Y2（エチルキシレン）
アラブ連盟 Y2 新エネルギー燃料研究所スマート契約
再生不可能な資源を再生可能な資源に転換する
追加：中東国際貿易通貨

アラブ連盟のエンブレムのリーグ、Y2 コインのロゴ、Y2 新エネルギーの燃料ラボのロゴ

アラブ連盟事務局長

Ahmed Aboul Gheit 署名確認 Y2

要約：

2009 年 1 月に Satoshi が Bitcoin ブロックチェーンを開始したとき、彼はまた、世界に 2 つの新しい未検証の革新的な概念を導入しました。最初のものは、資産保証、本質的価値、または中央発行者なしで価値を維持する分散型のピアツーピアのオンライン通貨である Bitcoin です。これまで、Bitcoin は多くの注目を集めてきました。政治面では、中央銀行を持たない通貨であり、大幅な価格変動があります。

しかし、中本哲の偉大な実験は Bitcoin にとっても同様に重要な部分を持っています。仕事の証明に基づくブロックチェーンのコンセプトは、人々が取引の順序に同意できるようにします。 Bitcoins のアプリケーションが（最初にファイル）最初のアプリケーションのようなシステムを説明することができるように：誰かが 50BTC を有している場合、この 50BTC A 及び B を送信すると同時に、トランザクションの最初の確認を有効にします。この 2 つの取引のどちらが最初に到着したかを判断する固有の方法はありません。この問題は、長年にわたって分散型デジタル通貨の発展を妨げています。

Nakamoto のブロックチェーンは、最初の信頼できる分散ソリューションです。 Bitcoin テクノロジの第 2 の部分、およびブロックチェーンがお金以外の領域にどのように適用されるかについて、開発者の関心がすぐに移り始めます。

そのようなドメイン名などの一部の基礎となる物理デバイス（スマ

ート資産）の所有権は資産の代替性と同じではありませんカスタム通貨及び金融商品（カラー通貨）を、表現するデジタル資産のチェーンの使用を含め、多くの場合、前述のアプリケーション、（ドメインコインまた、分散型エクスチェンジ、金融派生商品、ポイントツーポイントギャンブル、チェーンアイデンティティおよびレピュテーションシステムなどの高度なアプリケーション。

また、事前に決められたルールに基づいてデジタル資産を自動的に転送するシステムである「スマート契約」が、しばしば尋ねられます。例えば、人はの形で、貯蔵の契約を有していてもよい「まで X に一日あたりの現金クレジットを撤回することができ、A、Y B は一日まで、自由に A 一緒に抽出することができ、B は、A が B の言及今すぐ停止することができます」論理的な拡張は、この契約（の DAO）の自律的組織の中心部に行くことです - 長期的な組織の資産と知性契約の組織のコーディングルールが含まれています。 Y2 通貨の目標は、内蔵の洗練されたチューリング完全な言語でブロック鎖を提供することで、あなたは私たちがすることができ、変換機能では、ユーザーは単に、この言語でロジックを実装するために数行のコードを使用してエンコードするためにどのような状態の契約を作成することができます上記のすべてのシステムと想像できない他の多くのシステムを作成します。

ディレクトリ

●歴史

○状態遷移システムとしての Bitcoin

○メルケルツリー

○別のブロックチェーンアプリケーション

○スクリプト

●Y2 通貨

○Y2 通貨口座

○ニュースと取引

○Y2 コイン状態変換機能

○コード実行

●用途

○トークンシステム

○Y2 エネルギーデリバティブ

○アイデンティティとレピュテーションシステム

○分散ファイルストレージ

○地方自治組織

○さらなる申請

●雑多な注意

○改善されたゴーストプロトコルの実装

〇料金

〇計算とチューリングの完了

〇通貨と発行

〇拡張性

●概要：分散アプリケーション

●結論

●コメントと高度な読解

歴史

財産登録の代替適用のような分散型デジタル通貨の概念は、数十年前に持ち出されました。 1980 年代と 1990 年代のほとんどの匿名の電子現金協定は、Chaumian の盲目的な技術に基づいていた。これらの電子現金決済は非常にプライベートな通貨を提供しますが、これらのプロトコルはすべて中央仲介に依存しているため人気がありません。 1998 年には、B-お金の大魏（魏大）は、前記第 1 のコンピューティングの課題と分散コンセンサスを解くことによってお金を作成するためにアイデアを紹介しますが、この提案は、中心に与えられたコンセンサスを達成するためにどのようにメソッドを指定しません。 2005 年、Hal Finney は、b-money の考え方と Adam Back の計算上困難なハッシュキャッシュ（Hashcash）の両方を使用する「再利用可能な実証」というコンセプトを導入しました。 ）cryptocurrency 通貨を作成するのが難しい。しかし、このコ

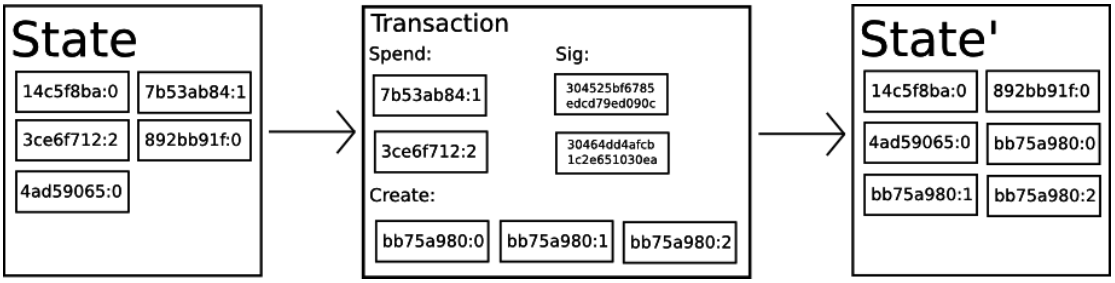
ンセプトは、バックエンドとして信頼できるコンピューティングに依存しているため、理想化では再び失われます。

通貨は事前申請のアプリケーションであるため、取引の順序が重要であるため、分散型通貨は分散型コンセンサスを達成する方法を見つける必要があります。すべての電子マネープロトコルが遭遇する前に主な障害ビットコインは、安全な（ビザンチン・フォールトトレラント）を作成する方法についてのコンセンサスビザンチン将軍問題の問題にもかかわらず、複数政党制の研究では、年間続いているが、これらの契約は半分しか問題を解決します。これらのプロトコルは、システムのすべての参加者が既知であり、「N パーティがシステムに参加する場合、システムは N / 4 の悪意のある参加者に耐えられる」などのセキュリティ境界の形式を生成すると想定しています。しかし、攻撃者は、単一のサーバやボットネット上で数千のノードを作成するので、あなたが一方的なの過半数を持っていることを確認することができますので、この仮定の質問は、匿名を条件に、セキュリティ境界は、魔女を攻撃する脆弱なシステムで設定されていますシェア

Nakamoto のイノベーションは、非常に単純なノードベースの分散型コンセンサスプロトコルとワークロードプルーフメカニズムを組み合わせたコンセプトの導入です。ノードは、ワークロードプルーフメカニズムを介してシステムに参加する権利を取得し、トランザクションは 10 分ごとに「ブロック」にパッケージ化され、常に

成長するブロックチェーンを作成します。多くの電力を持つノードはより大きな影響力を持っていますが、100 万ノードを作成するよりも、ネットワーク全体より多くの電力を得ることははるかに困難です。ビットコインブロックチェーン・モデルは非常にシンプルですが、それは今後 5 年間で、簡単に十分に証明しているが、それは世界の通貨とのプロトコルを超える 200 の礎となります。

状態遷移システムとしての Bitcoin



技術的な観点から見ると、Bitcoin の本は、既存の Bitcoin 所有状態と「状態転送関数」をすべて含む状態遷移システムと考えることができます。 状態遷移関数は、現在の状態とトランザクションを入力とし、新しい状態を出力します。 例えば、標準的な銀行システムでは、ステータスは貸借対照表であり、A 口座から B 口座への X USD の転送要求はトランザクションである。状態転送関数は A 口座から X USD を引いて B 口座を増やす。 X ドル。 A アカウントの残高が X ドル未満の場合、状態遷移関数はエラーメッセージを返します。 したがって、次のように状態遷移関数を定義できます。

```
APPLY(S,TX) > S' or ERROR
```

上記の銀行システムにおいて、状態遷移関数は以下の通りである。

```
APPLY({ Alice: $50, Bob: $50 },”send $20 from Alice to Bob”) = { Alice: $30,Bob: $70 }
```

しかし、

```
APPLY({ Alice: $50, Bob: $50 },”send $70 from Alice to Bob”) = ERROR
```

Bitcoin システムの「状態」とは、掘り起こされていない、使用されていないすべての Bitcoin（技術的には「未使用トランザクション出力または UTXO」と呼ばれます）の集合体です。各 UTXO には額面の値と所有者（20 バイトの暗号化公開鍵のアドレスで定義）があります。トランザクションには、1 つ以上の入力と 1 つ以上の出力が含まれます。各入力には、既存の UTXO への参照と、所有者のアドレスに対応する秘密鍵によって作成された暗号署名が含まれています。各出力には、状態に追加された新しい UTXO が含まれています。

