セルフキー

# セルフキー基金

2017 年 9 月 11 日

Copyright 2017 | SelfKey Foundation | すべての権利を保有

# 内容

問題：自分のアイデンティティを所有していない。 ..... 4

背景情報 ..... 5

アイデンティティ取引における締約国 ..... 5

集中管理されるアイデンティティシステムの制限： ..... 6

制限付きアクセス ..... 7

独占 ..... 7

データ保護への準拠 ..... 8

KYC の規制要件 ..... 9

ソリューション：″セルフキー″自己主権デジタルアイデンティティエコシステム ..... 10

発売時に入手可能な製品: ..... 11

ブロックチェインは答えですか？ ..... 12

ブロックチェーン（単独）は答えではありません。 ..... 12

会社のセルフキーのしくみ ..... 16

クレーム発行者のためのセルフキーのしくみ ..... 17

セルフキーネットワーク ..... 18

財団 ..... 18

非営利のステータス ..... 18

ガバナンス ..... 19

法的 ..... 19

セルフキー財団 ..... 20

セルフキーテクノロジースタック ..... 21

キー管理/回復 ..... 22

従来のアイデンティティシステムに比べてセルフキーネットワークの利点 ..... 23

KEY トークン ..... 25

未来を見る ..... 27

セルフキー財布 .....28
セルフキー生態系 .....28
セルフキー市場 .....28
セルフキーチーム .....29
結論 .....30

# 問題：自分のアイデンティティを所有していない。

インターネットが世界中で増殖するように、それはほとんどあらゆる範囲の人間の日常生活の本質的な要素になる。インターネットは、従来の国境によって制限されていない、本質的にデジタル、国際的、指数的、技術的ネットワークです。ペーパーからのデジタル計算およびインターネットへの転位 1.0[i]そして 2.0[ii]最近の近代史の最も根本的な変化の偉大さ。今日、ほとんどすべてがデジタル化、コンピューティング、ブロックチェーンの開発は多くの人がインターネットを可能にすると考えられています 3.0.[iii]

但し、他の範囲の進歩そして中断にもかかわらず、私達が今日頼るアイデンティティ システムは現在紙ベースである、国家主導の政府のアイデンティティ・システムであり、インターネット 3.0 の力を活用していません。多くの人々が現在頼りにしていますーまたは現代技術の欠如のためにアイデンティティシステムから除外されているインフラ.[iv]

ほとんどのアイデンティティ システムは中央に、他のシステムに統合しなかったりまたはリンク、そして資格賦与および力の場所に置かないアイデンティティの所有者を計画され、管理され。これらのシステムはプライバシーの非能率、データ漏出、脅威、損失および個人情報漏洩をもたらす[v]どのような種類の財政勘定もなく数十億を残している.[vi]

多くの中心にされたアイデンティティ システムに非常に深刻な安全保障問題がある.[vii] 最近の分点データは 1 億 4300 万の個人の個人的なデータが質問に脆弱性どこに感度が高いデータの大きい中心にされたセットの収集の継続的だった練習妥協されたハイライト中心にされたデータベースおよび呼出しのであるかもしれないか破る.[viii] 場合によっては、全体の国の市民(スウェーデン[ix]) 可能性としては破裂的に個人的なデータ違反に苦しんだ。その代りに違反は頻繁に切れ刻むか、または他の悪意のある努力の結果としてデータへの不正アクセスを防護するために適切な安全装置がある なかなかで起こらないが.[x]

現在のアイデンティティ システムは主としての巧妙なアイデンティティ システムのための基本条件提供しなかった: アイデンティティの所有者への保証、プライバシー、所有権、アクセス、保護、インターオペラビリティ、またはつながれたデータ可搬性。

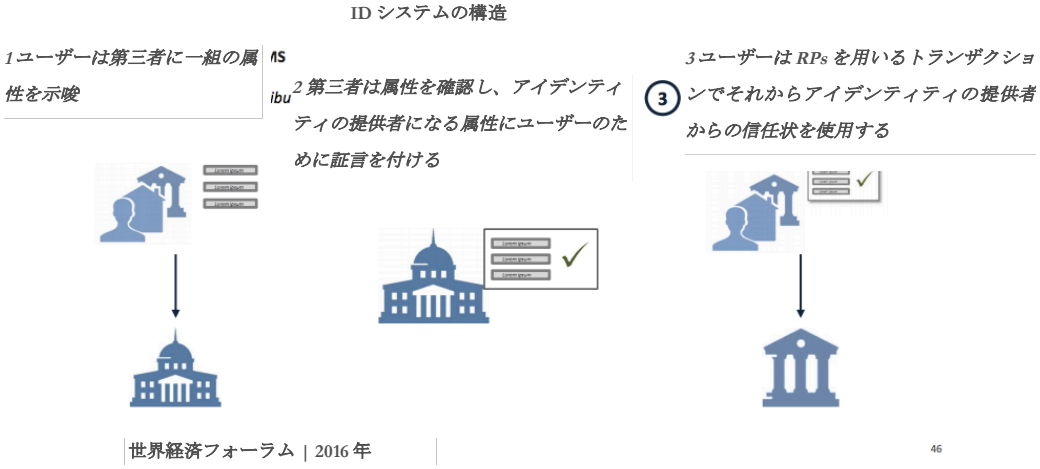
「現在のアイデンティティ システムはフィンテックの革新を限って、また金融サービスおよび社会の有効なサービス提供より広くしっかり止める。 デジタル アイデンティティはアイデンティティ システムの次のステップとして広く確認される」。 - WEF[xi]

伝統的な集中アイデンティティシステムの失敗は明らかです。個人が彼らのアイデンティティの所有権を保つことを保障してが、私達の展開の全体的な社会のための支持できるデジタル アイデンティティ モデルの開発は今必要である。

# 背景情報

## アイデンティティ取引における締約国

アイデンティティトランザクションに普通 3 つの党がある; アイデンティティ所有者（IO）（個人または会社など）、アイデンティティクレーム発行者（CI）または第三者（公証人の公証人または公平のような）（RP）（銀行、仲介業者または他の金融機関など）を含むことができる。O には、1 つまたは複数の ID クレーム（IC）があります（たとえば、「私の名前は John H. Smith」または「1975 年 1 月 1 日に生まれました」など）。これらのクレームは、第三者に証明または確認され、IO は、信頼できる当事者の製品およびサービス（銀行口座の開設など）にアクセスするために、検証されたクレームを信頼当事者と共有することができます。




例として、個人（IO）は、彼らが米国人（クレーム）であり、彼らが米国のパスポート（証拠）を有し、彼らが送信している電子コピーが オリジナルの真正なコピーを証明しています。これは、公証人からの証明書を受け取り、証明された請求となる電子的な身元証明請求です。 検証されたクレームは、デジタルアイデンティティの未来です。

これらの党すべては現在のペーパー運転され、中心にされたアイデンティティ システムと戦い、デジタル化された、分散させていたアイデンティティ システムから寄与する。

## 集中管理されるアイデンティティシステムの制限：

1) セキュリティおよびその他のリスクほとんどのアイデンティティシステムは、何百万（または何十億）の ID レコードを含む大きな集中データベースを持っています。 これらの集中データベースは、サイズが大きいため、ハッカーにとって高価値のターゲットです。それらが含んでいるアイデンティティデータは、盗みや使用が比較的容易です.[xii] 巧妙な違反のための報酬がそのデータベースに保持されるアイデンティティーの数と指数関数に基づいて増加するで，データベースが大きくなるにつれて、攻撃に対して脆弱になります。なお、単一の大きいデータベースは頻繁に（多数の、区分された、分散させていたデータベースに対して）失敗の一点を意味する。

   中心にされたアイデンティティ システムは通常単一党によって管理され、その党はそしてデータベースにアクセスし、データベースをさらにもっと傷つきやすくさせるデータ違反にデータを-頻繁に十分な安全装置および手落ちなしで-処理するのに第三者プロセッサを使用する。オペレ

ータが信頼できて、中心にされたアイデンティティ システムは承認されたアクセスを用いる三番目の党を通して傷つきやすい。個々のアイデンティティ文書は、闇市場で容易に販売される貴重な商品です。盗まれた身元データの購入者は、この情報を使用して、無実の身元所有者の名前を使用して詐欺やその他の犯罪を行うことができます。明白な損害の盗難以外に、アイデンティティ所有者の盗難にもかかわらず、そのような違反は、中央データベースのオペレータにとって重大な負債を生み出します。

## 制限付きアクセス

これらの中心にされたデータベースへの不正アクセスを試み、防ぐために、データへのアクセスはオペレータによって制限される。ただし、これにより、ID 所有者が自分のデータにアクセスできなくなることがよくあります。[xiii] オペレータがデータへのアクセスを許可しない場合、[xiv]そのデータはアイデンティティ所有者の利益にリンクすることはできません。 リンクされたデータは、デジタルアイデンティティの重要な要素です，データをリンクすることは、アイデンティティの所有者がデータ間のリンクされた関係を作成することができることを意味します。

