THEMIS

数字资产托管公链

去中心化“支付宝”

2018/03 v3

https://themis.network

目录

一、 概述

以区块链为基础的数字货币蓬勃发展，正在成为人类新的货币形式，越来越深入地参与到商业活动中来。各类数字货币交易所应运而生，交易规模迅速增长。同时，随着数字货币应用范围的不断扩大，越来越多的国家和地区（如日本等国）的许多商家都接收数字货币作为付款方式。可以预见，在全球范围内使用数字货币购买实物商品有着广阔的市场。

图 1.1　数字货币发展趋势

目前，数字货币交易所和点对点交易服务提供者大都聚焦在保证交易的安全性，对交易的公平性关注不多。例如，在被广泛使用的哈希时间锁合约（Hashed Time-lock Contract，HTLC）技术中，退款时间锁有可能被攻击者利用，发起拒绝服务攻击，导致交易对手方无法在限定的退款时间内完成交换。

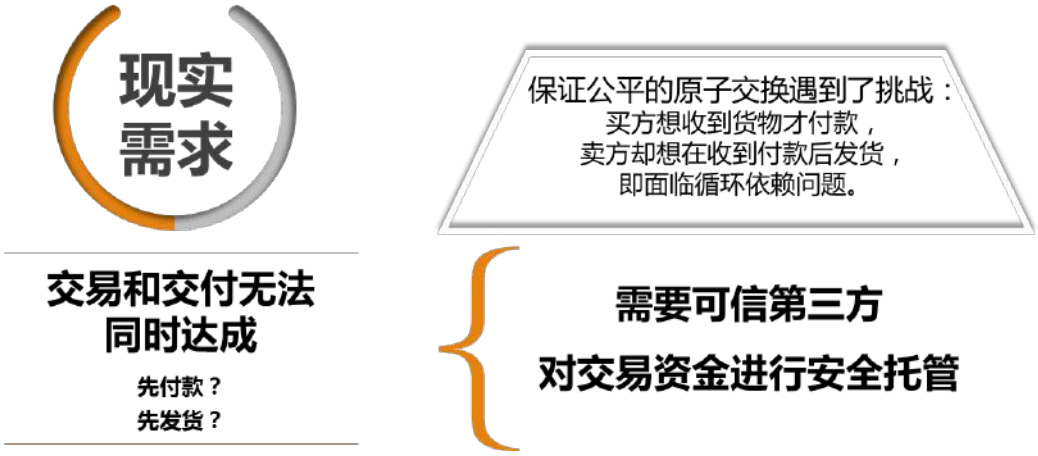

图 1.2　需求分析

与此同时，在数字货币与实物商品交换过程中，买方想收到货物再付款，卖方却想在收到付款后发货，使得交易和交付无法同时达成，难以保证公平的原子交换。通常的解决方案是依托可信赖的第三方，然而，因为存在单点失效问题，依赖单个第三方的解决方案并非安全可靠，历史上的比特币交易所和在线市场都有过遭受黑客攻击（例如 Mt. Gox、Coincheck）的情况。

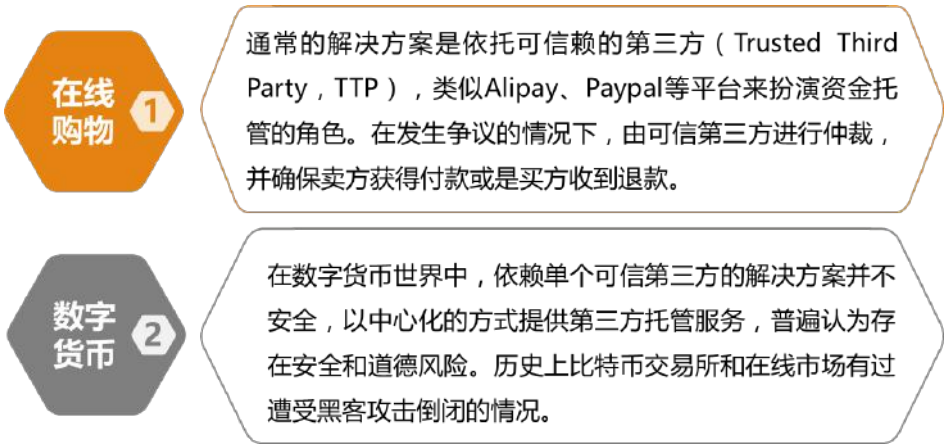

图 1.3　现实情况

过去对传统公平交换协议的大量研究都在努力试图削弱公平交换对可信第三方的依赖。区块链的出现让公平交换协议焕发了新的生机。我们利用区块链技术构建了一个以数字货币为媒介的公平交换系统 **Themis**[1]，提供去中心化的数字货币托管服务，解决以数字货币为媒介的公平交换问题，例如数字货币、数字资产和实物商品之间的公平交换问题。

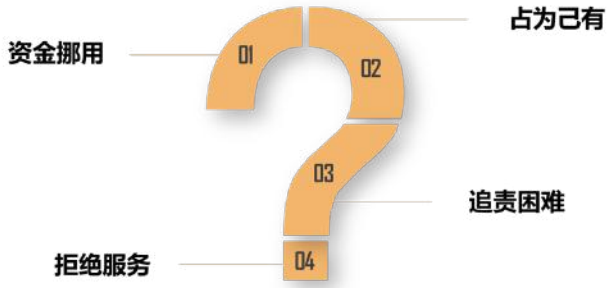

图 1.4　面临问题

Themis 基于经济学激励的群托管机制，使用了门限密码、匿名声誉机制、非交互式零知识证明以及高并发数字签名算法等关键技术，能在群成员中恶意成员的数量小于一半的情况下保证公平交换，并具备安全、隐私、去中心化和抵御拒绝服务攻击等特性。Themis 能够为比特币、以太币以及其它基于区块链的密码学数字货币提供安全托管服务。

[1] Themis（忒弥斯）是宙斯最尊重最信任的妻子。作为法律和正义的女神，是秩序的创造者、守护者。

二、 以数字货币为媒介的公平交换

公平交换是指保证互不信任的多个主体之间按照事先约定完成资产互换的协议。以数字货币为媒介的交换，是指作为交换主体的某一方以数字货币作为交换对象的情况，例如不同类别数字货币之间的交换，或者数字货币与实物商品的交换。以上都需要公平交换协议提供安全保障。

