Findora 简版白皮书 (简略版本)

Findora Foundation
contact@findora.org

版本 3.2 (2020 年 11 月)

摘要

Findora 是一个完全保密但可审计、高吞吐量和可扩展的公共金融基础设施。处于 Findora 构架核心的加密透明的去中心化金融分类账本可实现高效、高可访问和透明的金融服务。

在过去几年中，“区块链 “因其影响深远的金融应用引起了人们的关注。这源于区块链提高交易系统透明度、可信度和协调性的能力。Findora 目标服务于整个金融基础设施中最迫切需要提高透明度的部分，而现有的其他公共区块链不能满足这些部分对隐私保护和合规的要求。这些领域包括投资基金、市场化贷款平台和证券交易所等金融服务。这些服务不透明地处理着价值数万亿美元的资产，经常是低效率运行并且极易受到欺诈行为的影响。

Findora 预见到一个新世界。在这个世界中，金融体系中的每项资产始终都是合规的，并可随时进行公开审计。每项资产都包含有关所有权、可转让性和合规性的规则。一个验证者节点网络在分发信任的同时强制执行合规性。想象一下：一支基金能证明他们只在被授权范围内进行投资，一位投资者能匿名的提供资质认证，或者一个监管机构能使用细粒度审计密钥，所有这一切的实现同时保持完全机密性和可互操作性。

内容目录

1 区块链和金融

区块链是一项有望提高金融系统的透明度和效率的新技术。比特币是开创性的加密货币，它源于一项创建新的全球“人民货币”的倡议，这种货币不受任何特权组织的治理或控制。随着技术进步，包括智能合约、零知识交易、多签名钱包等许多新功能的涌现，该行业开始意识到超越无政府主义（去中心化）货币的深远潜在应用。

1.1 协议标准

在许多方面，金融基础设施的现状很像在广泛采用 TCP / IP，TLS，HTTP 和 SMTP 等互联网标准协议之前的互联网。一个网络在没有中心化协调的前提下运行的最基本要求是采用通用语言，以便独立系统间可以无缝地相互通信并共享信息。对于电子邮件，SMTP 提供了标准数据传输协议，以便可以在不同的邮件客户端和服务器之间发送电子邮件。在金融系统中，相互依赖的信息存在传递的附加约束。例如，将同一笔电子化资金从一家银行转移到另外两家银行的双重银行转账将会出现问题。

最近区块链和加密货币行业的爆炸式增长为期待已久的全球金融体系改造提供了机会。在短时间内，它促进了分布式数据库、点对点对等广播协议和拜占庭共识算法的新开源基础设施的发展，以及改善数据完整性和隐私的新密码学工具库的实现，例如多签名技术和零知识证明。

1.2 金融身份

在金融系统的语境之下，身份证明之于资产所有权来说传统上就是必需的。除有形资产外，建立所有权依赖于对应现实世界身份的法律文件。这种建立所有权的方法可以同样适用于更多样化的资产。公司股票可以合法地发行给某公钥 (public key)，以便只有知道相应密钥 (secret key) 的人才可以主张所有权。

但是，与其他领域相比，全球金融系统中各种资产的所有权通常具有更严格的身份证明和帐户验证要求。例如，在接受新客户之前，银行和经纪服务必须遵守了解您的客户（KYC）和反洗钱（AML）规则。

加密货币背后的区块链并未如此细节化的解决参与者的身份认证。公钥单独来看不包含有关用户的任何信息。不过，重要的是，用户可以轻松地将有关其身份的其他信息添加到他们可以访问的公钥中。这种身份可以赋能围绕 KYC、AML 和其他合格认证的丰富规则的强制执行。这些规则可以厘定参与不同类型的金融交易的要求。但是，现有的区块链没有为现实世界身份管理和认证提出全面综合的标准。

1.3 透明度和同步化

无论是由单一服务器、联盟还是大规模分布化的运营节点网络管理，所有区块链网络都有一个共同点：区块链数据结构。区块链是一种简单的经过验证的数据结构 (Authenticated Data Structure)：多个记录以密码学方式链接在一起组成一个仅可附加的列表 (append-only list)，以便于对存放在一个共享式开放数据库中的交易历史达成共识。经过验证的数据结构使运营节点网络、用户和审计人员可以轻松地对公共金融数据库进行开放访问，而无需信赖由某中央服务器诚实地提供对数据的访问途径。交易的历史是不可更改的，任何人都可以验证所有交易都是有效的。Findora 的高级经验证数据结构是基于加密累加器 (RSA Accumulator) 和向量承诺 (Vector Commitments) 等最新技术。

