(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7316295号
(P7316295)

(45)発行日　令和5年7月27日(2023.7.27)

(24)登録日　令和5年7月19日(2023.7.19)

(51)国際特許分類

H04L 9/08 (2006.01)	H04L	9/08	A	
H04L 9/14 (2006.01)	H04L	9/14		
H04L 9/32 (2006.01)	H04L	9/32	200B	

請求項の数　14　（全22頁）

(21)出願番号　特願2020-552031(P2020-552031)
(86)(22)出願日　平成31年3月26日(2019.3.26)
(65)公表番号　特表2021-519541(P2021-519541A)
(43)公表日　令和3年8月10日(2021.8.10)
(86)国際出願番号　PCT/IB2019/052428
(87)国際公開番号　WO2019/193452
(87)国際公開日　令和1年10月10日(2019.10.10)
審査請求日　令和4年2月28日(2022.2.28)
(31)優先権主張番号　1805633.3
(32)優先日　平成30年4月5日(2018.4.5)
(33)優先権主張国・地域又は機関
英国(GB)

(73)特許権者　318001991
エヌチェーン ライセンシング アーゲー
スイス・６３００・ツーク・グラーフェナウヴェーク・６
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100135079
弁理士　宮崎 修
(72)発明者　フレッチャー，ジョン
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス ７ス フロア アーカート－ダイクス アンド ロード エルエルピー

最終頁に続く

(54)【発明の名称】　デジタル資産へのアクセスを移すためのコンピュータ実施方法及びシステム

(57)【特許請求の範囲】

【請求項１】

デジタル資産へのアクセスを移転させる方法であって：

複数の第２コンピュータシステムの各々によって、第１コンピュータシステムから、第１ブロックチェーントランザクションを受け取るステップであって、前記第１コンピュータシステムは、暗号システムの第１秘密－公開鍵ペアの第１秘密鍵を有し、各々のコンピュータシステムは、前記暗号システムの第２秘密－公開鍵ペアの第２秘密鍵のそれぞれの共有分を有し、前記第１ブロックチェーントランザクションは前記第１秘密鍵で署名される、ステップと；

複数の前記第２コンピュータシステムによって、前記第１ブロックチェーントランザクションが前記第１秘密鍵で署名されていることを検証するステップと；

前記第２秘密鍵のそれぞれの前記共有分を前記第１ブロックチェーントランザクションに適用して、第１秘密値のそれぞれの共有分を生成するステップであって、前記第１秘密値は、前記第２秘密鍵で署名された第２ブロックチェーントランザクションであり、前記第１秘密値は、前記第１秘密値の前記共有分の第１閾値数がアクセス可能であり、前記第１秘密値の前記共有分の前記第１閾値数未満はアクセス可能ではないステップと；

前記第１コンピュータシステム及び複数の前記第２コンピュータシステムからの前記第１秘密値の少なくとも前記第１閾値数の前記共有分を組み合わせて、前記第１秘密値を生成するステップと；

を含む、方法。

【請求項２】
複数の前記第２コンピュータシステムの各々は、前記暗号システムのそれぞれの秘密鍵を有する、
請求項１に記載の方法。
【請求項３】
前記第１コンピュータシステム及び少なくとも１つの前記第２コンピュータシステムの間で、前記第１コンピュータシステムの所有する前記第２秘密鍵の共有の共有分を分配するステップ、
を更に含む、請求項１又は２に記載の方法。
【請求項４】
前記第２コンピュータシステムが非応答性になった場合、前記デジタル資産へのアクセスを、前記暗号システムの第３秘密鍵に移転させるステップ、
を更に含む、請求項１乃至３のいずれか一項に記載の方法。
【請求項５】
前記デジタル資産は、所定の時間の間、前記第３秘密鍵の制御下にとどまる、
請求項４に記載の方法。
【請求項６】
複数の前記コンピュータシステムの間で、前記第２秘密鍵の前記共有分を分配するステップ、
を更に含む、請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
デジタル資産へのアクセスを移転させる方法であって、当該方法は：
第１コンピュータシステムから複数の第２コンピュータシステムに第１ブロックチェーントランザクションを送信するステップであって、前記第１コンピュータシステムは、暗号システムの第１秘密－公開鍵ペアの第１秘密鍵を有し、各々のコンピュータシステムは、前記暗号システムの第２秘密－公開鍵ペアの第２秘密鍵のそれぞれの共有分を有し、前記第１ブロックチェーントランザクションは、前記第１秘密鍵で署名される、ステップと；
複数の前記第２コンピュータシステムから、第１秘密値のそれぞれの共有分を受け取るステップであって、前記第１秘密値は、前記第２秘密鍵で署名された第２ブロックチェーントランザクションであり、前記第１秘密値は、前記第１秘密値の前記共有分の第１閾値数がアクセス可能であり、前記第１秘密値の前記共有分の前記第１閾値数未満はアクセス可能ではなく、前記第２秘密鍵の各々の前記共有分は、前記第１ブロックチェーントランザクションが前記第１秘密鍵で署名されたことを、対応する前記第２コンピュータシステムによって検証した後、前記第２ブロックチェーントランザクションに適用される、ステップと；
前記第１コンピュータシステム及び複数の前記第２コンピュータシステムからの前記第１秘密値の少なくとも前記第１閾値数の前記共有分を組み合わせて、前記第１秘密値を生成するステップと；
を含む方法。
【請求項８】
複数の前記第２コンピュータシステムの各々は、前記暗号システムのそれぞれの秘密鍵を有する、
請求項７に記載の方法。
【請求項９】
前記第１コンピュータシステム及び少なくとも１つの前記第２コンピュータシステムの間で、前記第１コンピュータシステムの所有する前記第２秘密鍵の共有の共有分を分配するステップ、
を更に含む、請求項７又は８に記載の方法。
【請求項１０】
前記第２コンピュータシステムが非応答性になった場合、前記デジタル資産へのアクセ

スを前記暗号システムの第３秘密鍵に移転させるステップ、
を更に含む、請求項７乃至９のいずれか一項に記載の方法。
【請求項１１】
前記デジタル資産は、所定の時間の間、前記第３秘密鍵の制御下にとどまる、
請求項１０に記載の方法。
【請求項１２】
前記第２秘密鍵の前記共有分を複数の前記コンピュータシステムの間で分配するステップ、
を更に含む、請求項７乃至１１のいずれか一項に記載の方法。
【請求項１３】
前記暗号システムは、楕円曲線暗号システムであり、各々の公開－秘密鍵ペアの公開鍵は、秘密鍵と楕円曲線ジェネレータ点の乗算によって、対応する秘密鍵に関連付けられる、
請求項１乃至１２のいずれか一項に記載の方法。
【請求項１４】
請求項１乃至１３のいずれか一項に記載の方法を実行するためのコンピュータ実装システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に、データ及びコンピュータベースリソースのセキュリティに関する。より具体的には、本発明は、暗号通貨及び暗号法、並びに楕円曲線暗号法、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ：Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）及び閾値暗号法にも関する。本発明は、（例えば）ビットコインのようなブロックチェーンで実装される暗号通貨に関連して有利に使用することができるが、この点に限定されず、より広範な適用性を有することができる。本発明は、一実施形態では、閾値デジタル署名スキームを提供するものとして説明され得る。
【背景技術】
【０００２】
本出願において、「ブロックチェーン」という用語は、電子的なコンピュータベースの分散台帳のすべての形式を包含するように使用される。これらは、コンセンサスベースのブロックチェーン及びトランザクションチェーン技術、許可及び未許可台帳、共有台帳並びにそれらの変形を含む。ブロックチェーン技術の最も広く知られている用途はビットコイン台帳であるが、他のブロックチェーン実装が提案され、開発されている。本明細書では、単に便宜性及び例示の目的のためにビットコインが参照され得るが、本発明は、ビットコインブロックチェーンでの使用に限定されず、代替的なブロックチェーン実装及びプロトコルが本発明の範囲内にあることに留意されたい。
【０００３】
ブロックチェーンは、ブロックにより構成される、コンピュータベースの非集中システムとして実装されるピアツーピア電子台帳であり、ブロックはトランザクションにより構成される。各トランザクションは、ブロックチェーンシステム内の参加者間におけるデジタル資産のコントロールの移転を符号化するデータ構造であり、少なくとも１つの入力と少なくとも１つの出力を含む。各ブロックは、以前のブロックのハッシュを含み、その結果、ブロックは一緒にチェーン化されることになり、その始めからブロックチェーンに書き込まれたすべてのトランザクションの永久的な変更できないレコードを作成する。
【０００４】
非集中化の概念は、ビットコイン方法の基礎である。非集中システムは、分散又は集中システムとは異なり、単一障害点（ｓｉｎｇｌｅ ｐｏｉｎｔ ｏｆ ｆａｉｌｕｒｅ）が存在しないという利点を提供する。したがって、それらは、強化されたレベルのセキュリティ及び障害許容力を提示する。このセキュリティは、楕円曲線暗号法及びＥＣＤＳＡのような既知の暗号技術の使用により更に強化される。

