自身のアイデンティティ究極保護

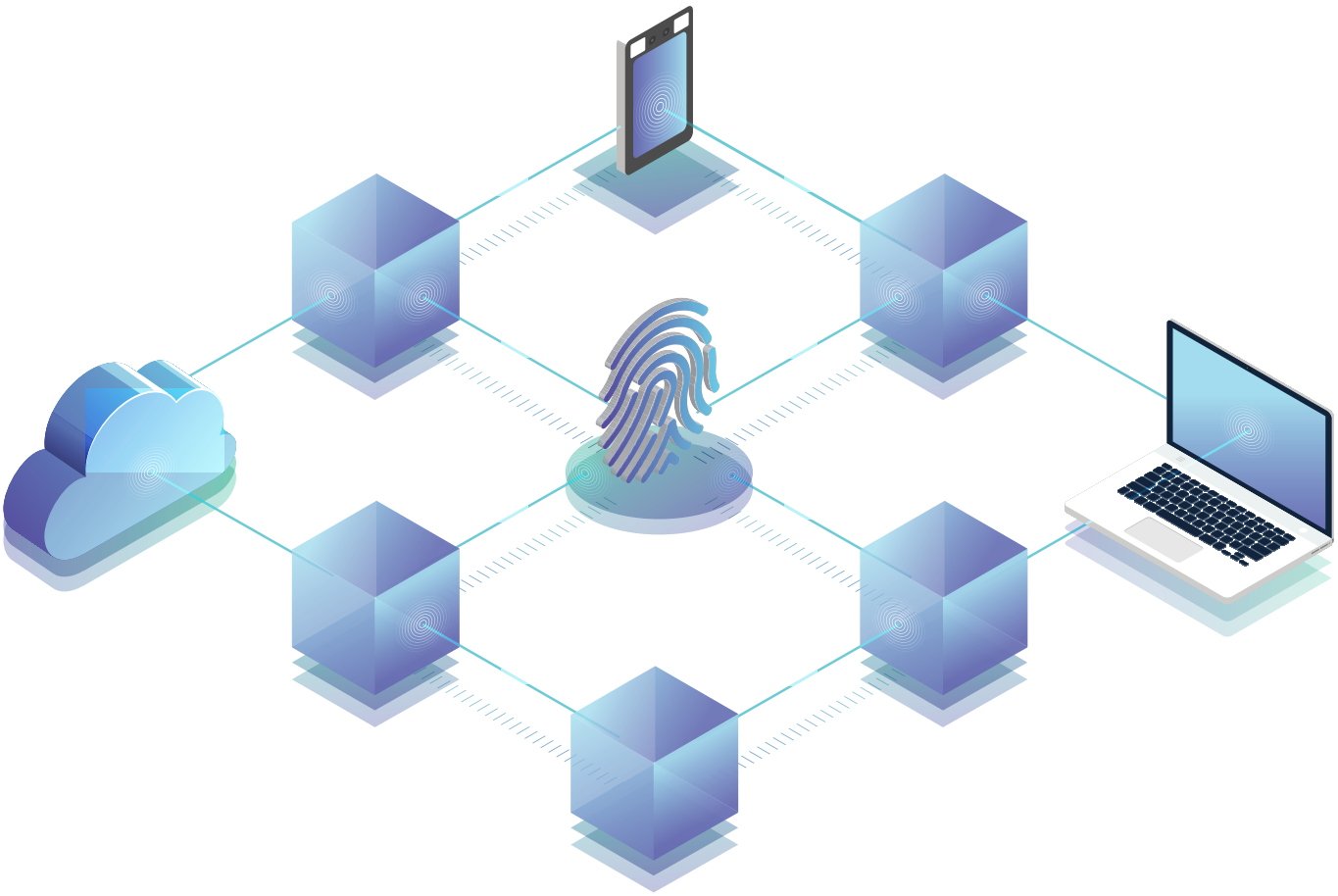
ブロックチェーン保護バイオメトリクス

イーサリアムプラットフォームを搭載

バックグラウンド

ブロックチェーンは、人々として近年最もホットなテクノロジートピックの1つです。それに多くの注意を払い始めました。ビットコイン以来（最初の暗号通貨は 世界）2009年にこのテクノロジーを最初に適用し、独自のP2P通信方式で、 タイムスタンプ機能とデータ特性の不変の記録、それは最高保障取引方法。文字通り、ブロックチェーンはハッキングできません センス。もちろん、すべてのテクノロジーには、特に古いテクノロジーには制限があります。ブロック内 チェーン、ブロックの情報フォーマットは標準化され、追加情報はありませんでした ブロックに追加することが許可され、生体認証と ブロックチェーン。