1.4 隐私与合规

透明度和开放参与是基于区块链的金融的基石。但是，完全透明是以隐私为代价的；而隐私性是绝大多数金融服务的绝对要求。因此尽管完全透明提供了可审计性，这种特点也让多数区块链平台无法部署大部分金融应用。另一方面，诸如 Zcash 和 Monero 之类的加密货币利用加密技术来保护通证转移的匿名性。但是，这些系统的局限性在于机密性是全有或全无的。交易只证明原生加密货币的简单转移是有效的，但不能证明更细致的陈述 (而丧失了可审计性)。因此匿名区块链也无法提供部署金融应用所需的合规要求。

传统金融为用户提供了针对公众的隐私性，但提供的透明度接近于零；并且，不保护用户对于金融机构的隐私性。第一代基于区块链的金融提供完全透明度或完全保密性。Findora 旨在通过我们所谓的*加密学透明度*提供两全其美的解决办法。

加密学透明度提供比传统金融更好的隐私保护，甚至详细的用户数据对基础设施的运营节点也是保密的，同时仍允许运营节点能验证所有交易的有效性。它还成功保留了第一代区块链提供的透明度和可审计性，使用户能够证明有关私密交易细节的复杂陈述。Findora 为资产通证，身份证明/KYC 集成，公共和监管审计，资产追踪以及许多其他特殊目的零知识证明功能提供以隐私为中心的工具，以证明交易是合规的：例如，证明交易所具备偿付能力和基金投资于白名单资产。

1.5 共识机制

关于区块链的最大误解之一是它们可以简单地取代金融机构的信托角色。而事实上，运营区块链的网络本身就是新的金融机构。它运作的共识协议决定了影响力如何在网络参与者之间分配。

1.5.1 分布式共识之案例

共识协议是一种算法，可以使组织更具弹性并降低变更成本。

去中心化 去中心化宽泛地描述了更加一种开放和分布式的共识参与。纯粹的民主制国家比共和制更去中心化。

中心化控制的风险 当金融分类账本由一家私营公司经营时，该公司具备完全控制权，并无义务正确公平地操作分类账本。如果该公司设定的价格太高，审查交易，或者被抓到接受无效交易，那么用户唯一的追索行为就是转而加入由竞争对手运营的新分类帐本系统。

合作社引喻 Findora 对公共金融基础设施的愿景类似于一个允许全球自由参与的大型金融合作社，由其用户和操作人员拥有和民主的控制。这样的分类账本更能抵御私人管理的中心化分类账本的风险，并且可以投票以去中心化的方式剔除反常的运营节点。一个运营层面的共识协议有助于解决此问题，而无需依赖受信任的协调人。

运营层面共识机制 运营层面共识机制的目的是将投票和运营节点更换与日常运营更加无缝地结合起来。在区块链分类帐本系统中，这是可行的，因为运营者扮演简单而客观的角色，因此很容易更换。运营节点运行自动交易验证软件，并按照先到先得的原则将任何有效的交易附加到分类账本。此外，在区块链分类帐本中，运营节点可以看到的信息与公众能看到的没有区别。纵然在像 Findora 这样的保密交易区块链中，运营节点也可以使用神奇的加密学技术验证交易的有效性，而无需解密查看交易的私密内容。

1.5.2 共识协议参与

经典共识协议是为一组固定的选举人设计的，他们共同提出，批准并最终就陈述达成一致。这有时被称为*许可制共识*。我们称这些选举人为*验证者节点*，因为在我们的上下文中，他们将验证区块链交易。拜占庭容错（BFT）共识协议对于*拜占庭错误*是强大的，其中一部分验证者节点可能不仅失效而且也变得腐败并试图破坏共识或接受无效/冲突的交易。未腐败的验证者节点称为*诚实验证者节点*。