【０００５】
マルチ署名システムは一般に、デジタル資産へのアクセスを提供するために２以上の当事者の署名を必要とすることによって、セキュリティを強化するようビットコインブロックチェーンで使用される。
【０００６】
ＥＣＤＳＡ閾値署名スキームは、ビットコインウォレットを保護するための「マルチ署名」システムに取って代わり、向上したセキュリティとプライバシー、並びにより小さな（したがって、コスト的により安価な）トランザクションを提供することができる。非特許文献１及び非特許文献２は、すべての１＜ｔ≦ｎについて、ｎ個の鍵共有保持者のうちの任意のｔ＋１が協力して完全な署名を対話的に生成し得るよう、閾値最適ＥＣＤＳＡ署名スキームのバリエーションを提示している。
【０００７】
しかしながら、これらのスキームは少なくとも２つの制限にわずらわされる。第１に、これらのスキームは、時間のテストにまだ耐えていない、新たな暗号法及び関連する仮定、例えば完全準同型（ｆｕｌｌｙ　ｈｏｍｏｍｏｒｐｈｉｃ）の暗号スキームに依存する。第２に、それらの複雑性及びゼロ知識プルーフの関与のために－例えば書き込み時にゼロ知識プルーフの生成及び検証だけでも、参加者ごとに約１０秒かかるために－それらのスキームは計算コストが高く、したがって遅い。結果として、これらのシステムは、多くのディポジットを保護するために信頼されるべきではなく、（為替操作のように）迅速な署名を必要とする特定の用途には適さない。
【０００８】
例えばこれらのスキームは、例えば非特許文献３に開示されるような、高頻度支払いチャネルベースのシステムで使用することができない。暗号通貨交換所（ｃｒｙｐｔｏｃｕｒｒｅｎｃｙ　ｅｘｃｈａｎｇｅｓ）は、双方向支払いチャネルのための１つのアプリケーションであり、その１つでは高速署名が特に望ましい。
【０００９】
ＥＣＤＳＡ閾値署名の生成のために、より早く低複雑性でよりセキュアなスキームが存在するが、そのようなスキームには特定の制限がある。特に、「２　ｏｆ　３」スキームのような一般的な選択肢を含め、ｔとｎの特定の組合せが除外される。さらに、これらのスキームでは、部分署名の組合せを通して署名を生成するために必要とされるものよりも少ない鍵共有分（ｋｅｙ　ｓｈａｒｅｓ）で、秘密鍵を再構築することが可能である。したがって、「２　ｏｆ　３」マルチ署名技術を採用するビットコイン交換所によって採用される、セキュアなウォレットサービスシステムに対する改善の必要性が存在する。
【００１０】
例えば非特許文献３に開示されるような双方向支払いチャネルは、クライアントが交換所に置かなければならない信用（ｔｒｕｓｔ）を大幅に減少させつつ、資産の取引を許可することができる。従来のモデルでは、クライアントは、交換所でビットコイン及びフィアット通貨のディポジットを保持し得る。クライアントが取引するとき、それらが所有するビットコインとフィアットの比率は変化する。しかしながら、これらの比率は、交換所によって記録される取引に依存するため、クライアントは、正確な記録を維持するために交換所を信用しなければならない。言い換えると、ビットコイン（及びトークン化されている場合は、フィアット）のディポジットは、エスクローサービスを採用することによって（ある程度）盗難から保護され得るが、クライアントは、交換所が危険にさらされて取引の記録が失なわれたり変更されたりした場合には、依然としてそれらのディポジットを失う可能性がある。
【００１１】
双方向支払いチャネルは、複数の更なる欠点にわずらわされる。双方向支払いチャネルの標準的な実装を考える。アリスとボブは、彼らの間で暗号トークンを送り合いたい。彼らは各々、合意した数のトークンを有する「２　ｏｆ　２」マルチ署名を提供し、その後、トークンは、チャネルの以前の状態を効率的に無効にする「値（ｖａｌｕｅ）」とともに

、コミットメントトランザクションを交換することによって送信される（チャネルは更新される）。古いコミットメントトランザクションが、ある当事者によってブロードキャストされた場合、他の当事者は、適切な「値」を含む「違反救済トランザクション（ｂｒｅａｃｈ　ｒｅｍｅｄｙ　ｔｒａｎｓａｃｔｉｏｎ）で応答することができ、それによって、チャネル内の残高（ｂａｌａｎｃｅ）全体を請求することができる。

【００１２】

アリスとボブのいずれかがチャネルを清算（ｓｅｔｔｌｅ）したいとき、彼らは各々、最新のチャネル状態（いわゆる「ソフト解決策（ｓｏｆｔ　ｒｅｓｏｌｕｔｉｏｎ）」）に従って残高を分配するトランザクションに署名することに同意し得る。このようにして、コミットメントトランザクションは、両当事者が協力する限り、ブロードキャストされる必要はない。

【００１３】

しかしながら、非特許文献３で説明されるように、支払いチャネルは、多数のチャネルを開いている当事者が長期間非応答性を提示している場合に起こる可能性がある、いわゆる「故障モード」が存在するという点で、主要な未解決の脆弱性を有する。これは、それらに接続している他の当事者に、コミットメントトランザクションをブロードキャストさせようとする可能性があり、当事者の数が多い場合、ブロックチェーンネットワークが圧倒される可能性がある。接続されている当事者が違反救済トランザクションに間に合うように応答することができないことを期待して、悪意ある当事者が、古いコミットメントチャネルをブロードキャストすることによって資金を盗もうとする可能性があるので、そのような状況は、支払いチャネルのコンテキストでは特に危険である。非特許文献３で説明される構成の別の制限は、（チャネルに資金が提供された後、両当事者のうちの一方が、第１コミットメントトランザクションを提供したがらない又は提供することができない可能性を回避するために）Ｓｅｇｒｅｇａｔｅｄ　Ｗｉｔｎｅｓｓを必要とする複雑性である。

【００１４】

背景

最新の交換セキュリティ

多くの仮想通貨交換所プラットフォームは現在、多くの場合はＢｉｔｏＧｏによって供給されるような第三者サービスを介して、ビットコインスクリプトのマルチ署名機能に基づくセキュアなウォレットシステムを採用している。これらのシステムは、クライアント又は為替資金を、「２－ｏｆ－３」マルチ署名スクリプトで（すなわち、任意の２　ｏｆ３公開鍵に対応する有効な署名を供給することによって）取り返す（ｒｅｄｅｅｍ）ことができる出力下に置く。３つの対応する秘密鍵は、交換所、クライアント及び信頼できる第三者／エスクロー（ＢｉｔＧｏ）に分配されるであろう。（署名された有効なトランザクションを介する）資金の移動は、次いでｉ）クライアントと交換所又はｉｉ）（クライアントが非協力的であったか、鍵をなくしていた場合）交換所とＢｉｔｏＧｏ、のいずれかによって許可され得る。ＢｉｔＧｏサービスは、交換所からの認証されたＡＰＩ要求を介して署名オペレーションを実行するであろう。

【００１５】

この保護システムは、ＢｉｔＧｏ自体及びそのアプリケーションプログラミングインタフェース（ＡＰＩ）のセキュリティオペレーション及びポリシーに加えて、いくつかの主要な欠点を有する。第１に、２－ｏｆ－３マルチ署名（ｍｕｌｔｉｓｉｇ）出力の使用は、クライアントと交換所の双方のプライバシーを危うくする。２－ｏｆ－３マルチ署名トランザクション出力の数は、出力総数のごく一部であり、その結果、この匿名性の低下は、ブロックチェーンの観察者が、ＢｉｔＧｏに関連付けられる資金及び交換ウォレットを識別することをより容易にする。加えて、２－ｏｆ－３マルチ署名出力の使用は、ブロックチェーン上で内部交換オペレーションも明らかにする。外部観察者は、３つの鍵のうちどの鍵が特定のトランザクションを許可するために使用されたかを、スクリプト内のそれらの位置に基づいて判断することができる。例えば（２－ｏｆ－３マルチ署名ＢｉｔＧｏ