ムーアの法則によると、コンピューターの処理能力は2つに2倍になります 年、ブロックチェーンの開発もそうです。イーサリアムはブロックの重要な概念です。 chain2.0は、ブロックチェーンを拡張することにより、分散化の概念を大幅に拡張します。 の新しい概念を開始することにより、暗号通貨からあらゆる種類のサービスまでのテクノロジー 「添付ファイル」をブロックに追加します。Blockchain1.0では、ビットコインを例にとると、情報 ブロックに保存されている情報は標準化されているため、ビットコイン自体を除いて、他の情報はありません。 ブロックに追加できます。Blockchain2.0、ユーザーはでより多くの情報を追加することができ 「トークン」と呼ばれるブロックの新しい概念を形成するブロック。そして「トークン」は 生体認証とブロックチェーン間の相互作用の鍵となります。



ブロックチェーンとは何ですか？

ブロックチェーンは、チェーン内の誰でも完全にオープンな分散型台帳です。一度 データがブロックに記録されると、変更が非常に難しくなります。

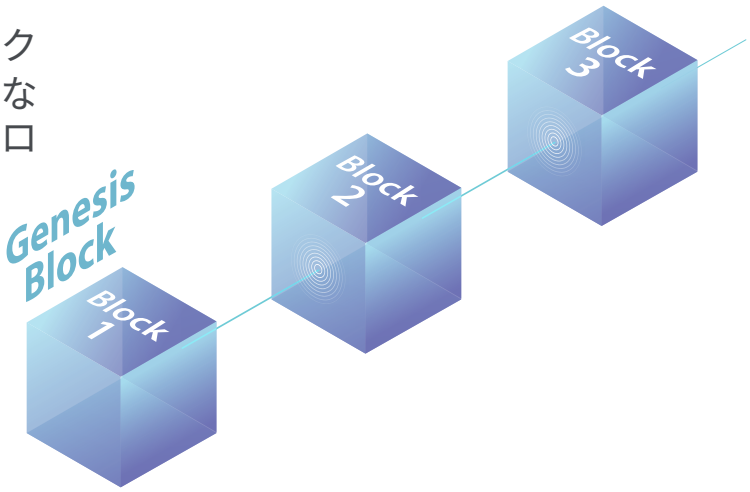
各ブロックには、「データ」、「ハッシュ」、「前のブロックのハッシュ」、データが含まれます ブロック内に保存されているものは、ブロックチェーンのタイプの影響を受けます。たとえば、生体認証 ブロックチェーンは、テンプレートタイプ、登録などの生体認証テンプレートの詳細を保存します。日付、ユーザー名、登録端末SNなど。

各ブロックには一意のハッシュがあり、ユーザーはハッシュによってブロックとコンテンツを識別できます。 ブロックが作成されると、ブロック内に変更がある場合、ハッシュも変更されます。 つまり、ブロックのハッシュがブロックのハッシュである場合、ハッシュはブロックの変更を示します。 変更され、それはもはや同じブロックではありません。

