



# THEMIS

デジタル通貨世界のセンターレス化

「アリペイ」

<https://themis.network>



一、 概要 .....	1
二、 デジタル通貨による公正な交換 .....	4
2.1 異種のデジタル通貨の交換 .....	4
2.2 デジタル通貨と実物の交換 .....	5
2.3 THEMIS の設計目標 .....	6
三、 THEMIS 全体のアーキテクチャ .....	8
3.1 THEMIS ブロックチェーン .....	8
3.2 グループマネージドプロトコル .....	11
3.3 紛争解決 .....	13
3.4 ノード選択ポリシー .....	16
3.5 セキュリティ設計 .....	16
3.6 典型的なワークフロー .....	19
3.7 THEMIS ウォレット .....	21
四、 キーテクノロジー .....	25
4.1 グループマネージドに基づく公正な交換プロトコル .....	25
4.2 検証可能なシャッフルと関連リング署名に基づく匿名評判メカニズム .....	27
4.3 非対話型ゼロ知識証明 .....	28
4.4 高並行性の同時検証に対応するデジタル署名アルゴリズム .....	30
五、 シナリオ .....	33
5.1 ピアツーピアのマネージド支払い .....	33
5.2 デジタル通貨取引 .....	34
5.3 マネージドアカウントのセキュリティマネージド .....	35
5.4 マルチエージェント取引の資産マネージド .....	37
六、 チームの紹介 .....	38
6.1 コアチーム .....	38
6.2 コンサルタントチーム .....	42
6.3 パートナー .....	43

## 一、概要

ブロックチェーンをベースとしたデジタル通貨は急速に成長し、ますますビジネス活動に関わる新しい形の通貨となっている。あらゆる種類のデジタル通貨取引が行われ、取引の規模は急速に拡大している。同時に、デジタル通貨の適用範囲の継続的な拡大に伴い、より多くの国と地域（日本など）で多くの業者は支払い方法としてデジタル通貨を受入れるようになっている。全世界でデジタル通貨によるショッピングは広大な市場があることが予見される。

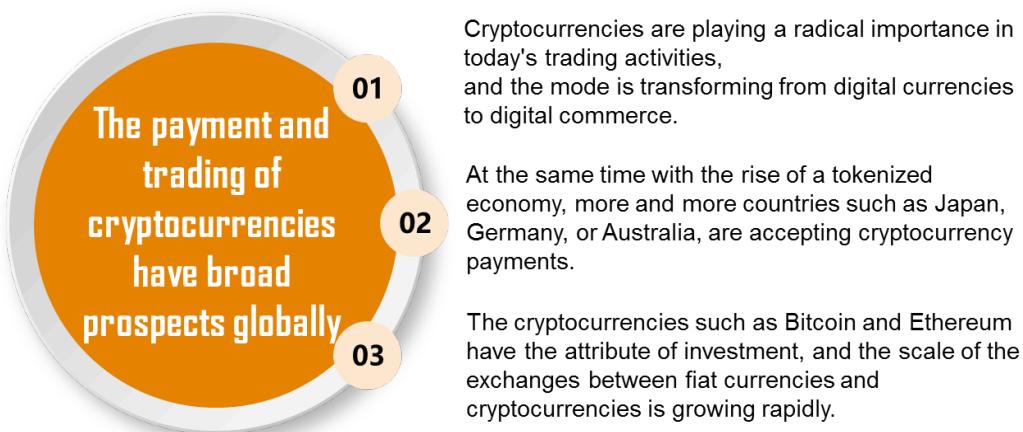


図 1.1 デジタル通貨の発展動向

現在、デジタル通貨取引所およびピアツーピア取引サービスプロバイダは、取引のセキュリティの確保に焦点を与え、取引の公平性にほとんど注意を払っていない。たとえば、広く使用されているハッシュタイムロック契約(Hashed Time-lock Contract, HTLC)技術では、払い戻しタイムロックが悪用されて、サービス拒否攻撃が実行され、取引相手が所定の払い戻し時間内に取引を完成できなくなる。



図 1.2 要件分析

また、デジタル通貨による交換では、買手は商品を受け取ってから支払いたいが、売り手は支払いを受けた後に出荷することを望むため、取引と納入が同時に完了できず、公正なアトミック為替を確保できない。信頼性の高いサードパーティに依存するのは従来の一般的なソリューションである。しかし、単一の障害点などの課題があるため、単にサードパーティに依存するソリューションは安全ではなく、歴史的に、ビットコイン取引所やオンライン市場はハッキング攻撃を受け、廃業されたことがある(Mt. Gox、Silk Roadなど)。

従来、公正な交換プロトコルに関する検討は殆ど、公正な交換における信用できるサードパーティへの依存を低減することに焦点を与えている。ブロックチェーンの登場により、公正な交換プロトコルに新たな手を与えた。我々はブロックチェーン技術を使用して Themis<sup>1</sup>という公正な交換システムを構築し、センターレス化デジタル通貨マネージドサービ

<sup>1</sup> Themis(テミス)は、ゼウスの最も尊敬し、最も信頼する妻である。法と正義の女神として、秩序の創造者であり、保護者でもある。

スを提供し、デジタル通貨、デジタル資産、物品の間の公正な交換など  
デジタル通貨による公正な交換の問題を解決できる。

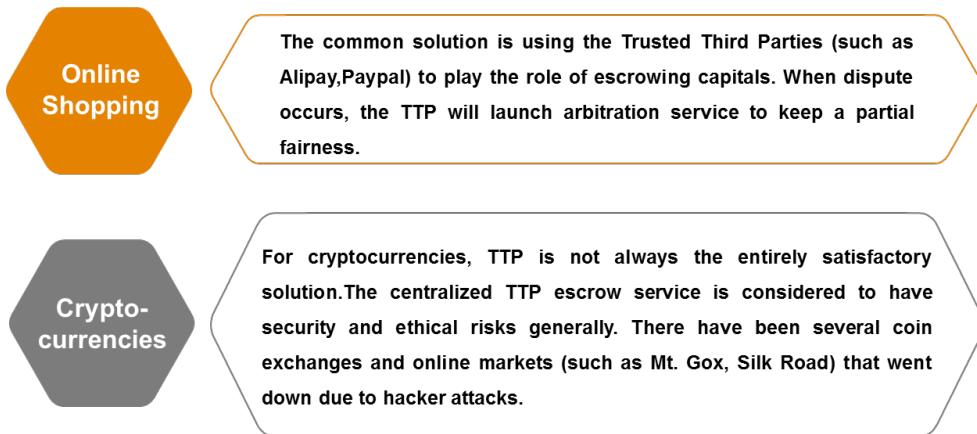


図 1.3 現実の状況

Themis は経済学インセンティブのグループマネージドメカニズムに基づき、しきい値パスワード、匿名評判メカニズム、非対話型ゼロ知識証明及び並行性の高いデジタル署名アルゴリズムなどキー技術ノロジーを使用し、グループ内で悪意のあるメンバー数が半分未満の状況で公平な取引を確保でき、セキュリティ、プライバシー、センターレス化及び DoS 攻撃防止などの特徴がある。Themis はビットコイン、エーテルおよびその他のブロックチェーンに基づく暗号化デジタル通貨に対して安全なマネージドサービスを提供する。

## 二、デジタル通貨による公正な交換

公正な交換とは信頼のない複数の当事者間で、事前の約束に従つて資産の取引を完成するためのプロトコルである。デジタル通貨による交換とは、異種のデジタル通貨の交換、デジタル通貨と実物の交換などのように、交換の主体である一方の当事者はデジタル通貨を交換の対象とすることである。以上はすべて公正な取引プロトコルを用いてセキュリティを確保する必要がある。

### 2.1 異種のデジタル通貨の交換

異種のデジタル通貨間の交換を実現するために、最初に登場したのは取引所モデルである。取引所は内部アカウントを確立し、即ち IOU(I Owe You)アカウントモデルでユーザ間の異種のデジタル通貨の交換を実現する。取引所モデルでは高頻度の取引が達成できるが、次のような欠陥があると認められる。セキュリティリスクがあり、ユーザー資産が取引所によってマネージドされ、ハッキング攻撃や倫理的リスクがあるとみなされる。流動性の欠如が発生し、取引所が離島となり、ユーザー資産が取引所内でしか流動できない。償還の遅延が発生し、取引結果をブロックチェーンでリアルタイムに提出せず、直ちに現金を引き換えることはできない。

