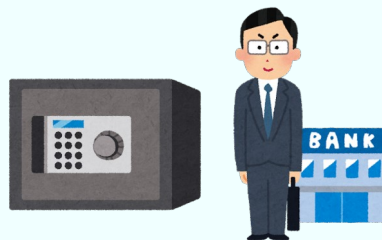


Bank Contract/Contract Wallet using One time password authentication/code payment UX.

(暫定版：ワンタイムパスワード認証機能/及び対面UXにより取引を行う銀行コントラクト・コントラクトウォレット)

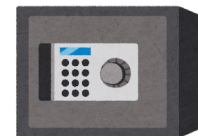
- ShinCoin Vault-

August 18 , 2023



SINGULION CORPORATION (8010001230232)

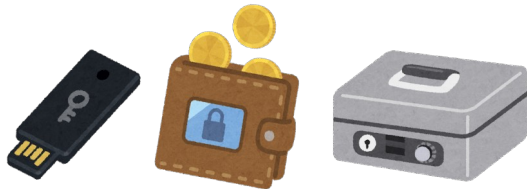
CEO Katsuya NISHIZAWA



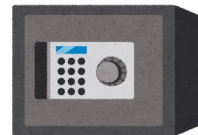
銀行コントラクト
金庫コントラクト
Bank/vault
Contract



現行ウォレット
鍵値に試算を預ける。
鍵値知るものが支配者
ID = 秘密鍵 = 資産



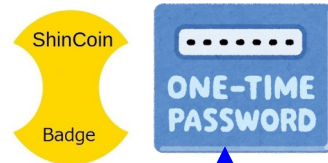
EOA/秘密鍵
鍵に乗せたマネー



CA・AA・ERC4337

鍵とマネーの分離。ID ≠ 秘密鍵 ≠ 資産
ユーザ名義による銀行預金的に？

銀行コントラクト 金庫コントラクト
弊社OTP技術により銀行のコントラクトを実現。



EOA/秘密鍵

OTPトークン保有
デジタルID保有
OTP認証、
対面コード認証決済



現行ウォレット
鍵値に試算を預ける。
鍵値知るものが支配者
ID = 秘密鍵 = 資産



EOA/秘密鍵
鍵に乗せたマネー



●既存のビットコイン、イーサリアムでは**鍵の失効がしづらい問題があった**

電子証明書とその秘密鍵は有効期限経過後は切り替えたり、証明書・鍵を失効させることができる。

他方、**WEB3**の秘密鍵は発行容易だが、失効はできないのでは？

* 秘密鍵を攻撃者に知られた場合、秘密鍵に乗っている資産・コインを移し替える等必要。

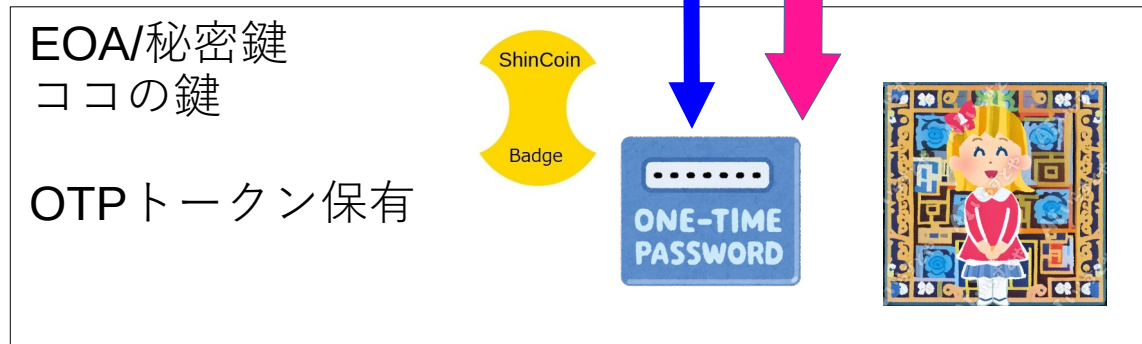
* そして、**問題なのは、過去に使っていた秘密鍵が増えていき、それは自身の名義口座的なもので失効できず、その口座が不正に使われたら困るのでメモって管理する必要が生じそうなこと。**



OTPトークンは譲渡出来ないトークン
(SBT) + 銀行コントラクト側で付与・ミ
ント又は除去・バーンしてよい。対面OTP
認証済ホワイトリストユーザのEOAにユー
ザの名義で付与する

OTPトークンはNFT-ID的な識別子、製造番
号で管理する。後述の秘密鍵漏洩時に、或
る識別子番号のOTPトークンを異なるEOA
間で保管振替・移替する事もできる

金庫銀行コントラクト 金庫コントラクト
弊社OTP技術により銀行のコントラクトを実現。



不正利用時に攻撃者からOTPトークンをはく奪し、
アクセス権を失効させる試み

銀行コントラクト 金庫コントラクト



EOA/秘密鍵
ココの鍵
OTPトークン有



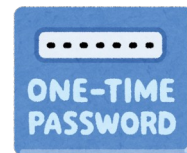
EOA/秘密鍵

ナルの複製した
ココの鍵

OTPトークン有



攻撃者：怪盗ナル



①攻撃者：ナル
ナルの鍵＝ココの鍵を複製
OTPトークンを不正操作、

②高額決済時OTP生成時ガス消費する場合
攻撃しようとOTP生成するとココの見覚えのない
トランザクションが生じる

③ココは不正に気付く。
銀行コントラクト管理者に連絡し別のEOAにOTP
トークンを振替・発行を依頼

(ココの旧秘密鍵からOTPトークン除去・バー
ン・証明書失効され、ココの新秘密鍵にOTPト
ークン付与・証明書発行される。)