ビットコインシステムにおいて、状態遷移関数 APPLY（S、TX）→S' は、以下のように大まかに定義することができる。

1.取引の各入力：

●参照されている UTXO が現在の状態（S）に存在しない場合、エラーメッセージが返されます

●署名が UTXO 所有者の署名と矛盾する場合、エラーメッセージが返されます

2.すべての UTXO 入力ファセット量がすべての UTXO 出力ファセット量より少ない場合、エラーメッセージが返されます

3.新しい状態 S 'に戻って、すべての入力 UTXO が新しい状態 S'で除去され、すべての出力 UTXO が追加されます。

最初のステップの最初の部分は、トランザクションの送信者が存在しない Bitcoin を消費しないようにし、2 番目の部分は、トランザクションの送信者が他の人の Bitcoins を消費するのを防ぎます。 2 番目のステップは、値の保全を保証します。 Bitcoin の支払協定は以下の通りです。 Alice が Bob 11.7 BTC を送信したいとします。実際、アリスは正確に 11.7 BTC を持つことはできません。彼女が得ることができる Bitcoin の最小量は：6 + 4 + 2 = 12 であると仮定してください。そこで、3 つの入力と 2 つの出力を持つトランザクションを作成することができます。額面の第一出力 11.7BTC であり、所有者は、ボブ（ボブビットコインアドレス）であり、第二出力の額面が 0.3BTC で、所有者は、アリス自身では、つまり、変化を与えます。

信頼できる集中サービス組織があれば、状態遷移システムを簡単に実装でき、上記の機能を簡単に正確にコーディングすることができます。しかし、我々は分散型通貨システムとしてビットコインシステムを構築したいと考えています。誰もがトランザクションの順序に同意するためには、状態遷移システムとコンセンサスシステムを統合する必要があります。 Bitcoin の分散集中コンセンサスプロセスでは、ネットワーク内のノードは常にトランザクションを「ブロック」にパックしようとします。ネットワークは、約 10 分ごとのブロックを生成するように設計され、各ブロックが発生するので、

タイムスタンプ、乱数（すなわちハッシュ）上のブロックを参照すると、すべてのトランザクションにブロックが発生含まリスト。このようにして、継続的に成長するブロックチェーンが時間とともに作成され、Bitcoin ブックの最新の状態を表すように継続的に更新されます。

このパラダイムによれば、ブロックが有効かどうかをチェックするアルゴリズムは以下の通りである。

1.ブロックが参照する前のブロックが存在し、有効であるかどうかを確認します。

2.ブロックのタイムスタンプが前のブロックのタイムスタンプよりも遅く、次の 2 時間より前であるかどうかを確認します。

3.ブロックのワークロードが有効かどうかを確認します。

4.前のブロックの最終状態を S [0]に割り当てます。

5. TX が n 個のトランザクションを含むブロックトランザクションリストであるとします。 0 ... n-1 に属するすべての i について、状態遷移 S [i + 1] = APPLY（S [i]、TX [i]）が実行される。トランザクション i が状態遷移で間違った場合は、プログラムを終了してエラーを返します。

戻り値は正しい。状態 S [n]はこのブロックの最終状態である。

基本的に、ブロック内のすべてのトランザクションは、正しい状態遷移を提供する必要があります。「状態」はブロックにはコード化されません。どのブロックでも、現在の状態を（実際に）計算する

ために、ブロックの作成状態から始めて各ブロックに各トランザクションを追加することができます。さらに、トランザクションがブロックに含まれる順序に注意する必要があります。 1 つのブロックに 2 つのトランザクション A と B がある場合、B は A によって作成された UTXO を使います.A が B の前にあれば、このブロックは有効です。そうでない場合、このブロックは無効です。

ブロック検証アルゴリズム興味深い部分は、概念「仕事の証拠」である各ブロックの SHA256 ハッシュである、得られたハッシュは、常に動的に調整されなければならない目標値よりも小さい値の 256 ビットの長さとみなさこの本の執筆時点では、目標数は約 2 ^ 190 です。作業負荷の証明の目的は、ブロックの作成を困難にし、それによって魔法使いの攻撃者がブロックチェーンを悪意を持って再生しないようにすることです。 SHA256 が原因擬似ランダム関数で完全に予測不可能であり、効果的に創造を阻止する唯一の方法は、新たなハッシュ値が目標値未満で表示するために、乱数の値を大きくしていき、単に試行錯誤です。現在の目標値が 2 ^ 192 の場合、平均で有効なブロックを生成するのに 2 ^ 64 回の試行が必要であることを意味します。一般に、Bitcoin ネットワークは 2018 ブロックごとに目標値をリセットし、平均ブロックが 10 分ごとに生成されるようにします。

Bitcoin ネットワークに悪意のある攻撃者がいる場合の処理を分析しましょう。 Bitcoin の暗号化基盤は非常に安全であるため、攻撃

者は暗号化によって直接保護されていない部分、つまりトランザクションの順序を攻撃することを選択します。攻撃者の戦略は非常に簡単です。

1.商品を購入するために 100BTC を売り手に送ります（特に郵送する必要のない電子商品）。

2.製品が発行されるまで待ちます。

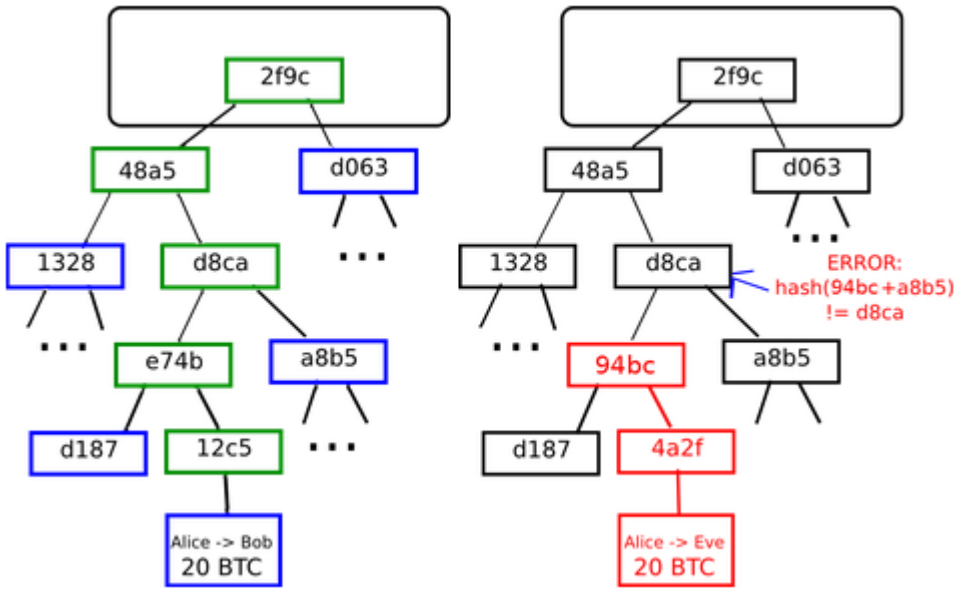
3.別の取引を作成し、同じ 100BTC をお客様のアカウントに送信します。

4. Bitcoin ネットワークで、お客様のアカウントに送信された取引が最初に送信されたものとみなします。

ステップ（1）が発生すると、270000 ブロックと仮定して、トランザクションは数分以内にブロックにパッケージ化されます。約 1 時間後、このブロックの後ろに 5 ブロックがあり、それぞれが間接的にトランザクションを確認するトランザクションを指しています。この時点で、売り手は支払いを受け取り、買い手にそれを出荷した。これはデジタル製品であると想定しているため、攻撃者はすぐに商品を受け取ることができます。今、攻撃者は別のトランザクションを作成し、同じ 100BTC を自分のアカウントに送信します。攻撃者がこのメッセージをネットワーク全体にのみブロードキャストする場合、このトランザクションは処理されません。状態遷移関数 APPLY（S、TX）が実行され、このトランザクションはもはや状態にない UTXO をとることがわかる。したがって、攻撃者はブロックチ

ェーンを分岐させて、269999 ブロックから 270000 ブロックを親ブロックとして再生成します。ここで、新しいトランザクションは古いトランザクションを置き換えます。ブロックデータが異なるため、ワークロードの証明が必要です。新たな第一 27 万ブロックの攻撃者は、別のハッシュを生産しているので、最初のブロックにオリジナルの最初の 270001 270005 は、攻撃者のように古いものと新しいブロックのブロック鎖が完全だった、それを指していません。また、ので、分離された。分岐は、270 000 の新しいブロックに一つだけ攻撃、ブロック鎖、枝のブロック鎖の長さは、正直なブロック鎖であるとみなされたときに、既存の法的最初の 270005 個のブロックに沿ってになりますが発生します。攻撃者が彼のブロックチェーンを最大にするためには、彼は彼以外のネットワーク全体（すなわち攻撃の 51%）よりも多くの操縦力を必要とします。

メルケルツリー



左：Merkle ツリー上に少数のノードを提供するだけで、支店の法的

証拠を提供するのに十分です。

右：Merkel ツリーの一部を変更しようとすると、最終的にチェーンのどこかに不一致が生じます。

Bitcoin システムの重要なスケーラビリティ機能の 1 つは、ブロックが複数レベルのデータ構造に格納されていることです。ブロックヘッダは、実際にはブロックヘッダのハッシュです。ブロックヘッダは、タイムスタンプ、乱数、最後のブロックハッシュ、およびすべてのブロックトランザクションを含む Merkel ツリーのルートハッシュの長さです。約 200 バイトのデータ。

メルケルツリーは、リーフノードのセット、中間ノードのセット、およびルートノードからなるバイナリツリーです。各中間ノードはその 2 つの子ノードのハッシュであり、ルートノードはその 2 つの子ノードのハッシュでもあり、Merkel ツリーの最上位を表します。メルケル目的は、ツリーデータブロックが散発的に送信することができる可能にすることである：ソース・ノードは、ダウンロード追加のソースツリーと関連付けられ、他の部分から、ヘッダ領域からダウンロードし、まだ全てのデータを確認することができる正しいです。これがそうであるので、拡散ハッシュアップ：ツリーの下部に悪意のあるユーザの試みは、偽のトランザクションを追加する場合、変更は、最終的にルートにつながる、ツリーの上位ノードによって引き起こされる変化、ならびに上位ノードの変化につながりますブロックハッシュの変更と変更により、契約では完全に異なるブ