センター化取引の欠点を克服するために、人々はセンターレス化取引所モデルを提案している。このモデルの大半は、マルチシグネチャ

方式またはハッシュタイムロック契約(Hashed Time-lock Contract, HTLC)方式に基づいてアトミック取引を保証する。ただし、マルチシグチャ方式は信頼できるサードパーティに依存するため、結託攻撃やサービス拒否攻撃の危険性がある。HTLC 方式の払い戻しタイムロックが悪用されて、サービス拒否攻撃が実行され、取引相手が所定の払戻時間内に取引を完成できなくなることがある。

## 2.2 デジタル通貨と実物の交換

デジタル通貨の取引に特化した既存のセンター化取引所とセンターレス化取引所は、デジタル通貨と実物間の公正な取引の要件を満たすことができない。デジタル通貨と実物の間の交換では、取引と納入が同時に完了できず、公平を確保するためのアトミック為替が挑戦に遭遇する。買手は商品を受け取ってから支払いたいが、売り手は支払いを受けた後に出荷することを望むため、循環依存の問題が発生した。したがって、信頼できるサードパーティに頼り、資金マネージドと仲裁を行う必要がある。取引が達成してから納入が確認するまで、公正の要件を満たすために、買手の取引資金に対してセキュリティマネージドを提供する。

2-of-3 マルチシグチャを利用する取引はマネージド支払いによく使われる形であり、買手、売り手および信頼できるサードパーティーはそれぞれ 1 つのキーを持つ。買手はデジタル通貨を最初にマルチシグチャのマネージドアドレスに支払い、このお金を使うには何れかの当

事者は何れか両者のキーを使用して、デジタル署名を生成する必要がある。取引がスムーズに進む場合、買手は売り手にキーを送り、売り手はマネージドされたお金を受け取ることができる。紛争が発生した場合、信頼できるサードパーティによって仲裁を行い、支払いを完成(または払い戻し)するために仲裁の勝者にキーを送る。

このマネージドプロトコルには 2 つの利点がある。第一、紛争がなければ、買手と売り手はサードパーティを介さずに決済を行うことができる。第二、サードパーティは1つのキーしか持てず、マネージド資金を取得するために少なくとも2つのキーを必要とするため、サードパーティはマネージドされた資金を奪うことができない。

しかし、この方式には重大な課題がある。先ず、共謀の課題があり、マネージドプロトコルが慎重に設計されている場合を除き、受託者は特定の買手や売り手に簡単に接続でき、共謀を実施できる。次にサービス拒否の課題があり、サードパーティがお金を盗むことができなくとも、何れかの紛争を仲裁することを拒否できるため、資金のロックが維持されてしまう。

## 2.3 Themis の設計目標

Themis は、デジタル通貨による公平な交換の問題を解決するために、デジタル通貨の世界で Alipay に似ているセンターレス化公正な交換システムである。技術的に、Themis は次の要件を満たす必要がある。

**公平性**: 交換が終了した後、両当事者は希望の対象物(デジタル通

貨、デジタル資産、実物商品など)を得るか、何も獲得できない(All-or-nothing)。

**セキュリティ**: 交換中、許可がなければ、誰もデジタル通貨を取ることはできない。

**受動性**: 論争がなければサードパーティの関与はない。

**正当性**: 取引と紛争解決が事前に約束した規則に従って実施されることを確保する。

**信頼性**: 紛争が発生した場合、受託者が仲裁決議を実行しないことで資金がロックされることを避ける。即ち、単一の障害点とサービス拒否を避ける。

**プライバシー**: 紛争がなければ、サードパーティは取引が完了したかどうかを知ることができず、非取引当事者は紛争があるかどうかを知ることができない。

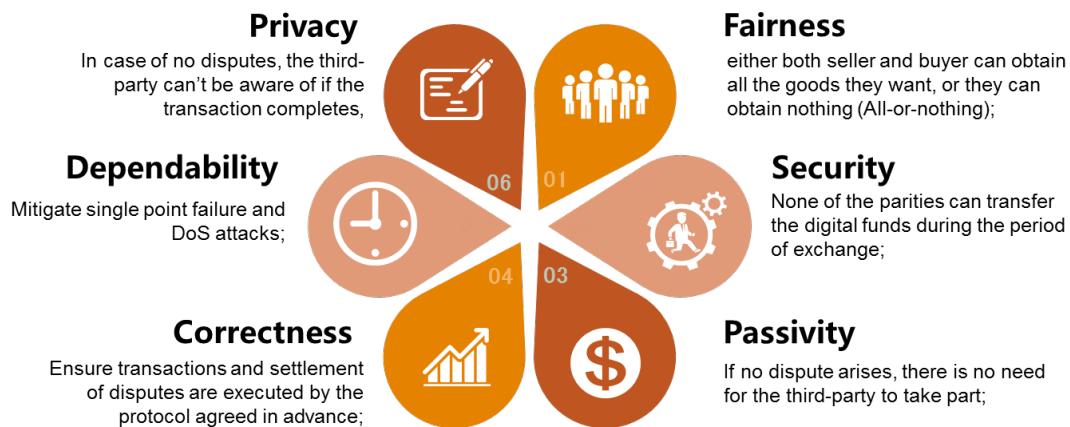


図 2.1 Themis の設計目標

## 三、Themis 全体のアーキテクチャ

### 3.1 Themis ブロックチェーン

Themis はサードパーティのマネージドサービス(現在ネットショッピングにおける Alipay の役割に似ている)を提供し、チェーンでトークンである Global Escrow Token(GET)を発行し、経済学インセンティブに基づくグループマネージドメカニズムと評判メカニズムによりブロックチェーンノードにインセンティブを与え、マネージドプロトコルと仲裁プロトコルを利用して、デジタル通貨の間、デジタル通貨と実物資産の間のピアツーピアの公正な交換を実現する。マネージド手数料と仲裁手数料の発行により、資金マネージドと紛争仲裁に積極的に参加するノードにインセンティブを与える。ユーザーがデジタル通貨で支払うには、GET トークンを支払い、マネージドサービスと仲裁サービスを獲得する必要がある。取引が完了した後、マネージドおよび仲裁に参加したノードは取引側から GET トークンの手数料と報酬を獲得し、GET トークンの Themis でのクローズドループの流れを実現する。

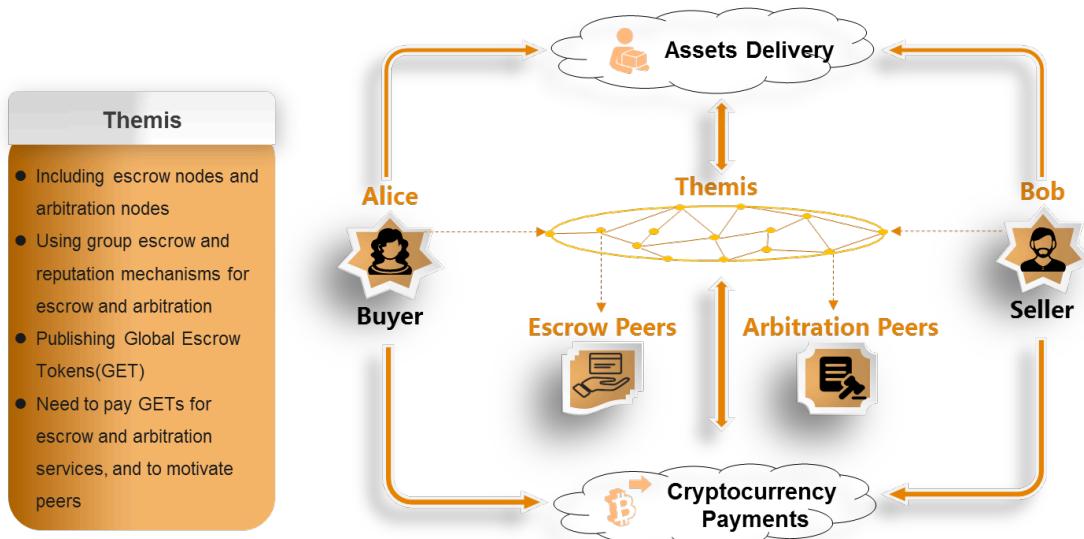


図 3.1 Themis 全体のアーキテクチャ

**DPoS コンセンサスメカニズム。** Themis は既存の委託権益証拠 (DpoS) プロトコルを改善し、新しいコンセンサス・メカニズムである DPoS (Deposit based Proof of Stake and Reputation)、即ち保証金に基づく権益と評判証明プロトコルを提出し、紛争処理に参加したノードの評判をコンセンサス・メカニズムに追加すると共に、ノードが受託者資格を競合するには、保証金を事前に支払う必要がある。ノードが信託ノードになる確率は、そのノードが支払う保証金、所有する権利と評判と密接に関連している。