2.1 不同类别数字货币互换

实现不同类别数字货币之间的互换，首先出现的是交易所模式。交易所通过建立内部账户完成用户之间不同数字货币的交换，即 IOU（I Owe You）账户模式。在交易所模式下高频交易容易达成，但被普遍认为存在以下缺陷：安全性风险，用户资产由交易所托管，存在黑客攻击和道德风险；流动性不足，交易所形成孤岛，用户资产只能在交易所内流动；兑付性时延，交易结果没有实时在区块链上提交，不能马上兑现。

为了克服中心化交易所的缺陷，人们提出了去中心化交易所模式。这种模式大多基于多重签名方案或哈希时间锁合约（HTLC）方案来保证原子交易。但是，多重签名方案依赖可信第三方，存在共谋攻击或拒绝服务攻击风险；HTLC 方案中的退款时间锁有可能被攻击者利用，发起拒绝服务攻击，导致交易对手方无法在限定退款时间内完成交换。

2.2 数字货币与现实商品互换

现有的中心化交易所和去中心化交易所致力于数字货币之间的交换，不能满足数字货币与实物商品的公平交换的需求。这是因为在数字货币与实物商品交换过程中，交易和交付无法同时达成，保证公平的原子交换遇到了挑战：买方想收到货物才付款，卖方却想在收到付款后发货，即面临循环依赖问题。因此，需要借助可信第三方进行资金托管和仲裁，在交易达成后、交付确认前，对买家的交易资金进行安全托管，从而满足公平性的要求。

一种常见的托管支付方式是使用 2-of-3 多重签名交易，买方、卖方和可信第三方各拥有一个密钥。买方先把一笔数字货币支付到一个多重签名的托管地址，任何一方需要提供这三方中任意两方的密钥生成数字签名，才可以花掉这笔钱。如果交易顺利进行，买方把密钥发给卖方，卖方可以拿到托管的钱。如果出现争议，可信第三方进行仲裁，并向争议获胜者发送密钥以完成付款（或退款）。

这个托管协议有两个优点。一是如果没有争议，买卖双方可以在不涉及第三方的情况下进行结算；二是第三方不能拿走托管的资金，因为第三方只有一个密钥，而取得托管资金必须至少两个密钥。

但这个方式同时存在严重问题：首先，共谋问题。除非托管协议经过精心设计，否则托管方能轻易连接到特定的买方或卖方进而实施共谋。其次，拒绝服务问题。即使第三方不能窃取钱，也可以拒绝调解任何争议，从而保持资金锁定。

2.3 Themis 的设计目标

Themis 是一个去中心化的公平交换系统，类似数字货币世界的支付宝，解决以数字货币为媒介的公平交换问题。在技术上，Themis 应能满足如下要求：

公平性：在交换结束后，要么交换双方都能够得到想要的标的物（如数字货币、数字资产、实物商品），要么都得不到（All-or-nothing）；

安全性：数字货币在交换过程中不能被任何人擅自拿走；

被动性：如果没有争议，无需第三方参与；

正确性：确保交易和争议解决按照事先约定的规则执行；

可靠性：出现争议后避免托管方不执行仲裁决议而导致资金锁定的问题，即避免单点故障和拒绝服务；

隐私性：在没有出现争议的情况下，第三方不能获知交易是否完成，非交易相关方无法获知是否出现争议。

图 2.1　Themis 设计目标

三、 Themis 总体架构

3.1 Themis 区块链

Themis 提供第三方托管服务（类似现在支付宝在网上购物的作用），在链上发行代币 Global Escrow Token（GET），引入基于经济学激励的群托管机制和声誉机制来激励区块链节点，利用托管合约和仲裁合约，实现数字货币之间、数字货币与现实资产之间的点对点公平交换。通过发放托管手续费和仲裁服务费的方式，为积极参与资金托管和争议仲裁的节点提供激励。用户在使用数字货币支付过程中，需要支付 GET 代币来获得托管和仲裁服务。参与托管和仲裁节点，在交易完成后，可以获得来自交易方的 GET 代币手续费和奖励，以实现 GET 代币在 Themis 上的闭环流动。

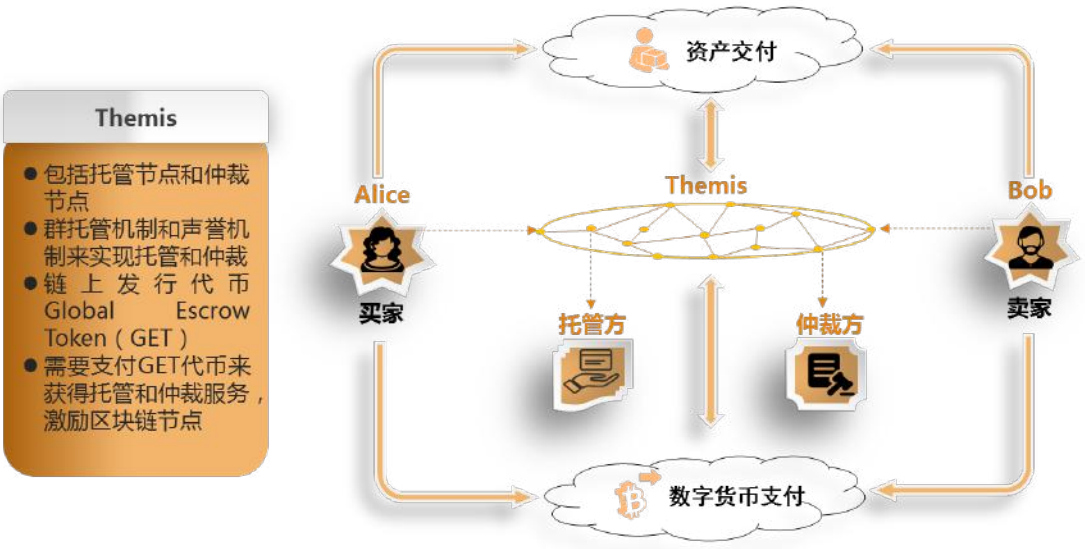

图 3.1　Themis 总体架构

DPoSR 共识机制。Themis 将改进现有的委托权益证明(DPoS)协议，提出新型共识机制 DPoSR(Deposit based Proof of Stake and Reputation)，即基于保证金的权益和声誉证明协议，将节点参与争议处理的声誉加入到共识机制中，同时节点竞争受托人资格需要先付出一笔保证金。节点成为受托节点的几率与其缴纳的保证金及拥有的权益和声誉密切相关。