ウォレットシステムを採用した）２０１６年の$６０mのＢｉｔｆｉｎｅｘハックでは、ビットコインブロックチェーン観察者は、資金を盗むために鍵１及び３が使用されたと判断することができた。さらに、２－ｏｆ－３マルチ署名の使用の結果、トランザクションサイズがかなり大きくなり、したがって、ブロックチェーン上で確実かつ迅速に確認するためには、より大きなトランザクション（マイナ）報酬（ｆｅｅ）が必要となる。また、２－ｏｆ－３マルチ署名スクリプトは、ビットコインクライアントでは「非標準」と考えられるので、それらは、Ｐ２ＳＨ（ｐａｙ－ｔｏ－ｓｃｒｉｐｔ－ｈａｓｈ）フォーマットでリディーム（ｒｅｄｅｅｍ）スクリプトとして実装されなければならない。Ｐ２ＳＨトランザクション出力タイプは基本的に、衝突攻撃（又はいわゆる「誕生日攻撃」）の対象となる可能性があるため、標準のＰ２ＰＫＨ（ｐａｙ－ｔｏ－ｐｕｂｌｉｃ－ｋｅｙ－ｈａｓｈ）出力よりもセキュアではない。Ｐ２ＳＨ出力は、ビットコインで１６０ビットのセキュリティを有し、これは、わずか８０ビットのセキュリティで衝突攻撃が防止されることを意味する。このレベルのセキュリティは現時点では、攻撃することは計算上実現可能ではないが、無期限にそのままであるとは限らない。衝突攻撃は、（単一の公開鍵だけを使用する）Ｐ２ＰＫＨ出力では可能でないので、（前画像攻撃（ｐｒｅ－ｉｍａｇｅ　ａｔｔａｃｋ）の場合）１６０ビットのセキュリティを保持する。

【００１６】

閾値署名スキーム

閾値署名プロトコルは、当事者（又はノード）のグループが、任意の時点で秘密鍵を再構築することなく、あるいは任意の参加者が任意の他の当事者の鍵共有分に関して何も学習することなく、閾値ｍ　ｏｆ　ｎ鍵共有分（ｔｈｒｅｓｈｏｌｄ　ｍ　ｏｆ　ｎ　ｋｅｙ　ｓｈａｒｅｓ）を使用して、共同してトランザクション署名することを可能にする。そのようなスキームの使用は、トランザクションを許可するために複数の別個の当事者を必要とするシステムにおける単一障害点を防ぐ。

【００１７】

閾値署名スキームを、秘密共有分を確立するためのディーラーフリー（又はディーラーレス）プロトコルと組み合わせることができ、この場合、共有される秘密（秘密鍵）はいずれの当事者にも知られない（実際、どの時点でもメモリ内に明示的に存在する必要がない）。しかしながら、グループが、（まだ知られていないが、示唆されている共有秘密鍵に対応する）楕円曲線公開鍵を決定することは可能である。これは、ビットコイン出力を、完全に信頼できない方法で共有グループ公開鍵（及び対応するアドレス）の制御下に置くことができ、個々の当事者が秘密鍵を学習することなく、当事者の閾値が共同するときにのみ、トランザクションに対する署名を生成できることを意味する。

【００１８】

楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ：Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）の数学的形式の性質は、このタイプの署名にとってセキュアな閾値スキームを構築することは普通のことではないことを意味する。特に、有効な署名を生成するために必要とされる鍵共有分の数が、完全な秘密鍵を再構築するために必要とされる共有分の数と同じである、効率的かつセキュアな閾値最適スキームを作成することは不可能であることが証明されている。閾値最適ＥＣＤＳＡスキームを構築する第１の方法は非特許文献１で説明されたが、このスキームはかなりの欠点を有する。第１に、これは非常に非効率的である：署名生成は、Ｐａｉｌｌｉｅｒの（更に準同型の）暗号化の実施と、一連のゼロ知識プルーフの作成及び検証の双方を必要とし：２－ｏｆ－２署名では、６回の通信と、（当事者ごとに）最大１０秒の計算時間を必要とする。第２に、秘密鍵は倍増的に（ｍｕｌｔｉｐｌｉｃａｔｉｖｅｌｙ）共有される：これは、ｎ－ｏｆ－ｎ鍵共有のみが可能であり、ｍ＜ｎのｍ－ｏｆ－ｎスキームを実現することは、組合せ鍵共有構造を必要とし、各当事者が、複数の鍵共有分を保持するために必要とされる（各当事者がn^m個の鍵共有分を必要とする）。加えて、信頼できるディーラーなしに、秘密鍵を倍増的に共有することは、（シャミアの秘密鍵共有スキームのように）鍵が多項式で共有される場合よりも更に複雑であり、計算コストが高い。

【００１９】
より最近では、改善された（が、依然として比較的低い）効率の閾値最適ＥＣＤＳＡスキームが、非特許文献２及び完全準同型暗号システムを採用している非特許文献４で提案されている。この暗号プリミティブは、高度な複雑性を有し、比較的テストされていない仮定（ｒｅｌａｔｉｖｅｌｙ ｕｎ－ｔｅｓｔｅｄ ａｓｓｕｍｐｔｉｏｎｓ）に依拠する。例えば非特許文献５及び非特許文献６で説明されるように、他の最近の完全準同型暗号スキームは、成功した暗号解読（ｓｕｃｃｅｓｓｆｕｌ ｃｒｙｐｔａｎａｌｙｓｉｓ）の対象となっており、実際上破られることにも留意すべきである。
【先行技術文献】
【非特許文献】
【００２０】
【文献】S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. A. Kroll, E. W. Felten, and A. Narayanan - Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme (2015)
R. Gennaro et al.. Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security (2016), International Conference on Applied Cryptography and Network Security. ACNS 2016: Applied Cryptography and Network Security pp 156-174
J Poon; T Dryja; The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments (2016)
Boneh, Dan, Rosario Gennaro, and Steven Goldfeder. "Using Level-1 Homomorphic Encryption To Improve Threshold DSA Signatures For Bitcoin Wallet Security."
Bogos, Sonia, John Gaspoz, and Serge Vaudenay. "Cryptanalysis of a homomorphic encryption scheme." ArcticCrypt 2016. No. EPFL-CONF-220692. 2016
Hu, Yupu, and Fenghe Wang. "An Attack on a Fully Homomorphic Encryption Scheme." IACR Cryptology ePrint Archive 2012 (2012): 561
【発明の概要】
【発明が解決しようとする課題】
【００２１】
本発明の好ましい実施形態は、既知のスキームの上記欠点の１つ以上を克服しようとする。
【課題を解決するための手段】
【００２２】
本発明は、添付の特許請求の範囲で定義される方法及びシステムを提供する。
【００２３】
デジタル資産へのアクセスを移転させる方法が提供されてよく、当該方法は：
複数の第２参加者の各々によって、第１参加者から第１ブロックチェーントランザクションを受け取るステップであって、第１参加者は、暗号システムの第１秘密－公開鍵ペアの第１秘密鍵を有し、各参加者は、暗号システムの第２秘密－公開鍵ペアの第２秘密鍵のそれぞれの共有分を有し、第１ブロックチェーントランザクションは第１秘密鍵で署名される、ステップと；
複数の第２参加者によって、第１ブロックチェーントランザクションが第１秘密鍵で署名されていることを検証するステップと；
第２秘密鍵のそれぞれの共有分を第１ブロックチェーントランザクションに適用して、第１秘密値（ｓｅｃｒｅｔ ｖａｌｕｅ）のそれぞれの共有分を生成するステップであって、第１秘密値は、第２秘密鍵で署名された第２ブロックチェーントランザクションであり、第１秘密値は、該第１秘密値の第１閾値数の共有分にはアクセス可能であり、第１秘密値の第１閾値数未満の共有分にはアクセス可能ではない（ｉｎａｃｃｅｓｓｉｂｌｅ）