**保証金メカニズム。** ノードが受託者資格を競合するには特定の金額を支払い、即ち Themis で預金を支払う必要がある。ノードが悪いことをした場合、保証金がシステムに没収される。受託者はシステム運営を維持すると報酬を受けることができ、即ち、他の受託者とブロック取引手数料を共有する。報酬によりポジティブ・フィードバックを形成し、受託

者がシステム・セキュリティの維持に取り組むことを促進する。ブロックが受託者によって順番に署名されるので、受託者はオフラインの原因でブロックの署名を逃したら、他の候補受託者によって置き換えられる可能性がある。したがって、収益を上げるためにには、受託者は十分なオンライン時間を確保する必要がある。

**マネージドノードのインセンティブメカニズム。**マネージドノードは保有する権益に応じたキーシェアを取得し、これに相当する署名シェアを計算して取引に添付し、キーシェアの割合に応じた手数料を獲得する。マネージドノードは正しいキーシェアを提供した場合、保証金に該当するシェアの取引手数料を受ける。オフラインかキーが紛失した場合、取引に参加できず、取引手数料を獲得できない。ノードが誤ったキーシェアまたは不正なキーシェアを提供した場合、マネージド身分は取り消される。要約するに、インセンティブメカニズムはマネージドノードが正しいキーシェアを提供し、オンラインを維持し、自分のキーシェアを安全に保管することを促進する。

**評判管理メカニズム。**Themis のノードは紛争解決に関与し、仲裁意見を提出する一方、他のユーザーが提出した紛争解決意見に対して匿名評価を継続的に実施する。ここでは、ユーザーのプライバシーニーズを満たすと同時に、大規模なユーザーグループで評判値をすばやく更新する実用的な匿名評判メカニズムを作成する。評判システムはユーザーに対する仲裁意見の結果について、システム内の他のユーザからのフィードバックを正確に計算し、当該ユーザの評判値を迅速に更新する。

評判値のレベルは、ユーザーが仲裁ノードになる確率に直接関係する。つまり、評判値の低いユーザーは、仲裁ノードとして選択することが難しくなる。

**一般ノードのインセンティブメカニズム。** Themis で十分な権益を持つノードのみマネージドノードとして選択され、マネージドに参加でき、マネージドノードにならない他のノードは一般ノードと呼ばれる。一般ノードはマネージドに参加できないが、保有している権益を信頼できるマネージドノードに委託できる。受託したマネージドノードは取引の確認で獲得した取引費用を委託の割合に応じて一般ノードに割り当てる。マネージドノードが処罰されると、一般ノードも対応する損失を負担する。このインセンティブ・メカニズムにより、Themis で権益の保有者は権益に関する収益を獲得することを保証し、彼らの保有している権益を信頼できるノードに委託することを促進し、Themis のセキュリティと安定性を向上できる。

### 3.2 グループマネージドプロトコル

Alice と Bob を例に取ると、取引の両当事者として共有する 2-of-2 アドレスをネゴシエーションして生成し、マネージドアカウントアドレスとする。Alice はマネージド秘密鍵  $x_A$  を生成し、Bob も相応にマネージド秘密鍵  $x_B$  を生成する。Thresh-Key-Gen プロトコル<sup>2</sup>に基づき、双方はそれ

---

<sup>2</sup> Gennaro, R., Goldfeder, S., Narayanan, A.: Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security, In: Applied Cryptography and Network Security 2016, pp.156-174.

それ  $y_A = g^{x_A}$  と  $y_B = g^{x_B}$  を用いて、マネージド公開鍵アドレス  $y = g^{x_A+x_B}$  を計算する。Alice と Bob の何れかは秘密鍵  $x_A$  と秘密鍵  $x_B$  を同時に保有すれば、マネージドアカウントのロックを解除できる。

Alice と Bob はブロックチェーンでグループマネージドを要求すると、幾つか(奇数)のマネージドノードからの応答が戻る。それから Alice や Bob はマネージドノードとやり取りを行い、それぞれ  $x_A$  と  $x_B$  のために  $n$  個の Shamir キーシェア<sup>3</sup>  $P_i$  を作成する。 $n = 2t + 1$  のマネージドノードの場合、 $t + 1$  のマネージドノードから  $x_A$  或  $x_B$  の関連するキーシェアを提供すれば、マネージド秘密鍵の  $x_A$  或  $x_B$  を効果的に回復できる。

Alice と Bob はそれぞれ各マネージドノードの公開鍵を用いて、自分のマネージド秘密鍵  $x_A$  或  $x_B$  を暗号化させ、 $c_i = E_{M_i}(P_i)$  を生成して各マネージドノードに送信し、これら暗号化したキーシェア  $\{c_1, c_2, \dots, c_n\}$  を相手に提供する。

詐欺を防止するために、上記の鍵シェアの交換プロセスでは Alice と Bob が相手に送信するキーシェアの信憑性を保証するために、検証可能な秘密共有プロトコルの Feldman VSS<sup>4</sup>やゼロ知識証明を用いて、Alice と Bob が相手に送信したキーシェアの信憑性を確保する。即ち、これらキーシェアは確かに Shamir 秘密共有プロトコルを実行して生成したマネージド秘密鍵  $x_A$  或  $x_B$  に関する秘密鍵シェアである。Alice は Bob に暗号化されたキーシェア  $c_i = E_{M_i}(P_i)$  を提供する時、同時に Feldman VSS 値  $w_i = g^{P_i}$  及びこれら 2 つの値の一致性に関するゼロ知識証明を

<sup>3</sup> Shamir A. How to share a secret. Communications of the ACM, 1979, 24(11): 612-613.

<sup>4</sup> Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: 28th Annual Symposium on Foundations of Computer Science, 1987, pp. 427-438.

提供する必要がある。これにより、Bob は受信した暗号文が $x_A$ の Shamir 秘密共有プロトコルで生成したキーシェアであることを検証できる。同様に、Alice も受信した暗号文が $x_B$ の Shamir 秘密共有プロトコルで生成したキーシェアであることを検証できる。

上記の操作が完了すると、Alice または Bob はデジタル通貨をマネージドアドレスに転送できる。紛争がなければ、支払い側は自分の秘密鍵を相手に送信し、2 つの秘密鍵を保有する側はマネージド資金を獲得することができる。

紛争が発生した場合、マネージドノードは仲裁サービスを呼び出す。仲裁の勝者は各マネージドノードに、相手から受け取った対応するキーシェアのデータを送信する。マネージドノードグループの殆どのノードが正常に動作すれば、データを受信すると、仲裁の失敗者のマネージド秘密鍵を再構築し、勝者に送信できる。これにより、勝者は 2 つのマネージド秘密鍵を持ち、マネージド資金をマネージド・アドレスから取得することができる。

### 3.3 紛争解決

紛争が発生し、即ち Alice と Bob の双方が自分の秘密鍵を相手に提供したくない場合、何れかの当事者は Themis で紛争解決を申請することができる。紛争が発生した時、Themis はマネージド時に両当事者が約束した紛争解決規則に従って仲裁手続を開始する。仲裁サービスは、紛争が発生した場合にのみ実行され、公正な取引のコストがゼロに近

いことを保証する。つまり、紛争の際にのみ仲裁手数料が支払われる。

紛争解決は2種類の方法がある。一つはスマート仲裁契約を実行することで仲裁の結果を自動的に生成する。もう一つは仲裁人が手作業で処理するもので、複数の仲裁人が投票を通じて仲裁の結果を形成する。

第1種類の紛争解決方法では、スマート仲裁契約は自動的にOracleサービスを呼び出し、外部の入力を取得し、スマート契約コードを実行し、仲裁結果を生成する。

第2種類の紛争解決方法では、評判スコアに基づくクラウドソーシング仲裁サービスを提案する。

**クラウドソーシング仲裁。** Themis の評判に基づいたクラウドソーシング仲裁サービスは、匿名仲裁人の評判を評価するメカニズムを通じて、取引の両当事者が信頼できる仲裁サービスを選択することを支援し、仲裁人もチェーンで相応の報酬を得ることができる。

また、Themis は仲裁人の評判を評価するためのオープンレビュー・システムを採用している。仲裁人の判決は匿名処理を経てから、レビューのために分散式帳簿に提出される。Themis のブロックチェーンの分散帳簿には仲裁人の取引の紛争処理に関する契約主体事項、事例、判決及び判決理由などの情報を記載しており、他のユーザーは仲裁人の判決を評価することができる。判決の好評レベルに応じて、匿名仲裁人は自分の評判値を獲得する。仲裁裁判権の乱用は直ちに仲裁人の専門的評判に反映される。評判の低いユーザーは将来の取引紛争にお