许可制的 BFT 适用于由预定的一组验证者节点的联盟运营的区块链。在此设置中，安全性很容易理解。它基于分布式信任，不涉及任何复杂的激励相容参数。

如今，我们拥有适用于更富弹性的验证者节点集的共识协议。通常被称为“非许可制”共识协议，这些协议以各种无法相比的方式改变了许可模型。通用化经典共识的一

种方法是联邦拜占庭协议（FBA），它允许每个验证者节点选择自己的信任圈子。具体来说，验证者节点可以为自己定义什么构成 *quorum*，即它将信任并一致行动的一组节点。在经典 BFT 协议中，任何 2/3 验证者集合是一个 quorum。其他方式坚持采用验证者集的统一观点，但要使此集合动态化，或与外部资源（例如，存储空间证明机制和工作量证明机制）相关联。利益证明共识协议是最直接的延伸，其中投票权与原生通证相关联。这些系统不是向符合条件的验证者分配固定的少数 "共识席位"，而是分配由通证代表的非常多的席位（例如大于世界上的人数）。单个验证者可以控制多个席位，还可以交易席位（即通证），利用共识协议本身更新席位所有权。

1.5.3 激励相容

如果恶意行为的潜在收益超过整个网络的价值，则支持比特币和以太坊等系统安全的激励相容（根据工作量证明机制或者权益证明机制分配投票权）会遭遇挑战。矿工的奖励或押注可能失去其相对重要性。如果共识网络用于管理超出原生通证以外的资产（在外部获得其价值），则尤其令人担忧。出于这个原因，采用纯粹的激励支持共识网络似乎是管理证券和在全球资本市场上交易的 100 多万亿美元资产的冒险选择。

另一方面，重要的是要认识到用于记录外部资产所有权的区块链与仅用于记录原生加密资产的区块链具有根本不同的重要性。比特币区块链是 "比特币" 所有权的唯一真相来源。相比之下，房地产、公司股票或美元支持储备等资产依赖外部实体来强制执行，例如管辖法院。区块链在相关交易对手和执法机构都信任它或实际上验证其数据完整性的情况下，提供令人信服的所有权证据。

为解决区块链针对现实世界资产的共识机制所面临的独特挑战，Findora 的共识协议 *Finsense* 将整合来自权益证明共识机制和联邦拜占庭共识网络的元素。在联邦拜占庭共识机制中声誉和信任关系发挥更大作用。

1.5.4 状态机复制

没有共识协议可以保证在所有网络条件下的完美一致性 (consistency) 和活跃性 (liveness)。如果网络验证者节点之间存在分区，则每组验证者节点必须在无限期停顿或冒失去一致性的风险继续确认交易之间做出决定。这也是存在多种共识协议的一个原因，这些共识协议都在有关底层网络的不同假设下实现一致性和活跃性。即使是在网络重新获得完全连接时恢复活跃性的共识协议，如果 1/3 或更多验证者节点腐败，也无法保证一

致性。[1]

1.5.5 共识协议的属性

大规模共识机制的效率 在潜在可能有海量验证者节点条件下计算所有投票是不切实际的。针对任意大验证者节点集的共识协议有时通过随机选择委员会（验证者席位的一小部分）来提出和确认交易块。可以在某时间点、每次更新之后或其组合周期性地触发选择过程。选择的随机性是加密保证的，而不是依赖于某个可信的运营者。确切的方法因共识协议而异。委员会选择的一个常用工具是可验证随机函数（VRF）系统。

腐败容错 这是在一致性或活跃性出故障之前可能由腐败的验证者节点控制的最大席位数。

响应 这是共识协议确认对分类帐本更新达成一致的速度。能够以接近网络通信的实际速度确认交易块更新的协议具有即时最终确认性。

分区容错 这就是共识协议对网络故障的响应方式。同步模型定义了所考虑的网络故障类型，其中可能包括脱机的节点，不可预测的通信延迟或网络的完整分区。

主动安全性 尽管每个委员会都是随机选择的，贿赂和有针对性的腐败是选择委员会的共识协议中的一个问题。为了解决主动腐败攻击，可以设计协议使得新选出的委员会成员仅在其被选中的时刻广播一条消息。[2]

问责与弹性（" 罚没"） 从许可制的共识协议中删除犯规的验证者节点相当于取消了它控制的所有共识席位。在使用基于权益证明的共识协议中，这相当于没收验证者帐户中的所有押注（称为罚没）。如果诚实的验证者节点们可以一致认为某验证者违反协议，那么他们可以一致地罚没该验证者节点。但是，这种方法存在一些挑战。

---

[1] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. *Consensus in the presence of partial synchrony.* J. ACM, 1988.

