原文：https://en.bitcoin.it/wiki/Smart\_Property

スマート資産

**スマート資産**はビットコイン[契約](https://en.bitcoin.it/wiki/Contracts)を活用し、ブロックチェーンを通じて所有権が管理されている資産です。車や電話、家屋など実体のある資産が例として挙げられます。スマート資産にはまた、企業の株式やコンピューターへのリモートアクセス権利など、実体のない資産も含まれます。ある資産をスマート化すると、信用がほとんどない相手とも取引を行うことが可能になります。詐欺や調停費用を減らし、これまでは考えられなかった範囲で取引が行えるようになります。例えば、スマート資産を担保に赤の他人からインターネット経由で融資を受けることが可能になります。融資の競争が激しくなり、信用取引のコストが下がるでしょう。

スマート資産は、Nick Szaboが1997年に発表した論文、[「スマート契約の概念」](http://szabo.best.vwh.net/idea.html)にて初めて提案されました。現時点では、彼の思想はまだ実行に移されていません。このページは[Mike Hearn](mailto:mike@plan99.net)によって記述されました。質問がある場合は彼に連絡するか、フォーラムに投稿してください。

背景

原始的な形態のスマート資産は既に普及しています。車をお持ちなら、おそらくエンジン始動ロック機構が備わっているでしょう。エンジン始動ロックは物理的なキー機構をプロトコル交換で補強することによって、正しい暗号化トークンの持ち主のみがエンジンを始動できるようにしたものです。これにより自動車盗難は劇的に減少しました。エンジン始動ロックはオーストラリアの車全体の約45%に備え付けられていますが、盗難車全体の中ではたったの7%です。

他にも、現在流通している資産の多くが暗号化を利用して盗難防止を図っています。例えば、携帯電話の中には正しいロック解除用PINが入力されないかぎり、一部のキーが利用不可になるものもあります。暗号化は盗難デバイスを使用不可にするだけでなく、個人用の電話番号の盗難を不可能にすることもできます。

暗号化の勝利は、こうした例に見られます。しかし、暗号化を組み込んだ資産の可能性はまだ開発され尽くしたわけではありません。秘密鍵は通常、物理的な容器に納まっており（例えば鍵の内部やSIMカードなど）、簡単に持ち運んだり変更することはできません。スマート資産によって、この状況は変わります。ビットコインの採掘者達が調停役を果たすことで、所有権を変えられます。

理論

本章は、読者がビットコインプロトコルをよく理解しており、 [契約](https://en.bitcoin.it/wiki/Contracts)の仕組みについてもよく理解しているという前提で書かれています。

車を例に出して見てみましょう。車に搭載されているコンピューターは、*所有者キー*を用いて認証を行うことを要求します。所有者キーとは、普通のECDSA-256フォーマットのビットコインキーです。車は工場から出荷される際に新規作成された所有者キーの公開鍵を与えられます。その公開鍵には引換用に少量のビットコインが入金されています。その金額を「T」としておきましょう（例えば、0.0001BTC程度です）。さらに、車にはメーカーが発行したデジタル認証が組み込まれており、その認証の公開鍵部分を組み込んだ*識別キー*が与えられています。識別キーにより、車の存在証明、年式、走行距離などが第三者にも確認できるようになります。

車が販売される際には、以下の手続きに沿って行われます：

1. 買い手はワンタイムパスワード（ランダムな数字です）を生成し、売り手に対して車の詳細情報を要求します。
2. 売り手は車にそのワンタイムパスワードを入力し、車からはその車の識別キーにより署名されたデータ構造が返されます。データはワンタイムパスワード、車の公的認証、車の詳細情報、現在の持ち主の公開鍵、そして前回に所有権を移した際の取引＋マークル枝（ハッシュ関数の一部）情報が含まれています。これにより、買い手は自分が得ようとしているものの詳細と、売り手が本物かどうか（二重販売ではないかどうか）を確認できます。
3. 売り手は代金を受け取るためのキー（k1とします）を選択し、価格を「P」に設定します。
4. 買い手は新たな所有者キー（k2とします）を作成します。
5. 買い手は入力と出力のペアを二つ持つビットコイン取引を作成します。第一の入力はビットコイン金額「P」を受け付けます。第二の入力は所有者のアドレスにてビットコイン金額「T」を保持する出力に接続されています。第一の出力はビットコイン金額「P」を「k1」に送信し、第二の出力はビットコイン金額「T」を「k2」に送信します。この時点では、署名できるのが第一の入力のみなので、取引はまだ成立していません。買い手はこの不完全な取引を売り手に送信します。売り手は第二の入力を車の現時点の所有者キーで認証し、取引を配信して公開します。
6. 売り手と買い手はここで、確認作業が終了するのを待ちます。
7. 買い手はビットコイン取引を車に入力します。ここでのビットコイン取引は、マークル枝の構造をとっています。取引はブロックヘッダーに接続され、かつその上にブロックヘッダーが積み上がり、車の現在の持ち主の取引とのギャップを埋めています。車の立場からすると、取引を通じて、現在のチェーンよりはるかに先の時点で所有権が移動するのが見えます。また、その先にも多くの作業が積み重なっており、取引を解消するのは不可能だということも見えます。その時点で、車は自身の所有者情報を更新します。車は取引用チェーンやそのヘッダーを全て記録しておく必要はありません。前回入力されたヘッダーに、将来のブロックヘッダーを接続するために必要な情報があれば十分です。