ロックとして記録されます（ほとんど間違いなくワークロードの証明が間違っています）。

メルケルの合意は、Bitcoin の長期的な持続可能性にとって不可欠です。 2014 年 4 月、Bitcoin ネットワークの全ノード（すべてのブロックのすべてのデータを格納および処理するノード）には 15 GB のメモリが必要で、1 か月あたり 1 GB 以上の速度で成長しました。現在のところ、このストレージスペースはデスクトップコンピュータでは許容されていますが、携帯電話ではこのような膨大なデータをロードできませんでした。将来的には商業団体と愛好家だけが完全なノードとして行動するでしょう。のみ、その商品に関連するメルケルツリー「ブランチをダウンロードし、他のノードの存在は、このノードが「光ノード」であり、それはワークロード証明を確認するためにヘッダ領域を使用して、ヘッダ領域をダウンロードすることができ、支払確認（SPV）プロトコルを簡略化します"これにより、軽いノードは、ブロックチェーン全体の小さな部分をダウンロードするだけで、Bitcoin トランザクションのステータスとアカウントの現在の残高を安全に判断できます。

他のブロックチェーンアプリケーション

ブロックチェインのアイデアを他の領域に適用する考えは、長い間現れています。 2005 年には、サーブニックは「タイトルの財産の所有権」の概念を提唱し、紙は、データベース技術の開発は、違法な侵略例えば、チェーンベースのシステムは、土地所有権の登記に

適用可能なブロックをコピーするなどの財産権を作成する方法について説明しますジョージアや土地税などの概念の詳細な枠組み。しかし残念ながら、現時点では実用的なコピーデータベースシステムは存在しなかったので、このプロトコルは実践されていませんでした。しかし、2009 年の Bitcoin システムの分散型コンセンサス開発の成功以来、ブロックチェーンの他の多くのアプリケーションが急速に登場し始めました。

●namecoin - 2010 年に作成された、分散された名前登録データベースです。 Tor、Bitcoin、BitMessage などの分散型プロトコルでは、他の人がユーザーとやり取りできるようにアカウントを確認する方法が必要です。ただし、既存のすべてのソリューションで利用できる唯一の ID は、1LW79wp5ZBqaHW1jL5TciBCrhQYtHagUWy のような擬似ランダムハッシュです。理想的には、人々は「ジョージ」のような名前のアカウントを持っていたいと考えています。しかし、問題は、誰かが "ジョージ"アカウントを作成できる場合、他の人が "ジョージ"アカウントを作成してふりをすることもできるということです。唯一の解決策はファーストツーファイルです。最初の登録者だけが登録に成功し、2 番目のアカウントは同じアカウントを再度登録できません。この問題は、Bitcoin のコンセンサスプロトコルを使用できます。ドメイン名コインは、ブロックチェーンを使用した名前登録システムを実装するための、最も早く成功したシステムです。

●色付きコイン - 色付きコインの目的は、Bitcoinブロックチェーン、またはより重要なことに、通貨 - デジタルトークンに独自のデジタル通貨を作成する機能を人々に提供することです。カラー通貨協定によれば、人々は特定の Bitcoin UTXO に色を割り当てることによって新しい通貨を発行することができます。このプロトコルは、他の UTXO をトランザクション入力 UTXO と同じ色として再帰的に定義します。これは、特定の色を維持するためのユーザのみ UTXO が含まれ、決意は、受信バック色の全て UTXO ブロックチェーンを介して、ビットとして正常硬貨を送信するよう UTXO を送信することができます。

●メタコイン - Metacoins のアイデアは、ビットコイントランザクションを使用して通貨トランザクションを保存するが、別のステート転送関数 APPLY 'を使用して、Bitcoin ブロックチェーンに新しいプロトコルを作成することです。ドル紙幣は、ビットコインブロックチェーンに無効なプロトコル要素通貨取引を防止することができないため、適用する場合、ルールが増加する（S、TX）= S を「（S、TX）がエラーを返し、デフォルトのプロトコルが適用されます」これにより、Bitcoin システムでは実装できない任意の高度な暗号通貨プロトコルを作成するためのシンプルなソリューションが提供され、ネットワークの問題は既に Bitcoin プロトコルによって処理されているため、開発コストは非常に低くなります。

したがって、一般的にコンセンサスプロトコルを確立するには、独

立したネットワークを確立し、Bitcoin ネットワーク上で合意を確立する 2 つの方法があります。ドメイン名コインなどのアプリケーションは最初のメソッドを使用して成功しましたが、各アプリケーションが別々のブロックチェーンを作成し、すべての状態遷移とネットワークコードを確立してテストする必要があるため、このメソッドの実装は非常に困難です。また、我々はべき乗則分布は、ほとんどのアプリケーションはフリーブロックチェーンのセキュリティを確保するには小さすぎるだろうコンセンサス予測技術の中心地に適用される、我々はまた、特に分散型、分散型アプリケーションの数が多いことに気づい自律組織はアプリケーションと対話する必要があります。

一方、Bitcoin ベースのアプローチには欠点があります。これは Bitcoin の特性を継承しないため、支払い確認支払い（SPV）を簡素化できます。 Bitcoin はブロックチェインの深さをバリデーションエージェントとして使用できるため、支払いを確認しやすくなります。ある時点で、トランザクションの祖先が十分離れたところで、法的状態の一部とみなすことができます。対照的に、Bitcoin ブロックチェーンに基づく通貨交換プロトコルでは、通貨交換プロトコルに準拠していない取引をブロックチェーンで除外することはできません。したがって、安全通貨プロトコルの簡略な支払い確認では、特定の取引が有効かどうかを確認するために、ブロックチェーンの最初のポイントまですべてのブロックを逆方向にスキャンする必

要があります。現在、Bitcoin ベースのドル通貨契約の「軽い」実装はすべて、信頼できるサーバーに依存してデータを提供しています。これは、信用の必要性を排除する暗号化通信のほんの次善の結果に過ぎません。

スクリプト

Bitcoin プロトコルが拡張されていなくても、ある程度「スマートな契約」を達成することができます。 Bitcoin の UTXO は、複数の公開鍵によって所有されることも、スタックベースのプログラミング言語で書かれたより複雑なスクリプトによって所有されることもあります。このモードでは、そのような UTXO を使用すると、スクリプトに適合するデータを提供する必要があります。実際には、公共所有の基本的なメカニズムは、スクリプトを介して達成される：スクリプト楕円曲線署名入力として、トランザクションを検証し、成功した場合 UTXO のアドレスを持っている、それ以外の場合は 0 を返し、1 を返します。他のさまざまなアプリケーションシナリオでは、より複雑なスクリプトが使用されます。たとえば、トランザクション確認のために 3 つの秘密鍵のうちの 2 つのコレクションを必要とするスクリプト（マルチシグネチャ）を作成できます。このスクリプトは、企業口座、貯蓄口座、および特定の商用エージェントに役立ちます。スクリプトを使用して、計算上の問題を解決するユーザーに報酬を送ることもできます。本質的には、「あなたは、これは、あなた次第です支払い確認の私の犬簡素化の証拠、ビット

コインUTXOに一定の金額を送信するために持っていることを提供することができた場合は、」一つでもビットコインシステムが異なるパスワードを可能にする、そのようなスクリプトを作成することができます通貨分権化された取引を学ぶ。

しかし、ビットコインシステムのスクリプト言語にはいくつかの重大な制限があります。

•チューリング完全性の欠如 - ビットコインスクリプト言語は複数の計算をサポートできますが、すべての計算をサポートすることはできません。主な欠点はループステートメントです。ループ文をサポートしない目的は、トランザクションの確認で無限ループを回避することです。道のif文任意のサイクルが繰り返されることによってモデル化することができるので、理論的には、スクリプトプログラマのために、この障害は、克服することができますが、そうすることは、例えば、スクリプト上のスペースの非効率的な使用にAの実施をリードします別の楕円曲線署名アルゴリズムは、おそらく別々の符号化を必要とする256回の乗算を必要とするであろう。

価値の盲目UTXOスクリプトでは、アカウントの引き出し量をきめ細かく制御することはできません。例えば、強力なアプリケーションのOracle契約（オラクル契約が）契約をヘッジされ、AとBはそれぞれ、30日後に、契約をヘッジするためにビットコインの$ 1,000価値を送信、スクリプトがBに、A $ 1,000 bitcoinsを送信残りのビットコインを送信します。ヘッジ契約を達成するには、ビットコイ

ンの価値がどれくらいの金額であるかを判断するオラクルが必要ですが、このメカニズムは、今日の完全に集中化されたソリューションと比較して、信頼とインフラストラクチャの削減において大きな進展をもたらしました。しかし、UTXO は不可分であるので、この契約の実現のために、唯一の方法は UTXO は、多くの異なる宗派の非常に非効率的に使用させることである（例えば、K 30 の各々の最大に対応する、2 ^ k 個の UTXO である）とオラクルが正しい UTXO を予測して A と B に送信するようにします。

•Missing state - UTXO は消費されるだけで、使われないため、他の内部状態を必要とするマルチフェーズ契約やスクリプトのための余裕がありません。これにより、多段オプション契約、分散型エクスチェンジ・オファー、または 2 段階暗号コミットメント契約（報酬の計算を保証するために必要）を実装することが困難になります。これはまた、UTXO は、分散型組織のようなより複雑な状態の契約ではなく、メタプロトコルを達成するのが難しいという単純な一回限りの契約の確立にのみ使用できることを意味します。バイナリステータスとバリューブラインドを組み合わせることで、別の重要なアプリケーション（離脱限度）を達成することは不可能です。

Blockchain-blindness - UTXO には、乱数や前のブロックのハッシュなどのブロックチェーンデータは表示されません。この欠陥は、ゲームなどの他の分野のアプリケーションを厳しく制限するランダム性に基づいて、潜在的な価値をスクリプティング言語から奪います。