データをリンクすることは、技術的に困難な作業ではありません。実際、これらの技術は現在広く普及しています。

リンクされたデータをサポートする主要な技術は、URI（エンティティを識別する方法）です。HTTP（資源を取り出すための簡単でしかし普遍的なメカニズム）; そして RDF（構成するべきおよびリンク データの一般的なグラフベースのデータ モデル）.[xv] これらのテクノロジは長年にわたって存在していますが、個人の ID 所有者はリンクされたデータの恩恵を受けることはできません。中心にされたデータベースの使用によってもたらされる技術的な限定およびセキュリティ上の問題に加えてアイデンティティ データの単一の大きいデータベース オペレータのいくつかの商社がある。

## 独占

地球上のすべての人のアイデンティティデータを含むデータベースを持つ単一の営利目的の組織があった場合、それは独占として作動し、それへの

アクセスのための高い値段を満たせたデータ。なお、オペレータが牽引を得たら、「ネットワーク効果」はネットワークに効果的にユーザーを締める。これは、それから、新市場の関係者のために重要な参入障壁を作り出す。競争圧力がない時、独占的な価格設定と減られた革新は多分生る.[xvi]

## データ保護への準拠

アイデンティティのための大規模でグローバルに集中化されたデータベースは、データプライバシーとデータ保護の法律に違反する可能性もあります.[xvii]

国民および超国家的なデータ保護の法律はそうしなければ個人的なデータを重い金融罰および可能な投獄の下の脅威できるだけ安全保つためにデータ コントローラーによって設置される方針およびプロシージャを保障するように設計されている。ただし、これらの法律は各管轄区ごとに異なり、遵守基準は非常に異なります。 近年、データ輸出規制を採用している管轄区域への傾向が高まっている。例えば、「EU は、米国のプライバシーに関する法律が EU の妥当性要件を満たしていないとみなしている[xviii]".それに答えて、「プライバシー盾」のフレームワークにもしばらくある特定の会社だけEU から米にデータを移す資格がある。これは、これらの厄介で潜在的に高価なコンプライアンス要件を満たすことができない新興企業の参入障壁である。この問題を複雑にするために、「プライバシーシールド」の枠組みは、欧州司法裁判所が不十分とみなした「安全な港湾」メカニズムに代わってから 18 カ月以内にすでに脅威にさらされています。

ほとんどのデータ保護の法律への本部はユーザーの承諾の概念である。これは個人によって普通それらがカチカチ ボックスか同じようなメカニズムを通して個人的なデータを提供する時与えられる。 しかし、個人が既存のアイデンティティ管理プロセスの震源地にいるわけではないため、同法に基づく権利を譲り渡すことはできないが、時間の経過とともに同意を得たり、同意を追跡したりすることは容易ではない。 ますますデータ保護は、これらの問題を克服するための動的同意メカニズムを必要としますが、紙ベースの大部分の同意モデルではこれを達成することは困難です。

近年、FATCA の導入、共通報告基準（共通の報告の標準）およびその他の国際的なデータ共有契約により、いくつかの異なる管轄地域の規制当局間で国際的なデータ共有制度が大幅に増加しています。これらの共有契約の多くは、国家データプライバシー法の下でのデータ主体の同意要件からも免除されるため、データを共有する前に個人の個人所有者の同意は必要ありません。アイデンティティデータが定期的にボーダーを交差させるセクターの 1 つは取消機関の間で共有される金融サービスとデータ定期的に含んでいる KYC プロセスによって得られるアイデンティティーデータをある。

## KYC の規制要件

KYC の法律は国民であり、規模で国際、依存の巨大で、多様なグループを表して（限定なしで）次を含んでパーティを楽しむ: 硬貨交換、fintech の開始、お金の送信機、不動産会社および代理人、貴金属のディーラーまたは貯蔵設備、受託者、団体のサービス・プロバイダ、貸方、銀行、証券会社、弁護士、会計士、非営利基礎、専門のサービスプロバイダ、公証人、政府、保険業者、再保険会社、金融機関および一般にお金か財政で対処する法的主体または自然人。

KYC は KYC の法律に従う失敗のためのローカルおよび国際機関によって課されて市民か刑事制裁が、必須選択ではない。 残念ながら、多くの個人そして大きい株式会社への小さい開始会社から、また依存党 KYC 承諾のために高く、苦痛な現実はある。

依拠当事者のために – KYC は高価で時間がかかる。 KYC コンプライアンスの年間平均経費は、平均銀行の場合 6,000 万米ドルですが、他の国の場合は 5 億米ドルまでです。[xix]最新の ID データに迅速かつ容易にアクセスしたり、データを検証したり、規制要件を満たすためにそれをスクリーニングすることができないため、このコストは必然的に高くなります。 したがって、依拠当事者はアイデンティティ所有者に新しい要求を送信し、すべてのアイデンティティ所有者を「ブランクキャンバス」として扱い、完全に堅牢な KYC プロセスを通じてそれらを強制しなければなりません。

KYC の確認の点検を行うために費やされる 1 つの依存党による時間そして努力は再使用されるか、またはリサイクルすることができないし、未来の要

求でてこ入れされない。アイデンティティの所有者がサービスプロバイダを変えることにすればこれらの同じ点検は新しい依存党によって完了する必要がある。アイデンティティデータは新しいサービスプロバイダに「移植」されず、複数のプロバイダによって保持されます。その多くは、もはや顧客または顧客ではなくなった個人のために、重複しているが高度に機密性の高い ID データを保持します。この手続きに伴う高コストは、サービスプロバイダーを変更して競争の激しい環境に陥り、身元の所有者、新興企業の創業者、イノベーションを損なう障壁となり、個人の個人情報盗難のリスクを増大させます。さらに、政府が発行した身分証明書がない人は、KYC 規則を遵守できないため、商業から完全に除外されています。確かに善意ではあるが、KYC の規制は合法的な市場[xx]参加者を容易に排除し、国際取引を遅らせることができる。この問題は迎合的な方法のボーダーを渡ってつながるある KYC データのための方法があったら再使用し、容易に左舷に取った容易に解決してもよい。

# ソリューション：〝セルフキー〞自己主権デジタルアイデンティティエコシステム

私達の考えは簡単である: そのユーザーは彼らのアイデンティティ管理プロセス、自己主権アイデンティティ（SSID）として知られている概念の中心にあるべきである。 私達は紙ベース文書のレガシー システムから脱出し、セルフキーのとのプライバシー、保証、透明物および個人の権利のデジタル アイデンティティに動いてもいいブロックチェーンテクノロジを使用して構築された SSID 実装で、対応する鍵はデジタルアイデンティティウォレットに保持されます。

セルフキーは、以下を含むいくつかの重要なコンポーネントで構成されるオープンプラットフォーム上で構築されたアイデンティティシステムです。セルフキー財団、チャーターとガバナンスが自己主権的アイデンティティーの原則を裏付ける非営利団体、アイデンティティの所有者のための自由な、開

いた源のアイデンティティの札入れが付いている技術の積み重ね、KYC の法律および規則に従う第三者のアイデンティティのマイクロ サービスへの進水、JSON-LD の（機械可読）議定書、関係、および天然トークンで利用できる実質の製品とサービスが付いている市場は有効な、完全デジタルの、自己主権方法の交換価値そして情報にセルフキーの生態系を可能にする「キー」を呼んだ。

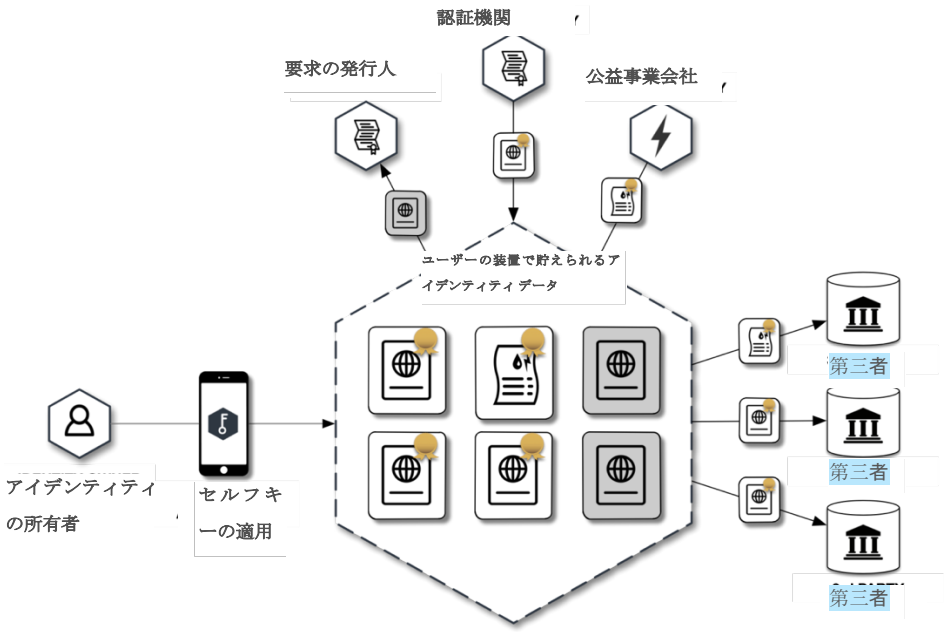
## 発売[xxi]時に入手可能な製品:

- ビット硬貨およびデジタル資産はサインアップを交換する
- 不動産アプリケーションへの投資による市民権
- 会社設立（株式、財団、LLC およびトラストによって制限される会社を含む）
- 銀行口座の紹介と申請
- 100 ヶ国以上のための在住の塗布
- E -札入れか貯えられた価値設備
- 金および貴金属保管
- 保険アプリケーション
- 送金と送金

有形実用性をアイデンティティの所有者の主トークンに提供して、頼って間、現実の世界の製品とサービスを通して、発行人をセルフキー克服する中心にされたアイデンティティ システムの限定をパーティを楽しみ、要求する、助けは広範囲の国民のデータ保護の法律および KYC の規則の承諾を達成し、個人-アイデンティティの所有者にアイデンティティ データの所有権そして制御を戻す。

セルフキーは、アイデンティティ取引をより安全かつプライベートかつ効率的にしながら、今日のさまざまな法律や規制に準拠させます。しかし、セルフキーは、デジタル署名された ID 要求の検証、データの最小化、個性の証明、適切なガバナンス、ユーザー中心の ID システムを備えたより良い世界への橋渡しをしています。この新しい世界では、ユーザーは偽りなくできるよう、制御し、デジタルアイデンティティーを所有することになります。セルフキーは、セルフファウンデーションを通して、よく設計されたオープンソース

テクノロジースタック、および透過的な法律とガバナンスのインフラストラクチャを通して、検閲、公正、包括的、機敏、そしてリーンになるように設計されています。セルフキーは現時点では現実に、現代社会および全体的なインターネットを展開する未来の必要性は、アイデンティティの人権で基本的な自由を保障して満ちている。




# ブロックチェインは答えですか？

ブロックチェーンは、データをすべての参加者に同時に複製する分散元帳です。 私たちのアイデンティティデータは、多数の参加企業（例えば、大手銀行や政府）によって管理されているブロックチェーンに保存され複製されるべきですか？

# ブロックチェーン（単独）は答えではありません。

すべての党へのすべてのアイデンティティ データを複製することは可能性としては前のセクション、とりわけ個人的なデータを「国内」保つ条件でまたは指定司法権の内で上で記述されているデータ保護の法律をさまざまな理由で破ることができる。なお会社が彼等のに関連しているビジネスおよび個人的なデータを貯えるように、規則および最良実施は要求する、だけだけ顧客の承諾と。

アイデンティティデータがすべてのブロックチェーンノードに複製されると、サイバーセキュリティリスクが増加します。 中央のデータストアは（上述のように）セキュリティを確保するのが難しい。したがって、ブロック・チェインを使用して多数党へこのアイデンティティデータを単なる複製することはきちんとこのデータを保証するために鎖の各ノードを強制する。各構成には自身のサイバーの保証練習（そしてギャプが ）あるので、これは攻撃者がデータを盗む事ができるようにそれをもっと簡単にする。個人データが暗号化されていても、暗号化されたデータは依然として個人データ規制を実行する可能性があるため、法的遵守の問題は解決しません.[xxii] 分散させていた帳で握られたトランザクション記録からの個人を再確認するように努めるように十分に動機を与えられただれでも多分他に利用できるデータベースからの個人を再確認する資力がある。ブロック・ チェインの匿名の事実は一部ではありません。「大きなデータ」時代では、強力な分析の技術はありません、これは個人的なデータを記録するブロック・チェインの解決のための重大なコンプライアンス試験である 個人的に確認可能な情報のようにあるマッチのデータベースに適用することができます。

**答えはなんですか?**

自己の主権デジタル アイデンティティの概念は私達が私達の非デジタルアイデンティティを今日貯え、管理する方法に類似している。 現在、私達のほとんどは私達の自身の制御の下で私達の家でパスポートのような身分証明書をおよび出生証明書またはガス電気水道代-安全に、しっかり、保つ。私達は他の実体と必要なときだけそれらを共有する。 私達のほとんどは三番目のこれらの重要な紙の文書（か不必要な個人情報を）党私達ほしいに貯えない。セルフキーの自己主権アイデンティティは既に私達のほとんど私達の物理的な身分証明書とするため何のデジタル等量である。

**セルフキーが個々のユーザーにどのように機能するか**

新しいユーザーは個人的な装置のセルフキーの札入れの塗布を単にダウンロードする。 アイデンティティ データは装置で、局部的に貯えられる。 ユーザーは別の装置または個人的なバックアップ解決にこの情報をバックアップできる。

ユーザーがセルフキーの札入れをダウンロードするとき、空である。これで貯えることをユーザーのニーズ最初の事は公共/プライベート キーの組（別名セルフキー）をコンテナに詰める。 このセルフキーは文書にアイデンティティの所有者の独特なデジタル署名を加えるのに使用することができるユーザーのデジタル「ペン」になる。

プライベート キーはアイデンティティの所有者にだけ知られているので、このデジタル署名が適用した時はいつでも、党を機密そしてしっかり要求することに所有者のアイデンティティを認証し、認可するのに役立つ（本人が姿を見せないで）。

セルフキーは従来のユーザー名とパスワードを超えて大きなメリットをもたらします。

各セルフキーは所有者に固有のものです。 ユーザ名とパスワードの組み合わせが第三者のデータベースに保存されている場合、セルフキーユーザは決して自分の秘密鍵を共有しません。これは常に秘密です。 しかし、ユーザは、公開鍵を安全かつ自由に共有することができます。

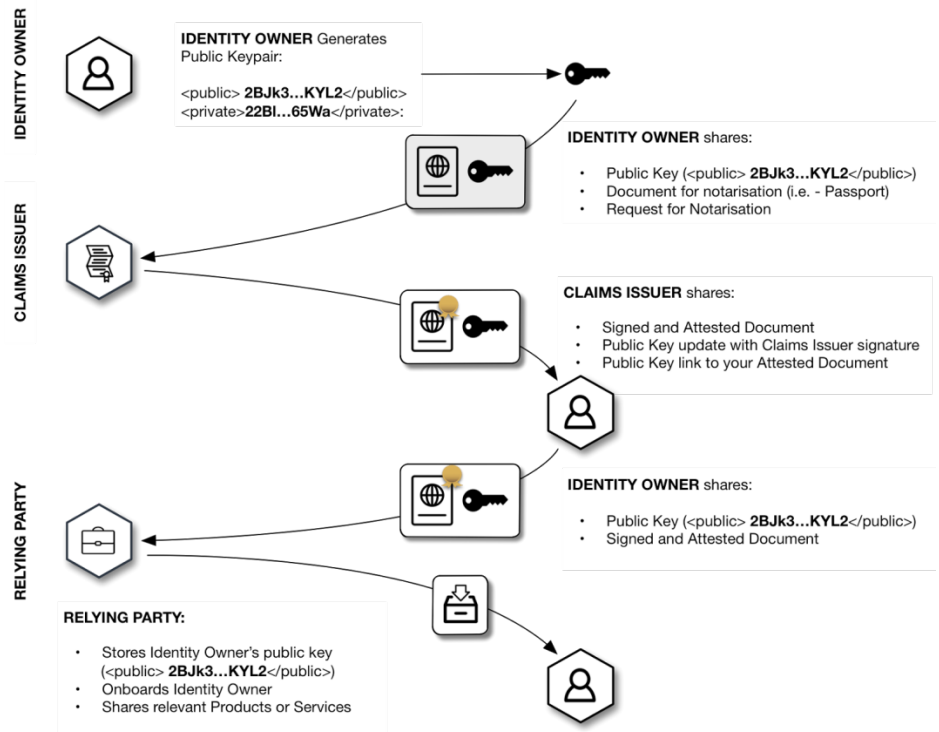
この段階では、一人ではないはセルフキー基礎これがユーザーの容器であるか、またはセルフキー数があったことを知っていない。他のエンティティはそれを発行しておらず、それはユーザーによってのみ作成されたものです。これはまさに自己主権を意味するものです。ユーザーは、自己証明書とともにセルフキーを使用して、公証人、政府機関などの関連する請求書発行者からのアテステーションを受け取ることができるようになりました。ユーザーが自分のデジタルウォレットに格納されているIDクレームを確認した後、セルフキーマーケットプレイスで商品とサービスを購入する資格があります（詳細は下記参照）。

