Product Crowd Sale for Consumer Protection (draft ver.)

日置　玲於奈　　昼間　輝一
leona.hioki@laurus-school.com　　hiruma.kiichi.72n@st.kyoto-u.ac.jp

2018 年 7 月 9 日

1　概要

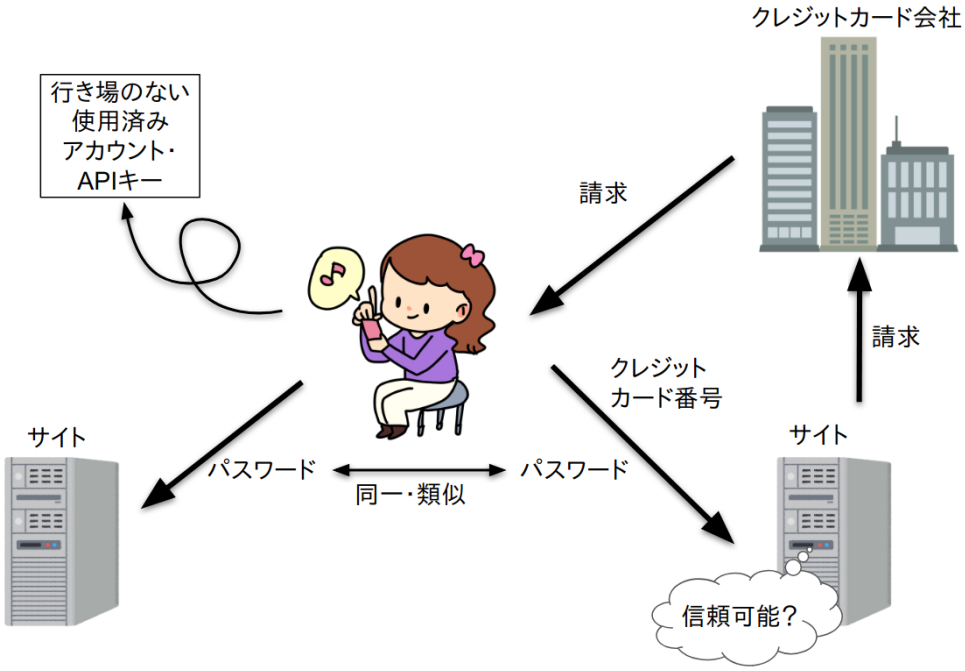
消費者の経済的・権利的保護およびサイバーセキュリティ上の保護を保障するための非代替トークンの公開鍵暗号による拡張である.

2　背景

現在のソフトウェア販売において一般的となっている, シリアルナンバーおよび API キーの配布とクレジットカードによる決済のプロセスには, ユーザー保護の観点として,

1. 適正価格の把握の困難
2. 中古・シェアリングの機会の不足
3. ウェブサイト・発行主体からのクレジットカードナンバーの漏洩
4. メールアドレス・パスワードのセットの漏洩

という問題が存在している. これらの問題は Ethereum 上の新規格 ERC721 に代表される非代替トークンの利用により, 暗号学的手法での解決が現実的なものとなっている.



1. 適性価格把握の困難は主に, ソフトウェア・プロダクトの販売が定額で行われており, 市場による価格評価を受けないことに起因すると考えられる.

2. 中古・シェアリングは消費者に希望価格での売買の機会を提供する. シリアルナンバーや API キーは永久的に記憶可能であるため, 事実上他者に譲渡することができない状況となっていることが原因となっている.