新しいブロックチェーンを構築し、ビットコインブロックチェーン上のスクリプトを使用し、ビットコインブロックチェーン上にメタコージング契約を確立するという 3 つの方法を検討しました。新しいブロックチェーンを確立する方法は、任意の機能を自由に実装することができます。そのコストは開発時間であり、努力を奨励します。スクリプトの使用方法は実装と標準化が非常に簡単ですが、その能力は限られています。通貨交換プロトコルは実装が非常に簡単ですが、スケーラビリティが低いという欠点があります。 Y2 コインシステムでは、これら 3 つのモードのすべての利点を同時に持つ共通のフレームワークを確立することを目標としています。

Y2 通貨

Y2 通貨は中東の変化に基づいており、Y2 の利用を高めるためにアラブ連盟首脳の方法により発行されたアラブ連盟の粗再生可能な資源のデジタル通貨は決議を可決さ：国際貿易通貨は 6 月に実装されます。 Y2 Y2 のお金新エネルギー研究所デジタル通貨、新しい燃料添加剤、燃料添加剤の立ち上げを加速するために設計された発行 Y2 の Y2 を発行することにより、新しい Y2 は、2035 年の約 20 倍の既存のセーブ Y2 がアップグレードされます、2020 年にデビューすると予想されます 170 以上の回を達成、Y2 に等しい通貨の 1 瓶、グローバル再生可能な資源を守るために、世界を救う（国連の資源は救いの計画として、米国の救済計画、Y2 の共同スポンサーと呼ばれる）技術は（、その値をチューリング完全を持っています値認

識、ブロックチェーン認識、および複数状態の追加機能は、ビットコックスクリプトが提供できるスマートコントラクトよりもはるかに強力です。

Y2 のアカウント

Y2 トークンシステムでは、状態は「アカウント」（20 バイトのアドレスの各アカウント）とオブジェクトの値と、その 2 つのアカウントの変換の間の状態遷移情報と呼ぶことにします。 Y2 コイン口座には 4 つの部分があります：

•トランザクションごとに 1 回しか処理できないカウンタを決定するために使用される乱数

•アカウントの現在の Y2 残高

•アカウントの契約コード（存在する場合）

•アカウントの保存（デフォルトは空です）

ニュースと取引

Y2 コインのニュースは、ビットコインの取引と多少似ていますが、両者の間には 3 つの重要な違いがあります。

第 1 に、Y2 コインメッセージは外部エンティティまたは契約によって作成することができますが、ビットコイントランザクションは外部でのみ作成することができます。

第 2 に、Y2 コインメッセージは任意にデータを含むことができる。

第 3 に、Y2 コインメッセージの受信者が契約アカウントである場合、応答することを選択することができ、これは Y2 コインメッセ

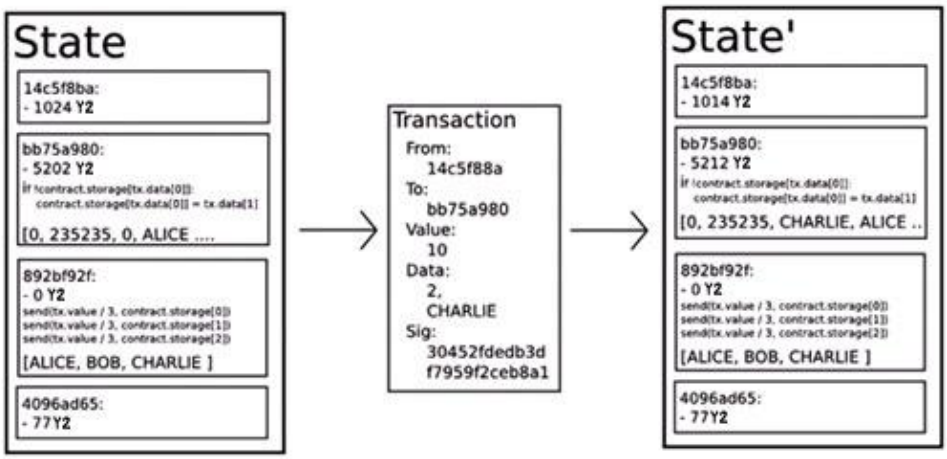
ージにも機能コンセプトが含まれることを意味する。

Y2 通貨の「取引」は、外部口座から送信されたメッセージを格納する署名データパケットを指します。取引メッセージは、送信者の署名を検証するための受信機、Y2 通貨の口座残高、及び送信すべき 2 つの値が GASPRICE の STARTGAS を参照されるデータを含みます。コードと無限ループの指数爆発を防止するために、各トランザクションは、コード実行のステップを計算する必要がトリガー - 最初のメッセージを含むメッセージは、すべての実行によってトリガーされる - の制限を行うこと。 STARTGAS は限界値、GASPRICE は各計算ステップのコストです。取引の実行中に「燃料が使い果たされた」場合、すべての状態の変更は元の状態に戻されますが、既に支払われた取引手数料は回収できません。取引の実行が中断されたときに燃料がまだ残っていると、燃料は送付者に戻されます。作成契約には、個別のトランザクションタイプと対応するメッセージタイプがあり、契約のアドレスは、アカウントの乱数とトランザクションデータのハッシュに基づいて計算されます。

外部アカウントが作成されたメッセージやその他の契約を送信する権利を含む同じ権利を持っているとの契約 - メッセージメカニズムの重要な結果は、Y2 通貨「第一級オブジェクト」プロパティです。この契約が同時に異なる役割の数として機能することができます、例えば、ユーザは、仲介アカウント（別契約）のメンバーになるために組織（契約）の中心部に行くことができ、証明蘭のカス

タムベースの量子を使って偏執的です Porter 署名（第 3 の契約）と 5 つの秘密鍵で保護されたアカウント（第 4 の契約）を使用する自己署名エンティティを持つ個人は、仲介サービスを提供します。Y2 コインプラットフォームの強みは、分散型の組織と代理店契約では、契約の各参加者がどのような種類の口座であるかを気にする必要がないということです。

Y2 通貨の状態の伝達関数



Y2 コインの状態伝達関数：APPLY（S、TX）→S 'は、以下のように定義することができる。

1.トランザクションの形式を確認してください（つまり、正しい値である）正しい、署名が有効と乱数と乱数の試合の送信者のアカウントかどうかです。そうでない場合、エラーが返されます。

2.手数料：手数料= STARTGAS * GASPRICE を計算し、署名から送付者の住所を決定する。送信者のアカウントから取引手数料を差し引き、送信者の乱数を増やしてください。口座残高が足りない場合は、エ

ラーが返されます。

3.初期値 GAS = STARTGAS を設定し、トランザクション内のバイト数から一定量の燃料値を減算します。

4.送信者のアカウントから受信者のアカウントに値を転送します。受信アカウントがまだ存在しない場合は、このアカウントを作成します。受領口座が契約の場合、コードがなくなるか燃料がなくなるまで契約コードを実行します。

5.そこに十分なお金が送信者のアカウントためではないか、コードの実行値の転写不良につながる燃料が不足すると、元の状態を復元するだけでなく、取引コストを支払う必要があり、取引費用は、アカウントに追加されます。

6.それ以外の場合は、残りの燃料をすべて送付者に返却し、使用済燃料は、配送手数料として物流センターに送付する。

コード実行

Y2 コイン契約コードは、低レベルのスタックベースのバイトコード言語で書かれています。コードは一連のバイトで構成され、各バイトは操作を表します。コードの実装が無限ループであり、一般的に、プログラム・カウンタは、単一の操作を実行する（最初はゼロ）一つずつインクリメントされ、コードが完了したか、エラーが検出されるまで、STOP または RETURN 命令。この操作では、データを格納するための 3 種類の領域にアクセスできます。

スタックは、先入れ先出し型のデータストアで、32 バイトの値を

スタックにプッシュできます。

●メモリ、無限に拡張可能なバイトキュー。

●長期保存契約、秘密鍵/値メモリ、キーと値は、異なるサイズの32バイト、計算、すなわち、端部であり、スタックメモリをリセットし、前記格納されたコンテンツは、長期であろう。

コードはブロックヘッダーデータがアクセスされるのと同じように、受信メッセージ内の値、送信者、およびデータにアクセスすることができます。コードはデータのバイトキューを出力として返すこともできます。

PCM コードの正式な実行モデルは、驚くほど簡単です。 Y2 コイン仮想マシンが実行されたときに、その完全な計算状態は block_state すべてのアカウント残高とストレージのグローバル状態を含むタプル（block_state、トランザクション、メッセージ、コード、メモリ、スタック、PC、ガス）によって定義することができます。実行の各ラウンドでは、コードの最初の pc（プログラムカウンタ）バイトを呼び出し、現在の命令が見つけられ、各命令はそれがタプル自体にどのように影響するかを定義します。例えば、ADD スタックから二つの要素とそれらをスタックガス（燃料）マイナス 1 とプラスワン PC、SSTORE 上の 2 つの要素を第二の要素を、スタックが最初に挿入されますコードの数百行実装するかもしれタイムコンパイラ Y2、Y2 が、クレジットの基本的な実施形態によって信用を最適化するための多くの方法があるが、契約の要素は、保管場所を定

義し、また、ガスの PC 値+ 200 の最大値を低減します。

アプリケーション

一般に、Y2 の上には 2 つのアプリケーションがあります。最初は、新エネルギーY2 のアプリケーションで、すべての国が原油、機関や個人が販売、投資およびその他の関連する用途に使用することができ、再生可能エネルギーのためのサポートを提供する必要があり、2 番目は金融アプリケーションで、Y2 から財源に変換することができ、未来は確かに世界の金融専門家が好む金融+エネルギー複合体になるでしょう。