セルフキーユーザーがセルフキーマーケットプレイスで利用可能な製品とサービスを利用するためには、まず、ID クレームを作成する必要があります。これらの ID クレームはユーザーの属性（国籍、生年月日、職業など）で、テキストフィールド（JSON-LD BLOB）に格納されます。手動でこれらのテキスト分野にデータをタイプするためにそれが取る時間を節約するため写真または文書のスキャンは救うことができ、光学式文字認識は自動的にプロセスを大いにもっと簡単にする情報を分析する。これらのアイデンティティの証拠は従来の KYC のドキュメンタリーの条件に従うためにただ必要とされる。 将来、セルフキーは私達がそれらを今日知っているように証言に除去する身分証明書をデジタル署名した。

アイデンティティの要求が作成されたら、プロセスの次のステップはこれらの要求の証言を受け取ることである。 証言はセルフキーの札入れで貯えるもことができる。 これらの証言はまたある特定の時間の窓の内で有効の場合もある機械可読の、デジタル式に署名されたアイデンティティの要求である。

公益事業会社、公証人、銀行、パスポート代理店、病院、運転免許証の権限、移住のような要求の発行人か関係当局は、可能性としてはユーザーの要求に署名できる。これらの主張は、最低限の情報のみを開示する方法で署名することができま

す。言い換えると、アイデンティティの所有者は、要求側当事者が知る必要があるものを共有することができますが、それ以上のことはありません。

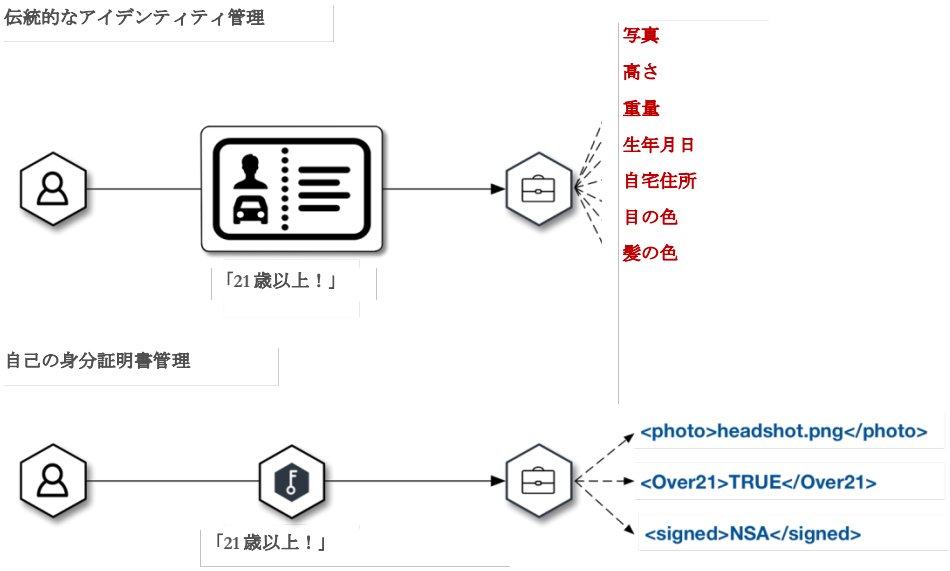



例えば、ユーザーは容易にそれらがある特定の国に存在することを証明できる。 または人はそれらが 18″にこの情報ことをより多くを明らかにしないであることを証明できるかもしれない。これらのアイデンティティ属性は無限であり、「プロの投資家」などのものも含めることができます。アイデンティティ所有者は、どのピラミッドの情報を信頼する人に渡すかを選択することができます。 アテストできるアイデンティティクレームのタイプはほぼ無限です。

データはデバイスに保存されます（所有者の管理下にあり、現在は自宅やオフィスに保管されています）。所有者が望む場合は、特定のデータを収集するために第三者に承認することができます。前記装置上の通知を確認することによってこれを行うことができる。 この経験は、フェイスブックアカウントを「リンク」することによる認証に似ています。

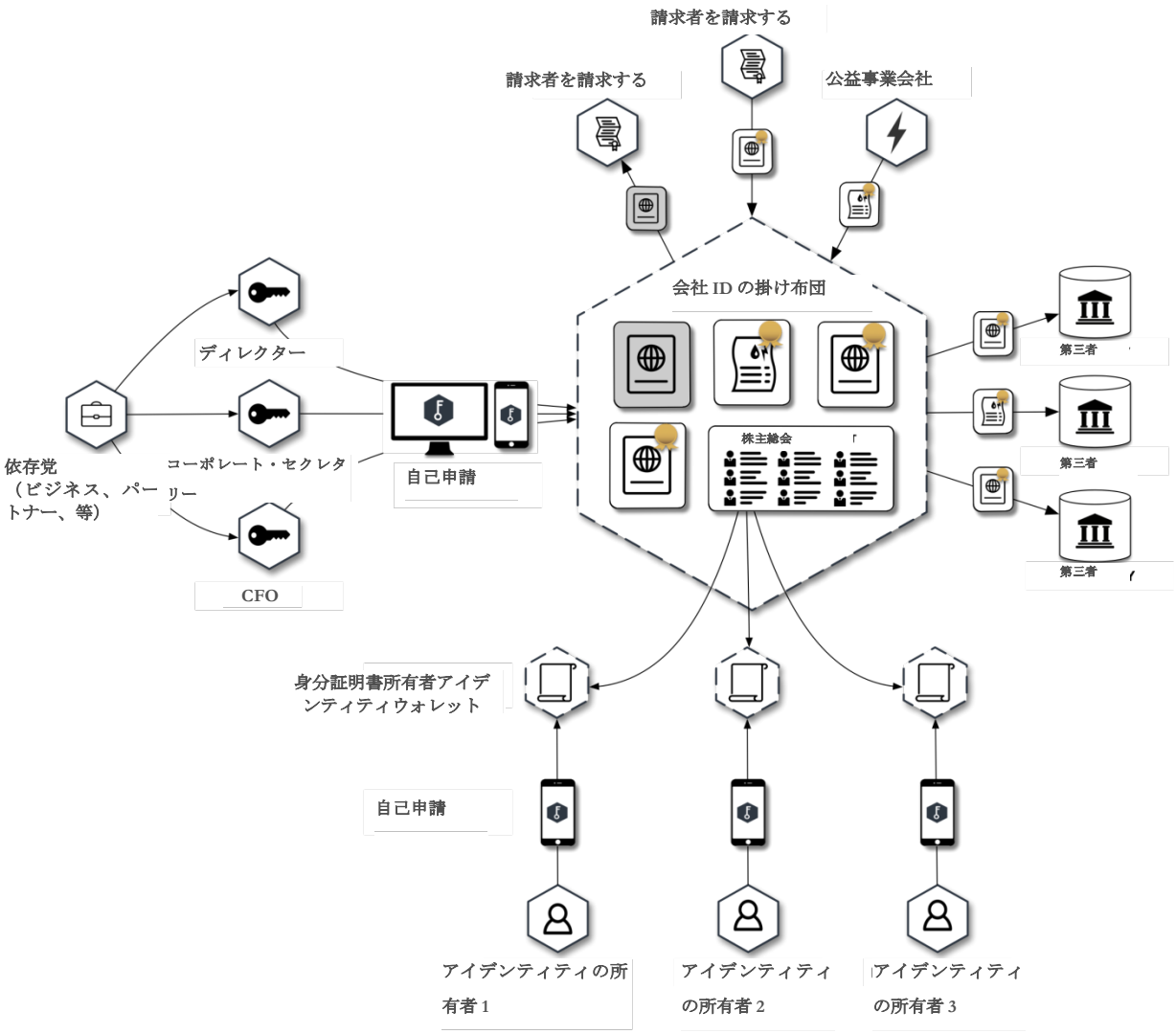
この類推は経験上似ているだけで、個人データを収集するためにフェイスブックのサーバーに行くのではなく、ユーザーが個人データストアから要求を許可し、共有されるデータを細かく制御します。特定のインターネット企業とは異なり、セルフキー財団は非営利団体です。 ユーザーデータの広告や販売によって収益化はありません。

共有される必要があるデータの量を最小にすることはより安全アイデンティティの提供者および依存党のための両方である。アイデンティティの所有者は不必要なか感知可能データであるかもしれない情報を共有しないし、-受け手はそれを貯える必要はない。これは、セキュリティと管轄の個人の法律要件への準拠の両方に役立ちます。