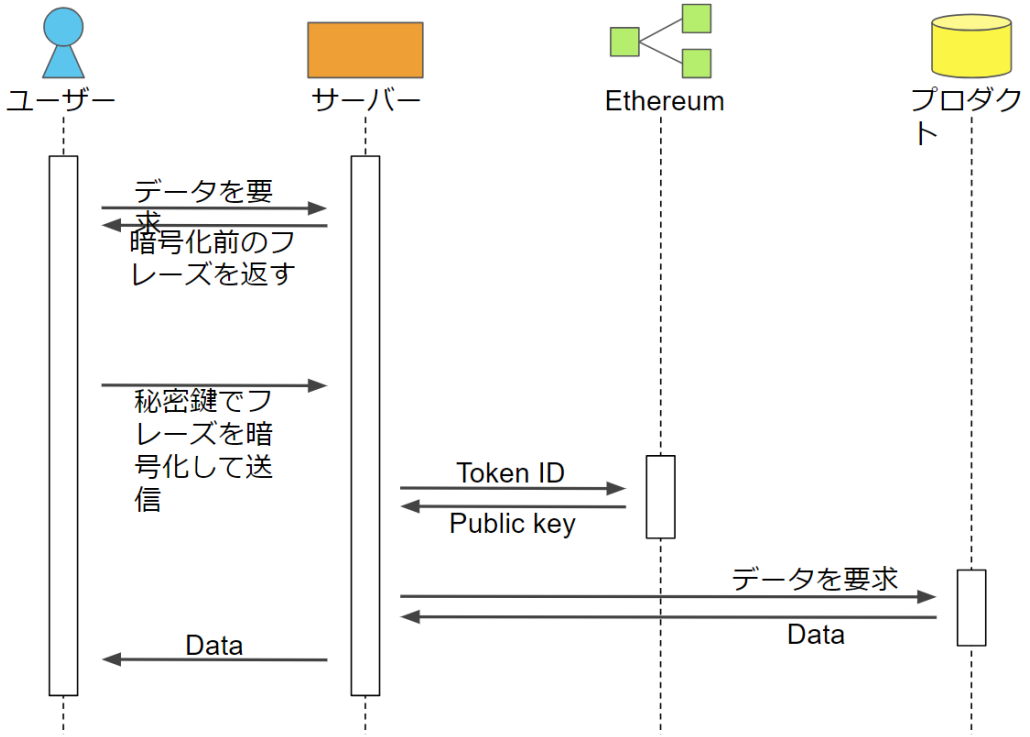
3. クレジットカードのナンバー送信は不正請求につながる可能性があるため, 使用者はプロダクト提供者のセキュリティと非犯罪性を信頼する必要がある状況となっている. クレジットカードナンバーの送信は秘密鍵送信と同じ危険性を有する.

4. メールアドレス・パスワードも同様に保存や処理の過程を消費者が知らないため, 漏洩・悪用がないことを信頼する必要が生まれている. これらのペアの複数サイトでの使用は, 不正アクセスを行う最も簡単な手段を攻撃者に提供する.

3 OR-MultiSig と非代替トークンによる解決案

非代替トークン (NFT) に所有者にのみ設定・変更可能な公開鍵 (SubSig) を設定する機能を付与する. この仕様 (OR-MultiSig) では, Ethereum の鍵生成で生まれた秘密鍵を 2 つ使用することとなる. この非代替トークンを通貨と交換可能な取引所を設置する.

- プロダクト提供者はユーザーのトークンに設定された公開鍵と, ユーザーからの署名を照合して認証し, ユーザーに使用を許可する
- プロダクト提供者は非代替トークンのクラウドセール (PCS) を行うことで販売を行う
- 交換・譲渡はトークンの送信機能により行われる
- 交換・譲渡の後に新しい所有者は公開鍵を再設定する
- 使用者は使用継続しないプロダクトを取引所で売却する



4　問題解決詳細

2 節で述べた問題点の前節の設計による解決を以下に示す.

4.1　適正価格の把握の困難

取引所により, プロダクトの市場での流動性を実現する. トークン化されることにより, プロダクトは Ethereum 上での売買および譲渡が可能となる. 最終約定価格等, 適正価格を判断する指標が取引所機能によりもたらされる.

4.2　中古・シェアリングの機会の不足

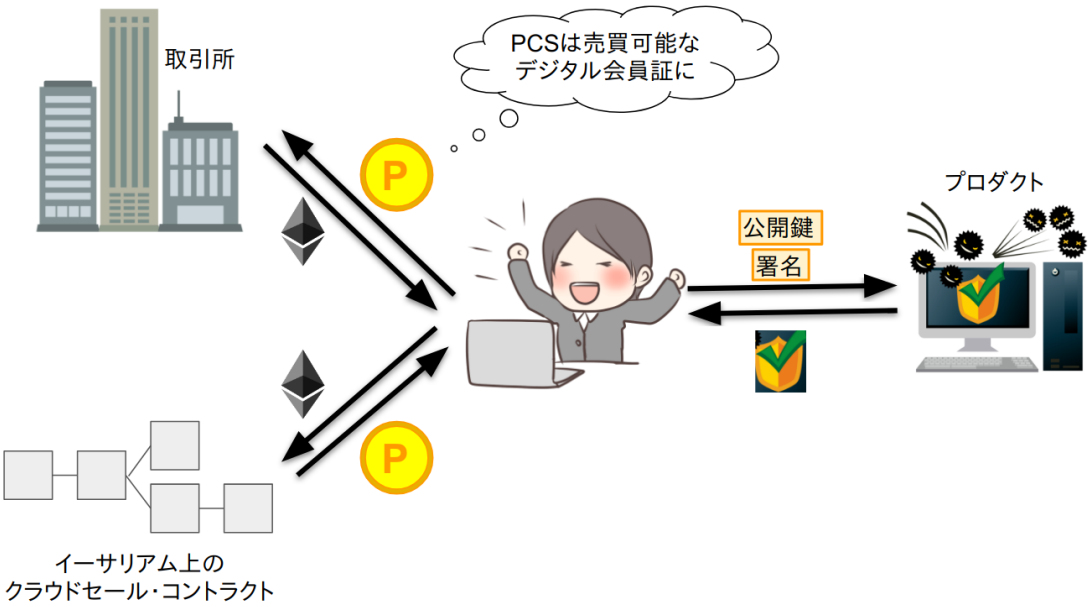
取引所により, ユーザーは任意の時期において売却・購入する機会を得る.

