What it does
【背景】ブロックチェーンによる内部トークンを消費させるトランザクションは郵便によるはがきのメッセージと切手を封筒に添付して送付するイメージと似ており、また本ハッカソン中に短文型 SNS が話題になっている事から、タイムリーであると考えて提出しました。

＊Github ページに特許出願形式の明細書・図面などをアップロードしています。

【何をするのか】

（１）ブロックチェーン部に記録したはがきデータの形ではがき・信書・短文の SNS のつぶやきでもよいメッセージデータを差出人から受取人に伝える情報処理システムを提供したい。分散型 SNS 提供？

暗号化メッセージは信書用。平文メッセージは SNS のつぶやき用。

（２）メッセージデータの送信者・差出人がボットではなく信頼できるユーザーか調べるためのホワイトリストを作りやすくしたい。ユーザ同士が対面でお互いの顔とスマホを見ながらユーザ認証・ユーザの確認をしたい。

（例えばストアスキャンをスマートコントラクトベースで行う。）

（３）目の前にいるユーザが本当に EOA の秘密鍵を支配して管理できているか調べたい。ユーザが EOA を利用しているという意思表示や確認も得たい。

（例えばストアスキャンをユーザの持つ秘密鍵とスマートコントラクトベースを用いて行う）

【思うこと】

〇短文 SNS やはがきではメッセージの発信者・差出人がボットではないことを知る必要があると考えています。

そこで弊社の有するブロックチェーン・スマートコントラクトベースのワンタイムパスワード認証をユーザー間でのストアスキャン認証に用いるようにして、認証されたユーザリスト（ホワイトリスト）を作成しそのリストをはがきや SNS のメッセージをブロックチェーン部から拾い上げて閲覧アプリに伝え、ホワイトリストに記載のユーザのメッセージを優先してユーザに閲覧させることを目指しています。

〇またメッセージを暗号化させてデジタル郵便に用いたり、メッセージを公開して短文 SNS のように用いる事を想定していますが、暗号化されているメッセージに誹謗中傷が含まれていたり、短文 SNS においても無責任な発言などあるかもしれません。（逆に匿名だから趣味のことなどつぶやいたり発言できることもあるかもしれません。）

既存のブロックチェーンはパブリック型であることが多く、透明性はあるものの、だれからも閲覧できデータが残るという特徴・問題もあります。

ブロックチェーン式 SNS は日常の SNS コメントも改ざんできずに残り続けるのです…

〇ブロックチェーンコメントを隠す場合にはメッセージを暗号化する必要があります。（さらには一定期間経過後に削除すると好ましい。）

しかしメッセージを暗号化すると透明性はなくなり、発信者・送信者が隠され、犯罪者たちのコミュニケーションツールになる懸念も生じます。

〇犯罪利用を防ぎつつ（捜査機関が調査するときに証拠になるデータを確保しつつ）、匿名利用もしたい。いいとこどりしたい。

そこで本提案のシステムはパブリック型のチェーンで通信内容を秘匿化するため暗号化を用いつつ、暗号化メッセージを送信した差出人が誰であるか、差出人が責任をもってメッセージを出しているかを判別するために、はがきメッセージ部にホワイトリストに登録されたユーザの署名を求めるようにします。

さらにホワイトリストはユーザ同士の対面でもよいストアスキャン方式により作成します。

＊ストアスキャン方式ではユーザが手にもっているスマホなどのユーザ端末の認証コードを認証用端末に提示する必要があり、その際にユーザが確かに EOA と EOA のもとになる秘密鍵を用いてストアスキャン用のコードをブロックチェーンスマートコントラクトから呼び出しているかどうか知ることができます。

＊ストアスキャンは例えば郵便局やコンビニエンスストアの店舗が認証を行うユーザとなって一般ユーザを認証しホワイトリスト作成してもよいです。あるいは友達同士でストアスキャンしあって仲間内のホワイトリストを作成してもよいです。メッセージ暗号化の鍵（図中 AKTB）も交換してもよいでしょう。

上記の様にボットによるユーザの投稿を防いだり見分けるために、ホワイトリストを作成しますが、

ホワイトリスト作成時に、やや素早く、対面で、ユーザが手に持っている（秘密鍵を含んでいる）スマホ端末とそれを持つユーザとを認証したいと考えました。

ユーザースキャン方式、又は単にユーザ端末に EOA・ユーザ識別子（公開鍵部）を QR コードで表示させ読み取るだけでは、

前記 EOA・ユーザ識別子は台帳に記載され誰でも知ることができる情報であって、表示したコードがなりすましされてしまうリスクがあるかもしれません。

そこでストアスキャン方式、又はユーザ側が端末（主にスマートフォン）に提示した QR コードを、認証を行う店舗側ユーザ、あるいは認証を行う一般ユーザがスマホやスキャナを用いて読み取る方式を採用しようと考えました。

弊社ではブロックチェーンのスマートコントラクト部にワンタイムパスワードを生成させ、認証させる知見を有していたので、その知見を応用し、前記ストアスキャンもブロックチェーンとユーザ端末間で行えるように開発したいと考えています。

The problem it solves
〇本提案の方法を用いることでブロックチェーン上のユーザ識別子 EOA を実在のユーザが利用しているか確認しやすくなるかもしれません。

〇そして確認された認証済みユーザリスト・ホワイトリストにあるユーザの署名がはがき・信書データや短文 SNS のつぶやきのようなデータ付与されているか調べることでボットによる SNS の書き込みを防いだり、誹謗中傷のあるメッセージがあっても署名とホワイトリストからメッセージを送付したユーザを特定し後日ユーザ間で紛争を解決できるかもしれません。

〇さらには本提案のはがきシステム・SNS システムに用いるホワイトリストは一種のデジタル ID・名刺データのリストの様に用いられるかもしれません。

また本提案でもちいるホワイトリスト入りした EOA はユーザ認証が行われているためデジタル ID・名刺・身分証のアカウント・ウォレットになると考えています。

Challenges I ran into
ユーザと秘密鍵・EOA が結びついているか手軽に認証すること。ユーザがアカウントを使用しているという意思表示も含めて確認したい。

防犯の為、ユーザとユーザの持つ秘密鍵・アカウントとを結び付けたいときにユーザが秘密鍵を用いていることを認証したい。

Technologies I used
上記課題の解決策としてユーザーが端末に認証コードを表示させ、認証用の読み取り端末に意思をもって提示する形式のストアスキャン方式を採用しました

ブロックチェーン基盤はイーサリアムを用いました。

How we built it
ユーザ認証用のプログラムはスマートコントラクトを持ちています。フロントエンドについては構想中です。デモ動画はないです。

ホワイトペーパー状態です。

What we learned
スマートコントラクトを用いたストアスキャンは決済用や NFT トレカの真贋判別用に開発したが、はがき・短文 SNS のようなメッセージ通信にも利用できるかもしれないと感じた。通信と決済を絡めたスーパーアプリ的なものにつながるのではないかと期待する。

・デジタル郵便の分野ではブロックチェーン技術を用いているので紙の郵便物の様に水にぬれるなど郵便物がダメージを受けることないと期待する。

・ブロックチェーン型のため、一社だけの管理する SNS と比べユーザーがシステムを管理する側に参加できかもしれないと期待する。

What's next for
更なる開発を進めるかもしれない。

現状ホワイトペーパー、考案特許出願段階で実際に開発してい見なければわからない。

（脇道：本提案のロゴの様に、「信書」用のコイン、切手のように通信専用のトークン、シンコイン、ShinCoin あってもよいかも。）