## 会社のセルフキーのしくみ

前に述べられるように、アイデンティティの要求および証明された証拠は人に限られなかったりまた会社に適用できる。会社はアイデンティティの札入れからの起動文書を同様に管理できる。セルフキーに基本的な帽子のテーブル管理があり、開始が銀行口座の開始のような現在厄介である事をするようにする基本的な企業管理を提供できる。当事者を新会社に頼る場合、KYC は、特定の会社レベルで行うだけでなく、最終的な有益な所有者に達するまで、エンティティの上の各所有レベルでの重要な株主に対しても行う必要があります。この種のドキュメント検証は非常に面倒です。 さらに、複数の子会社や関連会社を複数の国に持つ多くの企業にとって、これは、リンクされた ID がマルチレベルの検証を提供し、国家的な集中システムが解決できないものであれば、e-KYC の利点がより魅力的です。セルフキーを使うと、会社は毎日変わることができるかどれが）認可するためにことができる容易に事伝統的に集中的で、証明すること困難アイデンティティの所有者の時間であるおよび依存党を示す（多数所有権は、複雑な構造、資本化のテーブル水平になる。




## クレーム発行者のためのセルフキーのしくみ

何人かの会社があり、パーティを楽しむかかだれが依存による使用のためのアイデンティティの所有者に代わる問題の（または出ることができる）要求によってが全体的の施設。KYC 空間内では、このような有力企業の現実的な例がある（現在紙文書を発行している）。 銀行（証明書を提出する者）および会社登録簿（紙の書類を発行する者）。セルフキーは、依拠当事者が喜んで支払うこれらの身分請求をデジタル化し収益化するために、今日使用することができます。これはセルフキーの生態系の暗号化の補強を助ける。クレーム発行者は、セルフキープラットフォームで完全にデジタル証明書を発行することもできます。 この会社の所有者は、株式を登録するために使用された SelfKeys を保有していることを証明することによって、所有権を即座に検証することができます.[xxiii]

### セルフキーネットワーク

セルフキーネットワークはインターネットに安全な、暗号化された P2P、構造化されたデータ ファイル共有のためのちょうどアイデンティティ システムより多くである。セルフキーネットワークは次のパラグラフで探検される複数の革新的な属性とそれに長期採用および成功のための最もよいチャンスを与えるように設計されている。

# 財団

まず第一に、このペーパーで前に記述されているように、それは単一の会社のために維持不能アイデンティティ システムを制御するか、または支配するためにである。したがって、ネットワークを支配するのではなく、特定の核心的憲法原則（以下に述べる）を維持するための基盤が形成された。基礎は自己主権アイデンティティの創設の原則を保護し、維持する。

### 非営利のステータス

セルフキー財団は、ネットワーク全体とネットワーク（KEY）を実行するネイティブトークンの成功を最優先にしています。基礎は非営利で、彼らの適用を開発し、商業化するのにブロック・チェーンの技術の会社によって使用することができる規定する砂場の立法から寄与するマリシャスでセットアップされる。セルフキー財団は、システム内を流れる ID データを販売したり、広告として提供したりしません。 ネットワーク内のすべての値は、ネイティブの KEY トークンを使用したり、使用したりするように設計されています。

セルフキーネットワークの重要な要素は、KEY と呼ばれるネイティブの ERC-20 トークンです。これは、「自分自身を暗号化する鍵」を表します。このトークンは、ネットワーク上の製品やサービスにアクセスするために使用することができます。たとえば、KEY に参加する必要があり、参加、優れた行動や使用を奨励するために使用され、価値のある価値のあるアイデンティティの自己強化暗号経済を可能にします。 より多くの個人と企業がネットワークに加わり、KEY の需要が増加しています。ネットワーク上の特定のアクションは KEY の交換を必要とし、他の人は KEY をロックされた契約（ネッ

トワークにアクセスし、反 Sybil メカニズムを介してスパムを防止する）に置くことを伴うでしょう、この研究は POI ネットワークに大きな影響を与える可能性があります。

## ガバナンス

セルフキーは利益の会社、KYC 鎖株式会社（KYCC）のための a によって創設された供給されたコードを開け、基礎をセットアップするために金融貢献をした。 基礎のためのソフトウェアを開発し続けるセルフキーネットワークのため主トークン ホールダーが開いた源のプラットホームを同様に発達させることができるようにそれ繁栄することは必要である。メンバーは、セルフキー財団からの配当金または利益の分配を受ける資格がありません。 KEYの所有者は、ネットワークを成長させるための独自の努力によって得られた財政的インセンティブを受け取るかもしれませんが、KEY トークンの取得による利益の期待はありません。しかし、

## 法的

目的が臨界量と採用を達成するとデータ機密性、データ機密保護、その他の重要な方法については約因の既存の法律はそのままと残余の迎合的なあらゆるアイデンティティーシステムのための重要な代表団である これを受けて、セルフキーの建築はかのようにデータ機密性の法律の規定することと迎合的、特ににあるために、全体的に入手しやすそうに分散しているようにため、 設計されている。これは適用範囲が広いののユーザーにあらゆる 1 つの特定の貯蔵システムで文書を貯えさせるアイデンティティの所有者の承諾がアイデンティティトランザクションを誘発するように常に要求し、ユーザーによってによって堪能運転されるアプローチである。

アイデンティティの所有者は彼らのアイデンティティを管理していつもある、依存党はアクセスを認可されたアイデンティティの要求もっとすぐに缶詰にし、要求の発行人は彼らの貢献および証言のための支払を受け取ることができる。このフレキシブルでユーザー主導のフレームワークは、海外のデータ転送に関するさまざまな国の要件を満たすのに役立ちます。

アイデンティティ システムが展開するかもしれない法的および技術の抑制そこが原因で変えることはある点で適用範囲が広くまたは何か、（貯蔵の層のような-それどころかタイム スタンプとしてブロック・チェーンに切り刻まれる）他で堅く、指導の精

神べきであると同時に個人の権利および自己主権アイデンティティの保存のような。T その目的のために、以下はセルフキー財団の憲章の原則です。

## セルフキー財団

これらの憲法原則はセルフキーの基礎のまさに支配そして制御機構に文字通り焼ける。これらの原則を違反することは、これらの原則を技術的かつ法的拘束力を持つ憲法に反している。

**存在。**ユーザーに独立した存在が常にある。どの自己主権アイデンティティでも生命の証拠から得られる。 および支えられ、支えられる自己の穀粒、セルフキーがあらゆる 1 つの国民システムを越えてあるように私達のシステムを設計するように努力すること州代りあらゆる 1 の国家に優先順位を置くかわりに促進することは私達のシステムの最も重要な関係者に個々の自然な生きている人をする。

**コントロール。**ユーザーは常に自分の身元を完全に管理します。ユーザーは自分のアイデンティティに関する最終的な権限です。ユーザーは自分の ID を参照したり、更新したり、非表示にしたり、消滅させたりすることができます。 ユーザーは自分の好みで宣伝やプライバシーを選択することができます。

**アクセス。**ユーザーは自分のデータにアクセスできます。彼らは簡単にすべてのクレームやその他のデータを取得することができます。 換言すれば、ネットワークはユーザに関する隠されたデータを許容しない。 これは、ユーザーが自分の裁量でのみクレームを変更できることを意味するものではありませんが、ユーザーは自分の身元についてのいかなる請求についても気付くでしょう。

**透明性。**セルフキーが所有し、運営しているシステムとアルゴリズムは、それらがどのように機能し、どのように管理され、更新されるかにかかわらず、透明かつオープンなソースです。システムを管理する基盤は透明です。

**持続性。**アイデンティティは耐久性があり、長命である。 プライベート キーは失われるかもしれ回る必要があり、データは変わる必要があるかもしれないアイデンティティは主張し、残るべきである。

**移植性。**すべての情報は単一の第三者の実体、アイデンティティを管理するアイデンティティの所有者の残物によって運送可能、最終的に握られなくて。

**同意。** アイデンティティ所有者は、データの移転または使用に同意する必要があります。

**最小化。**要求の発表は最小にならなければならない。 データが表われるとき、その発表は手もと仕事を達成するのに必要なデータの最少量を含むべきである。 ユーザー情報の最少量は右の状況の下の右の実体--にだけさらされる。

**保護。**対立がアイデンティティ ネットワークの必要性と個々のユーザーの権利の間に起こる場合、セルフキー ネットワークはネットワークの必要性上の個人の自由そして権利を維持する。 アイデンティティの証明は分散させていた方法の検閲抵抗力があり、力弾力性のあり、そして操業である独立したアルゴリズムによって起こる。

**相互運用性。**セルフキーは相互運用可能であることを向ける。プライベートキーおよび自己主権アイデンティティの検閲のブロック・チェーンそして自主性の固有の持続は企業の広い範囲の広く、連続的な供給を、保障する。 努力は他のアイデンティティ システムとの互換性を保障するためのなされる。

これらの原則は、財団の憲法の一部であり、メンバーによって選出された理事会または理事会は、これらの原則に従った決議または措置にのみ合意することができます。

# セルフキーテクノロジースタック

**ノードの検証** -私達のシステムの中心のレベルでエテリアムノードを認可している。私達は権限のエテリアム「証拠」を使用して問題があるときだけこのレベルで考慮したが、エテリアムの正常な一致のメカニズムを使用し、変わることを選択する持っている。 テストでは、私達は EVM、Eris、月曜日斧および貨幣の真新しい一致の議定書使用し、もし基礎板が最もよい企画としてこれを定めれば代わりとなるブロック・チェーンはセルフキーのための将来選択に残る。 私達は公共のブロック・チェーンが最も公平、現在ある最も含んだ、よく最も採用されたブロック・チェーンだったことを見つけた。

