目として、**ベンチマーク、ストレステスト、およびホワイトペーパーの最適化、さらにはシステムの心臓部であるウロボロスの最終的なデザインに多くのリソースを費やした研究であった事です。**尚且つ、学術出版に適しており、ピアレビューも通って、これまでの努力はやっと成功しました。

良いニュースの一部としては、ウロボロスが Crypto 17 の PoS アルゴリズムとして受理された最初の暗号化プロトコルであり、8 月に米国サンタバーバラ（米国カリフォルニア州）で発表の予定です。

次に、カルダノプラットフォームを作成するために使用したコード言語は **Haskell です**。
Haskell は非常に複雑な言語です。これは、過去 10 年間で工業用アプリケーションが見つかっていますが、主に学術プロジェクトに使用されています。 Haskell を選んだのは、最終的に正式な検証と基盤プロトコルの仕様策定に向けて最速かつ簡単に手を差し伸べることができるからです。
これは当然のことですが、欠点は、特定のライブラリや特定のコア技術、特に開発運用（オペレーショ

ン）側で Haskell が未熟なことです。
この結論により、ここ数カ月間に多くのハードルに遭遇しました。ライブラリを整理し改善する必要があり、開発プロセスをクリーンアップして改善も必要でした。開発メンバーすらも入れ替えをする必要がありました。残念なことですが、これは Haskell が一番未熟な部分です。
良いニュースは、時間がかかりましたが、私たちはこれらの問題を克服し、本当に堅牢なプロセス、優れたソフトウェア、そしてほとんどの課題をクリアでき、かなり良いチームを構築することもできました。

もう 1 つの遅れた原因は、いくつかの暗号プリミティブに関わることでした。カルダノプラットフォームでは、ビットコインで使用されていたものとは異なる楕円曲線暗号を使用することを選択しました。 ビットコインは、secp256k1 という曲線を使用します。
これは大きな曲線であり、多くのアプリケーションと多数のライブラリを持ち、非常にうまくいっています。残念ながら、このカーブは使用したいアプリケーションには最適ではありませんので、Ed25519 という別のカーブを使用することにしました。
妥当であると思われる非常に優れた仕様が存在しますが、誰も Ed25519 の HD ウォレットを作成したことはありませんでした。
だから私たちの遅れの一部は、実際にこの特定の曲線の HD ウォレットを実行し、その実行性を適切に監査するという困難な作業をしていました。これを行う能力のある専門家はほんの一握りであるため、私たちはそれらの専門家がそのコードを検証してもらうまでに待たなければなりませんでした。
これらの専門家は RPI sec という場所のレンセラー工科大学にいました。それには時間がかかりましたので、ADA ユーザーの保証のためにこれらの時間を費やしました。私たちは、作業が既に正しく行われたことを非常に確信しています。
今後登場するテストネットは、HD ウォレットの最初のリリースとなり、TLS と同様に新しいネットワークの改良がリリースされます。我々がプロトコルに入れている他の多くのものもリリースされる予定です。

最後の遅れはカルダノのために選んだアーキテクチャが原因です。
アーキテクチャは 3 段階モデルで、バックエンドで Haskell ベースのサーバーを実行していましたが、PureScript タイプブリッジがあり、次に Chrome とノードの両方を組み合わせた電子というコピーを実行しました 。このアーキテクチャは、Chrome とノードのエコシステムのすべてを活用してユーザーエクスペリエンスやユーザーインタラクションロジックに Javascript を使用できるようにしてくれているため、非常に堅牢ですが、他のすべてに対して Haskell を使用することもできるミッションクリティカルなソフトウェアです。
挑戦は、このアーキテクチャを組み合わせることで、すべてを正しく会話しなければならなくなりました。

