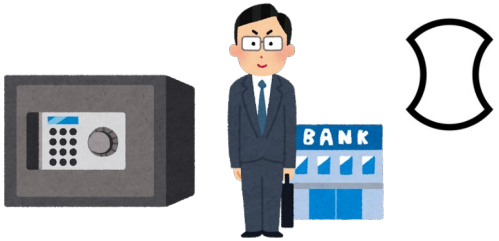
Bank Contract using code payment UX.
- ShinCoin Vault-

August 18 , 2023

SINGULION CORPORATION (8010001230232)
CEO Katsuya NISHIZAWA

株式会社SINGULION (法人番号8010001230232)
代表取締役　西沢克弥

デジタル署名者 : 0402010000001
日付 : 2023.08.19 14:28:13 +09'00'



銀行コントラクト
金庫コントラクト
Bank/vault Contract

【要約】秘密鍵・デジタル証明書の発行と失効の問題を
コード認証トークン利用したコントラクトウォレットを用いて解決したい

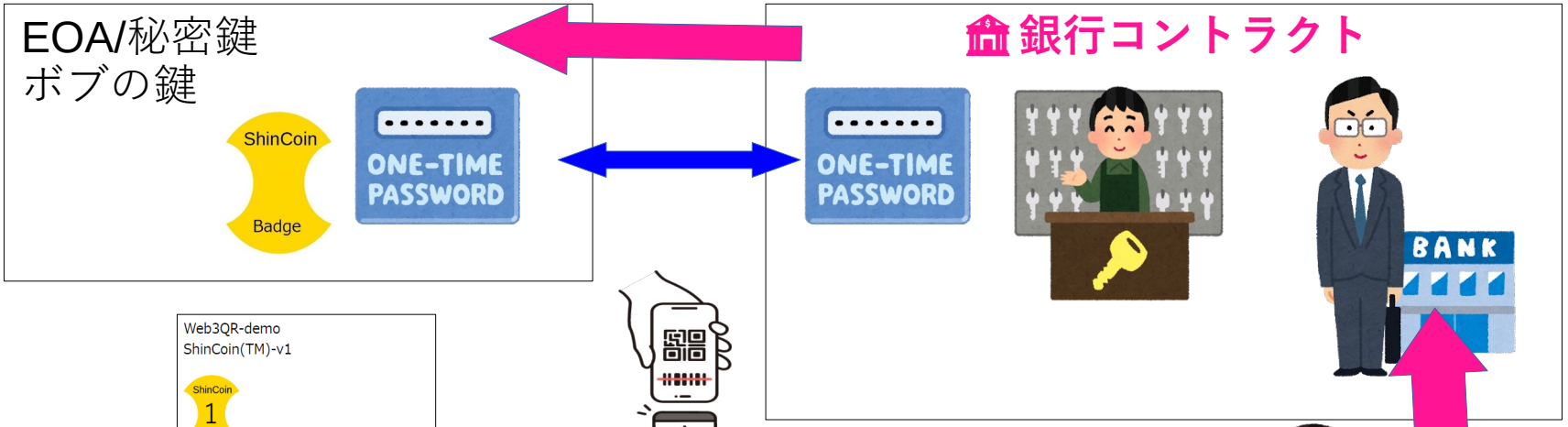
＜イーサやビットコイン＞
鍵の生成発行はできるが、鍵の失効についてはノータッチ。一度鍵を決めるとその鍵を口座としてずっと管理しなければいけない。そして鍵データが他者に漏洩しても鍵失効できない。⇔他方、マイナカードやドメイン電子証明書は有効期限や証明書の失効が可能。

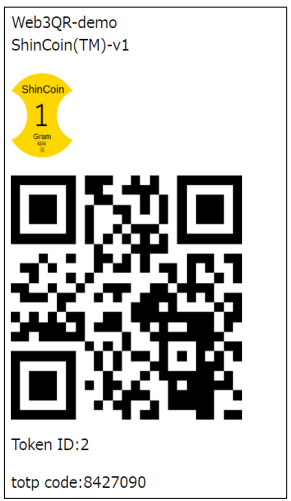
＜本提案：コントラクトウォレット、銀行コントラクトによる証明書ID管理、失効処理＞
🏦銀行コントラクト🔐金庫コントラクトを用いて、**OTPトークンでもある証明書トークンを付与したEOAを有効な秘密鍵としてもちいること提案する。**