**ブロックチェーン層**-セルフキーキーペアは、エテリアムパブリックネットワークからのものです。

**貯蔵**–アイデンティティの国際的なシステムの承諾に挑戦があるので、私達はアイデンティティの所有者の思慮分別まで貯蔵の層を完全に作った。 文書はユーザーの装置で（承諾および思慮分別で）アイデンティティの所有者が文書かデータを他の所で動かす場合までの局部的に置かれる。 後で、貯蔵の運転者はユーザーの制御記憶機構のために造られる。

**キー管理/回復**

それはユーザーによって管理されるアイデンティティ システムで避けられない何人かの基づいてユーザーが彼らのキーをに置き違えるか、または失うブロック・チェーンのキー。 このような場合すべてのキーを–そして回復する方法がなかったら、証言は失われる。 幸いにも、私達は解決を開発した。セルフキーは起動時に便利なキー回復メカニズムである Uport を使用することで、ユーザーは選択した 1 つ以上のアカウントに回復の責任を委任できます。 Uport は相互運用性を提供し、エテリアムのコミュニティが既に認めて受け入れている標準をベースにしています。

代理契約ソリディティコードは非常にシンプルで、参考のためここに示します

```
contract Owned {
    address public owner;
    modifier onlyOwner(){ if (isOwner(msg.sender)) _ }
    modifier ifOwner(address sender) { if(isOwner(sender)) _ }

    function Owned(){
        owner = msg.sender;
    }

    function isOwner(address addr) public returns(bool) { return addr == owner;
}

    function transfer(address _owner) onlyOwner {
        owner = _owner;
    }
}

contract Proxy is Owned {
    event Forwarded (address indexed destination,uint value,bytes data);

    function forward(address destination, uint value, bytes data) onlyOwner {
        if (!destination.call.value(value)(data)) {throw;}
        Forwarded(destination, value, data);
    }
}
```

**プロトコル**–セルフキーネットワークを最大限に相互運用可能にさせるためには、いくつかの標準および進行中の仕事はプロトコル レイヤに専用される。これはデータが 1 つの場所と別のものの間で構成されたフォーマットでいかに動くかである（別のものへの可能性としては 1 のブロックチェーン）。

仕事は他の一流のアイデンティティ システムとのこの区域でインターオペラビリティを保障するために行われている; Sovrin、W3C、Uport、等。

**ID ウォレット**– セルフキーアイデンティティウォレットは、起動時に使用可能であり、すべてのアイデンティティトランザクションの出発点です。 ウォレットには KEY も保存できます。

アイデンティティの札入れを通してユーザーはまた適用業務層の異なったにアクセスできる。 どの会社でもこの適用業務層で造ることができる。 どのアイデンティティの提供者でもまたキーの相互運用可能任意政府の電子商取引の法令の下で修飾するセットをか証明書、例えばさまざまな x509 証明書作るかもしれない。

**ID マイクロサービス**- マイクロサービス層は、主に国際法および規制への準拠を可能にし、主に債権発行者および依拠当事者によって使用されます。どの会社でも、KYCC 造ったこれらのマイクロ サービスを提供する、セルフキーシステムにてこ入れする複数の ICO および最初の適用業務層支えるかもしれないし、認可のようなある最初のマイクロ サービス提供されるスクリーニング（仲介される再）、会社の登録調べおよび文書のコレクションおよび確認（コレクター）リストしなさい。

**アプリケーション層**-完全オープンソースのウォレットを含むオープン API のオープンソースコードを持つため、どのアプリケーションもセルフキープラットフォーム上に構築できます。

# 従来のアイデンティティシステムに比べてセルフキーネットワークの利点

アイデンティティの所有者を含むアイデンティティの生態系のすべての党に利用できる多数の利点がある頼ってそれぞれに異なった議題がある発行人をパーティを楽しみ、要求する。次図表は分散させていたアイデンティティシステムがすべての党のために有利である場合もあることを示すべきである。

| | 集中型伝統的アイデンティティシステム | **セルフキーの分散アイデンティティシステム** |
|---|---|---|
| アイデンティティの所有者 | -同一性を所有または制御しない<br><br>-繰り返し搭乗プロセスの多数によって調整装置を満たすことを行く必要性<br><br>-ログイン プロセスのための手の多数の証明装置を保つ必要性<br><br>-あるサービスから別のサービスに情報を容易に移植できない（高いスイッチングコスト）<br><br>-識別文書を共有しなければならず、最小限の情報しか共有できない<br><br>-政府の許可それでは権限の下に依存する党にだけ存在する<br><br>-アイデンティティまたは KYC プロセスの出力を再利用またはリサイクルすることはできません<br><br>-会社の文書を簡単に管理したり、重要な意思決定のために署名を集めることはできません | -彼らのアイデンティティを完全に承諾し、管理する<br><br>-ウォレットに格納された単一のキーペアで複数のサービスで認証する<br><br>-最小限の情報を共有することができます<br><br>-失われた鍵を回復することができます<br><br>-ひれの技術プロダクトおよびアイデンティティ サービスの市場にアクセスできる<br><br>-容易に会社として文書と範囲の一致に署名できる |
| クレーム発行者 | -アイデンティティクレーム（つまり、公益企業）で収益化しないでください。<br><br>-請求を取り消すことができません<br><br>-請求をすばやくすることはできません<br><br>-アイデンティティクレームは時には詐欺的です | -アイデンティティを収益化することができます<br><br>KEY による申し立て<br><br>-請求を取り消すことができます<br><br>-請求をすばやく与えることができる<br><br>-出される要求により多くの信任がある |
| 依拠当事者 | -搭乗の顧客に法的な要求事項を満たす時間および努力をたくさん使わなければならない | -素早く ID 所有者に搭乗することができます |

| | | |
|---|---|---|
| | -顧客に不十分な経験がある搭乗の経験で悩むことを持っている<br><br>-顧客データをインポートする方法がない<br><br>-多くのお金を KYC を認めるために要する<br><br>-費用がかかり、国際的な対応が難しい<br><br>-プロセスは、コンプライアンスチームによる紙ベースの手作業によって推進されます | -クライアントを喜ばせることができます<br><br>-追加のクライアントの詳細を簡単に要求できます<br><br>-スケールメリットの恩恵を受けることができます<br><br>-国際的に準拠することができます<br><br>-プロセスは KEY によって駆動され、RP によってチェックされます |
| 総合システムの特徴および利点 | -データの巨額の金は大きいサイロに坐る<br><br>-従ってハッカーのための報酬はより大きく、より大きいターゲットである<br><br>-独自の秘密<br><br>-データの独占を創造する<br><br>-他者との相互運用性が低い<br><br>-価値はユーザーに戻らなかった<br><br>-一人の当事者が所有し、管理する<br><br>-単一障害点<br><br>-伝統的に大きいデータ損失、欺瞞の例に導き、自己主権デジタル アイデンティティからの世界を握っている | -流通網は多数の小さい貯蔵を可能にする<br><br>-侵入に対する報酬は低い<br><br>- ユーザー中心主義<br><br>-オープンソース<br><br>-失敗のポイント無し<br><br>-中心にされた管理か制御無し<br><br>-国際的な文脈に適される<br><br>-より透明な |

# KEY トークン

キーはすべての製品とサービスがいろいろな行為によって「アイデンティティ生態系」に動力を与えるのに使用されるキーでわずかな支払によって利用できるので生態系を動かすことに重大である。 例えば要求証言のための支払のような事をするのに、キーが使用することができる; アイデンティティ

の要求を受け取れば（ユーザーに戻って価値を与えなさい）; 市場のリストの支払をしなさい; そして一般に、交換価値に、使用および採用に報奨金を支払い、トークンとしてアクセスを許可しなさい。

次図表に示すように、生態系の各メンバーは有望なシステム使用、キーを利用すること、およびアイデンティティの証拠および証明された要求を提供することで遊ぶべき貴重な役割がある。 下はキーの使用の徹底的なリストではないが、-ネットワークの進水から豊富なトークン実用性がある、他の多くのトークンとは違って、キーに実在価値があることは明確なはずで。