トークンシステム

チェーントークンシステムは、資産インテリジェンスの代わりにこのような企業の株式に金やドル、別々のトークンとしてサブ資産の代表からお金など、多くのアプリケーションを、持っている、セキュリティが連絡しなくても使用の伝統的な価値観で、クーポンを偽造することはできません報酬ポイントのためのトークンシステム。Y2 コインにトークンシステムを実装するのは驚くほど簡単です。重要な点は、お金またはトークンシステムの全ては、基本的に以下の操作を使用してデータベースであることを理解すべきである。減算ユニット A 及び B から X が、但し、その A と、単位 X に印加される（1）。取引前に少なくとも X 個のユニットがあり、（2）取引が A によって承認されているトークンシステムを実装することは、そのようなロジックを契約に実装することです。

Serpent 言語でトークンシステムを実装するための基本的なコードは次のとおりです。

```
from = msg.sender

to = msg.data[0]

value = msg.data[1]

if contract.storage[from] >= value:

contract.storage[from] = contract.storage[from] value

contract.storage[to] = contract.storage[to] + value
```

これは本質的に、本書でさらに説明する「銀行システム」状態遷移関数の最小限の実装です。他の契約で住所の残高を照会できるようにする機能を追加するのが理想的です。それで十分です。理論的には、Y2 コインに基づいて子供の通貨として機能するトークンシステムには、ビットコインに基づくチェーン通貨に欠けている重要な機能が含まれます。通貨を使用して取引手数料を直接支払う機能。

安定した価値を持つ金融デリバティブと通貨

金融デリバティブは、「スマート契約」の最も一般的なアプリケーションであり、コードで実装するのが最も簡単です。金融契約を達成する上での主な課題は、大部分が外部の価格発行者を参照する必要があることです。例えば、非常に要求の厳しいアプリケーションは、Y2（または他の暗号侵害）をドル価格に対してヘッジするスマートな契約です。しかし、契約は米ドルに対する Y2 の価格を知る必要があります。最も簡単な方法は、特定の組織（ナスダックなど）

によって維持管理されている「データ提供」契約で、代理店が必要に応じて契約を更新し、他の契約が契約書に価格情報を含む返信を得るためのメッセージ。

これらのキー要素がすべて設定されている場合、ヘッジ契約は次のようになります。

A が 1000 Y2 通貨を入力するのを待ちます。 。

B が 1000 Y2 の通貨を入力するのを待ちます。

データ提供契約を照会することにより、1000 Y2 コインのドル価値、例えば x ドルがメモリに記録される。

30 日後、A または B「アクティブ化」は Y2 A に（新しい価格と計算を得るために契約を提供し、再照会データ、）$ X の Y2 通貨の契約値を送信することができ、残りのお金は B に送られ、

そのような契約は、暗号ビジネスにおいて驚異的な可能性を秘めています。暗号はしばしば批判された問題の一つは、その価格の通貨変動であり、ユーザーや企業の大多数は、安全性と利便性から生じる暗号資産を必要とするかもしれないが、彼らは一日資産に直面することをいとわない可能性が低い 23％をスライドさせます価値のある状況。これまでに最も一般的に推奨された解決策は、サイト運営者が資産を承認したことでした。

しかし実際には、発行者は必ずしも信頼できるとは限らず、場合によっては、銀行システムが脆弱であるか、そうしたサービスを不可能にするのに十分なほど正直ではない。金融デリバティブは代替ソ

リューションを提供します。資産を保有するための準備金を提供する別個の発行体は存在しないが、代わりに暗号資産の価格を引き上げようとする投機家で構成される分散型市場となる。発行者と違って、投機家はヘッジ契約が契約の準備金を凍結させるため、交渉権がない。このアプローチは完全に分散化されていないことに注意してください。まだ価格情報を提供する信頼できるデータソースが必要ですが、依然としてインフラストラクチャ要件を削減していると論争しています（パブリッシャーとは異なり、ライセンスは自由な発言として分類されるようです）、潜在的な不正リスクを減らすための大きな前進です。

アイデンティティとレピュテーションシステム

最も初期の代替通貨であるドメイン名コインは、ユーザーが共通のデータベース内の他のデータに名前を登録できる名前登録システムを提供するために、ビットコーンのようなブロックチェーンを使用しようとしました。最も一般的な使用例は、 "bitcoin.org"（またはドメイン名通貨で "bitcoin.bit"）のようなドメイン名と IP アドレスを持つドメインネームシステムです。他のアプリケーションの例には、電子メール検証システムや潜在的により高度な評判システムがあります。ここでは、Y2 通貨でドメイン名通貨に似た名前登録システムを提供するための基本的な契約があります：

```
if !contract.storage[tx.data[0]]:

contract.storage[tx.data[0]] = tx.data[1]
```

契約は非常にシンプルですが、追加することはできますが変更や削除はできない Y2 コインネットワークのデータベースです。誰でも値として名前を登録し、決して変更することはできません。より洗練された名前の登録契約は、他の契約は「特徴句」クエリが含まれていることができ、データや所有権の移転を変更するために、「所有者」（すなわち登録者）メカニズムの名前を行います。信頼性と信頼性の高いネットワーク機能を追加することもできます。

分散ストレージ

人気のオンラインファイルストレージのスタートアップの数は、最も顕著なバックアップ・ストレージ・サービスを提供し、ユーザーが自分のハードディスクのバックアップをアップロードすることができるように努め、ユーザーがアクセスし、加入者に課金ので、月額料金を可能にする Dropbox は、ある過去数年間に登場しました。主流の、ぞんざいな観察は、特に「神秘の谷」20〜200 ギガバイトの既存のサービス、フリースペースも企業顧客のレベルでもないその割引することを示している。しかし、この時点で市場は時々、比較的非効率的なファイルストレージであります毎月のファイル保管コストは、ハードディスク全体を 1 か月で支払うコストを意味します。 Y2 通貨契約は、分散型ストレージ・エコシステムの開発を可能にするので、自分のハードディスクまたは未使用のネットワーク空間を介してユーザがそれによって、ファイルストレージのコストを削減、収入の少量を取得するために貸し出さ。

そのような施設の基本的な要素は、「分散型 Dropbox 契約」と呼ばれるものです。契約は以下の通りです。まず、アップロードする必要があるデータをチャンクに分割し、プライバシー保護のために各データを暗号化し、Merkel ツリーを構築します。次に、以下の規則を含む契約を作成し、すべての N 個のブロック、ランダム指数が(ランダム性を提供するために、ブロック・ハッシュ・コードアクセス契約に使用することができる)契約メルケルツリーから抽出し、その後、第一にエンティティ X Y2 コインは、ツリーの特定のインデックスで同様の簡略化された確認支払い（SPV）を持つブロックの所有権証明をサポートします。コストの観点は、最後のトランザクションまで公開していない人のために支払うための最も効率的な方法であるから、しかし、ユーザーが自分のファイルを再ダウンロードしたいとき、彼はファイルを復元する（32K バイト 1 サーブあたりの支払いなど）マイクロペイメント・チャネル・プロトコルを使用することができます 32k バイトごとに元のトランザクションを、同じ乱数でやや費用効率の高いトランザクションに置き換えます。

本契約の重要な特徴は、多くの人がランダムにノードがファイルを失うする準備ができていない信頼のように見えるけれども、ということですが、彼はまだ契約を監視することにより、多くの小片と各片に秘密のファイルを共有することができますノードによって保存されます。契約がまだ支払われている場合、誰かが文書を保存し

ているという証拠が提供されます。

地方分権自治組織（DAO）

「自律分散的組織（DAO、自律分散的組織）」の概念は、通常の意味で、そのようなお金を使うと、コードを変更することを決定するために 67％の大多数に頼るとしてメンバーや株主、一定の数の仮想エンティティを指します。メンバーは、組織がどのように資金を配分するかを決定する。資金を配分する方法は、報酬、賃金、または内部通貨による報酬の働きなどのより魅力的な仕組みにすることができます。これは、暗号化ブロックチェーンテクノロジを使用して、伝統的な企業や非営利組織の法的意義を根本的に再現するだけです。この時点で、DAO の周りの議論の多くは、「資本主義」モデルの配当金と取引を受ける株主の利害と「自律分散的・カンパニー（DAC、自律分散的企業）」の周りであり、代替として、と記載されています「地方分権型自治コミュニティ」は、すべてのメンバーが意思決定において平等な権利を持つことを可能にし、メンバーを加減する際に大多数の同意を必要とする。誰もがメンバーシップを 1 つだけ持つことができます。このルールはグループによって強制される必要があります。

次に、コードを使用して DO を実装する方法の概要を示します。最も単純な設計は、メンバーの 3 分の 2 が同意すれば自己修正できるコードです。コードは理論的には変更できませんが、コードスケルトンを別の契約に置き、契約コールのアドレスを変更可能なストア

に指定することで、コードを簡単に変更できます。このような DAO 契約の単純な実装には、トランザクションによって提供されるデータによって区別される 3 つのトランザクションタイプがあります。

●[0、i、K、V]登録インデックスはストレージアドレスインデックス K の内容を v に変更することをお勧めします。

●[0、i]提案 i の投票を登録します。

●[2、i]十分な票があれば推薦を確認する。

次に、契約には各項目に固有の条件があります。これは、すべてのオープンストレージの変更の記録と投票した人のテーブルを維持します。すべてのメンバーのテーブルもあります。保存されたコンテンツの変更に対して 3 分の 2 以上の大多数の同意が得られた場合、最終的な取引でこの変更が実行されます。より複雑なフレームワークは、（つまり、誰もが自分に代わって投票する別の人が、この委員会に委託することができ、トランザクションを送信するよう選挙を実現するために、組み込み関数を上げるメンバーの変化、さらには議決権行使クラスの民主的なシステムを提供します関係を渡すことができるので、A を B に代理し、次に B を代理 C にすると、C は A の投票を決定する）。この設計では、コミュニティのメンバーは、時間の専門家で自分の立場を変更するとともに、現在のシステムは、容易に起こるであろう人々が最終的に専門家へのタスクのための右の人を選ぶことができるようになりますように、DAO が分散型コミュニティとして、有機的に成長できるようになりますそして