ステップと；
　第１参加者及び複数の第２参加者からの第１秘密値の少なくとも第１閾値数の共有分を組み合わせて、第１秘密値を生成するステップと；
　を含む。
【００２４】
　第２秘密鍵のそれぞれの共有分を第１ブロックチェーントランザクションに適用して、第２秘密鍵で署名された第２ブロックチェーントランザクションのそれぞれの共有分を生成し、署名された第２ブロックチェーントランザクションは、第１秘密値の第１閾値数の共有分にはアクセス可能であり、第１閾値数未満の共有分にはアクセス可能ではなく、第１参加者及び複数の第２参加者からの第１秘密値の少なくとも第１閾値数の共有分を組み合わせて、署名された第２ブロックチェーントランザクションを生成することにより、これは、第２参加者のうちの１人が非アクティブ又は非協力的になるべきである場合、トランザクションの署名を可能にするという利点を提供し、それにより、システムのセキュリティ及び信頼性を改善することができる。また、第１参加者からの第１ブロックチェーントランザクションの受け取りに応答して、第１秘密値の共有分を生成することにより、これは、第１秘密値の少なくとも３つの共有分が生成されるよう、第１秘密値のその共有分が自動的に生成されることを可能にするという更なる利点を提供し、それにより、２　ｏｆ３署名スキームのエミュレーションを可能にすることができる。
【００２５】
　複数の第２参加者の各々は、暗号システムのそれぞれの秘密鍵を有してよい。
【００２６】
　これは、秘密鍵に対応する公開鍵によって、秘密鍵での署名の検証を可能にするという利点を提供し、それによりシステムのセキュリティを強化する。
【００２７】
　方法は、第１参加者及び少なくとも１人の第２参加者の間で、第１参加者を所有（ｉｎ　ｐｏｓｓｅｓｓｉｏｎ）して第２秘密鍵の共有の共有分を分配するステップを更に含んでよい。
【００２８】
　これは、セキュリティを更に強化するという利点を提供する。
【００２９】
　方法は、第２参加者が非応答（ｕｎｒｅｓｐｏｎｓｉｖｅ）になった場合、デジタル資産へのアクセスを、暗号システムの第３秘密鍵に移転させるステップを更に含んでよい。
【００３０】
　デジタル資産は、所定の時間の間、第３秘密鍵の制御下にとどまってよい。
【００３１】
　方法は、複数の参加者の間で、第２秘密鍵の共有分を分配するステップを更に含んでよい。
【００３２】
　デジタル資産へのアクセスを移転させる方法が提供されてよく、当該方法は：
　第１参加者から複数の第２参加者に第１ブロックチェーントランザクションを送信するステップであって、第１参加者は、暗号システムの第１秘密－公開鍵ペアの第１秘密鍵を有し、各参加者は、暗号システムの第２秘密－公開鍵ペアの第２秘密鍵のそれぞれの共有分を有し、第１ブロックチェーントランザクションは、第１秘密鍵で署名される、ステップと；
　複数の第２参加者から、第１秘密値のそれぞれの共有分を受け取るステップであって、第１秘密値は、第２秘密鍵で署名された第２ブロックチェーントランザクションであり、第１秘密値は、該第１秘密値の第１閾値数の共有分にアクセス可能であり、第１秘密値の第１閾値数未満の共有分にはアクセス可能ではなく、第２秘密鍵の各共有分は、第１ブロックチェーントランザクションが第１秘密鍵で署名されたことを、対応する第２参加者によって検証した後、第２ブロックチェーントランザクションに適用される、ステップと；

第１参加者及び複数の第２参加者からの第１秘密値の少なくとも第１閾値数の共有分を組み合わせて、第１秘密値を生成するステップと；
を含む。
【００３３】
メッセージにデジタル署名する方法が提供されてよく、当該方法は：
第１秘密値の第１共有分を複数の参加者間で分配するステップであって、第１秘密値は、暗号システムの公開－秘密鍵ペアの秘密鍵であり、該秘密鍵は、第１閾値数の第１共有分によってアクセス可能であり、第１閾値数未満の第１共有分にはアクセス可能ではない、ステップと；
第２秘密値の第２共有分を複数の参加者間で分配するステップであって、第２秘密値は、デジタル署名を生成する際に使用するための短期鍵（ｅｐｈｅｍｅｒａｌ　ｋｅｙ）であり、該短期鍵は、第１閾値数の第２共有分によってアクセス可能であり、第１閾値数未満の第２共有分にはアクセス可能ではない、ステップと；
第３秘密値の第３共有分を複数の参加者間で分配するステップであって、各第３共有分は、第４秘密値のそれぞれの第４共有分を生成するためにメッセージに適用されるよう適合され、第４秘密値は、短期鍵を使用して秘密鍵で署名されたメッセージであり、第４秘密値は、第２閾値数の第４共有分によってアクセス可能であり、第２閾値数未満の第４共有分にはアクセス可能ではない、ステップと；
を含む。
【００３４】
第３秘密値の第３共有分を複数の参加者間で分配し、各第３共有分は、第４秘密値のそれぞれの第４共有分を生成するためにメッセージに適用されるよう適合され、メッセージが、秘密鍵及び短期鍵で署名されており、第４秘密値は、第２閾値数の第４共有分によってアクセス可能であり、第２閾値数未満の第４共有分にはアクセス可能ではないことにより、これは、デジタル署名共有分のかなりの割合（ｓｕｂｓｔａｎｔｉａｌ　ｐｒｏｐｏｒｔｉｏｎ）があらかじめ生成され、迅速な署名が必要とされるときに、メッセージに適用されることを可能にするという利点を提供する。これは、トランザクションの迅速な非インタラクティブな署名を可能にし、したがって、交換所での使用に適している。
【００３５】
各参加者に分配された共有分は、各々の他の参加者にはアクセス可能ではなくてよい。
【００３６】
共有分を各参加者に分配するステップは、参加者又は各参加者とのそれぞれの暗号化された通信チャネルを提供することを含んでよい。
【００３７】
第１及び／又は第２共有分は、それぞれのシャミア秘密共有スキーム（Ｓｈａｍｉｒ　ｓｅｃｒｅｔ　ｓｈａｒｉｎｇ　ｓｃｈｅｍｅｓ）によって作成されてよい。
【００３８】
複数の第１及び／又は第２共有分は、第１多項式関数（ｆｉｒｓｔ　ｐｏｌｙｎｏｍｉａｌ　ｆｕｎｃｔｉｏｎ）のそれぞれの値であってよく、対応する秘密値は、第１閾値数の共有分から多項式関数を導出することによって決定され得る。
【００３９】
少なくとも１つの第１及び／第２秘密値は、ＪＲＳＳ（ｊｏｉｎｔ　ｒａｎｄｏｍ　ｓｅｃｒｅｔ　ｓｈａｒｉｎｇ）によって複数の参加者間で共有されてよい。
【００４０】
少なくとも第３秘密値を共有することは、ＪＺＳＳ（ｊｏｉｎｔ　ｚｅｒｏ　ｓｅｃｒｅｔ　ｓｈａｒｉｎｇ）によって生成されるマスキング共有分（ｍａｓｋｉｎｇ　ｓｈａｒｅｓ）を共有することを含んでよい。
【００４１】
暗号システムは楕円曲線暗号システムであってよく、各公開－秘密鍵ペアの公開鍵は、秘密鍵と楕円曲線ジェネレータ点（ｅｌｌｉｐｔｉｃ　ｃｕｒｖｅ　ｇｅｎｅｒａｔｏｒ

ｐｏｉｎｔ）の乗算（ｍｕｌｔｉｐｌｉｃａｔｉｏｎ）により、対応する秘密鍵に関連付けられる。

【００４２】

本発明の更なる態様によると、上記で定義された方法を実行するためのコンピュータ実装システムが提供される。

【図面の簡単な説明】

【００４３】

本発明の実施形態は、限定的意味ではなく単なる例として、添付の図面を参照して説明される。

【図１】本発明を具現化するデジタル署名システムを示す図である。

【図２Ａ】図１のプロセスで使用するためのデジタル署名の共有分を生成するためのシステムを示すである。

【図２Ｂ】図１のプロセスで使用するためのデジタル署名の共有分を生成するためのシステムを示すである。

【図３】図２のプロセスで生成された共有分からデジタル署名を生成するプロセスを示す図である。

【図４】秘密鍵の共有分を分割するためのプロセスを示す図である。

【図５】非応答性又は悪意のある参加者の場合にデジタル署名を実行するためのシステムを示す図である。

【発明を実施するための形態】

【００４４】

<u>システム概要</u>

図１を参照すると、ブロックチェーントランザクション４の迅速な署名を実行するために本発明を具現化するシステム２は、閾値署名スキームの４つの当事者を有する。当事者は、クライアント６、交換所（ｅｘｃｈａｎｇｅ）８、信頼できる第三者（ＴＴＰ：ｔｒｕｓｔｅｄ　ｔｈｉｒｄ　ｐａｒｔｙ）１０及びエスクロー１２である。各当事者は、それぞれ、それぞれの楕円曲線公開／秘密鍵ペア（y_C，x_C）、（y_{Ex}，x_{Ex}）、（y_T，x_T）、（y_{Es}，x_{Es}）を有する。先行技術の典型的な「２　ｏｆ　３」エスクロー構成と比べると、本発明は、追加の当事者であるＴＴＰ１０を特徴とする。以下で更に詳細に説明されるように、ＴＴＰ１０は、（不良分解能（ｆａｕｌｔ　ｒｅｓｏｌｕｔｉｏｎ）の場合）エスクロー１２を含まないすべての署名の生成に参加することを必要とされる。

【００４５】

ＴＴＰ１０は、交換所８との高速（低レイテンシ）かつ信頼性のある接続を有することを必要とされ、ＴＴＰ１０はすべての他の当事者から物理的に分離されているべきである。

【００４６】

暗号化と認証の双方を可能にするセキュアな通信チャネルが、クライアント６と交換所８との間、交換所８とＴＴＰ１０との間、クライアント６とＴＴＰ１０との間及び交換所８とエスクロー１２との間で確立される。これらの通信チャネルは、国際特許出願ＷＯ２０１７／１４５０１６号で説明されている方法を使用して追加の通信なしに周期的に更新できる、共有秘密を確立する。