## 鍵トークンの使用

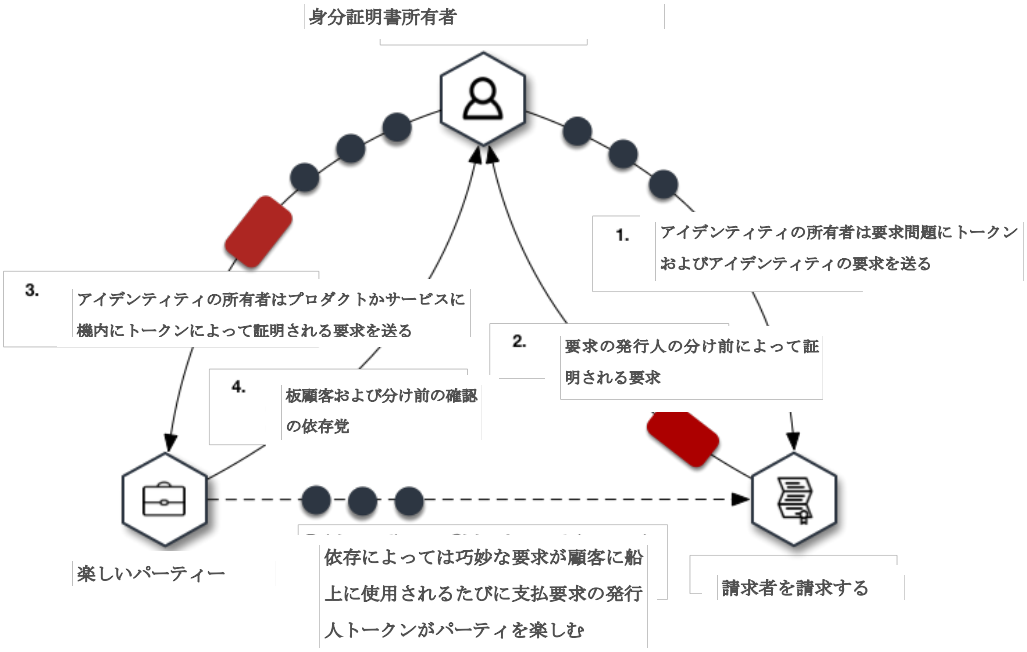
セルフキーネットワークの進水で、次のサービスは利用できる：

- 設立
- レジデンシー
- 投資による市民権
- 送金
- 国際保険（許可されている場合）
- eWallet / SFV 施設
- 銀行口座の設定

この生態系の中では、3 つの党だけ交換価値。 アイデンティティの所有者によっては、頼って発行人がパーティを楽しみ、要求する。

セルフキーに依存党、アイデンティティの所有者によって署名し、発行人を要求する信頼フレームワークがある。「信頼フレームワークは新しい概念ではない。それらはデジタル アイデンティティの世界のの内側と外側の両方に一般的である。大抵それらが関係者が共通のタイプの他の関係者のだれでものトランザクションで従事する機能を支配し望む一貫した、予想できる方法で使用されているいろいろ複数政党制システムをそうするのに。このような場合、それらは働き、量ると証明される。” [xxiv]

セルフキーの信頼フレームワークはまたきちんとよい行動に報奨金を支払うために特定の議定書のレベル情報をキーについての情報含んでいる。アイデンティティの所有者が、発行人を要求し、依存党がネットワークの適切な使用に報奨金を支払うのを助けることができるこの信頼フレームワークに署名することが期待される。これらの文書は、公開されたネットワークの公開やコミュニティのフィードバックに向けてリリースされる予定です c




# 未来を見る

私達の作業仮説はあらゆる司法権のすべてのデータ機密性の法律と迎合的のシステムを開発することは非常に困難であることである。 従って、アイデンティティの所有者はデータがどこにを貯えられる、すべての行為はアイデンティティの所有者によって運転されるか担当し。

重要なのは、個人的なデータおよびアイデンティティ データはトランザクション元帳からデータへの暗号化された参照とそれらを取り替えることによって-「挽肉料理」全体で保たれる。 これらは切り刻むまたはデータがある特定の日付にあったが、-証明すると「指紋」の助けは実際のアイデンティティの要求を共有しているアイデンティティの所有者なしでアイデンティティの所有者鎖のデータは完全に匿名および混乱させる。使用はのまた助けを演説する理論にブロック・チェーンという点において」忘れられているべき「右がない場合もあることを意味する起こったすべてのトランザクションの永久的な、不変の記録を保つためにブロック・チェーンの技術が構成されるという事実に切り刻む。データ保護の法律は世界そうする目的があるので個人的なデータだけが長い間保たれるように要求する。 私達はブロック・チェーンで切り刻まれる個人的なデータの入手の可能性を限る暗号化制御がデータ保護の承諾のための実行可能な解決であることを信じる。 それはホールダーが暗号鍵を所有している限り暗号化された個人的なデータがまだ

ある司法権の個人的なデータとして分類されるかもしれないこと本当である。但しキーは個々によって定まる状況で使用できるようにされてただ決定すること示すことができればそしてデータ保護の見通しからの異議を見ることは困難である。

データは Https を介してある場所から別の場所に流れ、P2P メッセージングプロトコルとデータ転送のためのペアワイズ暗号化手法で作業が行われています。 本質的に、一般人は以下のことを保証することができます：1.データは同意のもとに移動するだけです。 2.データのプライバシーは重要であり、データは誰とも決して共有されません。3.各アイデンティティトランザクションでは暗号化が使用されます。4.データはブロックチェーン自体ではなく、さまざまな暗号化されたメッセージングや 構造化されたデータプロトコル。

ブロック・チェーンはデータが変わらなかったことそれが証明することができることデータを切り刻み、方法でそれ貯えられる。 メカニズムを押す今回は文書のタイムリー性を証明してある特定の状況で重大である。 心配はデータが関連しないし、プライバシーの損失を引き起こさないように取られる。

## セルフキー財布

札入れは（ユーザーが貯え、ID を管理するために要求帰因するかところに）すぐに利用でき、Mac、Linux および Windows のために卓上で利用できる開いた源であり。セルフキーの道路図および即時の交付できる s はこの札入れを可動装置で利用できるために求める。

### セルフキー生態系

セルフキーアイデンティティエコシステムは、私たちが改善するために取り組むもう一つの主要な要素です。セルフキーには、3 つのプライマリパーティー、1）アイデンティティ所有者、2）依拠パーティー、3）クレーム発行者が含まれます. セルフキーは、ネットワーク上でこれらのパーティーをすべて獲得するための 3 者間のマーケティング開発プッシュを行います。

### セルフキー市場

市場はセルフキーの生態系へどの依存党がセルフキーシステムを使用しているかアイデンティティの所有者が見ることができるように可能にするので主要部分である。 市場では、アイデンティティの所有者はさまざまな財政の提供を拾い読みし、特定プロダクトのための注文することができる。 依存党/サービスプロバイダはまたは料金のための提供を市場の自由にリストできる。市場が両面であるので価値を交換するのに、主要なトークンか商品としてキーが使用することができる。

**セルフキーデータの最小化**

の一つの重要なシステムのデータの最小化、すなわち-アイデンティティの断片です。 この本人オーナーを提供して少量の情報を満たすに依拠当事者又は債権力を上回ることが可能である。 ことができる先端技術などの範囲を証明又はゼロ知識証明(ZKP)で行うこともできより特定のプロトコルやアイデンティティの断片です。人がたとえば、あることを証明在留にしたシンガポールを明かさずにその正確な住所です。これが達成できるかを速やかに適切な設計が不要にな長い開発プロセスの ZKP ます。一部の資金の供財団″が主目のデータを最小化します。

**セルフキー個体証明(バイオメトリックリサーチ)**

私達の最初創設の主義として存在、セルフキーのプロジェクトの重要な要素は人のアイデンティティが政府によって出される身分証明書からむしろ人命から始まらないことであるある。これをするためには、特性(POI)の証拠のある程度の研究は生きるようにだれでも、どこでもできる彼ら自身がある特定時に証明行われるおよびセルフキーネットワークへのある特定のアクセスを得なさい。POI の検証とテストが本格的に始まると、このプロセスに関する別のホワイトペーパーが発表され、リリースされます。私達は現在提案されている何がエテリアムのコミュニティ-一連のビデオ呼出しで POI が生物測定学とよりよりよく解決することができることを信じる。1 つがすべて必要とするようになお、基礎は試みるために補助金を出し、あなたのキーを失ったら全く生物測定の基づいたキー回復のメカニズムをすることは、ない複雑な頭脳パスワード、あなた自身でありではない。

# セルフキーチーム

セルフキーのプロジェクト チームはアイデンティティおよび未来について熱情的である、また企業で最も明るい法的およびビジネス心のいくつかを取囲む非常にベテランの改新者のグループ。詳細 www.SelfKey.org

# 結論

セルフキーは私達の展開の全体的な社会のための最もよいモデルとして自己主権アイデンティティ システムを提案する。セルフキーは分散キー マネージメントおよび回復システム、JSON-LD の多用性があるフォーマットの W3C と基づいて、十分に分散させていたブロック・チェーンによって互換性がある動力を与えられる、確認された要求におよび分散支配の非営利基礎によって開発される議定書を維持するプライバシーである。約 3000 年前、デルファイのアポロ神殿の前景に描かれています: γνῶθι σεαυτόν, または英語に翻訳されたとき。汝自身を知れ。それが当時のように今はっきりしています、あなたは自分の身元を管理するのに最適な人です。私達がますますデジタルである世界を始めるので、私達の生命は公衆インターネットの下部組織に想像もつかないほどの方法で動く。私達のデジタルアイデンティティはアイデンティティの所有者によって危険な状態そして現在所有されなくて。