消える。

別のモデルは、任意のアカウントが 0 以上の株式を持つことができる会社を分散させることであり、決定には、株式の 3 分の 2 が同意することが必要です。完全な枠組みには、株式の売買注文とそのような注文を受け入れる能力を提示する能力（契約に注文マッチングの仕組みがある場合）が含まれます。議員は依然として任命民主主義の形で存在し、「理事会」の概念を生み出している。

より高度な組織統治機構が将来的に実現することができる。今分権組織（DO）が自律分散的組織（DAO）を記述するために始めることができます。 DAO との違いは、ラフの境界線は、あなたが政治プロセスを通じて制御することができますか良い勘テストを達成するために類似した「自動」プロセスは、「共通言語」標準ではありませんかどうかで、曖昧で DO：2 人のメンバーがない場合同じ言語の組織がまだ機能していますか？ 明らかに、持株会社のシンプルな伝統的なスタイルが失敗し、ビットコインプロトコルなどのようになります•ロビン・ハンソンの「futarchy を」成功する可能性が非常に高い、市場を予測することによって、組織のガバナンスを実現するメカニズムは本物です「自律的」ガバナンスがどのように見えるかの良い例。人はすべてに優れた、すべての DAO が行うことを前提とする必要はないことに注意してください。自治は、特定のシナリオでちょうど大きな利点である、それは実現可能なパラダイムをではないかもしれないが、多くの半 DAO は別の場所に存在して

もよいです。

さらなるアプリケーション

1.財布を保存する。アリスは自分のお金が安全であることを確認したいと考えていますが、彼女は自分の秘密鍵を盗むために失われたり、ハッキングされることを恐れています。彼女は Y2 を Bob と契約しました。以下に示すように、この契約は銀行です：

アリスは毎日 1％の資金を引き出すことができます。

ボブは毎日最高 1％の資金を引き出すことができますが、アリスは自分の秘密鍵を使ってボブの引き出し権を取り消す取引を作成できます。

アリスとボブは任意に資金を引き出すことができます。

一般的に、1 日 1％で Alice にとっては十分です。もし Alice がもっと引き出したい場合は、Bob に連絡して助けてもらうことができます。 Alice の秘密鍵が盗まれた場合、Bob はすぐに新しい契約に資金を移すことができます。彼女が秘密鍵を失った場合、Bob はゆっくりと資金を調達することができます。ボブが悪意を持っていると、撤退権を無効にすることができます。

2.作物保険。データエントリとして価格指数の代わりに気象条件を使用して、金融デリバティブ契約を簡単に作成することができます。あなたは干ばつが発生した場合、農家は自動的に、彼は意志の資金の支払いを受け取ることになりますので、降雨の十分な量がある場合にアイオワ州の農民は、アイオワ州の降雨量に基づいて支払いを

逆にする金融派生商品を購入する場合彼の作物は非常に良いので、非常に幸せ。

分散データ配信者。差異に基づく金融契約については、実際には、「Xerin ポイント」プロトコルを渡すことによってデータ発行者を分散させることが可能です。シェリング・ポイントは、以下のように動作します、すべての値が順序付けされる N 系（例えば Y2 / USD 価格）に指定された入力値のデータによって提供される、各ノードは、75％から 25％の間の値を提供します報わ、誰もが他の人によって提供される答えを提供するインセンティブを持って、選手たちの多くは本当に明白なデフォルトに答えることに同意するものとすることができますベルリンでの温度、Y2 / USD の価格を含む理論的に価値の多くを提供するように構成されて正解、あります特に計算が難しい結果を伴う、集中化されていないプロトコルさえも。

4.複数署名のスマート契約。 Bitcoin では、マルチサインベースの取引契約が可能です。たとえば、5 つの秘密鍵を使用して資金を集めることができます。唯一の 3 が、その後 2 つだけが唯一の毎日資本の 0.5％を過ごすことができ、毎日資本金の 10％までを過ごす場合は Y2 のお金は、例えば、4 の組立の 5 つの秘密鍵は、すべての資金を費やすことができ、より詳細な行うことができます。また、マルチ署名における Y2 の通貨は双方が異なる時間にレジスタブロックチェーンを署名できることを意味し、非同期である、それは自動的に代わりに最後の署名後にトランザクションを送信します。

5.クラウドコンピューティング。 PCM 技術は、ユーザーが正常に完了し、次いで選択一定のランダムに選択されたチェックポイントで計算される必要な証拠を計算するために他のユーザーを招待することを可能にする検証コンピューティング環境を作成するために使用されてもよいです。これは、の作成を作ることができ、オンサイト検査と保証金は、システムが信頼できることを確実にするために使用することができるようすべてのユーザーが自分のデスクトップ、ラップトップまたはクラウドコンピューティング市場に関与した専用サーバーを使用することができます（つまり、どのノードが不正行為から得ることができませんリー)。このようなシステムは、すべてのタスクには適していない可能性がありますが、たとえば、高度なプロセス間通信を必要とするタスクは、大きなノードクラウドでは容易に実現できません。しかし、SETI @ home、folding @ home、および遺伝子アルゴリズムは、このようなプラットフォームで実装するのが非常に簡単です。

ポイントツーポイントギャンブル。任意の数のピアツーピア・ギャンブル契約を、Frank Stajano や Richard Clayton の Cyberdice などの Y2 コインをブロックするために移動することができます。最も簡単なギャンブルの契約はほぼゼロコストを実現するために、実際にはカザフスタンとの違いを賭けに使用して、より複雑なギャンブルの契約を作成することができ、ブロックの推測の価値が希薄化されるような単純な契約であり、かつ詐欺的なギャンブルサービスはあ

りません。

市場を予測する。組織と管理協定の中心に適用されるシェリング通貨市場予測は最初の主流の「futarchy」になるかもしれないとそこにあるか、Oracle シェリング通貨があるかどうか、市場予測は、実装が非常に簡単になります。

8.チェーンは、アイデンティティとレピュテーションシステムに基づいて、中央の市場に行きます。

雑多な注意

改良されたゴーストプロトコル実装

「ゴースト」合意(「貪欲最も重い観測されたサブツリー」(GHOST)プロトコル）技術革新を導入するために 2013 年 12 月における Yonatan Sompolinsky とゾハルテルアビブです。ゴーストプロトコルのモチベーションが低いため、セキュリティ上の問題の対象と無効ブロックの高レートの高速電流ブロック鎖を確認することが提案されている。それは、ボイドが高い場合（セット t）は、ネットワーク全体に広がる時間の特定のブロックがかかるため、シンプルにコンピューティングパワーのシェアが高いため、効率的です。

それは言うことである、唯一のブロックを、説明したように計算ブロックはまた、廃棄物を含有するストランド「最長」によって Sompolinsky とゾハルは、幽霊プロトコルの最初の問題は、ネットワークセキュリティを低下解決来親ブロックとそれ以前の祖先はブロック、廃止されたブロックの子孫の先祖ブロック（「第 3 級ブ

ロック」と呼ばれるY2語クレジットは、）が算出される支持ブロックを持っているミックスに追加することも仕事の最大量であります証明。入れて、中心傾向、ブロック報酬の87.5％を貢献するために、廃棄物の新しいブロックの身元を確認するために「第3級ブロック」に支払ったY2のお金 - 私たちは、第二の問題を解決するために合意Sompolinskyゾハルを越えて行くと説明します計算された「ダンプスターブロック」は報酬の12.5％を受け取るが、トランザクション料金は叔父のブロックに与えられない。

Y2コインはゴーストプロトコルの簡略化されたバージョンを実装し、5階にしか流れません。第三廃ブロックのみ（例えば、若い親の第6世代の領域をブロックしなく若い世代のブロックのより遠い関係より、若いブロックの第五世代の第二世代に親によってブロックすることができるように、その特性は、あります祖父ブロックのブロックまたは第3世代の子孫ブロックが計算に含まれます。これにはいくつかの理由があります。第1に、無条件ゴーストプロトコルは、所与のブロックの三分木ブロックが正当であるかどうかの計算に過剰な複雑さを与える。

経費

ブロックチェーンにリリースされた各トランザクションはダウンロードと検証のコストがかかるため、スパミングトランザクションを防止するための取引手数料を含む規制メカニズムが必要です。しかし、簡略化の特別な、あまり正確でない仮定が与えられたとき、

この市場ベースのメカニズムの抜け穴は奇跡的にその影響を排除した。引数は次のとおりです。前提条件：

1.貿易は、貿易を含む者に報酬 kR を提供するための k ステップをもたらし、ここで R はトレーダによって設定され、k と R の両方は事前に（大まかに）見える。

2.各ステップを処理するノード当たりのコストは C です（つまり、すべてのノードの効率は一貫しています）。

3. N 個のノードがあり、それぞれが同じコンピューティングパワー（つまり、ネットワーク全体のパワーの 1 / N）を持ちます。

しかし、これらの前提および実際の状況からいくつかの重要な逸脱があります。

図 1 に示すように、余分な検証時間はブロックのブロードキャストを遅延させ、したがってブロックが廃棄ブロックになる可能性を高めるので、トランザクションコストを他の検証ノードよりも多く処理する。

2.実際に力の分布が極端に不均一になることがあります。

3、彼ら自身の、政治的な反対者と狂人としてネットワークを破壊する投機家が存在し、彼らはコストが他の検証ノードよりもずっと低くなるようにインテリジェントに契約を設定することができます。