【００４７】

当事者は、秘密鍵共有分x_nを保持する（閾値秘密鍵ｘにおいてｎ＝１，２，３，４）；共有分は、完全な秘密鍵が単一の場所に存在することが決してないように、以下で更に詳細に説明される方法に従って分散的に（すなわち、信頼できるディーラーなしに）生成される。これらの共有分は（署名初期化とともに）、部分署名（又は署名共有分）sig_n（メッセージｍにおいてｎ＝１，２，３，４）（ビットコイン・トランザクションハッシュ）を生成するために使用されてよい。ＴＴＰは、交換所８からの認証された要求に応答して、任意のトランザクションに対する部分署名を提供することになる。「３　ｏｆ　４」閾値スキームは、実際上、「２　ｏｆ　３」マルチ署名をエミュレートすることになる。

もう１つの可能性は、ＴＴＰが部分的に署名するトランザクションのタイプに対する制限が存在することである。例えばＴＴＰ１０は、特定のアドレスに送信するトランザクションにのみ署名するべきである。この構成は、ＴＴＰ１０がトランザクションに関して何も知る必要がなく、したがって、「ブラインドでそれに署名（ｓｉｇｎ　ｉｔ　ｂｌｉｎｄ）」できるという利点を有する。また、このスキームは、ＢｉｔＧｏの「２　ｏｆ　３」構造を最もよく模倣する。

【００４８】

当事者２、３及び４は、閾値秘密鍵における彼らの共有分が、保護された「エンクレーブ（ｅｎｃｌａｖｅ）」内で生成されるように、信頼できるハードウェアを使用すると想定される。メッセージを、エンクレーブに送信することができ、メッセージに対する（部分）署名は、特定の条件に合致する場合に出力されてよいが、秘密鍵共有分はエンクレーブを離れることはない。このスキームでは、２つの秘密鍵共有分を所与として、閾値秘密鍵を再構築することができる。しかしながら、信頼できるハードウェアの使用により、攻撃は、両方のハードウェア部分が同じ世代（ｓａｍｅ　ｇｅｎｅｒａｔｉｏｎ）の鍵共有分を含むときにハードウェアの２つのセットへの長期の物理的アクセスを必要とするであろう。したがって、そのような攻撃は、実際問題として実現することが非常に難しいであろう。

【００４９】

交換所の基本オペレーション

図１を参照すると、交換オペレーションに関連する閾値ウォレットの高レベル機能は以下のとおりである：

１．クライアント６は、ビットコインＢを、閾値スキームによって生成された（ディーラーレス）公開鍵に関連付けられる口座（ａｃｃｏｕｎｔ）にディポジットする。

２．様々な取引が実行され、クライアント６に属するＢの比率（ｐｒｏｐｏｒｔｉｏｎ）を残す。

３．（クライアント６によって又は交換所８によって）決済（Ｓｅｔｔｌｅｍｅｎｔ）が要求される。決済を要求しているのは交換所８であり、資金の正しい分配がトランザクションＴで符号化されているとする。

４．Ｔ及びＳｉｇ（Ｔ，x_{Ex}）が交換所８によってＴＴＰ１０に送信される。

５．Ｓｉｇ（Ｔ，x_{Ex}）が検証された場合、ＴＴＰ１０は、Ｔに対するそれらの部分署名（sig_3で示される）を交換所８に送信する。ＴＴＰ１０は、Ｔ内に含まれる情報を知る必要はなく、実際、そうでなかった場合、セキュリティの観点からより良いであろう。これは、部分的ブラインド署名オペレーションを介して達成され得る。

６．一方、要求が本物と見なされ（Ｓｉｇ（Ｔ，x_{Ex}）が検証され）、それらがＴのコンテンツに合意する場合、クライアント６は$Sig(T, x_C)$、sig_1、$Sig(sig_1, x_C)$を交換所８に送信する。

７．署名が検証された場合、交換所８はsig_2、sig_1、sig_3を結合し、署名Ｓｉｇ（Ｔ，ｘ）が検証されたことをチェックし、検証された場合、Ｔ、Ｓｉｇ（Ｔ，ｘ）はブロックチェーンネットワークにブロードキャストされる。

【００５０】

セキュアウォレットプロトコル

このセクションは、セキュアウォレットの作成及びその後の閾値署名オペレーションのためのプロトコルを説明する。プロトコルは、R. Gennaro, S. Jarecki, H. Krawczyk及びT. Rabinによる「Robust threshold DSS signatures」（In International Conference on the Theory and Applications of Cryptographic Techniques, 354-371 (1996)）で詳細に説明されている高レベルなプリミティブに関して説明される。

【００５１】

ディーラーフリー鍵生成

セキュアウォレットの作成は、（国際特許出願ＷＯ２０１７／１４５０１６で説明され

るように）スキーム内の４参加者間のセキュアな通信チャネルの再初期化で開始される。
【００５２】
交換所８は次いで、共有楕円曲線公開鍵のディーラーフリー生成を調整し、この場合、４参加者の各々が、（次数１の多項式における）対応する秘密鍵の共有分を保持する。秘密鍵を再構築するためにはこれらの４つの共有分のうちの２つで十分であるが、鍵共有分が信頼できる実行環境で保護される場合、これらの参加者のうちの２参加者の共謀では、このオペレーションは不可能である。トランザクションを許可する唯一の可能な方法は、４当事者のうちの３当事者に関与する閾値署名の生成によるものである。
【００５３】
鍵生成は、ＪＶＲＳＳ（Ｊｏｉｎｔ Ｖｅｒｉｆｉａｂｌｅ Ｒａｎｄｏｍ Ｓｅｃｒｅｔ Ｓｈａｒｉｎｇ）プロトコルを実行し、Ｅｘｐ－Ｉｎｔｅｒｐｏｌａｔｅプロシージャを介して共有多項式及び対応する共有公開鍵ｙを作成することを含み、各当事者はその多項式における共有分（x_i）を有する。Ｅｘｐ－Ｉｎｔｅｒｐｏｌａｔｅプロシージャは、楕円曲線ジェネレータ点によって乗算される少なくとも閾値数の共有分から、すなわち、閾値数の共有分から共有秘密を回復するために使用される同様の技術（すなわち、ラグランジュ補間）を使用して、楕円曲線ジェネレータ点によって乗算される共有秘密の回復である。秘密共有分の無条件のセキュアな検証（Ｕｎｃｏｎｄｉｔｉｏｎａｌｌｙ ｓｅｃｕｒｅ ｖｅｒｉｆｉｃａｔｉｏｎ）は、Ｐｅｄｅｒｓｅｎのプロトコル［Ｐｅｄｅｒｓｅｎ １９９１］を実行することによって保証される。このプロセスは図２に示されている。鍵生成が検証可能に実行されると、クライアント（又は交換所）は、共有公開鍵（ｙについて、対応するビットコインアドレス）に資金を支払い、これは次いで、交換所（又はクライアント）によって確認される。パラメータｒがw_0のｘ座標から計算されることに留意されたい。
【００５４】
短期鍵共有
所与のトランザクションに対して迅速で非インタラクティブな署名生成を可能にするために、署名手順の前に、署名を構築するために必要な短期鍵（ｋ）共有分及び秘密共有乗算（ｓｅｃｒｅｔ ｓｈａｒｅ ｍｕｌｔｉｐｌｉｃａｔｉｏｎ）を生成することができる。これは、署名が要求されると、各当事者が必要とされるのは、（特定のトランザクションハッシュmを所与として）彼らの署名共有分を計算することだけであることを意味する。その後、その署名共有分を、誰でもブロードキャストして補間し、完全な署名を生成することができる。
【００５５】
図２は、この「事前署名」プロシージャを（未知のランダム値を共有する）ＪＲＳＳ（Ｊｏｉｎｔ Ｒａｎｄｏｍ Ｓｅｃｒｅｔ Ｓｈａｒｉｎｇ）プロトコル及び（マスキングのために使用される、ランダム共有分でゼロを共有する）ＪＺＳＳ（Ｊｏｉｎｔ Ｚｅｒｏ Ｓｅｃｒｅｔ Ｓｈａｒｉｎｇ）プロトコルに関して示している。図２に示されるオペレーションは、いずれの当事者も完全な短期鍵を学習することなく、ｒの値を短期鍵共有分から共同で計算するために実行される。
【００５６】
本明細書で説明される共有鍵生成及び「事前署名」構成を並行して同時に実行することができ、これにより通信レイテンシを大いに節約することができる。
【００５７】
署名生成
図３に示されるように、（共有公開鍵ｙの）有効な署名の生成は、３当事者の同意を必要とする（署名は、次数２（ｔ＝２）署名共有多項式における３点から補間される）。通常のオペレーションでは、共有分は、クライアント６、交換所８及びＴＴＰ１０によって生成される。完全な署名補間（ラグランジュ）を任意の当事者によって実行できるが、本実施形態では、最終的なトランザクションをコンパイルしてネットワークにブロードキャストすることになる交換所８（又はクライアント６）によって実行される。図３は、各当