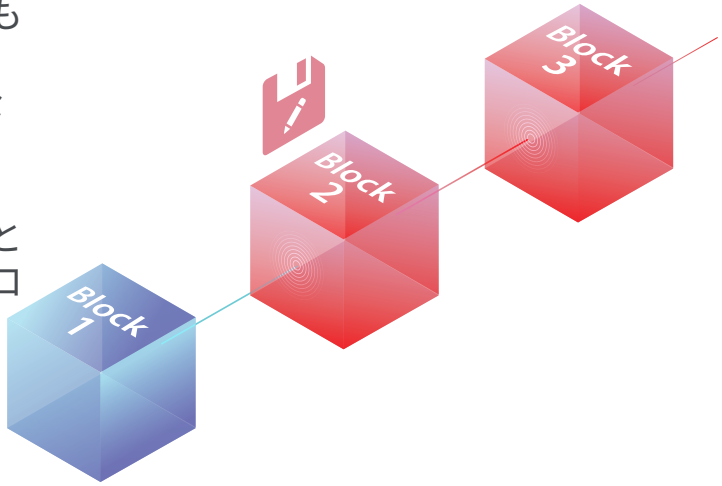
ブロックの3番目の要素は「前のブロックのハッシュ」であり、効果的に ブロックのチェーン、そしてこの要素はブロックチェーンをとても安全にします。

たとえば、ここには3つのブロックのチェーンがあり、各ブロックにはハッシュと、 前のブロックなので、ブロック3はブロック2にリンクされ、ブロック2はブロック1にリンクされます。

ブロック1は以前のブロックにリンクできません すでに最初のブロックなので、ブロックします 「創世記ブロック」と呼ばれます。

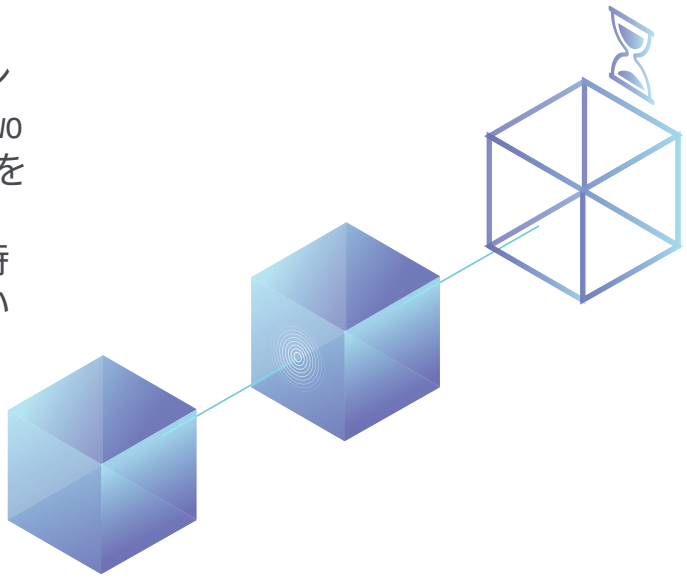


ユーザーがブロック2を改ざんしようとした場合、 ブロックのハッシュも変更します2。 したがって、ブロック3と以下のすべて 保存されなくなったため、ブロックは無効になります 前のブロックの有効なハッシュ。チャン 単一のブロックを使用すると、次のすべてになります 無効なブロック。



ただし、最新のコンピュータの処理能力は非常に高速であるため、 上INGのハッシュはもはや十分ではありません改ざんを防止します。ハッカーのコンピュータは簡単にできます 1秒あたり数十万のハッシュを計算するため、ハッカーは効果的に ブロックを改ざんし、他のブロックのすべてのハッシュを再計算して、ブロックチェーンを有効にします。

この問題について、ブロックチェーンには別の問題があります「Proof of work」と呼ばれるメカニズムは、 作成を遅くするメカニズム 新しいブロックの。たとえば、ビット才oinは 所要時間の計算に約10分作業の証明と新しいブロックを鎖。