保证金机制。节点竞争受托人资格需要先付出一定代价，即在 Themis 上缴纳一笔保证金。如果节点作恶，保证金将被系统没收。受托人维护系统运行将获得报酬，即与其他受托人共享区块交易费。酬劳对其形成正向反馈，从而激励受托人更加努力维护系统安全。由于区块被受托人轮流签署，如果某位受托人因离线错过了签署区块，将面临被其他候选受托人取代的风险。因此为了盈利，受托人必须保证充足的在线时间。

托管节点激励机制。托管节点根据其所持权益获得对应数量的密钥份额，并计算相应的签名份额附在交易中，进而根据密钥份额比例获取手续费。托管节点如果正确提供密钥份额，将会获得与其保证金相应份额的交易手续费用；如果离线或者丢失密钥份额，则无法参与仲裁交易，也就不能获得交易手续费。节点如果提供虚假或错误的密钥份额，会被取消托管身份。综上，激励机制会激励托管节点提供正确的密钥份额，保持在线并安全保管自身的密钥份额。

声誉管理机制。Themis 中的节点一方面参与争议解决，给出仲裁意见，另一方面持续对其它用户给出的争议解决意见进行匿名评价。

在此我们将创建一个实用的匿名声誉机制，能在大规模用户群中快速更新声誉值，同时满足用户的隐私需求。声誉系统将准确计算系统中其它用户对某个用户的仲裁意见结果的反馈，并快速更新该用户的声誉值。声誉值的高低直接关系到用户成为仲裁节点的概率，即声誉值较低的用户较难被选为仲裁节点。

普通节点激励机制。只有在 Themis 上掌握足够的权益才能被选为托管节点并参与托管，其它未成为托管节点的节点被称为普通节点。普通节点无法参与托管但可以将所掌握的权益委托给信任的托管节点，受委托的托管节点将验证交易所获取的交易费按照委托权益比重分配给普通节点。如果托管节点受到惩罚，普通节点也会承担相应损失。这一激励机制保证了 Themis 上权益拥有者均可以获得与权益相关的收益，同时也激励它们将所掌握的权益委托给可信的节点，从而提高 Themis 的安全性与稳定性。

3.2 群托管协议

以 Alice 和 Bob 为例，作为交易双方，首先他们协商生成一个双方共享的 2-of-2 地址作为托管账户地址。Alice 生成她的托管私钥x_A，Bob 也相应生成托管私钥x_B，按照 Thresh-Key-Gen 协议[2]，双方分别使用$y_A = g^{x_A}$和$y_B = g^{x_B}$计算得到托管公钥地址：$y = g^{x_A + x_B}$。Alice 和 Bob 任一方若同时拥有私钥x_A和私钥x_B便能解锁托管账户。

[2] 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.

Alice 和 Bob 在区块链上发起群托管请求，得到若干（奇数）个托管节点的响应。接下来 Alice 和 Bob 与托管节点交互，分别为x_A和x_B创建n个 Shamir 密钥份额[3]P_i。对于 $n = 2t + 1$ 个托管节点的情况，$t + 1$个托管节点提供x_A或x_B相关的密钥份额就能有效恢复托管私钥x_A或x_B。

Alice 和 Bob 分别使用每个托管节点的公钥加密各自的托管私钥x_A或x_B，生成$c_i = E_{M_i}(P_i)$发送每个托管节点，并将所有这些加密的密钥份额$\{c_1, c_2, \dots, c_n\}$提供给另一方。

在上述密钥份额的交换过程中，为了防止欺诈，我们利用可验证秘密分享方案 Feldman VSS[4]和零知识证明来保证 Alice 和 Bob 发送给对方的密钥份额的真实性，即这些密钥份额确实是运行 Shamir 秘密分享协议后生成的关于托管私钥x_A或x_B的密钥份额：Alice 给 Bob 加密的密钥份额$c_i = E_{M_i}(P_i)$时，需要同时提供一个 Feldman VSS 值$w_i = g^{P_i}$及一个关于这两个值一致性的零知识证明。这样，Bob 就可以验证收到的密文数据是否是x_A的 Shamir 秘密分享协议生成的密钥份额。同样，Alice 也可以验证得到的密文数据是否是x_B的 Shamir 秘密分享协议的密钥份额。

上述操作完成后，Alice 或 Bob 便可以将数字货币转账到托管地址。如果没有争议，支付方会把自己的托管私钥分配给另一方，同时持有两个托管私钥的一方可以拿到托管的资金。

如果发生争议，托管节点将调用仲裁服务。仲裁中的获胜方将给

[3] Shamir A. How to share a secret. Communications of the ACM, 1979, 24(11): 612-613.
[4] Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: 28th Annual Symposium on Foundations of Computer Science, 1987, pp. 427-438.

每一个托管节点发送从另一方收到的相应的密钥份额数据。只要托管节点群里大多数节点正常工作，收到数据后，他们就可以重构出仲裁失利方的托管私钥，并将其发送给获胜方。于是获胜方持有两个托管私钥，从而可以从托管地址拿到托管的资金。

3.3 争议解决

如若发生争议，即 Alice 和 Bob 都不愿意向对方提供自己的托管私钥，此时任何一方都可以在 Themis 申请解决争议。在发生争议时，根据托管时交易双方约定的争议解决规则，Themis 启动仲裁流程。仲裁服务只在发生争议时启动 ,以保证公平交易的成本接近于零，即只有出现争议时才需要支付仲裁费用。