4.3　クレジットカードナンバーの漏洩

公開鍵署名による認証においてユーザーは, クレジットカードナンバーに相当する秘密鍵を秘匿したまま秘密鍵の保有を証明できる. 故にクレジットカードナンバーを送信することに付随するリスクにユーザーは晒されない.

4.4　メールアドレス・パスワードのセットの漏洩

メールアドレス・パスワードのペアを非代替トークンによる認証では必要としない. トークン保持者は任意のパスワードから認証に使用する公開鍵を生成・設定することができ, 任意の時期に変更することができる. イーサリアムのアドレスがメールアドレスに相当する. このプロセスにおいて, 機械的に生成されたアドレスと公開鍵のみを送信するため, 第三者への信頼を必要としない.



5　イニシャル・コイン・オファリング (ICO) とプロダクト・クラウドセール (PCS) の比較について

PCS は仮想通貨規格である ERC20 の拡張である, ERC721 を使用するため, トークン販売の形態の多くの部分を共有する. ICO において消費者・投資家保護の観点から以下の問題が示された. これらは多通貨ベースのエコシステムの複雑性に起因し, 対して PCS による簡略化による有効な解決を提案することが可能である.

5.1　複雑な循環的エコシステムの価値・性能の不透明性

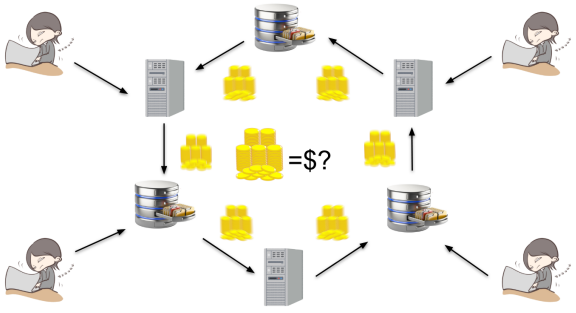
この ICO の問題に対し, 個々の製品のトークン化を行う PCS は, プロダクト提供者・消費者の関係において複雑なエコシステムを必要としない. PCS においては一つの製品に対する評価を行えれば, トークンの適正価格を評価することができるため, エコシステム全体に対する分析・評価を必要としない.

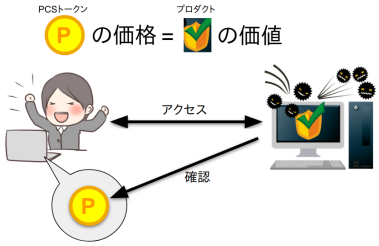
5.2　難読なコントラクトコードによる脆弱性

これは, ICO において各プロジェクトがそれぞれ独自のコントラクトを必要とすることに起因する. PCS によるプロダクト使用において, 主に認証と売買に関わる部分がコントラクト化される. 故に各コントラクトはコードの多くを共有するため, 少ない量のコードの信頼性を把握することのみが消費者に求められる.

5.3　トークンに関する法的処理の不透明性

Ethereum 上の ICO プロジェクトは Ether を含む他通貨ベースのプロジェクトとなることで, 現行法と摩擦が生じている. PCS はプロダクトの仮想通貨 Ether による購入というシンプルな形態であり, 代替性トークン間の交換における法的問題を伴わない. PCS で配布される非代替性トークンを扱う取引所においても同様である. ICO は日本国において代替性トークンの交換における法的問題が議論の的となっている. 加えて, PCS は現在のソフトウェア販売と類似しており, 現行の法的消費者保護を受けやすい形になっている. ソフトウェア販売の不履行や設計と製品の著しい乖離などは, 現行法の詐欺に対する法的処置を受ける.





