



ハイパフォーマンスの実現へ

訂正が不可能なブロックチェーンを訂正する

ビデオトランスクリプト

新たな訂正機能は、企業にとってのブロックチェーン技術の課題を解決し、実用性を向上させます。

ブロックチェーンは基本的に変更不可能なものとして設計されています。そのため金融機関にとっては必ずしも利用し易いものではありません。コーディングや取引で間違いは発生しますし、データ保持にかかる労力やコストも抑えなければなりません。規制対応のためにデータの変更や削除が必要なこともあります。

訂正機能についてご説明しましょう。

ここにひとつのブロックチェーンがあります。それぞれのブロックはハッシュ値によって鎖のように接続されています。ハッシュは、特定のアルゴリズムに通すことにより、各ブロックに保管されているデータから、次のようにユニークな固定長文字列を生成します。

```
465f9e22832e5c88f4b140db82c459064711a52182a3e438b4ebc7ecda62b9bb
```

データが記録されたブロックは、暗号化された監査証跡を使ってブロックチェーンの参加者に分散されます。監査証跡は、ブロックを独立してチェックする別のユーザーにより検証・保持されます。

「真実」を一意的に共有することが可能であるところに、ブロックチェーンの実用性の根本があります。データが変更されると、ハッシュ値が変更され、参加者全員に共有されるのです。

訂正機能は、「パーミッションド・システム」と呼ばれるシステムで使われます。このモデルでは、権限を与えられた特定のユーザーのみが厳格な規定に基づいて、変更を加えることが出来ます。特別なハッシュ関数は、ブロック間のリンクのロックを解除して変更を可能にし、変更の履歴を残して再度ロックをかけます。

このように適切なガバナンスにより、記録の修正、コスト管理、そして規制の遵守が可能となります。

ブロックチェーンの機能が貴社にとってどのような可能性もたらすか、ぜひアクセンチュアのレポートをご一読ください。