事者が署名共有分を計算し、次いでそれをブロードキャストすることを示している。この共有分は公開（ｐｕｂｌｉｃ）とすることができる－それは、秘密鍵又は短期鍵共有分に関する情報又は（ゼロの）マスキング共有分ｃ$_i$による任意の他の識別情報を含まない。図２に示される鍵及び署名共有分を分配するために使用される鍵共有スキームのより詳細な説明は、付録１に記載される。

【００５８】

クライアント鍵管理

セキュアな資金に対するディーラーフリー共有鍵からのセキュリティの利点に加えて、クライアント鍵共有分を分割することによって、クライアントのセキュリティを更に強化することができる。このプロセスは図４に示されている。ＪＶＲＳＳ（Ｊｏｉｎｔ　Ｖｅｒｉｆｉａｂｌｅ　Ｒａｎｄｏｍ　Ｓｅｃｒｅｔ　Ｓｈａｒｉｎｇ）プロトコルから確立されると、クライアント鍵共有分（ｘ$_1$）それ自体を２つ又は３つのサブ共有分（ｓｕｂ－ｓｈａｒｅｓ）に分割することができる。分割は、国際特許出願ＷＯ２０１７／１４５０１０で説明されるプロトコルに従って実行される。鍵共有分は分割されると、セキュアに削除される。サブ鍵共有分は、次いで異なるデバイスに送信され、トランザクション署名を許可するために、２因子認証（２ＦＡ：ｔｗｏ－ｆａｃｔｏｒ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を可能にする。交換所がクライアントのサブ鍵共有分のうちの１つを格納することによって、更なるセキュリティ強化を達成することができ－したがって、（２ＦＡを介して）クライアントと交換所の双方が、クライアントの部分署名を提供することに同意する必要がある。

【００５９】

悪意ある／非応答性当事者の場合における解決策

非応答性クライアント

図５を参照すると、この場合、交換所８は、Ｔに対する閾値署名を構築するために、エスクロー１２を必要としなければならない。状況はＢｉｔＧｏで起こるものと同じである。エスクロー１２に参加するよう説得する手順は比較的遅く、複数のチェックを伴う可能性がある（例えば交換所８のセキュリティが危険にさらされている可能性を防ぐために）。追加のセキュリティのために、エスクロー１２は、閾値署名の下で保護される特別な「保有口座」（回復アドレス：ｒｅｃ）に資金を移動させるトランザクションに対する部分署名のみを（最初に）提供するように構成されてよく、資金はそこで一定期間の間保持されなければならない。この口座の重要性は、閾値スキームの当事者に対してのみ知られ得る。この予防措置は、クライアント６が誤って非応答性であるとみなされた場合に、クライアント６に介入する時間を与える。

【００６０】

悪意あるクライアント

また図５を参照すると、悪意のあるクライアント６は、無効な署名共有分（すなわち、ｓ$_1$）を提供することによって、有効な閾値署名の生成（したがって、資金の移動）を妨げるように動作する。３つの署名共有分を組み合わせて完全な署名を形成すると、（共有公開鍵での検証の失敗により）その署名が正しくないことがすぐに明らかになるであろう。この場合、最初のステップは、３つの署名共有分（ｓ$_1$、ｓ$_2$又はｓ$_3$）のうちのどれが無効であるかを識別する。これを反復的に行うことができる：交換所８、ＴＴＰ１０及びエスクロー１２は、回復アドレスへのトランザクションに署名するよう試みることができ、これが失敗した場合、署名はクライアント６、ＴＴＰ１０及びエスクロー１２から共有分を生成することができる（すなわち、交換所８の共有分は悪意がある）。あるいは、署名共有検証スキームを用いることができる。

【００６１】

本発明は、「２　ｏｆ　３」マルチ署名技術を用いるビットコイン交換によって用いられるセキュアウォレットサービスシステムが、多項式秘密共有を用いる閾値署名に基づくスキームによって効率的に置換される（そして改善される）ことを可能にする。また、本発明は、（例えば非特許文献１及び非特許文献２とは対照的に）高頻度で署名することを可

能にするので、支払いチャネルを介した取引と互換性がある。
【００６２】
また、本発明を、非応答性交換の可能性に対してロバストにすることもできる。ＴＴＰは、すべてのコミットメントトランザクションを見る（そして、これに対する部分署名を提供する）ので、ＴＴＰは常に現在のチャネル状態を知っており、これは、ＴＴＰがエスクロー及びクライアントと協力して、交換が非応答になった場合に、ソフト解決策の順序正しいシーケンス（ｏｒｄｅｒｌｙ　ｓｅｑｕｅｎｃｅ）を提供することができ、したがって、上述の「障害モード」を回避することができる。
【００６３】
また、本発明は、オンチェーントラザクション内に第１コミットメントトランザクションを組み込むことによって、第１コミットメントトランザクションを交換することにより、Ｓｅｇｒｅｇａｔｅｄ　Ｗｉｔｎｅｓｓの必要性を回避する。エスクローは、これらのトランザクションのブロックチェーンをモニタし、適切な当事者と協力して、関連するトランザクションがタイムアウト前に観察されない場合に払い戻しを提供する。
【００６４】
当事者のいずれかの利用可能性及びセキュリティ（したがって、システム全体として）は、（プライベート）「コングレス（Ｃｏｎｇｒｅｓｓ）」のメンバ間で閾値秘密鍵の秘密鍵及び／又は共有分を更に共有することによって強化され得ることに留意されたい。例えばエスクローは、必要なＥＣＴがブロックチェーン上で観察されない場合に払い戻しを開始してよい。この場合、ブロックの難しさを、コングレスのメンバに属しているＴＥＥ内部でチェックすることができ、チャネルに資金提供された後に特定のブロック数内でコミットメントトランザクションが観察されない場合及びそのような場合にのみ、Ｇｈｏｓｔｃｈａｉｎをインスタンス化して、払い戻しトランザクションに対する（部分）署名を構築してよい。
【００６５】
上述の実施形態は、本発明を限定するものではなく、例示するものであって、当業者は、添付の特許請求の範囲によって定義される本発明の範囲から逸脱することなく、多くの代替的な実施形態を設計することができるであろうことに留意されたい。特許請求の範囲において、括弧内に置かれたいずれの参照符号も、特許請求の範囲を限定するものとして解釈されるべきではない。「備えている（ｃｏｍｐｒｉｓｉｎｇ）」及び「備える（ｃｏｍｐｒｉｓｅｓ）」等の語は、いずれかの請求項又は明細書全体に列挙されるもの以外の要素又はステップの存在を除外しない。本明細書において、「備える（ｃｏｍｐｒｉｓｅｓ）」は「含む又はから成る」を意味し、「備えている（ｃｏｍｐｒｉｓｉｎｇ）」は「含んでいる又はから成っている」を意味する。ある要素の単数形の参照は、そのような要素の複数形の参照を除外せず、また、その逆もそうである。本発明は、いくつかの別個の要素を備えるハードウェアによって及び適切にプログラムされたコンピュータによって実装されてよい。いくつかの手段を列挙しているデバイスの請求項において、これらの手段のいくつかは、１つの同じハードウェアのアイテムによって具現化されてよい。特定の手段が相互に異なる従属請求項に記載されているという単なる事実は、それらの手段の組合せを有利に使用することができないことを示すものではない。
【００６６】
<u>付録１　－　鍵共有及び鍵共有生成の詳細な説明</u>
<u>アルゴリズム１　－　鍵生成</u>
ドメインパラメータ（ＣＵＲＶＥ，カーディナリティｎ，ジェネレータＧ）
入力：　　ＮＡ
出力：　　公開鍵Q_A
　　秘密鍵共有$d_{A(1)}$，$d_{A(2)}$，・・・，$d_{A(j)}$
（ｊ）参加者からのｋスライスの閾値について、鍵（したがって、ビットコイントランザクション）に署名するために、参加者（ｉ）及び参加者（ｉ）が秘密を交換する他の当事者である参加者（ｈ）として指名された（ｊ－１）参加者に関連付けられる構築鍵セグ