6　秘密鍵紛失対策

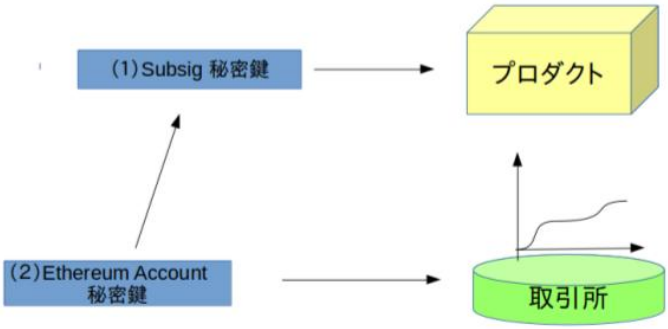
秘密鍵の紛失は, 不正侵入による盗難と並び, 暗号通貨・資産における最大のリスクである. この秘密鍵の紛失に際し, 上記のトークン規格での鍵管理 (OR-MultiSig) は 2 つの秘密鍵を紛失しなければ製品の使用権を消失することにはならない仕組みとなっている. この秘密鍵紛失対策は, 通貨としてのトークンではなく会員証としてのトークンの性質により, トークンの移動を行わなくてもプロダクトが使えることに拠る.

6.1 Subsig 秘密鍵紛失パターン

Subsig は所有アドレスからの操作により任意の時期での変更が可能であるため, 所有者に被害は発生しない.

6.2 Ethereum 秘密鍵紛失パターン

プロダクトの使用は Subsig での署名によって行われる. 故に所有者はプロダクトの使用を続けることができる. この際, 他のアドレスに送信する権利を消失する.



	プロダクト 使用	取引所 使用
(1)Subsig紛失	○	○
(2)アカウント紛失	○	×

7 抗フリーライド

プロダクトに対するフリーライドを禁止するシステムは, 提供者・消費者の双方にとって重要である. これは特に非代替トークンを利用した市場を想定した場合, 中古販売の価格を保障するためには必要なシステムであり, 消費者保護・投資家保護の重要な機能である.

以下のエコノミーに対する攻撃パターンを考える

7.1 SubSigExpose 攻撃

1. 1 つのトークンについた SubSig の秘密鍵が公開され, 全員が利用可能になる （フリーライド）

これは 1 つのトークン保持者が利他的に秘密鍵を公開することで, 不特定多数の人間をフリーライダーにしてしまうケースである. トークン保持者はプロダクトを使用しなくなった際にトークンを売却するまでに, この攻撃により無価値化されることが考えられる.

解決策は, SubSig の秘密鍵での署名によりトークンを無効化可能にする. SubSigExpose 攻撃の実行者は, 秘密鍵の公開によりすぐにトークンを無効化される可能性に晒され, 実行は良心的ノードに妨害されうる. SubSig は公開鍵と紐づくアドレスとして実装されるため, これに対応する秘密鍵でトランザクションを署名することができる.

7.2 SigExposeHoneyPot 攻撃

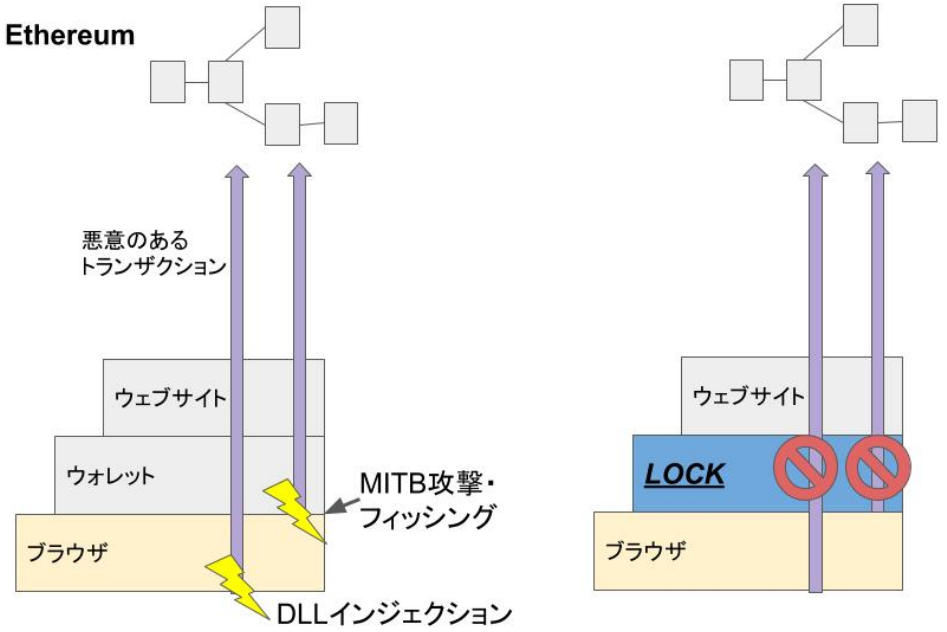
1. Subsig の秘密鍵を公開し, 全員にフリーライド可能にする
2. 良心的ノードによるトークン無効化のための Gas を払えなくするために, Eth 残高を 0 にする
3. トークン無効化のために送られてきた Ether を奪取するために, 攻撃者は自分の他のアドレスに送金するトランザクションを BroadCast し続ける

これはフリーライドを可能にした上で, 上記の良心的ノードから Ether を奪取できる可能性がある.