＜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アクセスキー・DID・証明書の失効を行う。
銀行コントラクトの管理者（銀行免許あるとよい？）や信頼できる証明書の秘密鍵署名或るトランザクションに従って失効除去を指示する。

アクセストークン（OTPトークン）発行スキーム

②After　STEP①,OTP token mint/Add
銀行コントラクトのユーザ名義口座番号への
アクセス用OTPトークンを付与・ミントする。





①KYC-UX
Using code authentication
of EOA.(EOAの保有者本人確認)
トークン不要でEOA確認

・認証のライブデモ
https://singulion.net/qrUser-astar/5500gen.html
https://singulion.net/qrUser-astar/5500scan.html

店舗、ATMによるコード認証
ユーザとコードの撮影
（銀行コントラクトの口座開設用にマイナカード連携できるとGOOD?）

＜OTPトークン式の証明書ID失効・除去を指示する場合＞
EOAからOTPトークンを除去することでアクセスキー・DID・証明書の失効を行う。

例えば個人番号カードで署名されたトランザクションを含むOTPトークン除去指令を銀行コントラクトが受け付けた時に、個人番号カードの署名・名義・銀行コントラクト内部でトークン番号・口座番号・ID（これはDIDに用いる想定）を検証する部分がコントラクトにあって、その部分で名義に対応するOTPトークンの除去や新規EOA割り当てを行う。

＜OTPトークン式の証明書IDをEOAに発行・再発行する場合＞
EOAの除去は個人番号カードだけでも可能だが、EOAへのOTPトークン割り当てには対面コード認証をしてEOAとEOAの支配者ユーザの確認必要。
（KYCの為。マネロン防止の為。）

＊たとえばゆうちょATMさんやCVSのATM等でこの対面EOA利用者確認できると良い？。

＜銀行コントラクトの銀行的立ち位置は？（都市銀行・その他銀行・地銀・信金の分類）＞
本提案の銀行コントラクトは、かつてのゆうちょ銀行さん（貸付無の貯金口座）と郵便局さん（はがき通信、住所確認、本人確認）に近い！（あるいはCVSコンビニ系銀行さん？）

☆弊社がHR3ハッカソンで別途応募中のブロックチェーン式デジタルはがきSNSシステムとの親和性高いと想定。ユーザの確認、通信、SNS、貯金送受信・決済等、チケットNFT等のNFT送付・受領・使用等を一気通貫で行える。

●銀行コントラクトではFT・デジタル通貨の受け入れとともに、NFTの受け入れも行わせる。NFTの置き場・貸金庫にも。（金庫と銀行を兼ねるコントラクト。）
証券・セキュリティートークンの置き場にも？

●所謂DeFiのようにWEB3で貸し付けするWEB3都市銀行的な物も可能？
＊他方代表西沢としてはゆうちょさん、CVS銀行さんを志向。貸金庫的な立ち位置や貯金箱的な貯金口座を志向。その形態は日常利用のなかで自然と対面本人確認可能なため。

（そしてユーザに同意を取って購買決済情報を頂ければ広告等とも親和性？）

●マネタイズについて、
①銀行コントラクト内の振込手数料（内部トークン消費）想定。
②預け入れられた資金をステーブルコイン風に債券運用し、債券運用利子を顧客分配したりコントラクト又はコントラクトを運営する法人の利益に充てること想定。（米国債、日本国債共に債券価格下落し、金利上昇傾向有。）
③あるいは、デジタル信書はがき利用時の切手風内部トークン手数料、スタンプ販売手数料も？　NFTチケット等販売仲介による手数料なども。

（ステーブルコイン及びトランザクション用内部トークン：シンコイン、信書コイン）

●銀行コントラクトの管理者は銀行免許・カストディ免許を持つ有限責任の登記された法人が好ましいように思える。管理者を無限責任の個人にするのはどうかと思う。
（AA,ERC4337のバンドラーなどの部分を銀行免許持つ法人に行わせる形態。）

