SecHack365

ZENYMA

暗号通貨サービスとQRコードを活用した署名システムの提案

開発駆動コース 仲山ゼミ 藤原出帆

私が実現したい世界

セキュアかつ**カジュアル**に暗号通貨サービスが利用できる世界 🌍

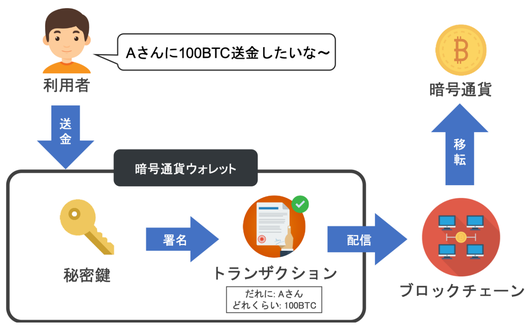
■ 暗号通貨の基礎知識

暗号通貨ウォレット
暗号通貨を管理するためのお財布

秘密鍵
暗号通貨ウォレットに入っている暗号通貨を移転するときやメッセージの署名に使う鍵、厳重に管理する必要がある

トランザクション
暗号通貨をだれにどれくらい送金するのかを記したもの
秘密鍵の署名がされていないトランザクションは誰でも作れるが署名がされていないトランザクションを使って暗号通貨の移転は出来ない

■ 暗号通貨の送金フロー



暗号通貨を送金する際には、まず利用者がだれにどれくらい送るのかを決めて未署名トランザクションを作ります。
次に、未署名トランザクションに秘密鍵を使って署名を行うことで、移転を行う暗号通貨の所有権を確認します。
最後にブロックチェーンに配信を行うことで実際に暗号通貨が移転されます。

■ 署名システムについて

署名システムとは暗号通貨ウォレットや暗号通貨を扱うサービスが未署名トランザクションに署名を行うためのシステムです。
トランザクションを契約書とすれば秘密鍵は印鑑のようなものです。
印鑑を盗まれてしまうと勝手に借金をしたり不動産を売られてしまうように利用者の資産が不正に送金されてしまうので安全に管理する必要があります。

■ 署名システムのあるべき姿

その１ **法的な対応へのコストが低い**

その２ **サービスがクラッキングされた時に資産が絶対に流出しない**

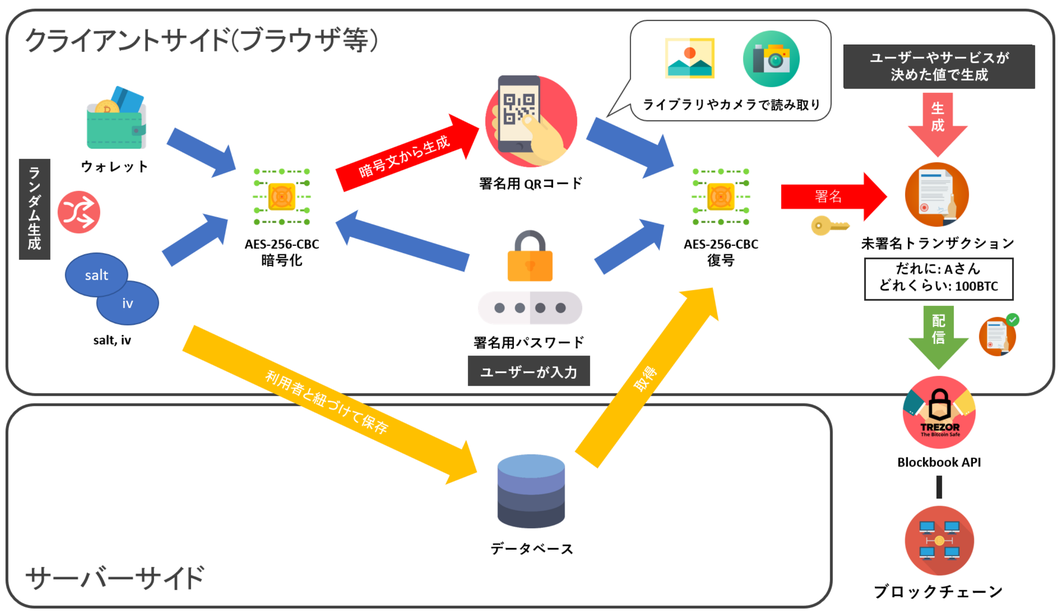
その３ **少ないステップで署名が出来る**

その４ **どんな端末でも簡単に利用できる**

■ 既存の署名システム比較表

	法的対応へのコストが低い	不正に資産が流出しない	少ないステップで署名ができる	どんな端末でも簡単に利用できる
運営者が利用者の秘密鍵を管理する署名システム	×	×	◎	◎
外部ウォレットと連携した署名システム	○	○	×	○