[2] J. Chen and S. Micali. *Algorand: The efficient and democratic ledger.* Arxiv.org, 2016; Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich. *Algorand: Scaling Byzantine Agreements for Cryptocurrencies.* SOSP, 2017.

1.6 另类投资

市场巨大的另类投资领域是被不透明的资本管理和低效率的信息追踪所困扰的众多金融领域之一，包括对冲基金和私募股权基金等投资基金以及点对点借贷平台。

即使在高度监管的市场中，信息不对称也到处可见，投资基金和贷款平台仍然高度不透明。一个典型的基金后台往往是复杂和过时的。汇报、税收和合规等功能主要以纸张或遗留系统为基础，需要人工检查并确保资金在合规范围内运作以及投资者及时收到信息。最后，在私人投资基金等流动性较低的基金市场中，没有统一的方法或平台来分配和交换部分所有权。任何此类系统都需要我们在公开市场中所见的功能-包括足够的透明度、成本效率和追踪。

2 Findora 平台

Findora 平台上的金融服务应用程序是围绕由全球网络管理和保障的数字分布式账本上的工具构建的。应用程序将利用工具进行保密的金融交易，并平衡隐私和合规性证明。

Findora 平台支持的一个示例应用是智能投资基金（SIF），这是一种基于智能合约的基金协议，在投资基金中引入新的信任和透明度，同时尊重机密性。虽然基金经理负责监管基金并决定资金流向何处，但所有资产的跟踪和记录都通过网络进行分配。该平台的隐私工具使用特殊目的零知识证明和多方计算，赋能监管机构和投资者确保基金合规，同时保证基金参与者的机密性需求。

2.1 系统构架

Findora 平台分为三层。

金融服务应用 金融服务应用程序位于最顶层。Finapps 可以由 Findora 网络上的开发人员自由开发和部署。

Findora 开发者工具 中间层提供多资产发行和转移，金融护照（Findora 的身份证明工具），审计和资产跟踪工具，以及使特殊目的用零知识证明和多方计算的隐私保护合规工具。

分布式账本协议 基础层是底层分布式分类帐本协议，支持机密支付，智能合约，多签名帐户和非托管交易所。Findora 的共识机制和治理模型利用了 Finsense 共识，而私有和联盟链作为侧链可以使用他们自己选择的共识协议。

2.2 金融护照

金融护照汇总了有关用户的信息，从用户的合格认证 (Accreditation) 和财务身份的基本信息开始，到信用评级/分数，反洗钱 (AML) 白名单等。

用户护照中的所有信息均由至少一个机构验证和签名。这些签署的声明以加密选择性公开凭证的形式呈现*加密学可选择性透露身份证明*[3]. 这意味着信息的验证方式使用户可以选择性的披露其身份的组成部分，而不会不必要地损害其整个个人财务状况的隐私。此外，用户可以展示关于其经过身份验证的个人资料的复杂陈情（例如，收入范围或几个资格的阈值交集），而根本不会泄露任何精确的个人详细信息。

2.2.1 可选择性披露的身份证明表单

一个可选择性披露的身份表格包含以下项目:

- `credPubKey`: 用户知道其私钥的公钥
- `attributeList`: 用户提供的自定义属性列表
- `attributeBitVector`: 指示身份验证提供商批准的属性的位向量
- `providerSignature`:-身份验证提供商在其他表单项上的签名

身份证明表单还可以包含来自多个身份提供者的签名，在这种情况下，表单内容的结构如下:

```
body {
   credPubKey
   attributeList
}

signatures {
```

[3]J. Camenisch and A. Lysyanskaya. *Signature schemes and anonymous credentials from bilinear maps.* Crypto, 2004; Alberto Sonnino, Mustafa Al-Bassam, Shehar Bano, Sarah Meiklejohn and George Danezis. *Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers.* NDSS 2019.

```
    List <providerPubKey, attributeBitVector, providerSignature>
}
```

身份证明表格从不公开披露，因为这会损害匿名性; 相反，Findora 提出了一种使用零知识证明的特殊选择性透露协议。身份证明表单上的“公钥”和签名不单是任何标准公钥和数字签名。它们以特殊方式使用基于配对的匿名身份凭证加密技术精心制作。这是为了在选择性透露和验证协议中实现有效的零知识证明。