ブロックチェーンキーの自己ソブリン ID は部分的な解決策に過ぎませんが、このホワイトペーパーではセルフキー財団が独自の ID を本当に所有するための分散テクノロジー、法律およびガバナンスのエコシステムを提案しています。

[i] “ウェブとは 1.0?” *TECHNOPEDIA*. 2017 年 8 月 3 日にアクセスし、https://www.technopedia.com/definition/27960/web-10.

iiなばかり読んでいるだけではなく、WEB2.0 のサイトでは、ユーザーの招聘に貢献するサイトのコンテンツによるコメント掲載記事はユーザーアカウントの作成やプロファイルのサイトならではのこの移行は---うお客様のビル---ビジネス(ES)"の企業]"のお見積りから"WEB2.0"の WIKIPEDIA には、アクセス 2017 年 8 月 3 日度 HTTPS://EN.WIKIPEDIA.ORG/WIKI/WEB_2.0 ます

iii ROB"MARVIN"は、"BLOCKCHAIN:目に見えない技術が世界を変えるには、"PCMAG、2017 年 8 月 2 日,HTTPS://WWW.PCMAG.COM/ARTICLE/351486/BLOCKCHAIN-THE-INVISIBLE-TECHNOLOGY-THATS-CHANGING-THE-WOR.

参照:

アダム-TINWORTH は、"NEXT16:BLOCKCHAIN 構築し、WEB3.0"ミク"課題に取り組むための本会議では、2016 年 9 月 23 日 HTTPS://NEXTCONF.EU/2016/09/NEXT16-BLOCKCHAIN-WILL-BUILD-WEB-3-0-SAYS-JAMIE-BURKE/します。

SIRIKIAT BUNWORASET"WEB3.0:ETHEREUM 変更ともに、"バンコクポストは、2017 年 6 月 20 日 HTTP://WWW.BANGKOKPOST.COM/BUSINESS/NEWS/1272219/WEB-3-0-ETHEREUM-WILL-CHANGE-EVERYTHING ます。

ロシルバには、"WEB3.0 をどう分散型の用途が変化するオンライン検閲、"ETHNEWS は、2017 年 2 月 5 日度 HTTPS://WWW.ETHNEWS.COM/WEB-30-HOW-DECENTRALIZED-APPLICATIONS-ARE-CHANGING-ONLINE-CENSORSHIP ます。

トリスタン-冬には、"WEB3.0-ト ETHEREUM ガビンの木は、"ビットコイン、雑誌などで発表されて 2014 年 4 月 25 日 HTTPS://BITCOINMAGAZINE.COM/ARTICLES/WEB-3-0-CHAT-ETHEREUMS-GAVIN-WOOD-1398455401/します。

"BLOCKCHAIN の新しい WEB3.0" によるアクセス 2017 年 8 月 3 日 HTTPS://WWW.MONEYOIP.COM/NEW-WEB-3-0 ます。

iv "このアイデンティティのグローバル状況"HUMANIUM アクセス 2017 年 8 月 3 日度 HTTP://WWW.HUMANIUM.ORG/EN/WORLD/RIGHT-TO-IDENTITY/します。

vジャン-キャンプに、"アイデンティティのデジタルの政府報告書は、2003 年に市民のシナリオでワークショップ"(イベントのケネディ-スクール卒業、政府、ハーバード大学、ケンブリッジマ 02138 2002 年 4 月 28 日）HTTP://WWW.I.JEAN.COM/FILES/IDENTITY.PDF ます。

viベン-シラー"の 2 億人から取り残されているのは、現代の金融システムはどのように迅速にできる変わっているのか？ 高速会社は、掲載 2015 年 11 月 3 日 HTTPS://WWW.FASTCOMPANY.COM/3051846/2-BILLION-PEOPLE-ARE-STILL-LEFT-OUT-OF-THE-MODERN-FINANCIAL-SYSTEM-HOW-QUICKLY-CAN-WE-CHANGE.

viiラヴィ-ラジャ KONATHALA は、"どこのプライバシーの問題 AADHAAR のか？" QUORA(質疑応答フォーラム）は、2017 年 4 月 5 日度 HTTPS://WWW.QUORA.COM/WHAT-ARE-THE-PRIVACY-ISSUES-WITH-AADHAAR ます。

[viii] EQUIFAX 株式の落としての質問をマウントデータの BREACHhttps //www.ft.com/content/f503ef3c-94b2-11e7-a9e6-11d2f0ebb7f0

ix TECH2 ニュースのカリキュラムの中で大量のスウェーデンのデータに違反からスウェーデン軍事秘密やアイデンティティのほとんどすべての国民が、"TECH2 は、掲載 2017 年 7 月 26 日 HTTP://WWW.FIRSTPOST.COM/TECH/NEWS-ANALYSIS/MASSIVE-SWEDISH-DATA-BREACH-LEAKS-SWEDISH-MILITARY-SECRETS-AND-THE-IDENTITY-OF-ALMOST-ALL-ITS-CITIZENS-3855113.HTML

xi "設計図のデジタル-アイデンティティと金融機関の役割ビジ理念"のもと、世界経済フォーラムにおいて、2016 年 8 月
HTTP://WWW3.WEFORUM.ORG/DOCS/WEF_A_BLUEPRINT_FOR_DIGITAL_IDENTITY.PDF ます。

xii「データ破綻追跡：2014 年 10 月 30 日公開、HTTP://TIME.COM/MONEY/3528487/DATA-BREACH-IDENTITY-THEFT-JP-MORGAN-KMART-STAPLES」、ハッキングされたすべての主要企業

[xiii]曲 MCNEVIN は、"の最大の課題とアイデンティティ管理と、その背後には、"コンピュータビジネスレビューでは、2016 年 5 月 20 日 http://www.cbronline.com/news/cloud/the-top-five-issues-in-identity-management-4899761/します。
[xiv]参照の号の"KYC-チェーンの"見出し"と使用例："国連-BLOCKCHAIN は、https://un-blockchain.org/use-cases/identity-under-construction/します。
xvWIKIPEDIA 者は、"セマンティック-ウェブは、"WIKIPEDIA,THE FREE ENCYCLOPEDIA アクセス 2017 年 8 月 3 日 HTTPS://EN.WIKIPEDIA.ORG/W/INDEX.PHP?TITLE=SEMANTIC_WEB&OLDID=793179594 ます。
xvi NITASHA 氏は、"デジタル-プライバシーが独占禁止法を豪快において、有線、2017 年 6 月 4 日度 HTTPS://WWW.WIRED.COM/2017/06/NTITRUST-WATCHDOGS-EYE-BIG-TECHS-MONOPOLY-DATA/します。

xviii "BLOCKCHAINS 示しています。 互換性のか？" ベーカーマッケンジーとの連携 R3 は、アクセス 2017 年 8 月 3 日度 HTTP://WWW.BAKERMCKENZIE.COM/EN/-/MEDIA/FILES/EXPERTISE/FIG/BR_FIG_BLOCKCHAINSANDLAWS_JUL17.PDF.

19 "トムソン-ロイター2016 年のお知らお客様の調査を明らかエコストと複雑さにより"プレスリリースに、トムソン-ロイター、2016 年 5 月 9 日 HTTPS://WWW.THOMSONREUTERS.COM/EN/PRESS-RELEASES/2016/MAY/THOMSON-REUTERS-2016-KNOW-YOUR-CUSTOMER-SURVEYS.HTML.

[xx]ガブリエラ JÓŹWIAK"KYC る金融排除"、保護者、出版年 2015 年 2 月です。
[xxi] *地域では無効となり、禁止します。 これらのサービスは提供する SelfKey までに直接財団がパートナーを受け入れた情報/KYC を送出身者による使用 SelfKey ます。
xxii NIGEL CORY は、"クロスボーダデータの流れが障害とは何かコストのか？" ITIF、2017 年 5 月 7 日度 HTTPS://ITIF.ORG/PUBLICATIONS/2017/05/01/CROSS-BORDER-DATA-FLOWS-WHERE-ARE-BARRIERS-AND-WHAT-DO-THEY-COST 2017 年 5 月 1 日度ます。

xxiii "REGTECH のためのノウハウをお客さまにお客様の手続きをしている中、営業に BLOCKCHAIN 技術 "2016 年 HTTP://WWW.SEC.OR.TH/FINTECH/DOCUMENTS/KYC.PDF ます。

xxivHTTP://WWW.OPENIDENTITYEXCHANGE.ORG/BLOG/2017/06/22/TRUST-FRAMEWORKS-FOR-IDENTITY-SYSTEMS-2/