不正利用時に攻撃者からOTPトークンをはく奪し、
アクセス権を失効させる試み

銀行コントラクト 金庫コントラクト (保管振替コントラクト)



管理者：承りました



ココ：EOAの鍵が盗まれたらしいので、
旧トークンをおもいっきりバーンしてください！

あと新トークン希望します。こちらのEOAに。
新EOA：対面認証ホワイトリスト登録済



新EOA
ココの新しい秘密鍵
振替えたOTP、新OTP

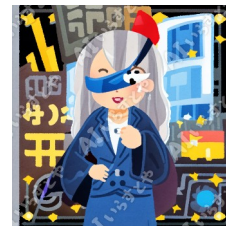
MINT、
ほふり



旧EOA
ナルの複製した
ココの古い鍵

OTPトークン有

BURN



ナル：うう、
OTPトークンが
強制除去された！

アクセス不可

③ココは不正に気付き、銀行コントラクト管理者（鍵屋さん・OTPトークン製造者）に連絡し別のEOAにOTPトークンを振替依頼。

ココの旧秘密鍵からOTPトークン除去・バーンされ（証明書失効され、）ココの新秘密鍵にOTPトークン付与される。（証明書発行される。）

④管理者はほふり的なOTPトークンの保管振替を行い、EOAに付与されたトークンの発行除去・保管振替を行う。）



<<秘密鍵・デジタル証明書の発行と失効の問題>>

<イーサやビットコイン>

鍵の生成発行はできるが、鍵の失効についてはノータッチ。
一度鍵を決めるとその鍵を口座としてずっと管理しなければならない。
そして鍵データが他者に漏洩しても鍵失効できない。

⇒マイナカードや商業登記、ドメイン電子証明書は有効期限や証明書の失効が可能

<本提案：コントラクトウォレット、銀行コントラクトによる証明書ID管理、失効処理>

 銀行コントラクト  金庫コントラクトを用いて、**OTPトークンでもある証明書トークンを付与したEOAを有効な秘密鍵としてもちいること提案する。**

<証明書ID付与>付与にはEOAベースのOTPによる対面QR認証を用いる。（そしてEOAをホワイトリストに入れてよく）対面認証されたEOAとユーザに向けて証明書ID兼電子証明書兼OTPトークンを発行付与し利用開始する。

<証明書ID失効・除去>

EOAからOTPトークンを除去することで証明書の失効を行う。
OTPトークンの付与・除去は管理者（銀行コントラクトのチーフ・CEO）が行う。

🏠 銀行コントラクト
🔒 金庫コントラクト

鍵とマネーの分離

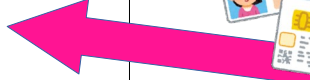
（既存の**OTP**トークンを駆使する**WEB2**のオンラインバンキングを**WEB 3**で行う）

鍵をワンタイムパスワードトークンとして**EOA**に割り当て・除去し**OTP**の発行と失効を行えるようにする（電子証明書や秘密鍵の発行と失効が鍵にマネー乗せた形態ではしづらい問題があったがそれを防ぐ。いちど生成した秘密鍵をずっと自分名義であると管理し続けるのは労力かかるが、**EOA**を**OTP**のトークンを置く住所に変えることで、鍵を管理するのではなく鍵に**OTP**が紐づけられるか管理することで秘密鍵の管理継続問題を避けたい。）（鍵を紛失しても全財産アクセスを**CA**で防ぐ）



銀行コントラクト

<スマートコントラクトor管理者>
承りました



EOAの秘密鍵紛失したので
新しいEOAにOTPトークン振り
替えしてください！マイナ署名し
て新しいEOA情報送ります。

* 本人確認必要時はQRコード認
証方式で本人確認可能

①管理者（ERC4337のBundler相当者）を指定する事に課題。

マルチシグのように、ガバナンストークン付与されたEOAに投票させてBundler\管理者を選任する？管理者は責任をもってユーザをQR対面認証で確認などして新しいEOAに切り替える。

②管理者不在でもよいようにするため、信頼する証明書署名のランザクションでリカバリ

分散性落ちるが、単にWEB3に銀行の機能をつけて運用したい場合に、信頼できる外部証明書(日本国マイナカード、あるいは会社発行証明書にて失効ん管理を行う？)にて銀行コントラクトに署名つきEOA変更ランザクションを送付させ、銀行コントラクト側では公的署名かどうか検証し、該当時はEOAの変更を許可する形。EOA秘密鍵が盗まれた場合は別途信頼できる証明書による指示を受けてリカバリする形。（トラストポイントは政府企業発行の証明書に発生のおそれも）

残る課題例：鍵の管理。Private key , OTP's keyの秘匿化。秘密化。

（Bundler OTP等複数鍵を用いるがその秘匿化、SSSやMPC等で行うなども？OTPについてはコード生成アプリ・dAPPS内部に鍵持たせるなど可能だが、さらに秘匿化するためにMPC利用も？）