我们把争议解决方法分为两类 :第一类是通过执行仲裁智能合约自动生成仲裁结果；第二类由人工介入处理，由多位仲裁人投票形成仲裁结果。

在第一类争议解决方法中，仲裁智能合约会自动调用 Oracle 服务来获取外界输入，运行智能合约代码，生成仲裁结果。

在第二类争议解决方法中 ,我们提出一种基于声誉评分的众包仲裁服务。

众包仲裁。Themis 的基于声誉评分的众包仲裁服务，通过给匿名仲裁人声誉评分的机制，来帮助交易双方选择可靠的仲裁服务，仲裁人也可以在链上获得相应的奖励。

同时，Themis 采用一个评估仲裁人声誉的公开审查制度。仲裁

人的判决会在匿名处理后提交到分布式账本上进行审查。在 Themis 上使用区块链分布式账本列出与仲裁人在交易争议处理中的合同主体事项、案例、判决以及判决理由等信息，其它用户可以对仲裁人的判决打分。根据判决获得的好评程度，匿名仲裁人将获得自己的声誉值。任何滥用仲裁权力的行为都将很快反映到仲裁人的专业声誉值上。声誉值低的用户在未来的交易争议中担任仲裁人的几率将会降低。

声誉管理机制。Themis 的声誉系统将可靠地提供其他用户对仲裁结果的反馈，而不会泄露用户的身份或评分细节信息，同时能保证声誉值不被恶意篡改。目前，常见的声誉系统通常根据统计来自其它用户的反馈来帮助用户评估信息质量，并通过算法更新声誉值来激励正面的行为。这些声誉机制统计用户的打分数据，但会将声誉值与用户的长期身份相关联，这会造成严重的隐私泄露，使用户的行为记录被恶意跟踪，也与仲裁人的匿名性相抵触。我们将创建一个实用的匿名声誉系统，能在大规模用户群中快速地更新声誉值，同时保证用户的隐私，即 Themis 的声誉方案不需要关联用户的长期身份。

Oracle 服务。Oracle 是仲裁服务中讨论和审阅交易双方提供的材料时所需要的机制，其本质是对现实世界中对应的真实事件的发生结果的信息发布。仲裁所需的数据和资料必须由 Oracle 来决定。这些 Oracle 提供了一系列的 API，Themis 通过调用这些 Oracle API 来决定仲裁结果并实现其后的操作。Oracle 可以是中心化的（如 RealityKeys），也可以是去中心化的（如 OracleChain）。

3.4 节点的选取策略

受托人的选举。在 DPoSR 共识机制中，节点为了得到竞争成为受托人的资格，首先需要缴纳一笔保证金，如果节点作恶，保证金将被没收。节点投票给某个节点，即选举该节点作为自己的受托人，系统根据节点所持股权在系统中的占比计算出票数最高的一定数量受托人，受托人按照事先规定的顺序轮流负责生成区块。

托管节点的选取。根据用户的托管请求，系统使用一致性哈希算法选取奇数$(2f+1)$个节点作为托管节点。

仲裁节点的选取。系统根据节点的声誉值采用加权随机算法，计算出奇数$(2f+1)$个仲裁节点。

3.5 安全性设计

我们的方案面临三类主要的攻击威胁，一是拒绝服务攻击，即第三方不能窃取钱，但可以拒绝调解任何争议，从而令托管账户保持锁定；二是托管节点和仲裁节点的共谋攻击，即仲裁节点分别告诉 Alice 和 Bob 各自都赢得了仲裁，这样两方都会将各自的密钥份额发给托管节点，托管节点就能恢复两个托管私钥，从而取走托管账户里的资金；三是 DPOS 的共谋攻击，即 DPOS 共识算法自身理论上面临参与者共谋攻击的威胁。

针对第一类攻击，Themis 引入经济学激励机制来提高节点拒绝

服务和共谋的机会成本，让托管节点在市场力量的驱使下采取诚实和道德的行动，使得 Themis 能够客观的完成托管和仲裁流程。

Themis 的激励机制，旨在鼓励托管节点提供有效的服务，所有正常参与托管的节点都会得到声誉提升，同时获得 Themis 的代币 GET。反之，非正常的托管节点会同时失去声誉和抵押给平台的 GET 风险金，作恶的机会成本大大增加，节点不会为破坏自己已有利益和长远收益而破坏整个网络，这样使得 Themis 能防止大多数来自恶意节点的攻击。

在实际应用中，我们将托管节点分为三个类别，即可信的委员会节点、经过认证的中介代理节点和普通节点。其中委员会节点是由可信的机构维护的一直在线的可靠节点，用来保证在受到拒绝服务攻击后，最后的仲裁结果依然能够执行。中介代理节点自身需要在系统中预先存入保证金，如果做出恶意行为，保证金会被罚没，从而约束其做出正常的操作。

针对第二类攻击，我们把 2-of-2 共享地址升级为 3-of-3 共享地址，第三个托管私钥x_C由 Alice 和 Bob 交易双方共享，但不透露给托管节点。这样，即使托管节点成功发起攻击，也只能获得私钥x_A和私钥x_B，无法取走托管资金。

针对第三类攻击，由于使用 Themis 进行托管和仲裁服务的人越多，Themis 承载的价值就越大，节点作恶的机会成本就越高，整个网络就更加安全，而更加安全的 Themis 会吸引越来越多的人加入进来使用托管和仲裁服务。这是一个彼此增益的过程，随着 Themis 网