いて仲裁人になる可能性が低くなる。

**評判管理メカニズム。** Themis 評判システムは仲裁の結果について、ユーザーの ID や評判の詳細を隠しながら、他のユーザーからのフィードバックを確実に提供する同時に、評判値に対する悪意のある改ざんを防止できる。現在、一般的な評判システムは、他のユーザからのフィードバックを統計することでユーザーが情報の品質を評価するのを支援し、アルゴリズムを通じて評判値を更新することでポジティブ行動を促進する。これらの評判メカニズムではユーザーの評判を統計するが、評判地とユーザーの長期 ID と関連するため、プライバシーの重大な損失を引き起こす可能性があり、ユーザーの動作履歴が悪意的にトレーシングされるだけでなく、仲裁人の匿名性にも適合しない。我々は実用的な匿名の評判システムを構築し、大規模なユーザーべるーふで評判値を素早く更新することができる同時に、ユーザーのプライバシーを確保でき、すなわち Themis の評判はユーザーの長期 ID と関連する必要がない。

**Oracle サービス。** Oracle は仲裁サービスで取引の当事者が提供した材料を検討しレビューする時に必要なメカニズムであり、実世界におけるイベントの発生の結果に関する情報発信である。仲裁に必要なデータと資料は Oracle によって決められなければならない。これらの Oracle では一連の API を提供しており、Themis はこれらの Oracle API を呼び出すことで仲裁結果と後続の操作を決定する。Oracle はセンター化 (RealityKeys など) でも、センターレス化 (OracleChain など) でも実装で

きる。

### 3.4 ノード選択ポリシー

**受託者の選挙。** DPoS のコンセンサスメカニズムでは、競合のチャンスを掴み、受託者の資格を得るために、ノードはまず保証金を支払う必要があり、ノードが悪いことをした場合、保証金は没収される。ノードはあるノードに投票し、すなわち当該ノードを自分の受託者として選定すると、システムはノードの保有している持分の割合により、投票数の高い順に一定数量の受託者を計算する。受託者は事前に規定した順に、ブロックを生成する。

**マネージドノードの選択。** ユーザーのマネージド要求に従って、システムは一貫したハッシュアルゴリズムを使用して、マネージドノードとして奇数( $2f + 1$ )のノードを選択する。

**仲裁ノードの選択。** システムは、ノードの評判値により、重み付きランダムアルゴリズムを使用し、奇数( $2f + 1$ )個の仲裁ノードを計算する。。

### 3.5 セキュリティ設計

我々のソリューションは主に次の 3 種類の攻撃の脅威に直面している。一つはサービス拒否の攻撃であり、サードパーティはお金を盗むことができないが、任意の紛争を仲裁することを拒否することでマネージ

ドアカウントがロックされたままとなる。二つはマネージドノードと仲裁ノードの共謀攻撃であり、即ち、仲裁ノードがそれぞれ Alice と Bob に仲裁の勝者であると発信し、当事者双方がそれぞれ自分のキーをマネージドノードに渡すと、マネージドノードは 2 つのマネージド秘密鍵を回復してマネージドアカウントから資金を取ることができる。三つは DPOS の共謀攻撃であり、つまり、DPOS コンセンサスアルゴリズムのロジックに関して、参加者の共謀攻撃の脅威に直面している。

第1種類の攻撃に対して、Themis は経済学インセンティブのメカニズムを導入し、ノードのサービス拒否や共謀のコストを増加させ、マネージドノードが市場の力によって駆動され、正直かつ倫理的な行動を取るようにすることで、Themis はマネージドおよび仲裁のプロセスを客観的に完成できる。

Themis のインセンティブメカニズムはマネージドノードが効果的なサービスを提供するように設計されており、マネージドに正常に参加するすべてのノードは Themis の GET トーケンを取得しながら評判が上がる。逆に、異常なマネージドノードは評判やプラットフォームに抵当に入れた GET リスクキャピタルを失い、悪の機会費用が大幅に増加するため、ノードが自分の既存の利益と長期的な利益を破壊することでネットワーク全体を破壊することはない。これにより、Themis は悪意のあるノードからの大部分の攻撃を防止できる。

実際の応用において、マネージドノードを信頼できる委員会ノード、認定された仲介エージェントノードおよび一般ノードの 3 種類に分類す

る。委員会ノードは信頼できる機関によって維持され、常にオンラインしている信頼できるノードであり、最終仲裁結果がサービス拒否によって拒否された後でも実行されることを保証する。仲介エージェントノード自体は予めシステムに保証金を入金しておかなければならず、悪意のある行為をした場合には保証金が没収され、正常動作が抑止される。

第 2 種類の攻撃に対して、2-of-2 共有アドレスを 3-of-3 共有アドレスにアップグレードし、3 番目のマネージド秘密鍵  $x_C$  を Alice と Bob の双方当事者が共有するが、マネージドノードに開示しない。このようにして、マネージドノードが正常に攻撃を行っても、秘密鍵  $x_A$  と秘密鍵  $x_B$  のみを取得するが、マネージド資金を取ることはできない。

第 3 種類の攻撃に対して、Themis によるマネージドと仲裁を利用する人が多くなるほど、Themis で運搬される価値が多くなり、ノードが悪いことをする機会費用が高くなり、ネットワークの全体がより安全になる。更に安全になる Themis では、ますます多くの人々がマネージドと仲裁サービスを利用するようになっている。これは相乗のプロセスであり、Themis ネットワークのノード数が増え続けるにつれて、Themis はより堅牢になる。

## 3.6 典型的なワークフロー

Alice が Bitcoin を支払い、Bob からギリシャのおもちゃを購入することを例にして、Themis による公正な交換のプロセスは次のとおりである。

### マネージド前のネゴシエーション:

Alice と Bob は Bitcoin のマネージドアドレスをネゴシエートする。

Alice と Bob は Themis で事前合意された紛争解決方法(スマート契約)、手数料および仲裁報酬を含むマネージドを要求する。

Themis はマネージド・スマート契約を実行し、Alice と Bob のマネージドノードリストを戻す。

Alice と Bob はそれぞれ各受託者に秘密鍵のキーシェアを送信する。

Alice と Bob は秘密鍵のキーシェアを互いに送信する。

### 資金マネージドと商品納入:

Alice は Bitcoin をマネージドアカウントに転送する。その時点で、Alice、Bob と受託者の何れかも許可なしに資金を取ることはできない。

Bob はおもちゃを Alice に郵送し、Alice はおもちゃを受け取り、間違いことを確認し、確認の領収書を出し、Bob に対してマネージド秘密鍵を送信する。