これは、開発者自身が異なる分野のコンピテンシーを持っているため、予想以上の時間がかかりました。

Daedalus 側で働く開発者は主に javascript 開発者であり、Haskell 側で働く開発者は主に Haskell 開発者であり、これらの 2 つのセットの間には文化的、知識的、技術的な違いがあります。 その隙間を橋渡し、それらの文化を橋渡しする必要がありましたが、それを行う方法を見つけることができました。
私たちはずっと克服してきました、そして私たちはすごく成長しました。
IOHK は現在、東京工業大学、エジンバラ大学、アテネ大学の 3 つの研究センターを運営しています。これらのセンターには驚異的な研究を行う数多くの偉大な暗号学者がおり、研究はカルダノに焦点を当てており、私たちはそれがどこへ行くのかを見て非常に興奮しています。

だから、メインネットが立ち上げられたらどこへ行くの？ メインネットはどういう意味ですか？

まず、人々が購入した ADA を還元して取引できることを意味します。第二は、Daedalus ウォレットを使用して ADA とのトランザクションをダウンロード、インストール、送信することができ、ブロックチェーンエクスプローラやその他の資産でそれらのものを検証することができます。しかし、より広義に言えば、私たちは現在ライブ暗号化を反復する立場にあるということです。
私たちがソフトウェアを開発する方法、私たちが持つプロセス、これらの事柄はすべて時間の経過とともに変化し、今年もカルダノの生態系にさらに頑強さと価値を付加していきます。
まもなく重要なマイルストーンを概説するロードマップを発表します。
私たちは Cardano SL のマイルストーンに名前をつけました。これは、ADA の財務レイヤーなので、Poets の後に、Byron はメインネットのリリースになります。年内の次のリリースは Shelley で、これには多くのアップグレードが含まれ、相互運用性とスケーラビリティの大幅な改善は見られます。

そして、来年後半には財務レイヤーを完成させる 2 つのアップグレードがありますが、スマートコントラクトが実行される演算レイヤーと、ゲームやギャンブル、規制された活動などができます。来年予期される 2 つのリリースです。
1 つは Backus で、次世代の EVM に焦点を当て、ゲームやギャンブルのための特別な MPC を追加するとともに、高保証スマートコントラクト用に開発した新しいプログラミング言語のフルバージョン Plutus です。 Milner と呼ばれる第 2 のバージョンは、信頼性の高いハードウェアとスケーラビリティの向上に焦点を当て、標準ライブラリと App 開発環境の改善にも取り組んでいきます。

私たちのロードマップは、これらのことをより詳細にカバーしますが、
この録音の目的は、私たちが最終的に本当にうまく実行していることを皆に保証することです。
遅れて申し訳ありません。大変厳しい環境を重々承知します。
私はそこにいまして、私は 10 カ国以上のチームを調整していたので、他の誰よりも厳しいと信じていました。私たちは Byron を誰より先に生み出すことを非常に熱望しています。

テストネットついて

そして、今まで Testnet 上でただ 3,000 人だけは ADA を還元しました。Daedalus をダウンロードするには、可能な限り多くの人がテストネット上でバウチャーを利用することをお願いしたいのです。これは、証明書が正しいこと、ベンディング中に何も障害されないこと、ソフトウェアを実際にインストールして使用できるという保証を高めることができます。
もしソフトウェアをインストールして使用することができないなら、私たちが物事を修正するオプションと機会が少なくなります。ですので、メインネットが正式に起動する前に、今のうちにテストネットを試して願います。
たとえば、破損した証明書があり、購入者が復旧オプションを選択しなかった場合、ADA を元に戻す方法はありません。
特に購入者にとっては、ネットワーク上の証明書、テストネットを使ってできることを検証することが非常に重要です。これが唯一の機会であり、メインネットの立ち上げるまでに、何かを行う可能性があるからです。

もう 1 つは、ユーザーのストーリーやユーザーの構成を本当に知りたいことです。例えば Mac ユーザー、Linux ユーザー、Windows ユーザーの各のユーザー数、Windows のバージョン、 基礎となるハードウェアなどです。テストネットの結果によって、我々が集中すべきシステムに関するより良いデータを提供します。また、メインネットに近づくため、開発チームが計画する必要のあるデータも参考になるからです。

皆様のご質問に対してのお答えになったら幸いです。
今後もカルダノ財団から情報を公開していきます。
今月は忙しい一か月になり、来月はもっと忙しくなります。
皆のお時間、ご理解、本当にありがとうございました。
良い一日を！