络节点数不断扩大，Themis 将变得越来越健壮。

3.6 典型工作流程

以 Alice 支付比特币从 Bob 处购买一只长颈鹿玩具为例，通过 Themis 完成公平交换的过程如下。

托管之前的协商：

Alice 和 Bob 协商一个比特币托管地址；

Alice 和 Bob 在 Themis 上发起一个托管申请，包括事先商定的争议解决方法（智能合约）、手续费和仲裁赏金等；

Themis 运行托管智能合约，返回 Alice 和 Bob 托管节点列表；

Alice 和 Bob 分别给每个托管人发送私钥的密钥份额；

Alice 和 Bob 互相发送私钥的密钥份额。

资金托管和商品交付：

Alice 将比特币转入托管账户，此时 Alice、Bob 和托管方中的任意一方都不能擅自取走资金；

Bob 邮寄玩具给 Alice；Alice 收到玩具，确认无误后，发起确认收款，向 Bob 发送其托管私钥；

Bob 收到私钥后，将托管账户里的资金转入自己的比特币地址；

Themis 上的智能合约计算并分配托管方的托管手续费。

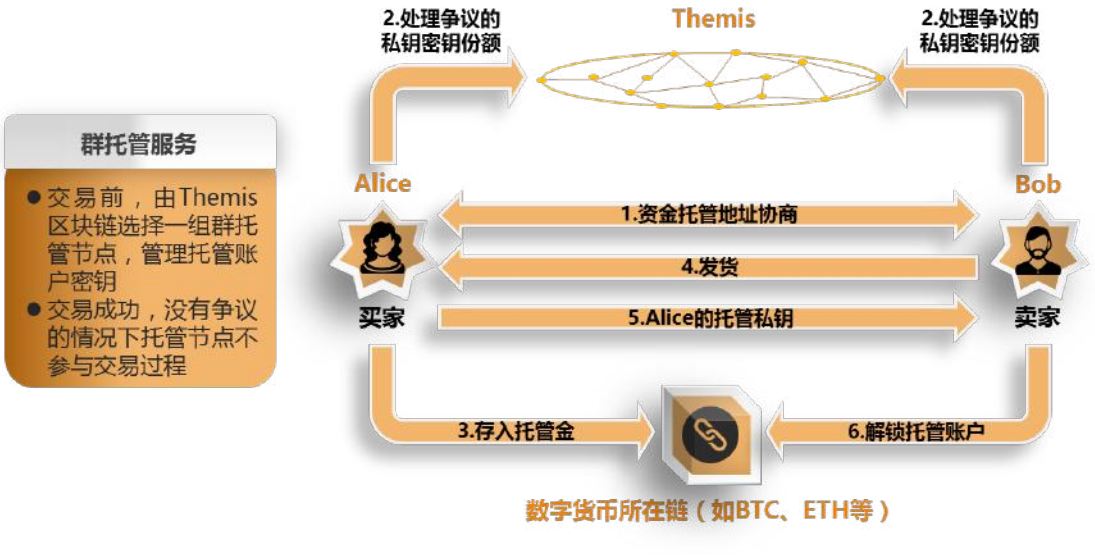

图 3.2 资金托管和商品交付示意图

争议解决：

Alice 和 Bob 在 Themis 上发起争议仲裁请求；

仲裁方按照实现约定的争议解决方法 ,形成裁决结果(假设 Alice 获胜，Bob 失利)；

Alice 向托管方成员发送从 Bob 处获得的私钥密钥份额消息；

托管方计算出 Bob 的托管私钥，发送给 Alice；

持有两个托管私钥的 Alice 解锁托管账户，将托管账户里的资金转入自己的比特币地址；

Themis 上的智能合约计算并分配各仲裁人的仲裁奖励；

Themis 上的智能合约计算并分配托管方的托管手续费。

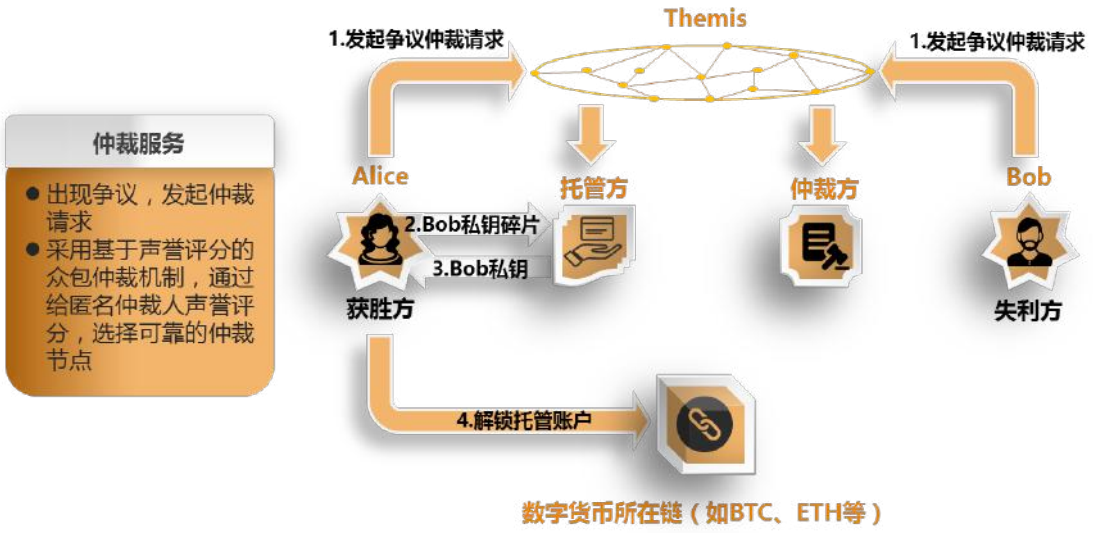

图 3.3 争议解决示意图

3.7 Themis 钱包

Themis 提供一种基于新型密码技术的层级钱包，即 Themis 钱包，为用户提供高效、低存储开销的私钥和地址管理，自动完成与 Themis 区块链的数据交互，方便用户使用 Themis 区块链托管服务。

在 Themis 的几类典型场景中，用户需要频繁地接收来自其他用户的付款。例如，通过 Themis 进行可靠的数字货币交易的网店商户，每一单交易都需要接收来自用户的付款，为了保护隐私，需要为每一单交易生成一个不同的地址，保存并管理这些地址及对应的私钥。当交易非常频繁、交易数量非常多时，由于地址和私钥数量和交易的数量成线性关系，对私钥和地址的管理给钱包系统带来巨大的存储和管理开销。

通常每当钱包生成新的地址，都需要将对应的私钥保存至私钥存储区，而访问私钥存储区的过程会带来巨大的安全风险。为了避免频繁访问私钥存储区，目前的钱包通常采用批量地生成地址的策略，即一次性生成多个地址及对应的私钥，再一次性将这批私钥保存在私钥存储区，从而降低对私钥存储区的访问频率。例如比特币钱包在默认配置下每次生成 100 个私钥及对应的地址，用户可以选择将私钥保存在离线的存储器上（如闪存盘、专用硬件设备，或者打印在纸张上）离线保存。而批量生成的地址在钱包客户端在线保存。当这批地址使用完毕，钱包再次批量生成私钥和地址并访问离线存储用于保存私钥。这种策略一定程度上降低了私钥存储区的访问频率，但仍要定期访问私钥存储区，也没有降低地址和私钥的存储和管理开销，私钥存储区的访问数量和存储开销仍和交易量成线性关系。