Bob は秘密鍵を受け取り、マネージドアカウントの資金を自分の Bitcoin アドレスに転送する。

Themis のスマート契約は、受託者のマネージド手数料を計算して

割り当てる。

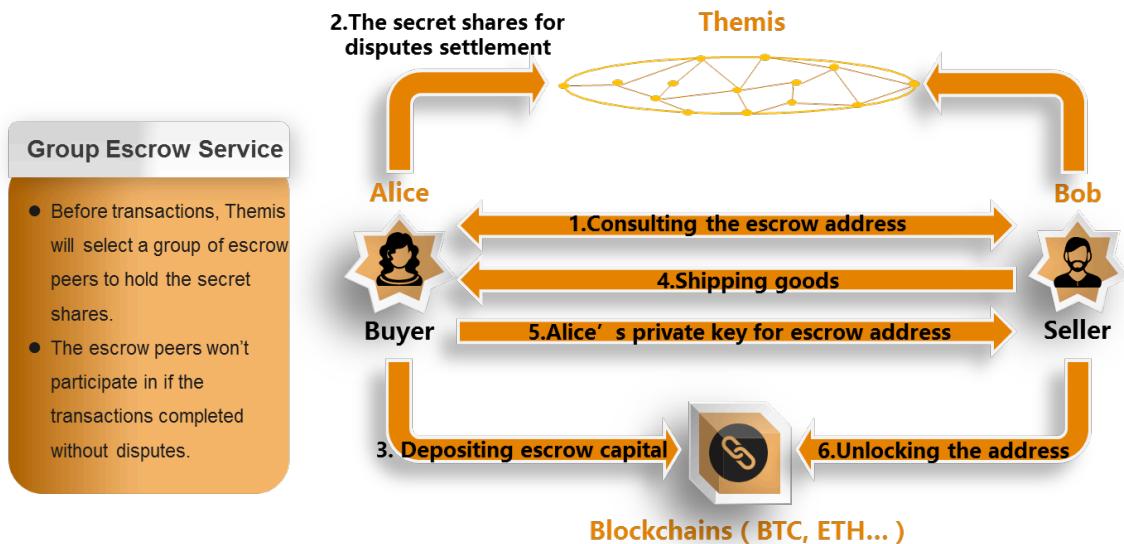


図 3.2 資金マネージドと商品納入のイメージ

### 紛争解決:

Alice と Bob は Themis で紛争仲裁を要求する。

仲裁側は合意された紛争解決方法に従って、裁決結果を形成する(Alice が勝ち、Bob が敗北すると仮定する)。

Alice は Bob から受け取った秘密鍵のキーシェアメッセージをマネージドメンバーに送信する。

受託者は Bob のマネージド秘密鍵を計算し、Alice に送信する。

2 つの秘密鍵を保有している Alice は、マネージドアカウントのロックを解除し、マネージドアカウントから自分の Bitcoin アドレスに資金を移転する。

Themis のスマート契約は、各仲裁人の仲裁報酬を計算して割り当

てる。

Themis のスマート契約は、受託者のマネージド手数料を計算して割り当てる。

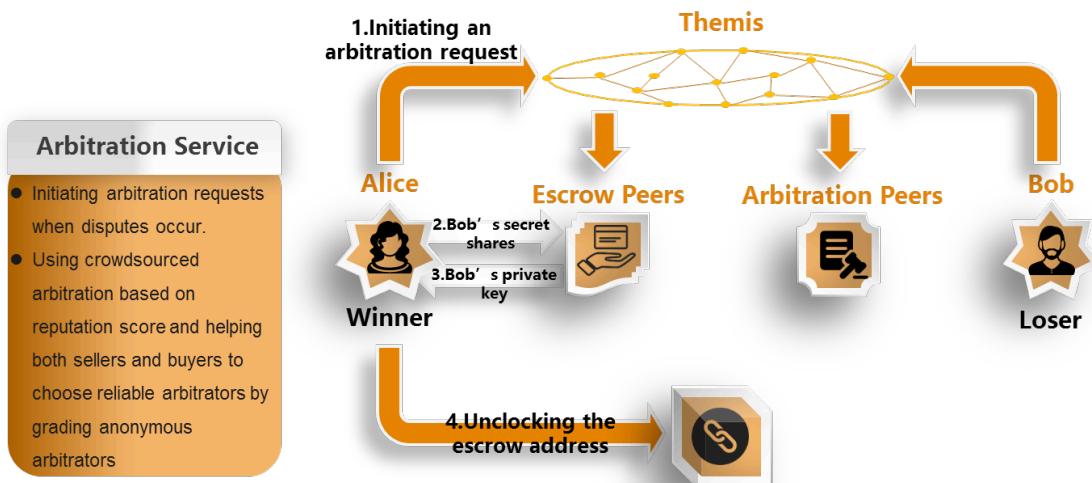


図 3.3 紛争解決のイメージ

### 3.7 Themis ウォレット

Themis は新しい暗号技術に基づく階層ウォレットすなわち Themis ウォレットを提供し、効率的かつ低成本の秘密鍵やアドレス管理をユーザーに提供し、Themis ブロックチェーンのデータとのやり取りを自動的に完成し、ユーザーが Themis ブロックチェーンを使用することに役立つ。

Themis の典型的なシナリオでは、ユーザーは他のユーザーからの支払いを頻繁に受け取る。例えば、Themis を通じて、信頼できるデジタル通貨の取引を行うオンラインストアは取引毎にユーザーからの支払

いを受け取り、プライバシーを保護するために、それぞれの取引のために異なるアドレスを生成し、これらのアドレスや対応する秘密鍵を保存して管理する必要がある。取引が頻繁に行われ、取引数が非常に多い場合、アドレスと秘密鍵の数と取引数の線形関係により、秘密鍵とアドレスを管理するために、ウォレットシステムに膨大なストレージと管理オーバーヘッドをもたらす。

通常、ウォレットが新しいアドレスを生成するたびに、対応する秘密鍵を秘密鍵格納領域に保存する必要があり、秘密鍵格納領域にアクセスするとセキュリティ上のリスクが大きくなる。秘密鍵記憶領域への頻繁なアクセスを回避するために、現在のウォレットは殆どアドレスを一括生成するポリシーを採用する。即ち、複数のアドレスと対応する秘密鍵を一回的に生成し、これらの秘密鍵を秘密鍵記憶領域に一回的に保存することで、秘密鍵記憶領域へアクセス頻度を減らす。たとえば、Bitcoin Wallet はデフォルトで 100 個の秘密鍵と対応するアドレスを生成する。ユーザーは秘密鍵をオフラインストレージ(フラッシュドライブ、専用ハードウェアデバイス、または紙に印刷するなど)に保存できる。一括生成したアドレスは Wallet のクライアントにオンラインで保存される。これらのアドレスが使い尽くされると、ウォレットは秘密鍵とアドレスを改めて一括生成し、秘密鍵を保存するためにオフラインストレージにアクセスする。この方式では、ある程度秘密鍵の記憶領域へのアクセス頻度は低下するが、秘密鍵の記憶領域に定期的にアクセスする必要があ

り、アドレスと秘密鍵の記憶と管理のオーバーヘッドを削減していない。秘密鍵の記憶領域へのアクセス数と記憶オーバーヘッドは取引数と線形関係がある。

Themis ウォレットは新しい暗号技術に基づく階層ウォレットであり、改善ポイントは次の通り。

1. Themis ブロックチェーンの API に対応し、Themis ブロックチェーンのデータとのやり取りを自動的に完成し、ユーザーが Themis ブロックチェーン機能を使用してマネージドタスクを迅速に完成することに役立つ。

2. ユーザーのために任意数のアドレスを生成でき、ユーザーの秘密鍵のオフライン記憶は 1 つの秘密鍵のスペースだけを必要とする。ユーザーは既存の秘密鍵のオフラインストレージ方式を簡単に利用でき、例えば紙ウォレット(秘密鍵を二次元コードの形式で用紙に印刷する)を利用し、又は秘密鍵をハードウェア USB Key に格納する(暗号学において通貨の秘密鍵は通常、標準的な楕円曲線暗号の秘密鍵であるため、この方式のマスターキーを楕円曲線暗号の秘密鍵の記憶に対応する全ての暗号装置に記憶できる)。

3. ユーザは支払いを受け取る過程で、秘密鍵記憶領域にアクセスする必要はない。つまり、この方式のマスターキーを完全にオフラインで保存できる。

4. ユーザーの公開鍵ファクタマトリックスの記憶空間は固定の常数であり、この記憶数はアドレス数の成長に従って増加しない。

5. ユーザーのアドレス管理は更に簡単になる。ユーザー住所は支払に関連する情報によって生成され、この情報を保存する必要はない。



## 四、キーテクノロジー

### 4.1 グループマネージドに基づく公正な交換プロトコル

公正な交換とは信頼のない複数の当事者間で、事前の約束に従つて資産の取引を完成するためのプロトコルである。公正な交換は公平な両当事者間のコンピューティングの特別なケースであり、相互信頼関係のない両当事者が互いに協力してデジタル商品を交換することを検討し、両当事者は相手の商品を得るか、何も獲得できない（All-or-nothing）。

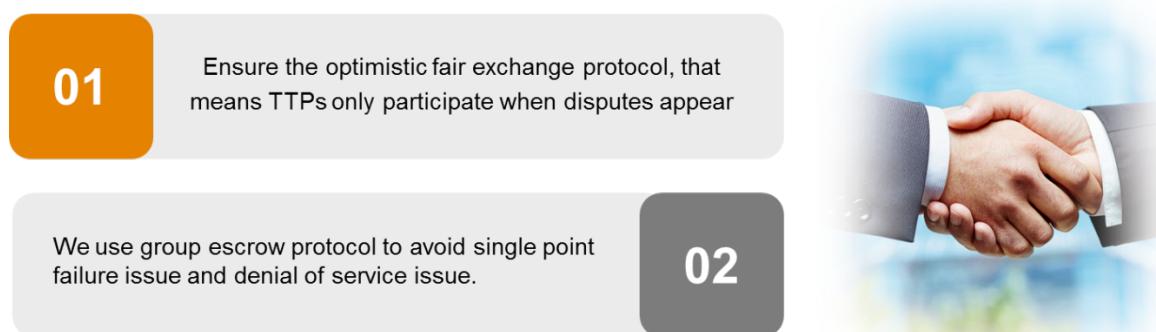


図 4.1 資金マネージドと商品納入のイメージ

公正な交換の非公式な記述は次のとおり。

プロトコルの参加者 A と B があり、それぞれ交換を希望する電子アイテム  $i_x$  及びその記述  $d_x$  を保有すると仮定する。ここで  $X=A$  または  $X=B$  とする。