解決策は, 同様に Ether の送信後, 対象トークンの無効化トランザクションをブロードキャストをすることで確率的にトークンを無効化できる. エコノミー攻撃者による秘密鍵の公開先に 1 つでも良心的ノードがいる可能性があることで, 問題は解決される. エコノミー攻撃者は高い維持コストを払うことになる上に, 容易に特定される上記の行動を行うことから, チェーン外のプロダクトの認証でブラックリスト化されるリスクに晒される.

8 アンチ・マルウェア

このトークンの保持によるプロダクトの使用許可には, トークン ID と Subsig の秘密鍵のみが必要であり, Ethereum の秘密鍵を必要としないため, 多くのマルウェアに対し実行機会を減らすことができる. この性質もまた, トークンの移動を行わなくてもプロダクトが使えることに拠る. 以下, 脆弱性を 2 種類に分類する.



8.1 MaliciousTransaction-Pattern

悪意のあるトランザクションを送らせるパターンである. ブラウザ上ウォレットでトランザクションを許可するボタンを押すように誘導するものが代表的である. Man-in-the-Browser 攻撃, スクリプトインジェクション攻撃と組み合わせることで達成されるケースが想定される. PCS トークンによるプロダクト使用許可において, ウォレットによるトランザクション署名は必要なく, この攻撃の機会を与えない.

8.2 DLLInjecion-Pattern

ブラウザウォレットに対して処理を奪い取ることで, ウォレットから秘密鍵情報を取得・使用するパターンである. ブラウザのプロセスに干渉し, 処理・情報を奪取する手法であるため, ウォレットのロックを保ち, コードを走らせないことにより防御することができる.

9 価格分析と消費者保護

消費者は使用後に売却できることを想定して購入する. よってこのトークン・製品の設計において, 以下の点に注意を払わなければならない:

1. 多くの価格帯での流動性の確保
2. 価格のボラティリティの安定

1. を満たすためには, 製品は需要の価格弾力性が小さいことが必要とされる. プロダクトの分野の選択・トークンの権利の設定において, 考慮すべき点となる. 特に, 短い期限のついた商品や 1 回限りの使用の商品はプロダクト・クラウドセールに不適合であると考えられる. 2. を満たすためには, 製品の供給の価格弾力性が大きいことが要請となる. この要請は投資家による売買の必要性を意味するものであり, 投資的目的をもつホルダーを一定数維持することで供給の価格弾力性は一定以上の閾値を保つことができる. 例えば, プロダクトのスケール可能性の問題で, トークンの販売が制限されたとき, この価格調整機能が必要となる.

10 トークンを動かさずに使う経済効果

多くの基盤エコシステムにおいて, 様々なコストと引き換えに行われるマイニングが通貨供給とセキュリティの役割を担っており, これらのノードによる活動の停滞はシステムの脆弱性を意味するため, コストを払うノードが離脱しないような信頼できる経済設計をする強いインセンティブを持つ. しかしながら, プラットフォーム上で発行されるトークンはセキュリティ上要請はなく, ほとんどコストなく残高データを創造し, 新規通貨を発行できる. 故に, 循環システムを公平に設計するインセンティブは, ICO 資金調達額が期待経済規模を上回る限り, 存在しない. プロダクトを使う際にトークンが循環する仕組みは, 内部に通貨供給あるいは信用創造による円滑化の必要性を持ち, 以下の問題をもつ:

1. プロダクト設計者の負担・困難の増加
2. Ethereum への処理負担
3. 余剰金投入の有無によるプロジェクト成功への影響

これらに対し, プロダクト・クラウドセールはトークンを動かさないまま, その認証機能を使えるため, 1. と 2. を問題としない. また, 製品を個別に売り, トークンを動かさない性質上, ユーザー体験は他の使用者・エコシステムの影響を受けない. この点は, 他のエコシステム参加者が充分にいることを条件にする通貨性トークンを使ったプロダクトと異なる. 同時に, 通貨性がなく決済に使用できないことから, このトークンは利用範囲が制限されるため, 実需を欠いた余剰金の投入のインセンティブは ICO と比べて小さくなると考えられる.