実際には、上記のプロセスはNFCデバイスを内蔵した携帯電話を用いて行われることになるでしょう。所有者キーを取り込んだ携帯電話でダッシュボードに触れば、スマート資産の取引を行える財布アプリケーションが特殊なモードで起動します。価格を入力した後、売り手と買い手は電話同士を接触させ、取引を完了します。暗号化は複雑な過程を経ますが、売り手や買い手は仕組みのことは何一つ知らずにすみます。携帯電話は、車のエンジンをスタートさせる役割も持ちます。

融資と担保

詐欺のリスク無しに物理的な資産の取引が行えるのは、それだけで使い勝手があります。その上、信用の低いローンを安全に行える方法を、さらに追加できます。小規模で事業を開始するために、融資が必要な場合を見てみましょう。銀行とやりとりするよりも、世界中から借金の入札を募り、最も条件のよい融資を得ようと決めたとします。これがうまくいくためには、融資の支払が滞った場合は担保を差し押さえられる、と赤の他人を納得させる必要があります。その一方、事業を立ち上げるためには融資された車を常に使える状態にする必要があります。

所有者キーに、*アクセスキー*を追加することでこれが実現できます。所有者キーを使ってメッセージを署名することで、アクセスキーを追加したり削除したりできます。アクセスキーは、その性質上、一時的なものです。つまり、融資の期間中は、融資された車の所有権は融資の貸し手に返還しつつも、同時にアクセスキーは自分の手元に残しておくことが可能です。

融資を返済し終われば、車の所有権は借り手に戻る、という保証がなされれば言うこと無しでしょう。これは、以下のようにして実現できます。

1. 貸し手はキー「k1」を作成し、融資の返済を受け取るために使用します。融資の額はビットコイン金額「L」です。
2. 貸し手はキー「Tx1」を署名します。このキーは車の所有権を借り手に移動するための入力／出力を備えており、SIGHASH\_ALL | SIGHASH\_ANYONECANPAYで署名されています。また、「k1」キーに対してビットコイン金額「L」を送信する出力を備えています。融資の返済が完了していないので、取引はまだ無効です。ですので、出力の合計は入力の合計より大きいままです。貸し手は取引を借り手に送り、借り手は取引を管理します。
3. 借り手は消費した分の金額を再回収し、Tx1へ入力を追加することでTx1の金額を増やせます。この結果、所有者キーの入力／出力ペア上の署名が破られることは起こりません。署名はSIGHASH\_ANYONECANPAYを用いて行われており、他の入力から独立しているからです。出力や他の取引要素を改ざんすることは、所有者の入力／出力（SIGHASH\_ALL）を無効にするので、不可能です。
4. 取引の入力金額が「L」に達すると、借り手は取引を配信して公開します。これにより融資を返済し、同時に車の所有権を得ます。

アクセスキーには期限が設けられるため、借り手が融資を期限内に返済しない場合は、アクセスキーの期限が切れて車のエンジンを始動できなくなります。新しい持ち主は自分で車を引き取りに来るか、またはそれができない場合は（例えば他の国に住んでいる場合）、上述した信用が低い場合の販売手続きに従って車を売却し、同じ方法でお金を回収することができます。

ほとんどの融資は複数回に分けて返済が行われます。入力／出力のペアを追加し、何らかの制御データを組み込むことで、上記と同じ手続きがこの例でも流用できます。所有者キーを変えるのではなく、署名の中にアクセスキーの期限をもう一ヶ月延期するコマンドが含まれることになるでしょう。車は取引データを解析することは可能なはずです。

実装の詳細

アクセスキーの期限切れを認証するために、デバイス側では時間を正確に刻む必要があります。車や携帯電話といったデバイスは自身で時刻を認識できます。デバイス自身による時刻管理が実用的でない場合は、堅牢なタイムスタンプサービスを利用することが考えられます。現在時刻とワンタイムパスワードを含んだメッセージを認証できるサービスです。デバイス側はワンタイムパスワードを発行します。アクティベーション／起動プロトコルの一環として、スマートフォンのようにネットワーク接続されたデバイスがタイムスタンプサービスへワンタイムパスワードを送信し、署名済みのメッセージを元のデバイスへ転送します。ブロックチェーン自体には問い合わせ／回答機能が備わっていないため、時刻ソースとしては利用できません。そのため、デバイスは最新のブロックを渡されたかどうかを判別できません。ワンタイムパスワードで時刻を認証することで、この問題を解決できます。

スマートフォンは、BluetoothやNFCを経由することでネットワーク接続手段を持たないデバイスとネットワークの間を橋渡しすることが可能なので、スマート資産においては重要な役割を果たします。例えば、家のドアに付いているスマートロックにインターネット接続を持たせようとすると、高くつく上に実用的ではありません。しかし、ロックにブロックヘッダーの処理状況をチェックするためのNFC接触ポイントを備え付けることは簡単に行えます。ビットコインとリンクしたスマート資産を実装するのに必要な作業はハッシュ操作、ECDSA、少量の記憶領域だけです。全てを内蔵したスマートカード用チップは広く普及しており、安く手に入ります。