検証可能な関数  $f(*)$  があり、 $d_x=f(i_x)$  プロトコルには成功と中止の

2つの終了状態を具備させ、参加者の両者は自分の終了状態を判定で  
きると仮定する。

非同期ネットワーク環境では誠実エンティティ A (B が誠実であるか  
否かを判断することはできない) にとっては、所望の電子アイテム  $i_B$  が  
受信されたことを確認した後、自分の電子アイテム  $i_A$  を支払うことを望  
む。逆に、誠実なエンティティ B にとっても同様である。これにより相容  
れない葛藤が発生する。A、B の何れかも自分の電子アイテムを先に支  
払うことを望まず、最終的には希望の電子アイテムを手に入れることができ  
ない。この矛盾に対処するには、効果的なソリューションは両当事  
者が自分のアイテムを信頼できるサードパーティエンティティ (TTP) に  
渡し、TTP を通じてトランジットするか、紛争の時に TTP によって裁決を  
行う。

Themis の設計は主に 2 つの問題を解決する。

第一、トランジットモードすなわち In-line TTP または On-line TTP  
モードでは、多くの TTP の参加を必要とするため、TTP の性能とセキュ  
リティが広く疑問視されている。これに対して、Themis は楽観的公正な  
交換プロトコルを提供し、TTP は紛争の際にのみ関与する。

第二、TTP の単一障害点やサービス拒否攻撃の可能性を考慮し、  
グループマネージドに基づく安全な交換プロトコルを提案し、上記のセ  
キュリティ脅威を効果的に緩和できる。

## 4.2 検証可能なシャッフルと関連リング署名に基づく匿名評判メカニズム

既存のブロックチェーンで使用されるインセンティブメカニズムは匿名を保証できず、観察者はユーザーの身元と投票の関係を調べることができる。また、デジタルトークンに基づく奨励メカニズムはユーザーに通貨を増やすことができるが、悪いことをしてもユーザの通貨を減らすことはできない。即ち、デジタルトークンの暗号学メカニズムにより、ユーザから金銭を取ることが自然に制限されるので、処罰の目的を達成することができない。これらの問題に対処するために、検証可能なシャッフルと関連リング署名に基づく Themis の評判メカニズムは、ユーザーID を明らかにせずに匿名の評判計算を実行できるようになり、賞罰付きのインセンティブを実現できる。

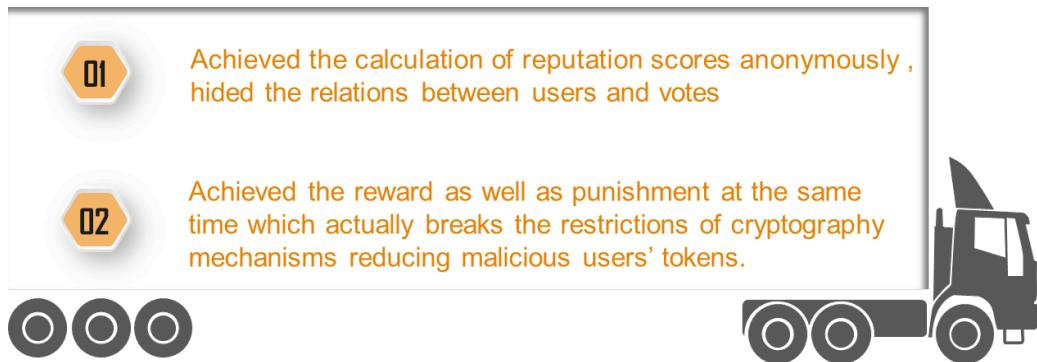


図 4.2 検証可能なシャッフルと関連リング署名に基づく匿名評判メカニズム

Themis 評判システムの作業メカニズムは、複数サイクルのメッセージ送信とフィードバックで構成されている。それぞれのサイクルの最初に、サーバーはすべてのクライアントの長期データベース ID とそれぞれの暗号化評判スコアをメンテナンスする。各サイクルでは、サーバは検

証可能なシャッフルプロトコルのスケジューリングアルゴリズムを実行し、評判リストを一度限り仮名の匿名リストと対応の平文の評判スコアに変換する。センターレスのスケジューリングプロトコルを使用し、サーバーとクライアント(所有者を除く)は、一度限りの仮名と長期 ID を関連付けることができない。クライアントは一度限りの仮名を使用してメッセージを匿名で投稿する。サーバーはクライアントの機密情報を知らなくても、これらのメッセージを対応する評判スコアと関連付けることができる。各クライアントは他のユーザの投稿されたメッセージにフィードバック(例えば投票)を提供する。各投票は関連リング署名を使用して署名され、サーバはどの顧客がどれに投票したことを明らかにせずにそれぞれの顧客が一度投票したことを確認できる。この設計により、サーバーは投票を正と負の投票をカウントする際に長期 ID と関連付けることができない。最後に、サーバーは一度限りの仮名によるフィードバックをもって評判スコアを更新する。その後、「逆スケジューリング」を実行し、これら一度限りの仮名や更新した評判を元の長期 ID や更新後の暗号化評判スコアに回復する。

### 4.3 非対話型ゼロ知識証明

ゼロ知識証明システム(Zero Knowledge Proof Systems)は 1983 年に登場してから、理論計算機と暗号化に大きな影響を与えてきた双方向(証明者と認証者)の暗号プロトコルである。

ゼロ知識証明プロトコルを実行することで、アサーションが真であるとき、証明者が検証者に対して証明を提出し、検証者がアサーションの信憑性(完全性:Completeness)ことを迅速に確認することができる。また、検証者は当該アサーションの信憑性を除き、何れの知識を獲得できない(ゼロ知識:Zero Knowledge)。アサーションが偽であるとき、無限の計算能力を有している証明者であっても、無視できない確率で検証者に騙して当該偽のアサーションを受入れさせることができない(合理性:Soundness)。アサーションについて、証明者には特定の秘密知識を具備するとき、ゼロ知識証明システムはゼロ知識の知識証明システム(Zero Knowledge Proof of Knowledge)に特化し、証明者は検証者に証明を提出し、検証者に証明者が主張した秘密情報を保有することを確認させ、証明の過程で秘密情報に関する知識を漏らさない。証明者と検証者との間のやり取りを必要するかにより、ゼロ知識証明システムは更に対話型ゼロ知識証明システムと非対話型ゼロ知識証明システムに分けられる。非対話型ゼロ知識証明システムは通信の要求が一番低く、更に実用的である。

我々は以下の 3 つの問題を解決するためにゼロ知識証明を使用する。第一、グループマネージドサービスプロトコルでは、ゼロ知識証明を利用し、各取引当事者からマネージドノードに提供されるキーシェアデータが真であることを保証する。第二、検証可能シャッフルプロトコルでは、シャッフル動作を実行することに加えて、各シャッフルサーバがゼロ知識証明を生成し、何れの観察者または検証者もこれを用いてシャッフ

リングサーバがそのランダム動作を正しく実行したかどうかを検査することができる。第三、評判システムではクライアントがメッセージを投稿する時に自分の評判予算のゼロ知識証明を生成し、1) 実際の評判スコアが予算値  $b$  以上であること、2)  $b$  を評判スコアとしてこのメッセージを投稿したいと主張する。

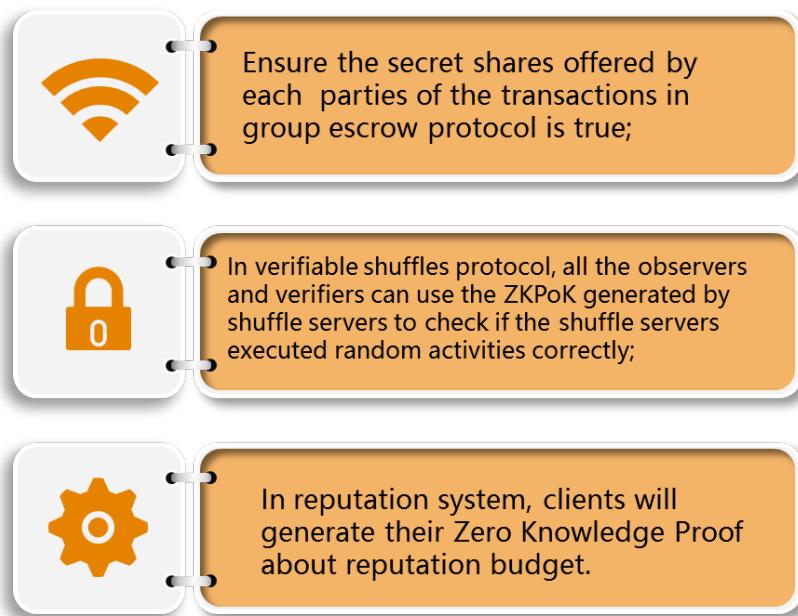


図 4.3 非対話型ゼロ知識証明

#### 4.4 高並行性の同時検証に対応するデジタル署名アルゴリズム

取引メッセージのデジタル署名を確認するための検証計算は、パブリック・ブロックチェーンの取引処理能力を制限する要因である。現在のブロックのチェーンでは一般的に 256 ビットプライムドメイン楕円曲線の署名アルゴリズムを使用しており、高い安全性を有するが、検証の効率