メントｄＡ（ｉ）が構築される。
・スキームにおいて、ｊは参加者の総数であり、ここで、ｋ≦ｊ、よってｈ＝ｊ－１である。
・したがって、（ｋ，ｊ）が存在する－閾値共有スキーム。
アルゴリズム１についての方法は以下のとおりである：
１）（ｊ）の各参加者Ｐ（ｉ）（ただし１≦ｉ≦ｊ）は、すべての他の参加者とＥＣＣ公開鍵を交換する。このアドレスは、グループ識別アドレスであり、任意の他の目的のために使用される必要はない。
２）各参加者Ｐ（ｉ）は、すべての他の当事者には秘密の方法で、ランダムな係数を有する次数（ｋ－１）の多項式ｆｉ（ｘ）を選択する。
この関数は、多項式自由項（ｐｏｌｙｎｏｍｉａｌ　ｆｒｅｅ　ｔｅｒｍ）として選択される参加者の秘密
【数１】

$$a_0^{(i)}$$

の形式の第１秘密値の対象となる。この値は共有されない。
ｆｉ（ｈ）は、点（ｘ＝ｈ）における値について参加者ｐ（ｉ）によって選択された関数ｆ（ｘ）の結果となるように定義され、参加者ｐ（ｉ）についての基本方程式は、以下の関数として定義される：
【数２】

$$f_{(x)} = \Sigma_{\mathrm{p}=0}^{(k-1)} \; a_p x^{\mathrm{p}} \bmod n$$

この方程式において、ａ０は、各参加者Ｐ（ｉ）の秘密であり、共有されない。
したがって、各参加者ｐ（ｉ）は、
【数３】

$$f_{i(x)} = \Sigma_{\gamma=0}^{(k-1)} \; a_\gamma x^{\gamma} \bmod n$$

となるように、参加者の秘密として定義されている自由項
【数４】

$$a_0^{(i)}$$

を有する次数（ｋ－１）の多項式として表される、秘密に保持される関数ｆｉ（ｘ）を有する。
３）各参加者ｐ（ｉ）は、参加者Ｐ（ｈ）（∀ｈ＝｛１，．．．，（ｉ－１），（ｉ＋１），．．．，ｊ｝）への第１共有分ｆｉ（ｈ）を、上記のようにＰ（ｈ）の公開鍵を使用して暗号化し、Ｐ（ｈ）の値を交換して復号する。各参加者Ｐｉは、例えば国際特許出願ＷＯ２０１７／１４５０１０に開示されている方法によって、各他の参加者Ｐｊとのそれぞれのセキュアな暗号化された通信チャネルを設定する。
４）各参加者Ｐ（ｉ）は、以下の値をすべての参加者にブロードキャストする。
【数５】

a) $a_\kappa^{(i)} G \quad \forall \kappa = \{0, \ldots, (k-1)\}$

b) $f_i(h) G \quad \forall h = \{1, \ldots, j\}$

５）各参加者Ｐ（ｈ≠１）は、受け取った共有分と各他の参加者から受け取ったものとの一貫性を検証する。
すなわち：　Σｈ^{K}ａ$_{K}$（ｉ）Ｇ＝ｆ$_{ｉ}$（ｇ）Ｇ
また、このｆ$_{ｉ}$（ｈ）Ｇは参加者の共有分と一貫している。
６）各参加者Ｐ（ｈ≠１）は、該参加者（Ｐ（ｈ≠１））によって所有され、受け取られた共有分が、他の受け取った共有分と一貫性があることを確認する：
【数６】

$$a_0^{(i)}G = \Sigma_{h\in \mathrm{B}} b_h f_i(\mathrm{h})G \qquad \forall P_{(h\neq i)}$$

実際、このステップは、ｆ$_{ｉ}$（ｈ）の暗号化されていないバージョンに対して実行される場合に、Ｇａ$_{0}$（ｉ）を回復するために秘密値ａ$_{0}$（ｉ）を回復することになるオペレーションを、共有分ｆ$_{ｉ}$（ｈ）の楕円曲線暗号化バージョン（すなわち、ｆ$_{ｉ}$（ｈ）Ｇ）に対して実行することから成る。したがって、シャミア秘密鍵共有スキームの場合、係数ｂ$_{ｈ}$は、その対応する共有分から秘密を回復するために必要なラグランジュ補間係数を表す。
これが一貫していない場合、参加者はプロトコルを拒否して再開する。加えて、各参加者Ｐ$_{ｊ}$は、自身の暗号化された通信チャネルによって参加者Ｐ$_{ｉ}$と通信するので、どの参加者Ｐ$_{ｊ}$が、一貫性のない共有分に関連付けられるかを識別することができる。
７）参加者ｐ（ｉ）は、以下のように、自身の共有分ｄ$_{Ａ}$（ｉ）を計算する：
【数７】

$$\text{共有分}(p_{(i)}) = d_{A(i)} = \Sigma_{\mathrm{h}=1}^{j} f_h(i) \bmod n$$

ここで、
【数８】

$$\Sigma_{\mathrm{h}=1}^{j} f_h(i) \bmod n$$

は、各参加者Ｐ（ｈ≠ｉ）から受け取られた第２秘密値ａ$_{0}$に応じた第２共有分である。また、ここで、
【数９】

$$\text{共有分}(p_{(i)}) \in \mathrm{Z}_n \qquad \text{及び} d_{A(j)}$$

【数１０】

$$Q_A = Exp - Interpolate\left(f_1, \cdots, f_j\right) \triangleright \left[= G \times d_A\right]$$

また、ここで、Ｅｘｐ－Ｉｎｔｅｒｐｏｌａｔｅ（）オペレーションは、楕円曲線暗号化共有分から楕円曲線暗号化秘密を回復するオペレーションとして定義される。
リターン　　（ｄ$_{Ａ}$（ｉ），Ｑ$_{Ａ}$）
参加者Ｐ（ｉ）は次に、署名を計算する際に共有分を使用する。この役割は、署名を収集するプロセスのコーディネータとしての機能を果たす、任意の参加者又は当事者ｐ（ｃ）によって実施され得る。当事者ｐ（ｃ）は異なる可能性があり、トランザクションに署名をするために十分な共有を収集する各試行において同じ当事者である必要はない。
したがって、秘密鍵共有分
【数１１】

$$d_{A(i)} \leftarrow \mathrm{Z}_n^*$$

は、他の参加者の共有分の知識なしに作成されている。

【００６７】

アルゴリズム２－秘密鍵の更新

入力：　　$d_{A(i)}$と示される、秘密鍵d_Aの参加者P_iの共有分

出力：　　参加者P_iの新たな秘密鍵共有分$d_{A(i)}$

アルゴリズム２を使用して、秘密鍵を更新し、かつプロトコルにランダム性を追加することができる。

１）各参加者は、その自由項としてゼロを条件とする次数（ｋ－１）のランダム多項式を選択する。これは、参加者が、すべての他の参加者の選択された秘密がゼロであることを確かめなければならないが、アルゴリズムと類似する。

ゼロ共有分を生成する：

【数１２】

$$z_i \leftarrow Z_n^*$$

２）$d_{A(i)}' = d_{A(i)} + z_i$

３）リターン：$d_{A(i)}'$

このアルゴリズムの結果は、元の秘密鍵に関連付けられる新たな鍵共有分である。このアルゴリズムのバリエーションにより、第１アルゴリズムのランダム性を高めることが可能であり、ビットコインアドレスの可能性を変更する必要なく、新たな鍵スライスをもたらす再共有エクササイズに従事することも可能である。このようにして、本発明は、基礎となる秘密鍵を変更することなく、グループが、秘密鍵共有分を追加的にマスクすることを可能にする。このプロセスを使用して、基礎となるビットコインアドレス及び秘密鍵を変更することなく、個々の鍵共有分の継続的な使用及び展開に関連付けられる潜在的な鍵漏洩を最小限にすることができる。

【００６８】

アルゴリズム３－署名生成

ドメインパラメータ：ＣＵＲＶＥ，カーディナリティｎ，ジェネレータＧ）

入力：　　署名すべきメッセージ　ｅ＝Ｈ（ｍ）

秘密鍵共有

【数１３】

$$d_{A(i)} \in Z_n^*$$

出力：　　署名

【数１４】

$$e = H(m) \text{について} (r,s) \in Z_n^*$$

Ａ）分散鍵生成

１）アルゴリズム１を使用して、短期鍵共有分を生成する：

【数１５】

$$D_{k(i)} \leftarrow Z_n^*$$

２）アルゴリズム１を使用して、マスク共有分を生成する：

$\alpha_i \leftarrow Z_n$

３）アルゴリズム２を使用して、マスク共有分を生成する：

【数１６】

$$b_i, c_i \leftarrow Z_n^2$$

ｂ及びｃの共有分は、参加者によって秘密に保たれる。

Ｂ）署名生成

４）ｅ＝Ｈ（ｍ）　メッセージｍのハッシュを検証する

５）ブロードキャスト

【数１７】

$$\vartheta_i = D_{k(i)}\alpha_i + \beta_i \bmod n \quad \text{及び}$$

$$\omega_i = G \times \alpha_i$$

６）

【数１８】

$$\mu = Interpolate(\vartheta_i, \ldots, \vartheta_n) \bmod n$$

$$\triangleright \left[= D_k \alpha \bmod n \right]$$

ここで、オペレーション

【数１９】

$$\mu = \text{Interpolate } \left(\upsilon_1, \cdots, \upsilon_j \right) \bmod n$$