■ QRコードを活用した署名システムとは



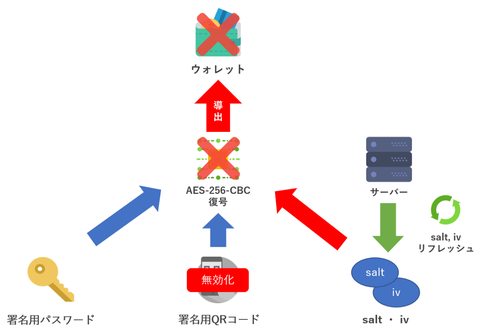
QRコードを活用した署名システムとはランダムに生成した暗号通貨ウォレットと暗号化に必要な情報、ユーザーが入力した署名用パスワードを使ってウォレットに暗号化を行い、暗号文をQRコードにして利用者のライブラリに保管することで秘密鍵を管理する署名システムです。
この署名システムを暗号通貨サービスに導入することで、運営者は利用者の資産が盗まれる心配がなくなり利用者はより安全に簡単に暗号通貨サービスを利用できます。

■ QRコードを採用した理由

画像として扱うことが出来る
暗号通貨サービスは様々な端末で利用される可能性があるので画像として管理できる形式のほうが扱いやすい

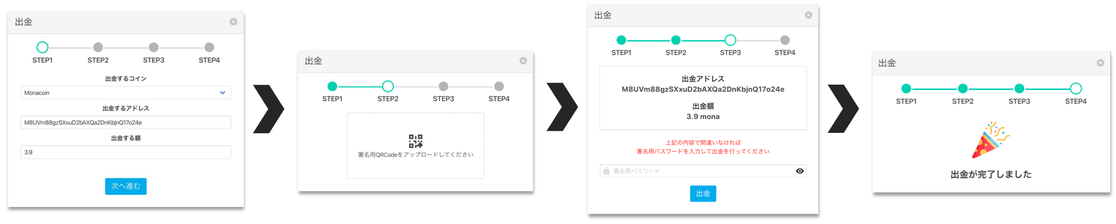
ペーパーウォレットとして扱うことが出来る
オンラインで暗号化された秘密鍵を保持したくない場合はQRコードを紙に印刷することでオフラインで管理することが出来る

■ QRコードのリフレッシュ



QRコードを活用した署名システムで暗号化に必要な情報を暗号通貨サービスのデータベースに保存するのは、利用者が署名用QRコードを紛失・盗難された際に対処できるようにするためです。
利用者が署名用QRコードを紛失・盗難された際は暗号通貨サービス上で暗号化に必要な情報をリフレッシュし紛失・盗難された署名用QRコードを復号できなくして無効化します。

■ 簡易暗号通貨ウォレット



QRコードを活用した署名システムを使って簡易暗号通貨ウォレットを実装しました。

■ さいごに

	法的対応へのコストが低い	不正に資産が流出しない	少ないステップで署名ができる	どんな端末でも簡単に利用できる
QRコードを活用した署名システム	○	○	○	◎

QRコードを活用した署名システムを暗号通貨サービスに導入することで
セキュアでカジュアルに暗号通貨サービスを使える世界を実現することが出来ます。

■これから

暗号通貨とモノをつなぐフリマサービスの開発
QRコードを活用した署名システムを使って暗号通貨とモノをつなぐフリマサービスの開発を行い、SecHack365では出来なかった利用者目線での意見を集めたいです。

ZENYMA

NICT 国立研究開発法人 情報通信研究機構

Icons made by Flaticon (https://www.flaticon.com)