公钥也是随机化的，这意味着有一个函数可以生成一个新的公钥（不可链接到旧的公钥）但具有相同的密钥 (secret key)。公钥充当对秘密密钥的加密承诺，并且随机化的公钥是对相同秘密密钥的新承诺。

用于可选择性披露的身份证明表单的关键函数是 `ac_keygen`, `ac_sign`, `ac_reveal`, `ac_verify`, 和 `ac_randomize_pubkey`.[4]

2.3 数字资产通证

Findora 支持创建和分发数字资产通证，以代表经济所有权以及投资者、基金经理和企业之间无数复杂的关系。例如，资产通证可以代表一个投资基金的部分所有权和基金对参与者的负债。

一个*数字资产通证*是一种价值的不可变且可转移的代表，类似于物理通证，例如可以从手到手传递的票证或美元钞票。通证可以被生成，销毁或转移。然而，数字通证是一种抽象化通证，并且有不同的方式可以用数字表达和传递它们。*数字证券通证*是一种特殊的数字通证，它代表一种负债，并承载着一些现实世界的司法管辖范围内的意义。例如，通证可以代表一个交易对手（通证持有者）起诉另一个（通证发行者）的能力。这与像比特币这样的数字资产不同，后者类似于商品货币（如黄金），并具有其持有者网络所赋予的内在价值。

2.3.1 锚点

数字资产通证的发行者称为锚点。例如，银行可能会锚定代表储备支持资产的通证。锚点使用通证标准形式来定义一个通证类别，指定通证函数。Findora 提供了一种新的智能资产框架（SAF），一种用于金融资产的可编程标准接口。SAF 涵盖多样化的金融资产，从 A 类股票到房地产投资。

锚定的资产通证可以被点对点转移和数字化追踪，但是它们仅在通证持有者与通证锚点具有法定（或基于信任的）关系前提下才对通证持有者有价值。理想情况下，资产

[4]该协议以及实现方式和优化细节在全本简版白皮书中有所描述。

通证持有者应该能够将其通证转移给与同一锚点无共享法律/信任关系的另一方。在这种情况下，一个证券通证卖方不能简单地将通证的所有权以当下形式转移给买方，因为该通证在当下形式下依法不代表对买方的任何价值。这可以通过识别负债路径 (liability path) 来解决，类似于在银行间转账的信用网络中识别路径的方式。可以通过交易费用或收益提成百分比等激励中介机构促进交易。Findora 应用层的交易所服务可以提供订单簿 (order books)，有效地确定参与交易的任何两个交易对手之间的最佳路径，并立即和原子地沿着该路径执行交易。

2.3.2 资产通证数据模型

Findora 上资产通证所有权的基本记录是三个值: $(address, amount, asset\_\ type)$.

$address$ 是一个公钥，资产所有者必须知道相应的私钥。$asset\_type$ 是唯一的引用资产定义，即此资产通证在 Findora 分类帐本上的资产定义。当锚点在 Findora 上发布新资产通证时，它必须首先通过创建资产类别来定义资产通证。资产类别是一个数据表单，包含有关资产的法定含义的所有信息，从其广泛的分类（例如期票，债券，股票，债务，房地产）到其更精细的合约细节。这可能包括限制其所有权和转让的资产制度 (asset policy)。资产类别包括锚点的公钥，并经由锚点进行数字签名。Findora 分类帐上定义的每个资产类别都有一个唯一的 *asset code*，默认情况下是对应数据格式内容的 32 位字节内容可寻址散列值。此资产代码用作所有权记录中的唯一 $asset\_type$ 引用。

可互换资产 (fungible assets) 可能有许多无法区分的相同资产单位 $asset\_type$（例如股票单位，银行发行的货币等）。在这种情况下，所有权记录中的 $amount$ 字段用于表示 $address$ 拥有相同 $asset\_type$ 的多个单位。对于不可替换的资产（例如房地产），给定的资产类别 k 可能只有一个单位存在，因此 $amount = 1$。

资产通证创建 在将资产通证发行到任何分类帐本公钥地址之前，必须在 Findora 的分类帐本上定义其资产类别。资产通证类的高层次结构如下:

- Code: 在分类帐本上表示此资产的唯一资产代码 (16 bytes)
- Digest: 静态通证数据的内容可寻址散列值
- Issuer: 至少包括锚点的公钥，以及可选的发行者描述，例如链接的经过验证的身份
- Memo: 资产的法律含义和分类的描述，例如钞票、债务、股票、本票、不动产。

- Confidential memo: 私密备忘录，用于保密资产
- Updatable: 指示资产发行者是否可以更新备忘录字段的旗标。所有更新都是仅附加操作，并跟踪备忘录历史记录。
- Units: 现有（公开）单位总数，不总是适用于所有资产类型。此字段不是静态数据的一部分，每次资产发行人在交易中减去新单位时都会更新。
- Confidential units：与 Units 类似，但跟踪现存的所有保密单位，隐藏在加密承诺中。这有助于保密资产发行。
- Policies: 限制和管理涉及此资产通证的交易的规则。具有制度的资产称为智能资产。

资产通证发行和转移 资产发行是一种经由锚点数字签名的交易，可创建新的资产所有权记录。它将给定资产类型的特定单位数量分配到分类帐本地址。数字签名必须根据相应资产类别定义中指定的发行者公钥进行验证。新创建的资产记录称为 *valid*，它们可能会被未来的交易废除。分类帐本跟踪所有有效/无效记录。

资产转移是将现有资产单位的所有权在两个分类帐本地址之间的转移交易。最简单的资产转移消耗（即废除）现有资产记录并创建仅更改 *address* 的新记录，但保持相同单位的 *amount* 和 *assettype*。更一般地，资产转移可以消耗多个现有有效资产记录，并创建新资产记录，其在新地址之间重新分配资产单位数量。作为基本规则，资产转移交易必须消耗与其创建的给定资产类型一样多的单位。但是，资产转移还必须遵守资产类别中指定的自定义资产制度。

2.4 保密资产转移

保密资产转移是将资产的所有权从一个地址转移到另一个地址的交易，但隐藏了转移资产的详细信息。在基本资产转移的情况下，这包括在交易期间消耗和创建的输入和输出资产记录中的 *amount* 和 *asset_type* 字段。

为了解释 Findora 中的保密转账如何运作，让我们仔细看看 Findora 资产转让交易的解剖结构。[5]资产简单地通过将 *transfer note* 发布到 Findora 分类帐本（简称为 `XfrNote`）来执行转移。

[5]技术上，Findora 交易捆绑操作和 Findora 中的资产转移是一项操作。

```
pub struct XfrNote{
  pub(crate) body: XfrBody,
  pub(crate) multisign: XfrMultiSig,
}

pub struct XfrBody{
  pub(crate) inputs: Vec<BlindAssetRecord>,
  pub(crate) outputs: Vec<BlindAssetRecord>,
  pub(crate) proofs: XfrProofs,
}
```

XfrBody 包含输入资产记录和输出资产记录的列表。出于机密性考虑，这些资产记录是 *blinded*，使用加密 *commitment*。这些是使用 Pedersen 承诺在名为 “Ristretto’ 的椭圆曲线组上实现的。我们将盲法记录数据结构称为 BlindAssetRecord，以区别于普通 AssetRecord。

```
pub struct AssetRecord{
  pub(crate) amount: 64,
  pub(crate) asset_type: Option<[u8;16]>,
  pub(crate) public_key: XfrPublicKey, // ownership address
}

pub struct BlindAssetRecord{
  pub(crate) asset_type: Option<[u8;16]>,
  pub(crate) amount_commitment: CompressedRistretto,
  pub(crate) asset_type_commitment: CompressedRistretto,
  pub(crate) blind_share:  CompressedEdwardsY,
  pub(crate) lock_amount: ZeiCipher,
  pub(crate) lock_type: ZeiCipher,
  pub(crate) public_key: XfrPublicKey,
}
```

lock_amount 和 lock_type 是资产记录字段 *amount* 和 *type* 分别的加密值. 它们在资产记录拥有者 (即接收者地址) 的公钥 public_key 项下加密。

加密学承诺是完美隐藏信息的，这使它们与加密 (encryption) 不同。它们不包含任何可以由具有密钥的人解密的信息。相反，它们可以被用作被提交信息的隐藏指纹，类似于服务器在共享文件之前如何发送文件的散列值。散列值是可以从文件中测量的独特指纹，但无法从散列值中获取文件。加密承诺只能是通过获得那个被提交的独特信息和一个称为盲因子的秘密值来 “打开” 或 “去盲化”。如果 C 是使用盲因子 r 对消息 m 的加密学承诺，则 C 可以通过获得 m 和 r 唯一的计算出来，r 是对于 C 是 m 的加