●対面コード認証を利用し、本人確認ルールや資金洗浄防止ルールを整備したWEB3銀行的なものが構築できる？

説明図

🏦銀行コントラクト／🔐金庫コントラクト

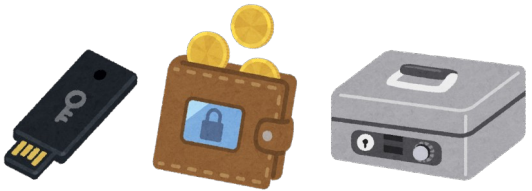
鍵とマネーの分離
（既存のOTPトークンを駆使するWEB2のオンラインバンキングをWEB３で行う）

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ず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）

＜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

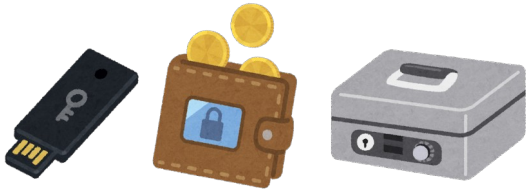
●既存のビットコイン、イーサリアムでは**鍵の失効がしずらい問題があった**

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？

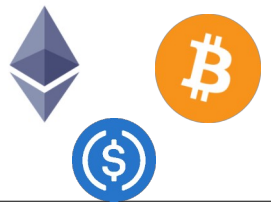
＊秘密鍵を攻撃者に知られた場合、秘密鍵に乗っている資産・コインを移し替える等必要。

＊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。**

＜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？
CAウォレットCAWに弊社OTP技術を組み合わせて銀行のコントラクトを実現できそう？