Themis 钱包是一种基于新型密码技术的层级钱包，具有以下改进：

1. 支持 Themis 区块链的 API，能自动完成与 Themis 节点的数据交互，方便用户使用 Themis 区块链功能快速完成托管任务。

2. 可以为用户生成任意数量地址，同时用户私钥离线存储只需要一个私钥的空间。用户可以容易地利用现有的私钥离线存储方案，如纸钱包（即将私钥以二维码的形式打印到纸上），或者将私钥存储在硬件 USB Key 上（密码学货币的私钥通常是一个标准的椭圆曲线密码私钥，因此可以将本方案的主密钥 s 存储在任何支持椭圆曲线密码私钥存储的密码设备中）。

3. 用户在接收付款的过程中不需要访问私钥存储区。这意味着本方案的主密钥完全可以离线存储。

4. 用户的公钥因子矩阵的存储空间为固定的常量，这个存储量不随生成地址数量的增长而增长。

5. 用户管理地址将更为容易。用户地址由某个和支付相关的信息生成，而该信息不需要存储。

四、 关键技术

4.1 基于群托管的公平交换协议

公平交换是指保证互不信任的多个主体之间按照约定的规则完成资产互换的协议。公平交换是公平双方计算的一个特例，主要研究互不信任的双方如何共同合作交换数字商品，要么双方都获得了对方的商品，或者双方什么都得不到（All-or-nothing）。

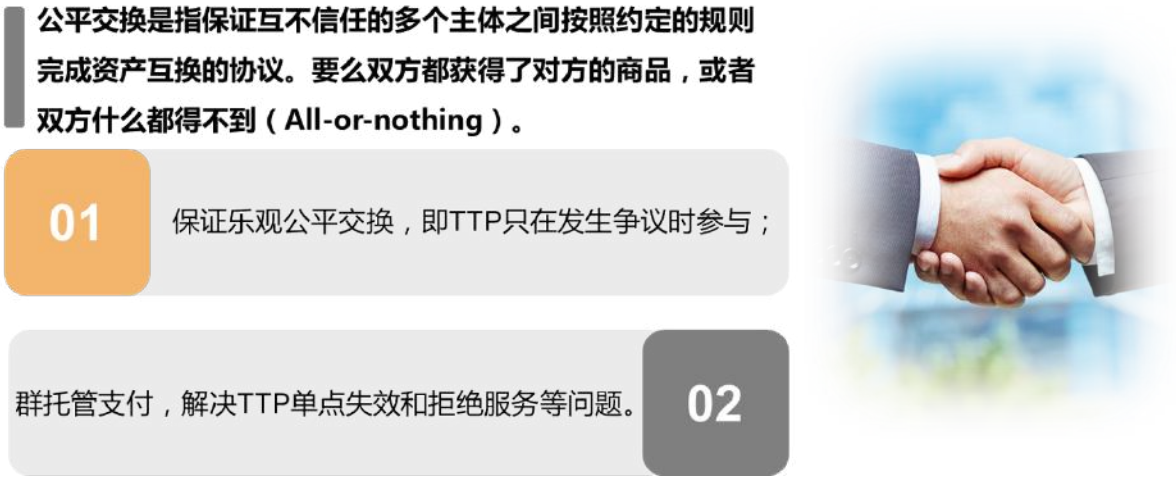

图 4.1 资金托管和商品交付示意图

公平交换的一个非形式化描述如下：

假设有两个协议参与者 A 和 B，分别拥有待交换的电子项 i_X 及其描述 d_X，这里 $X=A$ 或 $X=B$。

假设存在可验证函数 $f(*)$，使得 $d_X=f(i_X)$ 协议有成功和终止两种结束状态，参与双方可判定自身的结束状态。

在异步网络环境下，对于诚实实体 A（不可判定 B 是否诚实），只有在确认已收到期望的电子项 i_B 后才愿付出自己的电子消息 i_A ;反之，对于诚实实体 B 也是同样情形。这就形成了一个不可调和的矛盾：A、B 谁都不愿先付出自己的电子项，那么最终谁也得不到期望的电子项。针对这个矛盾，一种有效的解决方案是，双方都将自己的消息交给一个可信第三方实体（TTP），要么通过 TTP 中转，要么在出现争议的时候让 TTP 进行裁决。

Themis 的设计主要解决两方面的问题：

一是，在中转方式里，即 In-line TTP 或 On-line TTP 模式，需要 TTP 大量参与，导致 TTP 的性能和安全性受到广泛质疑。对此 Themis 给出了一种乐观公平交换协议，TTP 只在发生争议时参与；

二是，针对 TTP 可能存在的单点失效和拒绝服务攻击等问题，我们提出了一种基于群托管的安全交换协议，可有效缓解以上安全威胁。

4.2 基于可验证洗牌和关联环签名的匿名声誉机制

现有的区块链中使用的激励机制，一则不能保证匿名，观察者可以发现用户的身份和投票之间的关系；二则基于数字代币的奖励机制，只能给用户增加货币，而不能在用户作恶后减少用户的货币，即数字代币的密码学机制天然地限制了系统从用户处取走货币，从而不能达到惩罚的目的。为了解决上述问题，Themis 声誉机制基于可验证洗牌和关联环签名技术，可以完成匿名的声誉计算，不泄露用户身份，