が高くない。現在主流のプロセッサの検証回数は毎秒百万回未満であり、ネットワークで多数の取引メッセージが発生すると、メッセージの検証によるノードの遅延が高い。現在、一部のアライアンスチェーンやプライベートチェーンはトラステッド・コンピューティング環境を導入することにより、この技術的な課題を避ける傾向にあるが、同時に更なる複雑なセキュリティ要因を導入するため、パブリックチェーンのセキュリティニーズをサポートすることが難しい。

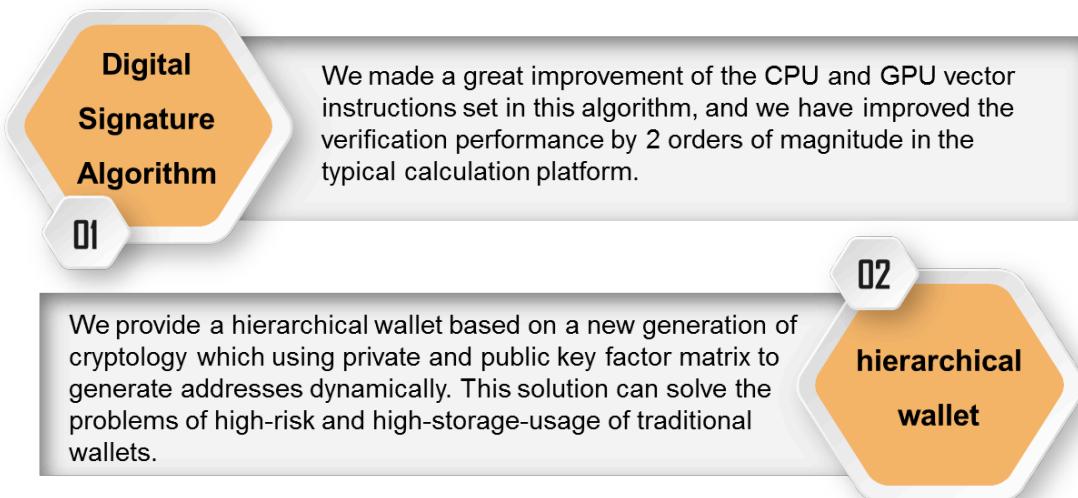


図 4.4 ブロックチェーン向けの新しい暗号アルゴリズム

Themis プロジェクトは高並行性の同時検証に対応する新しいデジタル署名アルゴリズムを導入することによって、この重要な技術用件を満たした。システムは多種類のオプションのデジタル署名方式をサポートし、ユーザーとアプリケーションの要求に応じた適切な署名アルゴリズムを選択することができる。署名用秘密鍵を一度だけ使用するシナリオでは、ハッシュに基づく検証性の高い使い捨て署名アルゴリズムを選択する。典型的なシナリオにおいて、256 ビットのセキュリティレベルを確

保した上、特別な特性を有する橙円曲線や検証アルゴリズムを選択することで、検証ノードは曲線パラメータ及びアルゴリズムの特長を利用し、時間と空間の最適化された技術を用いて、一括検証のコンピューティング効率を大幅に最適化する。アルゴリズムの実装では、特に GPU と CPU ベクトルコマンドセットを最適化し、プロセッサの各トランジスタのコンピューティング力を最大限に活用する。総合的な最適化を通じて、典型的なコンピューティングプラットフォームでは検証性能の約 2 枠オーダーの上昇を達成する。

## 五、シナリオ

Themis はブロックチェーンに基づく公正な交換システムを構築し、センターレス化デジタル通貨マネージドサービスを提供し、デジタル通貨、デジタル資産、物品の間の公正な交換などデジタル通貨による公正な交換の問題を解決できる。Themis はピアツーピアのマネージド支払い、デジタル通貨取引、マネージドアカウントのセキュリティマネージド、マルチエージェント取引の資産マネージドなど多くのシナリオで使用できる。

### 5.1 ピアツーピアのマネージド支払い

Themis は P2P オンライン市場(例えば OpenBazaar)のためにセンターレス化のデジタル通貨のマネージド支払いを提供し、買手と売り手の直接取引きを実現できる。Themis は電子ビジネスプラットフォームのデジタル通貨決済システムに接続し、Themis を通じて、元のチェーンで対応するマネージドアカウントを生成し、デジタル通貨の取引に対してセンターレス化マネージドを行う。取引では、買手が支払われるデジタル通貨を当該マネージドアカウントにマネージドし、実物商品の納入状況に応じて、正式に納入を確認した後、売り手に確認命令を出すと、売り手はマネージドアカウントからデジタル通貨を得ることができる。このよ

うなメカニズムにより、デジタル通貨の支払いと実物商品の納入を同時に完成できない課題を効果的に解決できる。

実際の電子商取引では、Themis プラットフォームは買手に前払いの保障を提供する。例えば、納入を確認してから 7 日以内に、売り手の資金の 5%を保証金としてスマート契約でプラットフォームアカウントに残す。7 日以内に紛争が発生した場合、Themis は保証金プールのお金を使って買手に前払い、その後売り手と払い戻しをネゴシエートする。これにより、売り手の信頼を高めながら、買手の満足度をさらに高めることができる。



図 5.1 ピアツーピアのマネージド支払い

## 5.2 デジタル通貨取引

Themis はブロックチェーンに基づく公正な交換システムであり、デジタル通貨と物品の公正な交換の要求を満たすだけでなく、異なるデジタル通貨間の貿易取引の需要を満たし、あらゆる種類のセンター化又はセンターレス化のデジタル通貨取引のために、公正な交換の保障を提

供する。

Themis は、デジタル通貨での店頭取引をサポートし、Bitcoin、エーテル及びその他のブロックチェーンベースの暗号化デジタル通貨での店頭取引に安全なマネージドサービスを提供し、元のチェーンで相応のマネージドアカウントを生成し、異なるデジタル通貨間の為替取引のニーズを満たし、デジタル通貨のクロスボーダー取引のために公正を確保する。

Themis supports OTC transactions of digital currencies, and it can provide secure escrow service for cryptographic digital currencies based on blockchain



図 5.2 デジタル通貨取引

### 5.3 マネージドアカウントのセキュリティマネージド

ブローカーがアカウントを開設した後に、銀行アカウントを開設することや、P2P ネットローンがマネージドアカウントを開設することなどのように、マネージドサービスは、従来の金融でユーザー資金の安全を守る

重要な手段である。プライベート・エクイティ・ファンド、クラウドファンディング・ファンド、最近に出現した ICO 投資ファンドなどについては、資金のマネージドがなく、サードパーティのセンター化マネージドメカニズムを採用するため、マネージド資金の投資対象、投資比率、投資収益率が不透明になり、情報の歪みや論理的なリスクがある。

Themis はスケーラビリティの高いスマート契約のクラスタとして、分散帳簿のインターフェースを提供し、デジタル通貨資金のマネージドサービスを提供することで、投資資金の安全性、プロジェクトのトレーサビリティ、投資利益分配の合理化などを効果的に確保できる。デジタル経済の盛んな発展に伴い、デジタル通貨の貸出、デジタル通貨の先物オプション、デジタル通貨 ETF、クロスリンク型デジタル通貨取引など、将来に多くのデジタル通貨の金融商品とシナリオを派生する。資金の安全を守るために、これらはすべて Themis システムによってマネージドされることができる。

Themis can provide decentralized escrow service for cryptocurrency funds regulatory accounts, such as lenders of digital currencies

Futures of digital currencies, ETF funds of digital currencies, cross-chain transactions of digital currencies and so on, and all of these can be managed by themis system to keep security



図 5.3 マネージドアカウントのセキュリティマネージド

## 5.4 マルチエージェント取引の資産マネージド

サプライチェーンファイナンス、不動産、大型機器などの取引では、取引の主体が多く、取引のプロセスが長く、取引の依存関係が強いため、論理的リスクや主体の不誠実な問題につながる可能性がある。