OTP token mint/Add burn/remove

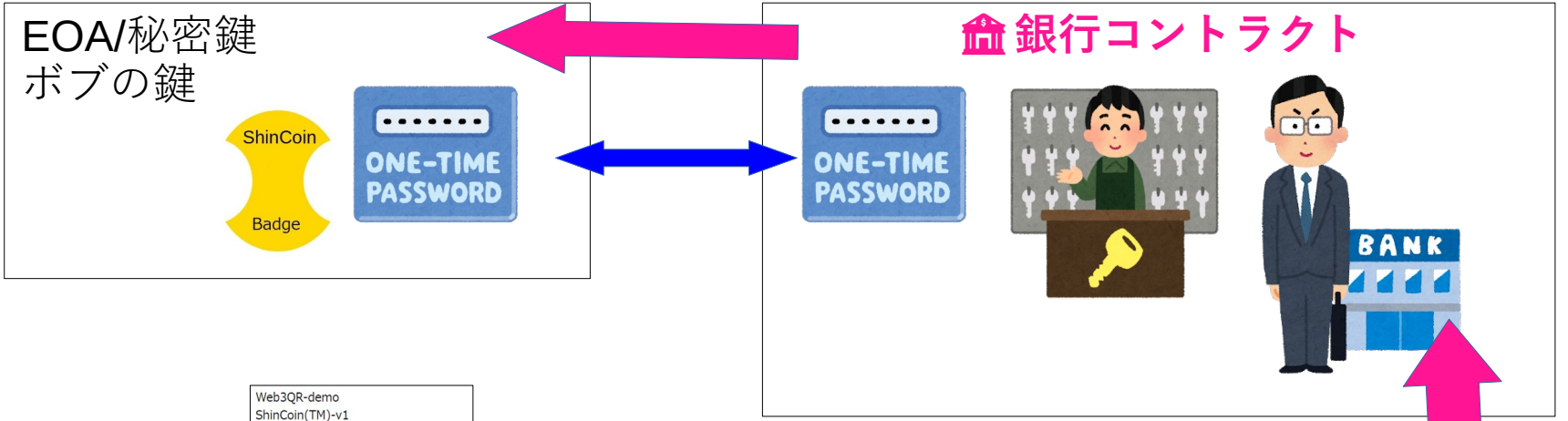
EOA/秘密鍵

OTPトークン保有
デジタルID保有

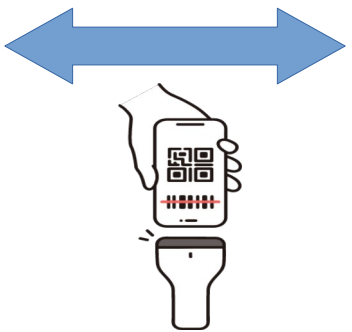
OTP認証、対面コード認証決済
UX向上、防犯性向上

アクセストークン発行スキーム

②After　STEP①,OTP token mint/Add
銀行コントラクトのユーザ名義口座番号への
アクセス用OTPトークンを付与・ミントする。



①KYC-UX
Using code authentication of EOA.
(EOAの保有者本人確認)



店舗、ATMによるコード認証
ユーザとコードの撮影
（銀行コントラクトの口座開設用にマイナカード連携できるとGOOD?）

EOA/秘密鍵
ボブの鍵

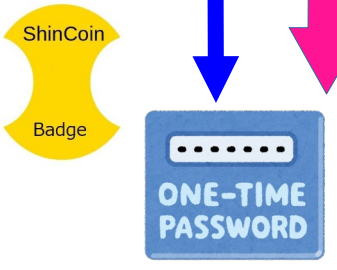
OTP token mint/Add

EOA/秘密鍵
アリスの鍵

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
ココの鍵

OTPトークン保有



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

- 銀行コントラクトは構想中の為、
  DEMOなしです

（すみません。前回Oasysさん、UDLさんで提示したコード認証のデモを提示します）

銀行コントラクトをDAOで行う場合や今後の課題解決については
別の国内外ハッカソンで開示予定・・・。

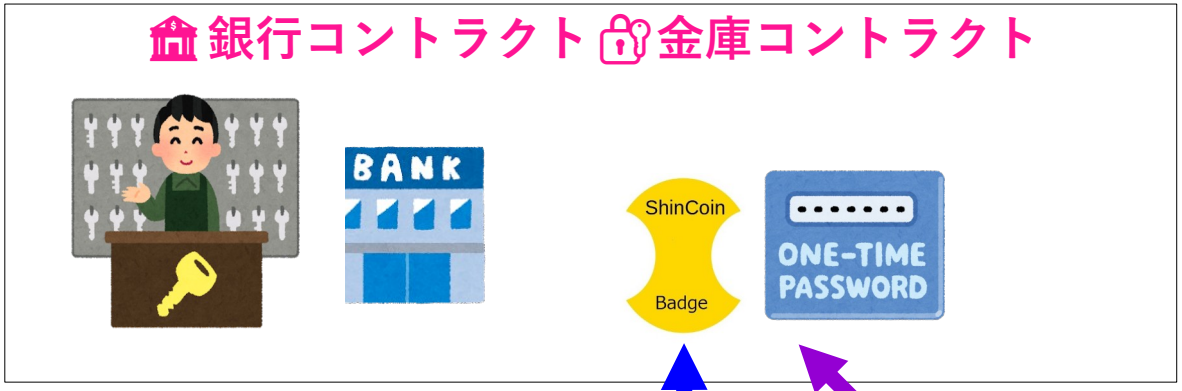
不正利用時に攻撃者からOTPトークンをはく奪し、
アクセス権を失効させる試み（寸劇）

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・内部トークン消費が生じる

③ココは不正に気付く。
（BCエクスプローラ経由で）
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。または公的身分証
証明書などでOTPを失効させるTX送信する。

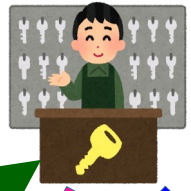
（その後、ココの旧秘密鍵からOTPトークン除
去・バーン・証明書失効され、ココの新秘密鍵に
OTPトークン付与・証明書発行される。）



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（寸劇）

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・管理部：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

NEW
MINT、
ほふり

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。）

旧EOA
ナルの複製した
ココの旧い鍵

OTPトークン有

OLD
BURN

ナル：うぅ、
OTPトークンが
強制除去された！

→アクセス不可