上記の最初のポイントはトランザクションの数を減らし、2 番目のポイントは NC を追加したため、これらの 2 つのポイントの影響が

少なくとも部分的に相殺されました。浮動上限：ブロックに BLK_LIMIT_FACTOR 倍以上の長期指数移動平均を含むブロックはありません。具体的には：

```
blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR - 1) + floor(pare
nt.opcount * BLK_LIMIT_FACTOR)) /EMA_FACTOR)

BLK_LIMIT_FACTOR と EMA_FACTOR は一時的に 65536 と 1.5 の定数に設定されますが、
後で解析して調整することができます。
```

計算とチューリングの完了

JUMP 命令は、プログラムがコード内のどこかにジャンプすることを可能にし、x <27：x = x * 2 のような条件文を許可する JUMPI 命令は条件付きジャンプを実装します。第二に、契約は他の契約を呼び出すことができ、再帰によってループを達成する可能性があります。これは自然に問題につながります。悪意のあるユーザーは、ノード全体を強制的に無限ループにして強制的にシャットダウンすることができますか？ この問題は、停電問題と呼ばれるコンピュータサイエンスの問題のために発生します。特定のプログラムが限られた時間内に実行を終了できるかどうかを一般的な意味で知る方法はありません。

状態遷移のセクションで説明したように、我々のソリューションは、トランザクションごとに実行する計算の最大数を設定することで問題を解決しますが、超過した場合は計算が元の状態に戻りますが、ニュースは同じように機能します。

攻撃者は、send（A、contract.storage [A]）; contract.storage [A] = 0 の

ような契約を含む契約を見て、第 1 ステップを実行するのに十分であるが、第 2 ステップを実行するのに十分ではない。トランザクション（つまり、払い戻しではありますが、勘定残高は減少しません）。契約の作成者は、実行が途中で終了するとすべての変更が元に戻されるため、同様の攻撃の防御について心配する必要はありません。金融契約は、リスクを最小限に抑えるために 9 つのプライベートデータ発行者の中央値を抽出することによって機能します。攻撃者はデータプロバイダの 1 つを引き継ぎ、DAO セクションで説明したように可変アドレス呼び出しメカニズムを変更可能に設計します。データ提供者は無限ループを実行してこの金融契約から資金を要求しようとする試みを説得しようとしたが、燃料の枯渇により中断される。しかし、金融契約は、そのような問題を防ぐために、メッセージの燃料制限を設定することができます。

Turing の完全な置き換えは Turing 不完全です.JUMP と JUMPI 命令が存在せず、指定された時間にコールスタック内に各契約のコピーが 1 つだけ存在することが許可されています。このようなシステムでは、契約の実行コストはその規模によって決まるため、前述のコストシステムと当社のソリューションの効率の不確実性は必要ないかもしれません。さらに、チューリングは不完全であるか、または大きな制約ではない。これまで想像したすべての契約例では、サイクルを 1 回だけ行う必要があり、このサイクルでも 26 のシングルラインコードセグメントの繰り返しで置き換えることができます。

Turingの完全性によってもたらされる重大な問題と限られた利益を考慮して、Turingの不完全な言語を単に使用しないのはなぜですか?チューリングが不完全であるという事実は、簡潔な解決策にはほど遠い。なぜ? 以下の契約を考慮してください:

```
C0: call(C1); call(C1);

C1: call(C2); call(C2);

C2: call(C3); call(C3);

…

C49: call(C50); call(C50);

C50: (run one step of a program and record the change in storage)
```

計算250個のステップを取るさて、こうした取引がAを送信するために、51回の取引では、我々は契約を持っている、最大ステップ数を維持し、再帰呼び出しのために他の契約を実行するために、すべての契約のためにしようとするかもしれないので、そのような論理爆弾を検出するステップを実行するように契約は、事前に計算することができるが、これは契約が他の禁止契約を（作成し、上記26契約の実行を容易に別の契約内に配置することができるように）を作成するであろう。もう一つの問題は、メッセージのアドレス・フィールドが可変であるので、一般的にも、事前に別の契約その1と呼ばれる契約を知らないかもしれない話すことです。だから、最終的に我々は驚くべき結論持っている:チューリング完全管理驚くほど簡単ですが、同時に管理制御チューリングの欠如は不完全驚く

ほど困難を - なぜ合意チューリングはそれを完了させませんか?

通貨と発行

背景説明:

リーグオブアラブ諸国は、アラブ諸国間の協力と協力を強化するために設立された地域国際機関です。略語アラブ連盟またはアラブ連盟。 1945 年 3 月、カイロで開催されたエジプト、イラク、ヨルダン、レバノン、サウジアラビア、シリア、イエメン 7 つのアラブ諸国の代表は、採択された「リーグアラブ諸国の条約を、」アライアンスは宣言しました。 1993 年までに 22 の加盟国があった。それは彼らの活動を調整、アラブ諸国の独立と主権を維持するために、加盟国間の緊密な協力を強化することを目指しています。 11 月中旬 2011 年、アラブ連盟はシリアの会員資格を停止し、同年 11 月 27 日に、アラブ連盟は、エジプトの首都カイロで、後に閣僚会議を開催することを決定し、すぐにシリアに経済制裁を課します。 2017 年 6 月 5 日に、サウジアラビアを率いるアラブ連盟が、カタールを組織から除外する声明を発表した。ミッション:経済、金融、交通、文化、保健、社会福祉加盟国に貢献して、お互いの間で政治活動を調整するアラブ諸国の独立と主権を守るために、そしてアラブ諸国の全体的な利益を促進加盟国間の緊密な協力、国籍、パスポート、ビザ、司法など国家の政治システムのための加盟国相互尊重、彼らの紛争は、他の国が他の国を拘束するものではないとの加盟国が締結し、条約や協定を解決するために強制的に頼るものではあり

ません。

現在、22 アラブ連盟のメンバーは以下のとおりです。アルジェリア、アラブ首長国連邦、オマーン、エジプト、パレスチナ、バーレーン、ジブチ、クウェート、レバノン、リビア、モーリタニア、モロッコ、サウジアラビア、スーダン、ソマリア、チュニジア、シリア、イエメン、イラク、ヨルダン、支店モロー2011 年 11 月 16 日には、アラブ連盟が正式にシリア、2013 年 3 月 26 日の会員資格を停止し、アラブ連盟はシリアシリア、「ナショナル・ユニオン」をアラブ連盟で野党の議席を付与することを決定したが、まだ実装され証明されていません。

分布モデルは次のとおりです。

●活動を売って、Y2 硬貨は販売上のすべての 1 個の Y2 通貨の価格となり、他のいくつかの暗号で、すでに開発者のためのメカニズムを支払っ Y2 Y2 新エネルギーや燃料添加剤は、通貨のための資金調達、研究開発体制を目指している方、実際の価格、通貨プラットフォームでの使用が成功しました。早期購入者は、プロジェクトの暗号生態系と Y2 新エネルギー燃料添加剤に入れ、BTC、ETH（正味変更）の販売が完全に開発者や研究者の給与や報酬を支払うために使用され、その結果、お金をより大きな割引をお楽しみいただけますグローバルな開発、流通、占有。

世界で初めて 2 億 7,000 万個、世界で初めて 7,000 万個が配布されました。

最初に発行された国、数量および割合：

国	数量	会計
アメリカ合衆国	300 万	3.75%
韓国	900 万	11.25%
中国	720 万	9%
ロシア	500 万	6.25%
イギリス	820 万	10.25%
EU	320 万	4%
日本	900 万	11.25%
フランス語	250 万	3.125%
サウジアラビア	550 万	6.875%
オーストラリア	250 万	3.125%
インド	550 万	6.875%
イタリア	200 万	2.5%
インドネシア	200 万	2.5%
カナダ人	200 万	2.5%
ドイツ	150 万	1.875%
南アフリカ	100 万	1.25%
メキシコ人	100 万	1.25%
トルコ	100 万	1.25%
ブラジル	90 万	1.125%

アルゼンチン	50 万	0.625%

アラブ連盟事務総長 Ahmed Aboul Gheit は世界を救うこの組織に誰もが参加するよう呼びかけた。

Y2 燃料新エネルギー研究所（旧アラブ連盟特別研究室）が 2003 年に設立され、2017 年に技術的なアラブ連盟の支援（科学的な特許および中東諸国の千種類を提供するために、新しい Y2 エネルギー研究所、15 年の期間に社名変更)、Y2 は、Y2 は、アラブ連盟副事務総長で金融機関を所属状態ユニットに属し、新しいエネルギー源を開発するアラブ連盟のメンバーにサービスを提供するために、連合のためにこれらの懸念を共有し、研究を使用することをお約束します。

Y2 の発売は世界のエネルギーを 20 倍以上に増加させ、2020 年には 10-25 倍のエネルギーを節約し、2030 年には 170 倍以上のエネルギーを節約します。

2018 年 4 月 1 日～6 月 6 日は世界的なイベントの始まりです。

グローバル通貨から 4 月 7 日は、Y2 を発行し、為替の Y2 は以下の通りであった。OKEX、BitMEX、Binance、GDAX、K ネットワーク、B ネット、HitBTC、よき、ビット-Z、P ネットで 7 つの取引所、発行価格協力価格の 6 倍以上です。