Themis はマルチエージェントの責任と権益のトリガーに基づくスマート契約を作成することで、デポ、初回支払い、手数料支払い、残高支払いなどマルチエージェント取引でマネージドを必要とする資金を、元のチェーンでマネージドする。取引が相応の段階に進むと、対応の取引エンティティは適切な命令を入力することで当該スマート契約をトリガし、公正な取引や権益の割り当てを実現する。取引の一方当事者が取引に関して紛争を起こした場合、Themis のグループマネージドサービスプロトコルや公正な仲裁メカニズムを利用して仲裁を要求し、グループマネージド側のめ一バーは紛争に対して仲裁、投票を行い、裁決結果を形成する。勝者はマネージドアカウントのロックを解除できる。

## 六、チームの紹介

### 6.1 コアチーム

#### Danish A.Alvi

##### ■ Themis 製品とアーキテクチャ全体の設計を担当

Danish は UCL ロンドン大学ブロックチェーン技術センター (CBT) の開発者であり、ERC223 プロトコルを使用して Overled プロジェクト ICO 用のスマート合同を作成した。Hadoop と Weka を使用するオンラインのビッグデータ検索とストレージサービスを促進し、開発環境向けの仮想マシンの自動プロビジョニング、フロントエンドサービスの仮想マシンの自動プロビジョニング、フロントエンドサービスと CKAN / Drupal の統合やデータ監査を支援した。情報技術サービス会社の Atos で最先端の研究プロジェクトを行っている。また、UCLU TechSoc でコーディネータとして役割を果たし、また顔認証システムの使用を促進し、大学のアクセスセキュリティの簡略化や強化に取り組んでいる。



#### Jennifer Chung

##### ■ Themis のビジネス展開と戦略計画を担当

Jennifer は Agility Sciences Limited の最高マーケテ



イング責任者であり、Blockchain Association の共同設立者である。彼女はロンドンビジネススクールから商業学士号を取得しており、卒業後には分散技術による潜在的な業界革命に取り組んでいる。ボストン・コンサルティング、プライベート・エクイティおよびベンチャーキャピタル・ファンドで働いた経験がある。

## Yuet Ning Chau

### ■ Themis の財務分析を担当

Yuet は、英国の PwC および Capital Markets チームの一員であり、伝統的な金融サービスに関する高い知識と経験を持ち、プロジェクトデューデリジェンスと M&A に携わっている。革命的な金融技術に取組み、金融技術ベンチャーキャピタル会社での仕事から始まった。市政府に対して中国のレベル 2・3 の都市における「特色の町」や、電子都市技術のインフラでの潜在的な利用を提案した。Yuet はまた、暗号通貨の研究に深く関わり、複数のプロジェクトで ICO に助言を行っている。CUKBA の共同設立者として、英国の金融技術企業家と密接に関連している。Yuet は、商業の修士号でロンドン経済学院を卒業した。



## James Johnson

### ■ Themis のビジネス分析

James は、ロンドン大学ロイヤルホロウェイで、アプリケ



ーションコミュニティの共同設立者で共同議長を務め、最高技術責任者(CTO)であり、UNIcoin の共同設立者でもありました。また、フリーランスの Web 開発者やシステム管理者としても働いています。シスコシステムズのテクニカルセールスエンジニアで、クライアントマネージャにビジネススマネージャと製品トピックのアドバイスを提供しました。

## Takuya Koide



### ■ Themis の運営と展開を担当

Takuya は英國ロンドン大学 Royal Holloway を卒業し、現在は Unicoin の成長ハッカーを担当し、マーケティング、エンジニアリングリサーチ、データ分析に豊富な経験を持っている。SEM のプロモーション、コンテンツマーケティング、プログラム・テスト、数学的なモデリングと他のスキルを身につけ、複数のブロックチェーンプロジェクトの開発や展開に参加し、ブロックチェーンと金融革新分野での複合的な人材である。

## Hubertas Trinkunas



### ■ Themis の通貨エコデザイン

Hubertas 氏はロンドン大学ロイヤルホロウェイで財務管理を専攻し、Royal Holloway Investment and Finance Society の副社長で、同社のコーポレートファイナンスマネージャーを務めています。彼は多言語コミュニケータであり、現在は UNIcoin の最高財務責任者を務

めています。UNIcoinは、学生共有経済学に焦点を当てたテクノロジーベンチャーであり、ブロックチェーン技術とデジタル通貨を対象とした研究が行われています。

### Amiri Marat

#### ■ Themis コミュニティ構築とアルゴリズム研究を担当

Amiriは、英国ロンドン大学 Royal Hollowayを卒業し、ブ



ロックチェーン技術と金融技術の長年の実務経験を持ち、暗号とブロックチェーンに関する深い知識を持ち、複数のオープンソースコミュニティで活動しており、公開鍵暗号学とコンセンサスアルゴリズムの研究と実装、市場調査やビジネスケースの開発には豊富な経験がある。彼は優れたコミュニケーション能力を持ち、3つの言語（ロシア語、英語、カザフ語）をマスターし、中国語も学んでいる。

## 6.2 コンサルタントチーム

### Donald Lawrence

- ロンドン大学ユニバーシティカレッジ客員教授
- 戦略コンサルティング会社、Genesis のパートナー



ロンドン大学の教授、ブロックチェーン技術センターのプロジェクト担当者、金融コンピューティング研究センタープロジェクトの担当者、アランチューリンデータ研究センタープロジェクトの担当者であり、シティグループ、Bank of America、American Express などでジェネラルマネージャー及びそれ以上の管理職を担当したことがあり、UCL にいた間、中央銀行、投資銀行、ヘッジファンド、清算センター、テクノロジー企業のプロジェクト研究と開発に関わっていた。

### Daniele Bernardi

- Diaman SCF 創業者兼最高経営責任者

### INVESTORS' Magazine Italia 会長

Diaman SCF の創設者兼 CEO であり、Investors Magazine Italia の会長である Daniele Bernardi は、高収益投資戦略の開発にコミットし、イノベーションを絶え間なく探求する企業家である。彼の研究は数学モデルの開発に向け、投資家や家族企業の意思決定プロセスを簡素化させ、リスクを軽減する。



## Robert Ferguson

### ■ ベインアドバイザー/Bee-One セールスディレクター

Bee-One の英国販売担当ディレクターである Robert

Ferguson は、小売および消費者製品の販売で豊富な経



験を持っている。ベインカンパニーの顧問であり、カテゴリー管理、ビジネス上の利点、購買戦略、製造ネットワーク最適化などのプロジェクトの分析と意思決定者の管理を担当している。Robert は意思決定を促進するためのセミナー設計や案内など、プロジェクト管理に豊富な経験を持っている。また、新しい世代のデジタル変換を開発した経験もある。インド、香港、中国でのプロジェクトを通じて、彼は新興市場でのチャンスとチャレンジを見つけることに全力で取り組んでいる。

## 陳鐘

### ■ 北京大学教授

陳教授は、北京大学ソフトウェア・マイクロエレクトロニ



クス学部学長、北京大学金融情報研究センター所長、北京大学ネットワーク・情報セキュリティ研究所所長を務めた。CCF の執行取締役、CCF 情報セキュリティ委員会の副ディレクター、CCF ネットワークとデータ通信特別委員会の委員である。

## 6.3 パートナー

1. 深セン市和信中欧金融技術研究院(<https://chieftin.org/>)。同研究院は深セン羅湖区政府の支援を受けて設立され、オックスフォード

大学コンピュータサイエンス学科の元理学部教授である Bill Roscoe 教授がリーダーとなり、ブロックチェーン、ビッグデータ、人工知能などの金融技術分野の研究開発と応用開発に力を入れている。フォーマル検証技術は世界でもトップクラスの地位を占めている。関連する研究プロジェクトと方向性は全て、深セン市政府が孵化している研究プロジェクトと産業化の方向性と一致している。Themis は研究院と協力して、スマート契約のセキュリティ問題に取り組み、フォーマル検証技術を使用して、システム内のスマート契約、特にマネージドプロトコルや仲裁プロトコルを検証する。

2. oraclechain (<http://oraclechain.io/>)。Oracle は仲裁サービスにおいて取引の両当事者が提供した資料を検討し、レビューするメカニズムである。Oracle Chains はブロックチェーン内で実世界のデータの Oracle サービスを提供し、そのエコシステムは一連のサービスと API を提供する。Themis はこれらのサービスと API を呼び出すことで、実世界のデータをブロックチェーンに導入し、仲裁の結果やその後の動作を決める。