はじめに

火と霜 - 科学の無知、物理的環境の軽視、人間の潜在能力の育成の失敗 - 私たちはもうそのような余裕はないのです。

Atala PRISM：ファウンデーションへようこそ。私たちは、今日のアイデンティティ、そして未来のアイデンティティを探求する旅に、皆様をお連れできることを楽しみにしています。以下の資料では、デジタル世界におけるアイデンティティの複雑さを探求し、現在使用しているシステムをどのように改善できるかを概説することを目的としています。

私たちが何者であるかは、個人的で親密なものです。それがオンライン上で企業やサービスとより密接に絡み合うようになっても、私たちを個人たらしめるものを保護する方法は見つかっています。多くの場合、私たちはアクセスや利便性のために、自分が何者であるかをコントロールすることを放棄しています。今日、私たちは岐路に立たされています。数百万ドル、数十億ドルの企業が私たちのアイデンティティとデータをコントロールすることを許す道を進むのか？それとも、私たちは自分のアイデンティティとデータを管理できるようになるのでしょうか？

ブロックチェーン

過去15年間、新たなテクノロジーが、ユーザーが自分のアイデンティティを管理できるようにするための扉を蹴破ってきました。ブロックチェーン技術は、革命的な発展を遂げました。ブロックチェーンの話題で多くの人が思い浮かべるのは暗号通貨であり、それらは不可欠なものですが、ブロックチェーンが提供する実用性はそれだけではありません。

ビットコインは、適切なタイミングでの火付け役でした。2009年、2008年の世界金融危機の余波の中で、その誕生は金融の独立を可能にし、ポータビリティ、アクセス、そして従来の銀行システムに代わる選択肢を生み出しました。当初は、ビットコインは実現不可能で価値がないと多くの否定派が言っていました。現在では、多くの人々、企業、そして国までもがビットコインを法定通貨として使用し、受け入れています。

実用性を論じる中で、ビットコインの話が参考になる。サトシ・ナカモトが概念化したブロックチェーンというツールがあり、このツールは新しい金融システムの構築に不可欠であり、金融危機というニーズがあったのです。ブロックチェーンと新しい金融プロトコルの組み合わせは、ブロックチェーン技術における長いイノベーションの最初の一歩となりました。

ブロックチェーンとは？「天空の台帳」と呼ばれるものです。分散型サーバーと考えてください。つまり、一個人が情報を管理したり、持っているわけではないのです。数百、数千のノードに分散されます。ノードはすべてのデータの1つのコピーであり、情報の整合性と分散性を強化します。これらのノードは、ブロックチェーンをサポートするネットワークを形成するために協力し合う。また、ブロックが作成される際に、ブロックの検証も行います。これにより、チェーンに書き込まれる情報が正確であることを保証します。チェーンの一部が停止しても、ネットワークに多くのノードが存在する限り、チェーンはアクティブに動作し続けることができます。

ブロックチェーン上の各ブロックは、トランザクションを格納するコンテナとして機能します。ブロック内の各取引は、様々なものを表すことができます。多くの人に馴染みがあるのは、金銭の取引だろう。ADAを購入すると、その取引は、購入／売却を含む他の数十の取引とともに、カルダノ・ブロックチェーンに書き込まれる。これらはブロックを形成し、ノードによって検証される。検証は、ネットワーク（全ノード）に分散されるデータが本物であることを証明するため、非常に重要である。

この議論は、アイデンティティについての議論にはふさわしくないように思えるかもしれませんが、そうではありません。私たちは、後で紹介されるコンセプトの基礎を築いているのです。ビットコインやブロックチェーンに関連する自然発生的な思考の1つは、ユーザーがそれを信頼し、安全で

検閲に強く、ポータブルであると信じていることです。中には、生まれて初めて金融システムにアクセスすることを許可された人もいます。これらの点は、マーケティングや話のネタとして捨ててはいけません。コンセプトをさらに掘り下げながら、なぜそれが自己主権的なアイデンティティに不可欠なのか、そしてそれがどのように可能なのかを議論していきたいと思います。

このようなささやかな先見性がなければ、倫理的規範は私たちの行動を導く力はほとんどないように思われます。なぜなら、時代を超えて普遍的に拘束力を持つ倫理的原則であっても、今日その原則を採用することが、明日の私たちの生活の質をどのように維持し、豊かにするかを想像できることが前提となっているからです。

アイデンティティとは何か？

アイデンティティとは、私たちが誰であるかを示す本質です。人種、性別、民族、生年月日などの不変の特徴と、オンラインアカウント、銀行口座、携帯電話会社などの可変のペルソナ（人格・個性・人間性）から構成されています。日常生活を送る中で、私たちが関わるすべての人、すべてのものが、私たちのアイデンティティの一部と融合しています。
とに抵抗がある場合は、それを強要されるべきではありません。この考えは、地球を揺るがすような大発見ではありませんが、決断するのは私たちであるべきだということを忘れてはなりません。

私たちは、自分が誰であるかということと、認証される自分についての情報を区別することができるはずです。私が好きな色は青だと言えば、それは正確かもしれませんが、それを証明する方法はありません。年齢を証明する必要がある場合、それは政府の身分証明書や出生証明書で認証できることです。

例えば、私がアクメ銀行の口座を持っているとしましょう。私がアクメ銀行の口座を持っているので、彼らは私のことを知り、私がいくらお金を持っているかを知っています。もし私がメガバンクに行き、私の資金を要求したら、彼らは私や私の資金についての記録を持たず、おそらく私が銀行を襲おうとしていると考えるでしょう。おかしな話だと思うかもしれませんが、そうなのです。私たちは自分の口座にアクセスするために別の銀行に行くのではなく、自分が知っている銀行に行くのです。この書類は私たちそのものではありません。しかし、それは私たちに関する何