并实现带有奖励和惩罚的激励。

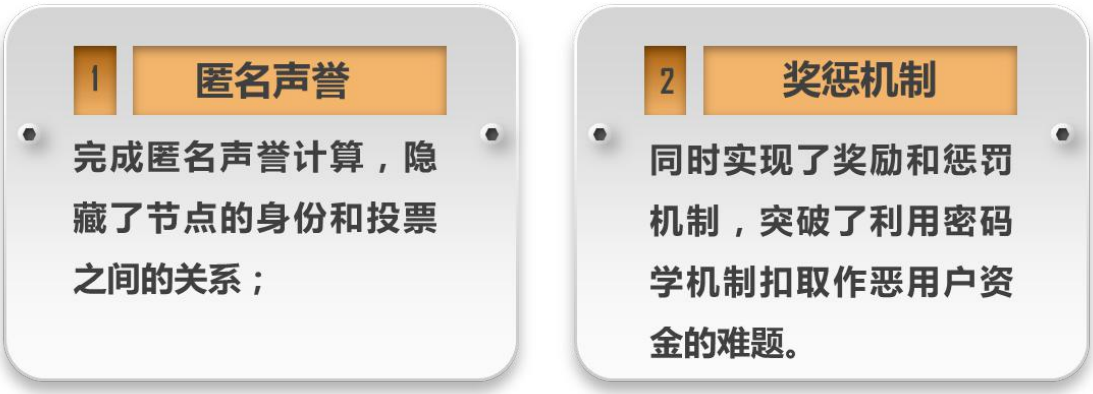

图 4.2 基于可验证洗牌和关联环签名的匿名声誉机制

Themis 声誉系统的工作机制主要是多轮消息的发送和反馈。在每轮的开始，服务器维护包含所有客户端的长期数据库身份和各自的加密声誉分数。在每轮中，服务器依次运行基于可验证洗牌协议的调度算法，把声誉列表变成基于一次性假名的匿名排列列表和对应的明文信誉评分。我们采用去中心化的调度协议，服务器和客户端（所有者除外）均不能将一次性假名和长期身份相关联。客户端使用一次性假名匿名发布消息。服务器可以关联这些消息与他们相应的声誉评分，而不会了解到客户端的敏感信息。接下来每个客户端会对其它用户的发布的消息提供反馈（例如投票）。每个投票都采用关联环签名进行签名，使服务器能验证每个客户只投票一次而不透露哪位客户提交了每一票。这个设计使服务器在统计正面和负面投票时不能将投票与长期身份相关联。最后，服务器根据一次性假名的反馈信息更新信誉评分，然后执行“反向调度”，将这些一次性假名及其更新的声誉恢复到原来的长期身份和他们的加密更新的声誉评分。

4.3 非交互式零知识证明

零知识证明系统（Zero Knowledge Proof Systems）是一种两方（证明者和验证者）密码协议，自 1983 年诞生以来，这一神奇的概念给理论计算机和密码学带来了深远的影响。

通过执行零知识证明协议，当断言为真时，证明者能够向验证者证明并使其快速确信该断言的真实性（完备性：Completeness），且验证者除了该断言的真实性以外无法获得任何知识（零知识性：Zero Knowledge），而当断言为假时，即使拥有无穷计算能力的证明者也无法以非可忽略概率欺骗验证者接受该虚假断言（合理性：Soundness）。当断言形如证明者拥有某个秘密知识时，零知识证明系统特化为零知识的知识证明系统（Zero Knowledge Proof of Knowledge），即证明者能够向验证者证明并使其确信自己确实拥有声称的秘密信息，且证明的过程不泄漏任何关于秘密信息的知识。根据证明者与验证者之间是否需要交互，零知识证明系统可以进一步分为交互式零知识证明系统和非交互式零知识证明系统。非交互式零知识证明对通信的要求最低，因此更适合实际应用。

我们利用零知识证明解决以下三个问题：一是，在群托管服务协议中，利用零知识证明来保证交易双方各自提供给托管节点的密钥份额数据是真实；二是，在可验证洗牌协议中，除了执行洗牌操作之外，每个洗牌服务器都生成零知识证明，任何观察者或验证者都可以使用它来检查洗牌服务器是否正确地执行了它的随机操作；三是，在声誉

系统中，客户端在发布消息时生成自己的声誉预算的零知识证明，声称 1）他的实际声誉得分不低于预算值 b，2）他想使用 b 作为声誉分数来发布此消息。

图 4.3 非交互式零知识证明

4.4 支持高并发验签的数字签名算法

对大量交易消息中数字签名的验签计算是制约公有区块链交易处理能力的主要因素，目前区块链中普遍采用的 256 比特素域椭圆曲线上的签名算法虽然具有较高的安全性，但是验签效率不高，目前主流处理器每秒能计算的验签次数通常不足万次，在网络中出现大量交易消息时，对消息验签会导致节点出现很高延迟。当前的一些联盟

链和私有链往往通过引入可信计算环境等方式来规避这一技术挑战，但同时也引入更复杂的安全基，难以支撑公有链的安全需求。

Themis 项目通过引入全新的支持高并发验签的数字签名算法来解决这一关键技术需求。系统支持多种可选的数字签名方案，可以根据用户和应用的需求选择相应的签名算法，当面对签名私钥只需使用一次的场景时，选择具有极高验签性能的基于哈希的一次性签名算法；在典型的应用场景中，在保证 256 比特安全等级的基础上，选择具有特殊性质的椭圆曲线及验签算法，使得验签节点可以利用曲线参数和算法上的特点，并通过时空权衡优化技术大幅优化批量验签的计算效率。在算法实现上特别针对 GPU 和 CPU 的向量指令集进行优化，充分利用处理器上每一颗晶体管带来的计算能力。通过综合优化，实现在典型计算平台上接近 2 个数量级的验签性能提升。

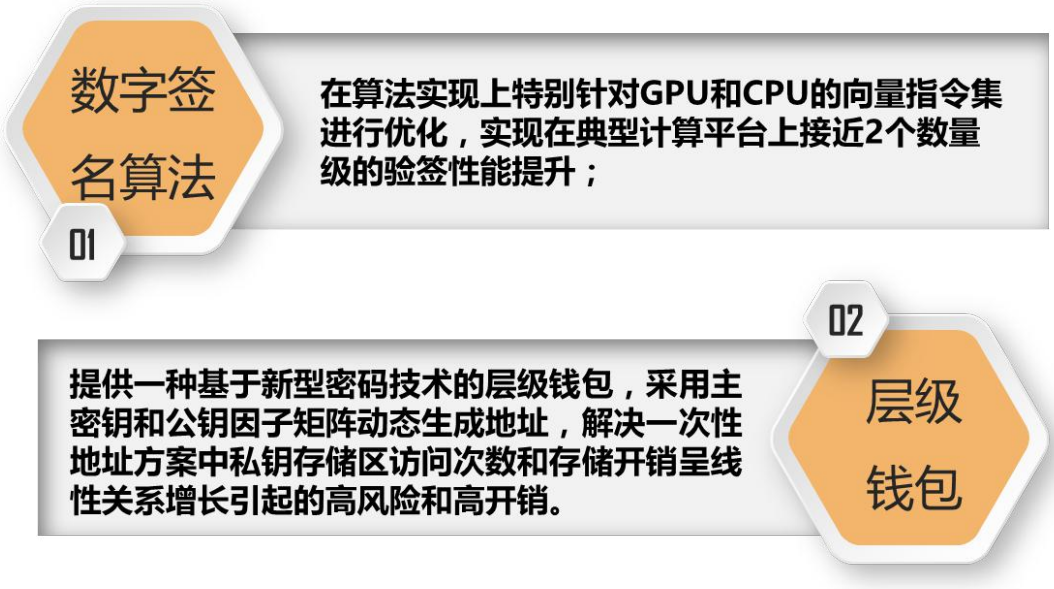

图 4.4 面向区块链的新型密码学算法

五、 应用场景

Themis 是一个基于区块链的公平交换系统，提供去中心化的数字货币托管服务，解决以数字货币为媒介的公平交换问题，例如数字货币、数字资产和实物商品之间的公平交换。Themis 可应用于点对点托管支付、数字货币交易兑换、监管账户安全托管、多主体交易资产托管等诸多场景。