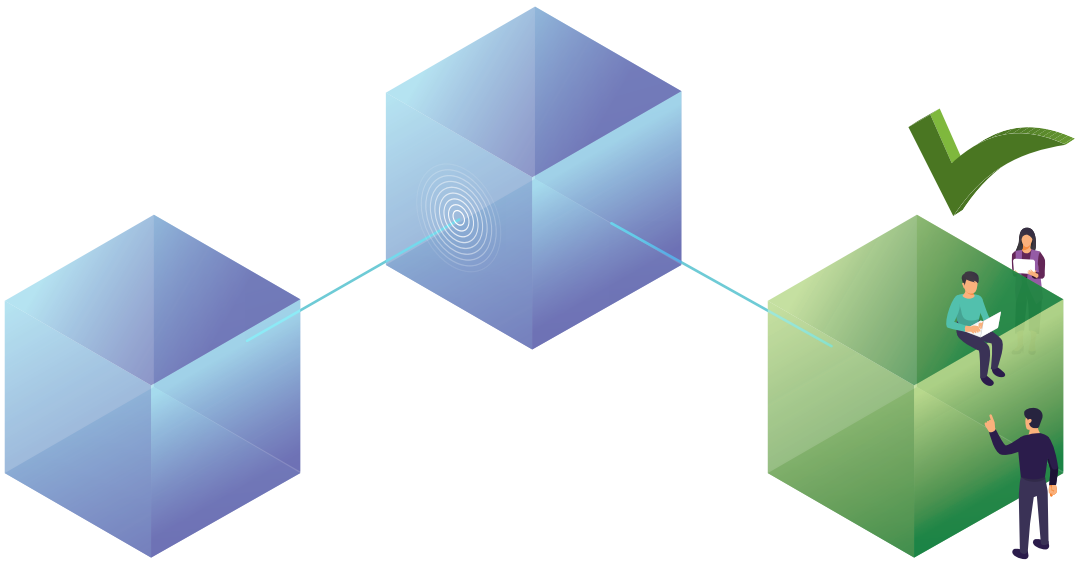


このメカニズムにより、ハッカーがブロックを改ざんした場合、ブロックを改ざんすることが非常に難しくなります ブロック、彼は次のすべてのブロックの「作業の証明」を再計算する必要があります。ある場合 ブロックチェーンでは10,000ブロックが利用可能で、ハッカーがすべてを完了するには100,000分かかります ほぼ7日間の作業プロセスの証明。

したがって、ブロックチェーンのセキュリティは上記の対策で非常に強固ですが、 あるもう一つの方法 Blockchainが代わりにaを用いている分散されることによって自分自身を確保していること チェーンを管理する中央エンティティ。

ブロックチェーンはP2Pネットワークを使用しており、誰でも参加できます。誰かが参加したとき ネットワーク、彼はそれを確認するために「ノード」と呼ばれるブロックチェーンの完全なコピーを取得します すべてがきちんと整っています。
誰かが新しいブロックを作成すると、そのブロックはネットワーク内の全員に送信されます。 各ノードはブロックが検証され、改ざんされていないことを確認します。

すべてがチェックされている場合、各ノードはこのブロックを独自のブロックチェーンに追加します。内のすべてのノード このネットワークは合意に達し、有効なブロックと有効なブロックについて合意します。



改ざんされたブロックは、ネットワーク内の他のノードによって拒否されます。したがって、成功するには ブロックチェーンを完全に改ざんするには、チェーン内のすべてのブロックを改ざんし、「証明」をやり直す必要があります ブロックごとに「作業の割合」を制御し、ピアツーピアネットワークの50%以上を制御します。 それまでは、改ざんされたブロックは他のすべての人に受け入れられます。 そうすることはほとんど不可能です。

ブロックチェーンはどのようにバイオメトリクスと関連付けまたは相互作用しますか？

間違いなく、バイオメトリクスはID認識のための最良の方法です。 最近の技術ブームの助け、バイオメトリクスの速度と精度 新しい高さ。ただし、最も先進的な地域では、バイオメトリクス技術のアプリケーション ogyは予想よりも遅く、その理由はプライバシー保護に向けられています。 cern 、ほとんどのバイオメトリクスターミナルでも実際にはバイオ機能をキャプチャしていませんが、 パニックフォームを公開することはできません。最後に、Blockchainがあると思われる、この最後の問題。

近い将来、すべての生体認証が は、バイオメトリクステンプレートを保存しません。 プレート、すべてのテンプレートはに保存されます 保存することになっているブロックチェーン クラウドサーバー。

ユーザーには委任された「トークン」が 独自の生体認証ブロックへのアクセス。「トークン」、誰もアクセスまたは編集または の情報を削除または上書きする ブロック。

ユーザーが生体認証を使用する必要がある場合 テンプレートは、彼らがする必要がありますアクティブ トークンを使ってブロックにアクセスし、バイオメトリクステンプレート 生体認証の1回限りの使用権 認識のためのターミナル。認識した後 バイオメトリクステンプレートは、 こと解消端末から。