は、共有分から秘密を回復するオペレーションとして定義される。

７）

【数２０】

$$\theta = Exp - Interpolate\left(\omega_1, \ldots, \omega_n\right)$$

$$\triangleright \left[= G \times \alpha \right]$$

８）（Ｒｘ，Ｒｙ）を計算する。ここで、

【数２１】

$$r_{x,y} = \left(R_x, R_y\right) = \theta \times \mu^{-1}$$

$$\triangleright \left[= G \times D_k^{-1}] \right]$$

９）ｒ＝ｒｘ＝Ｒｘ　ｍｏｄ　ｎ

ｒ＝０の場合、再開する（すなわち、最初の分配から）

１０）Ｓｉ＝Ｄｋ（ｉ）（ｅ＋ＤＡ（ｉ）ｒ）＋Ｃｉｍｏｄｎをブロードキャストする

１１）Ｓ＝Ｉｎｔｅｒｐｏｌａｔｅ（Ｓｉ，．．．，Ｓｎ）ｍｏｄ　ｎ

ｓ＝０の場合、最初（Ａ．１）からアルゴリズム３をやり直す

１２）（ｒ，ｓ）を返す

１３）ビットコインでは、（ｒ，ｓ）ペアでトランザクションを再構築して、標準のト

ランザクションを形成する。

【００６９】

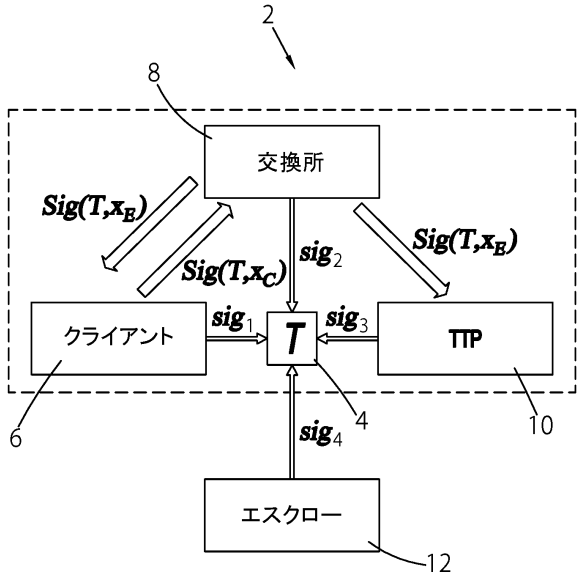
参考文献

【表１】

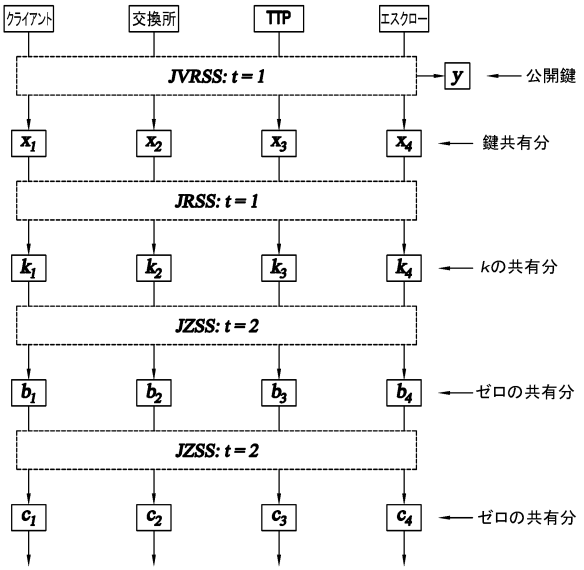
参照	著者、日付、名前及び場所
[Lightning 2016]	J Poon; T Dryja; *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments* (2016).
[Gennaro 1996]	R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold DSS signatures. *In International Conference on the Theory and Applications of Cryptographic Techniques*, 354-371 (1996).
[Goldfeder 2015]	S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. A. Kroll, E. W. Felten, and A. Narayanan. Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme (2015).
[Gennaro 2016]	R. Gennaro et al.. *Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security* (2016). International Conference on Applied Cryptography and Network Security. ACNS 2016: Applied Cryptography and Network Security pp 156-174.
[Boneh 2016]	Boneh, Dan, Rosario Gennaro, and Steven Goldfeder. "Using Level-1 Homomorphic Encryption To Improve Threshold DSA Signatures For Bitcoin Wallet Security."
[Wright 2016]	Wright, C. & Savanah, S. (2016) “Determining a common secret for two Blockchain nodes for the secure exchange of information” "International Patent Application Number: WO 2017/145010". 2016
[Bogos 2016]	Bogos, Sonia, John Gaspoz, and Serge Vaudenay. "Cryptanalysis of a homomorphic encryption scheme." ArcticCrypt 2016. No. EPFL-CONF-220692. 2016.
[Yupu 2012]	Hu, Yupu, and Fenghe Wang. "An Attack on a Fully Homomorphic Encryption Scheme." IACR Cryptology ePrint Archive 2012 (2012): 561.

【図面】

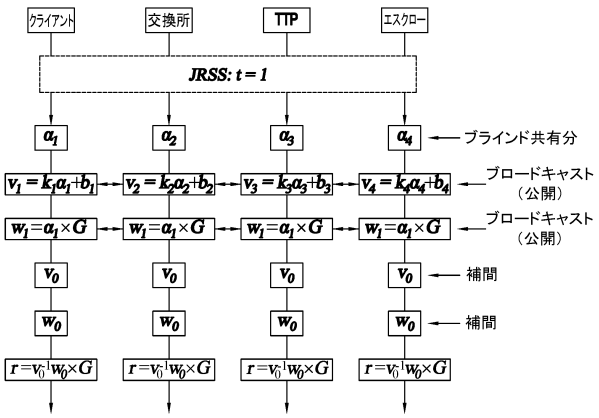
【図１】



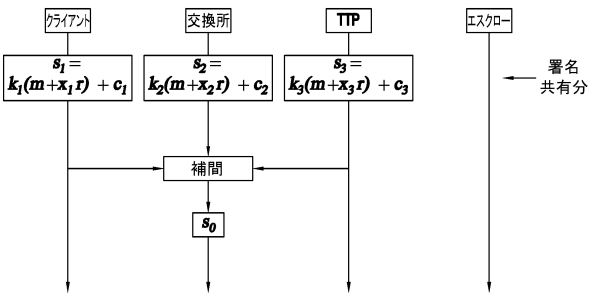
【図２Ａ】



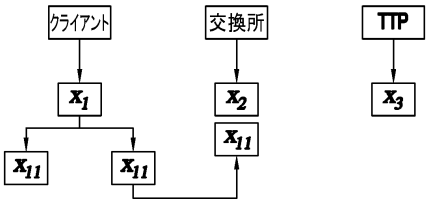
【図２Ｂ】



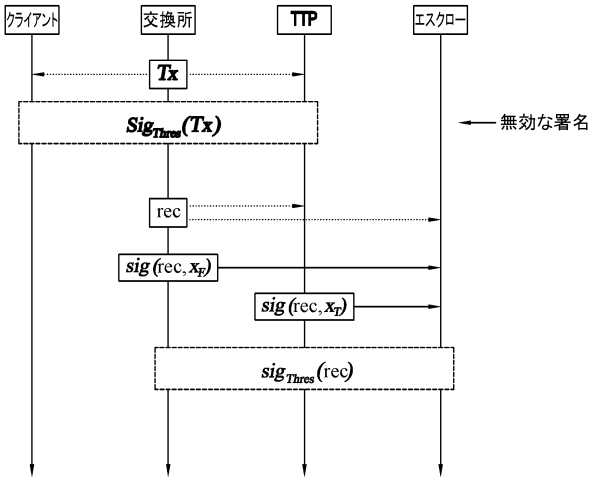
【図３】



【図４】


クライアント
交換所
TTP
エスクロー
x_1
x_2
x_3
x_4
x_{11}
x_{11}
x_{11}

【図５】


クライアント
交換所
TTP
エスクロー
Tx
$Sig_{Thres}(Tx)$
無効な署名
rec
$sig(rec, x_T)$
$sig(rec, x_T)$
$sig_{Thres}(rec)$

フロントページの続き

内
(72)発明者　トレヴェサン，トーマス
イギリス国 シーエフ１０ ２エイチエイチ カーディフ チャーチル ウェイ チャーチル ハウス
７ス フロア アーカート－ダイクス アンド ロード エルエルピー 内
審査官　中里 裕正
(56)参考文献　特表２０１７－５１５２５２（ＪＰ，Ａ）
国際公開第２０１７／１４５００２（WO，Ａ１）
国際公開第２０１７／１４５００７（WO，Ａ１）
国際公開第２０１７／１４５０１０（WO，Ａ１）
国際公開第２０１７／１４５０１６（WO，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／０８
Ｈ０４Ｌ　９／１４
Ｈ０４Ｌ　９／３２
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ Ｘｐｌｏｒｅ