5.1 点对点托管支付

Themis 可以为 P2P 网上市场（例如 OpenBazaar）提供去中心化数字货币托管支付，实现买卖双方的直接交易；Themis 可以连接电商平台数字货币支付系统，通过 Themis 在原有链上生成相应托管账户，对数字货币交易行为进行去中心化托管。交易中，买方将需要支付的数字货币托管到该托管账户中，根据实物商品交付情况，待正式确认交付后，向卖方发出确认指令，卖方即可从托管账户获得数字货币。这种机制能有效解决数字货币支付和实物商品交付不能同时完成的难题。

在电子商务实际应用中，Themis 平台将为买家提供先行赔付保障。例如，在确认收货之后的 7 天内，卖家的 5%的资金通过智能合约留在平台账户里，作为押金；7 天内出现纠纷，Themis 可以用押金池里的钱为买家先行赔付，然后平台与卖家交涉退款事项。这样可

以进一步提高买家的满意度，同时为卖家增信。

图 5.1 点对点托管支付

5.2 数字货币交易兑换

Themis 是一套基于区块链的公平交易系统，既能满足数字货币与实物商品公平交换的需求，又能满足不同数字货币间交易兑换需求，为各类中心化和去中心化数字货币交易兑换提供公平交换保障。

Themis 支持实现数字货币的场外交易，能够为比特币、以太币以及其它基于区块链的密码学数字货币提供去中心化安全托管服务，通过在原有链上生成相应托管账户，满足不同数字货币间交易兑换需求，为数字货币跨链交易提供公平交换保障。

图 5.2 数字货币交易兑换

5.3 监管账户安全托管

托管服务是传统金融中保障用户资金安全的重要手段，例如券商开户后要开设银行托管账户、P2P 网贷要开设监管账户。对于私募基金、众筹基金以及新近出现的 ICO 投资基金等，由于没有资金托管，或者采用第三方中心化的托管机制，使得托管资金的投资对象、投资比例和投资收益不透明，容易造成信息失真和道德风险。

Themis 作为一个具有高扩展性的智能合约集群，可以提供分布式账本的接口，为数字货币资金监管账户提供去中心化的托管服务，这样能有效保障投资资金安全、项目溯源和投资利润分配合理化等问题。随着数字经济的蓬勃发展，未来会衍生出众多数字货币金融产品及应用场景，诸如数字货币借贷、数字货币期货期权、数字货币 ETF

基金、跨链数字货币交易等 ,都可以通过 Themis 系统进行安全托管，以保障资金安全。

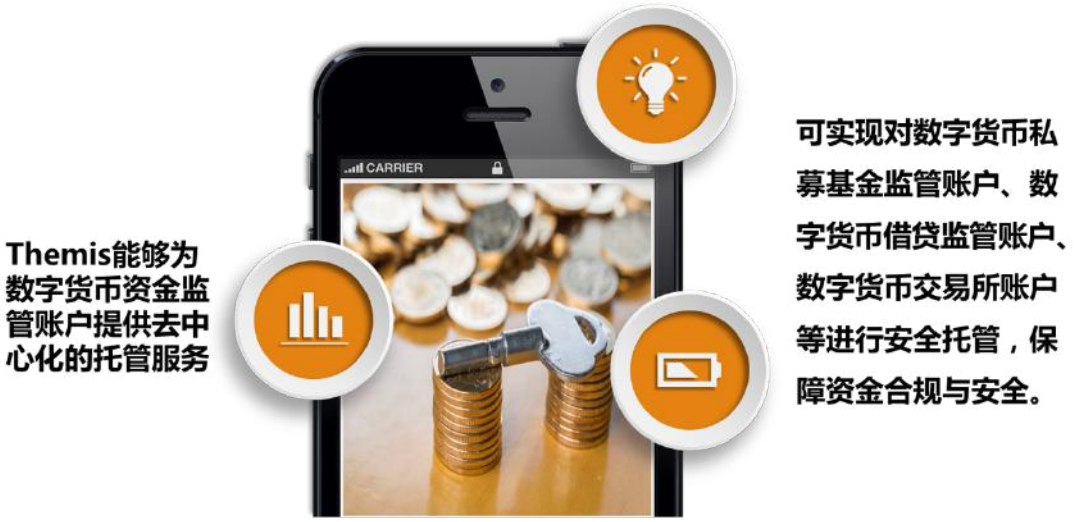

图 5.3 监管账户安全托管

5.4 多主体交易资产托管

在供应链金融、不动产、大型设备等交易中，由于交易主体多、交易环节长、交易依赖性强 ,极易导致道德风险和交易主体失信问题。

Themis 可以通过建立基于多主体职责和权益触发条件指令的智能合约，将多主体交易中需要托管的资金，诸如订金、首款、佣金、尾款等以数字货币的形式托管在原有链上。在交易进展到相应环节时，相应交易主体通过输入相应指令触发该智能合约，实现公平交易，及权益的交割。若交易某一方对交易环节产生争议，可利用 Themis 群托管服务协议及公平仲裁机制发起仲裁请求 ,群托管方中的每个成员将对争议进行仲裁、投票、形成裁决结果 ,获胜方即能解锁托管账户。

六、 发展线路图

- 2017 年 6 月，开展基于群托管机制的公平交换协议设计
- 2017 年 12 月，完成具有完备功能的最小化可行版本（MVP）
- 2018 年 3 月，去中心化托管服务内测，OTC 交易平台试运行
- 2018 年 6 月，Themis 区块链测试网络发布
- 2018 年 10 月，Themis 主网上线