発行ユニット：Y2 新エネルギー燃料研究所

（Y2وود لوقة دةظ جديد ةةال طاقة برال تة مخ)。

投資者：ムハンマドビンサルマンアル・サウド（サウジアラビア皇

太子)、ムケシュアンバニ（インドの富豪)、量子基金（ジョージ・ソロス)、UAE 中央銀行。

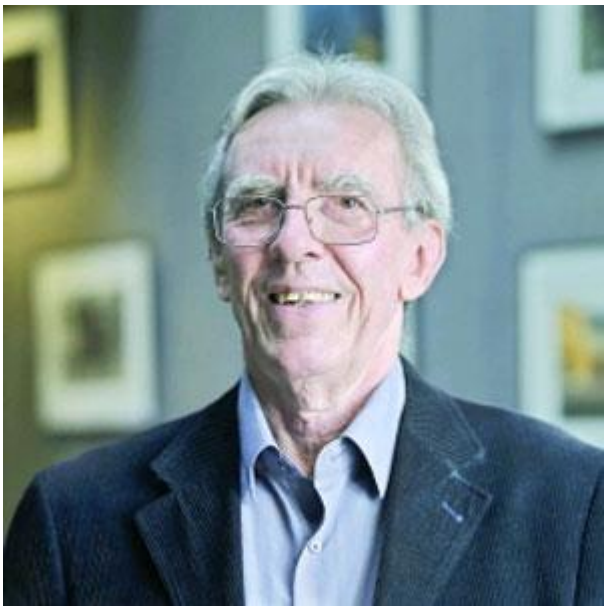
受賞：デジタル通貨取引許可証、国際貿易流通許可証、アラブ連盟リーグサミット通貨委員会委員など

主要員：

Y2 Lab チーフサイエンティスト、Y2 通貨 CEO、2011 年ノーベル化学賞、アラビア語デジタル通貨基金共同議長：Shechtman（شد يخ تمان）

ムハンマド・ビン・サルマン・アル・サウド（Mohammad bin Salman Al Saud）（محمد بن سلمان آل سعود）は、サウジアラビア王国の皇太子

Y2 Lab テクニカルコンサルタント、PayTabsCEO、最高技術責任者 Y2 通貨：Abdulaziz Al Jouf（عبد العزيز آل جوف）



Y2 Lab 科学者、ノーベル化学賞、Y16 通貨担当最高執行責任者（COO）2016 PIERRE SOVIC（مالا سوير）

サポートのみ：BTC、ETH（価格の変更）

例：1 BTC = 46,000 元、すなわち 1 BTC = 133.33333333 Y2

例：1ETH = 2500 元、つまり 1 ETH = 7.24763681 Y2

●0.099x（x は販売の合計額である）ETH 前の早期貢献の開発に参加するために、BTC に割り当てられます（実際の価格の変化）と現金の融資やその他の資金調達の確実な成功は、他の 0.099x は、長期的な研究プロジェクトに割り当てられます。

リリース分解

永久線形成長モデルは、Bitcoin における富の過度の集中のリスクを低減し、長期的に Y2 コインを獲得して保持するインセンティブを維持しながら、現在および将来に住む人々に通貨を得る公正な機会を与える"マネーサプライの成長率"がゼロになる傾向にあることを見てください。我々はまた、常に通貨損失は毎年マネーサプライの一定の割合であると仮定すると、発生します、循環における総マネーサプライの最終量が安定する損失のため、時間の経過の通貨によって引き起こさ不注意と死の、と結論しました値の損失の年率を分割し量に等しい通貨に（例えば、電源が 30 倍に達し、1％の損失率、0.3X 毎年が同時に存在掘られているとき 0.3X 平衡に達するように、失われました）。

リニア発行方式に加えて、Bitcoin 様 Y2 コインの供給の伸び率は、長期的にはゼロになる傾向があります。

拡張性

スケーラビリティの問題は、多くの場合、現地通貨 Y2 の注目されている、ビットコインのように、また、すべてのトランザクションに苦しん Y2 通貨は、ネットワーク処理苦痛で、このジレンマを各ノードが必要です。 Bitcoin の現在のブロックチェーンサイズは約 20GB で、1 時間あたり 1MB の速度で成長しています。 Bitcoin ネットワークが Visa クラスの 2000tps トランザクションを処理する場合、3 秒ごとに 1MB ずつ増加します（1GB /時、8TB /年）。単純な通貨で Bitcoin ではなく Y2 コインのブロックチェーンに多くのアプリケーションがあるので、Y2 コインも同様のまたはより悪い成長パターンを経験することがありますが、Y2 コインは完全なブロックチェーンの歴史の事実は状況を改善しました。

大きなブロックチェーンの問題は、集中化のリスクです。ブロックチェーンのサイズは、100TB まで増加した場合、正規のユーザーが光 SPV ノードを使用しながら、可能なシナリオは唯一の大企業の非常に小さな数は、完全なノードを実行することになります。これにより、完全なノードのパートナーシップにおける詐欺のリスク（例えば、ブロック報酬の変更、BTC の付与など）に対する懸念が生じます。軽いノードは、この詐欺をすぐに検出する方法がありません。もちろん、少なくともフルノード正直があるかもしれない、と詐欺のようなチャネルの Reddit に漏れるが、それは遅すぎた。この時間に関する情報の数時間後：普通のユーザーは既に作成されたブロックを廃止するものを努力してみましょう彼らはすべて、51％の攻撃

を成功させたのと同じ規模の膨大な実行不可能な調整問題に遭遇します。 Bitcoin ではこれが問題ですが、Peter Todd によって提案された変更がこの問題を緩和することができます。

最近、Y2 コインはこの問題に対処するための 2 つの追加の戦略を使用します。特定の数の完全ノードが保証されます。第 2 に、さらに重要なのは、各トランザクションを処理した後、ブロックチェーンに中間状態ツリーのルートを含めることです。ブロック検証が集中化されていても、正当な検証ノードが存在する限り、検証プロトコルによって集中化された問題を回避することができます。誤ったブロックが発行された場合、そのブロックは間違ったフォーマットか、状態 S [n]が間違っています。 S [0]が正しいので、（S [I-S [i]はなく、S は[I-1]正しいノードは、インデックス i を提供することを確認し、また、処理が設けられた第 1 エラー状態 APPLY が存在しなければなりません 1]、TX [i]） -> S [i]パトリシアツリーノードのサブセット。これらのノードは、結果の S [i]が以前に提供された値と一致するかどうかを見るために計算のこの部分を実行することが義務づけられます。

さらに、不完全なブロックを悪意を持って攻撃して攻撃することは複雑になり、ブロックが正しいかどうかを判断するための情報が不十分になります。この解決策は、チャレンジ/レスポンスプロトコルです。検証ノードがターゲットトランザクションインデックスにチャレンジし、チャレンジ情報を受け取ったライトノードは、別の

ノードまたは検証者がパトリシアノードのサブセットを正しいものとして提供するまで、対応するブロックを信頼できません。証拠。

レビュー：分散アプリケーション

契約のメカニズムは、仮想マシン上で（基本的に）で、誰でもネットワーク全体のコマンドラインアプリケーションを介して実行するにはコンセンサスを構築することができ、そのようにアクセスネットワーク全体の状態を変更することが可能である「ハードドライブを。」しかし、ほとんどの人にとって、トランザクション配信メカニズムとして使用されるコマンドラインインターフェイスの適切な使いやすさの欠如は、分散化を魅力的な選択肢にしています。最後に、完全な「分散アプリケーション」は、完全なクレジット、コインや他のシステムが Y2 クレジットにクライアントプログラムである Y2（例えば、P2P メッセージ層の組み合わせを使用するかどうか Y2 において基礎となるビジネス・ロジック・コンポーネントを[含むものエンド・オブ・ザ・ボックスまたは他のシステム・レベルの]グラフィカル・ユーザー・インターフェース・コンポーネント。 Y2 コインクライアントはウェブブラウザとして設計されているが、Y2 コインブロックチェーンと対話するためにクライアントが見た特定のウェブページによって使用される「PC」の Javascript API オブジェクトのサポートを含む。ブロック鎖と、他の分散プロトコルが完全にユーザーが開始した要求を処理するためのサーバーに置き換えられますので、ビューの「伝統的な」ウェブの観点か

ら、これらのページは、完全に静的なコンテンツです。最後に、分散型プロトコルは、ウェブページを格納するために何らかの形のY2コインを使用することを約束します。

結論

Y2通貨プロトコルは、もともと、そのような考えのギャンブル市場通貨暗号のアップグレード版として汎用性の高い言語、撤退の制限や金融契約の高度な機能により、チェーンなどの契約プランとして開発されました。しかし、Y2通貨により興味深いY2通貨協定をセンターにして、予測プロトコルの計算の中心に、市場の中心に、店舗の中央付近に移動し、さらに単なるお金よりも行くだけでなく、確立された同様の概念の数十、ということですアプリケーションは、根本的にコンピューティング業界の効率を向上させ、かつ経済的なP2Pプロトコルの別の層を追加することによって、初めて強力なサポートを提供する可能性は、最終的には、多数のアプリケーションは、お金とは何の関係も表示されないもありました。

Y2クレジット任意の状態プロトコル変換概念は、固有のインターネットの可能性を提供し、そのようなデータストレージ、ギャンブル又はデビット異なる単一目的の設計などのプロトコルのため閉鎖、Y2は、設計からオープンクレジットであり、そして私たちは、今後数年間に出現する非常に多数の財務および非財政協定に対応するための基本層として非常に適していると考えています。

コメントと高度な読解

ノート

1.経験豊富なリーダーは、実際にはアドレスビットコイン楕円曲線公開鍵ハッシュではなく、パブリック自体が、公共の公開鍵暗号化ハッシュと呼ばれる学術言語の観点から、実際には完全に合理的であることがわかります。これは、ビットの暗号トークンがカスタムデジタル署名アルゴリズム、公開鍵ハッシュ組成物曲線の楕円公開鍵、楕円曲線公開鍵署名署名された接続用組成物による楕円曲線であると考えることができるからである、と公開検証アルゴリズム備えるとして楕円曲線公的検査によって提供楕円曲線公開鍵ハッシュ鍵楕円曲線後の署名を検証するために、楕円曲線公開鍵を使用して、そして。

技術的に言えば、最初の 11 ブロックの中央値。

3.内部的には、2 と "CHARLIE"は数字で、後者は巨大な base256 エンコーディング形式です。数字は 0〜2 ^ 256-1 です。