密承诺的证明。在 Findora 的盲化资产记录中，使用类似于 Diffie-Hellman 密钥交换的方法与新的资产所有者（即转移接收者）共享盲因子。此用户从 blind_share 及其对应于 `public_key` 的私钥中获取盲因子。用户需要这些盲因子以检查记录的解密内容是否正确（即，经验证者节点批准），并且还需要使用它们 (盲因子) 来在未来的交易中转移资产的所有权。

```
pub struct OpenAssetRecord{
  pub(crate) asset_record: BlindAssetRecord,
  pub(crate) amount: u64,
  pub(crate) amount_blind: Scalar,
  pub(crate) asset_type: AssetType, //type AssetType = [u8;16]
  pub(crate) type_blind: Scalar,
}
```

`XfrProofs` 包含一个零知识证明，即证明盲化输出记录对于盲化输入记录是有效的。具体来说，它证明输出记录中每种资产类型的输出金额总和等于输入记录中相同资产类型的输入金额之总和。更精切地说，如果有 n 个输入记录和 m 个输出记录，并定义了以下变量：：

- α_i is the amount in the ith input record
- β_j is the amount in the jth output record
- $\mathsf{In}[t]$ is the set of input indices with asset type matching t
- $\mathsf{Out}[t]$ is the set of output indices with asset type matching t
- $\mathcal{T}$ is the complete set of types among the output records

则 `XfrProofs` 证明:

$$\text{For all } t \in \mathcal{T} \sum_{i \in \mathsf{In}[t]} \alpha_i = \sum_{j \in \mathsf{Out}[t]} \beta_j$$

当我们接下来解释加密承诺、范围证明 (Bulletproofs) 和 Pedersen 等式证明时，我们将仔细研究 `XfrProofs` 的解剖结构。

最后，`XfrNote` 仅在每个输入 `BlindAssetRecord` 正确引用之前的交易在分类帐本上创建的现有有效记录时才有效。因此，封装 `XfrNote` 的交易还必须包括对先前交易中的资产转移 (帐) 注释的引用。这些引用称为交易输出序列 ID（TxoSID）。

```
pub struct AssetTransferBody {
  pub inputs: Vec<TxoSID>,
  pub transfer: Box<XfrNote>,
}
```

可以访问整个分类帐本的全功能验证者节点使用每个 ith TxoSID 在先前的`XfrNote`输出中查找`BlindAssetRecord`并检查它在当前交易的`XfrNote`中是否与 ith`BlindAssetRecord`匹配。验证者节点还检查 TxoSID 是否仍然有效。一旦一个 TxoSID 在交易中被使用了，它就变为无效（即记录为被“消耗”）。

2.4.1 数学背景

有限群 在 Findora 中用于保密传输的加密协议需要一个素数阶的有限群作为工具，其中某些计算问题很难解决。有限群 $\mathbb{G}$ 是一个有限集合，对集合中的元素预定义了群组操作。我们使用“+”符号来表示一对群组元素之间的操作。对集合中任何两个元素的操作给出了集合中的另一个元素。有一个唯一的“0”元素，这样对于任何 $g \in \mathbb{G}$，$0 + g = g$。每个元素 g 都有一个反向元素，表示为 $(-g)$，这样 $g + (-g) = 0$。群的阶是集合中元素的数量。加模数 n 下的整数是一个群组的阶 n 的简单示例。这个群组用 $\mathbb{Z}_n$ 表示，包含所有小于 n 的整数。n 的互质整数是整数乘法下的一个群组，表示为 $\mathbb{Z}_n^*$。素数 p 的整数集 $\{0, ..., p-1\}$ 是加法项下数组 $\mathbb{Z}_p$，如果我们排除 0，则也是乘法项下数组 $\mathbb{Z}_p^*$。具有此属性的群组称为有限字段，此字段表示为 $\mathbb{F}_p$。

椭圆曲线群 通过在有限域上定义的曲线上查看 *points*，可以构建更高级的数群。p 之上的椭圆曲线 E 由 $y^2 = x^3 + ax + b \bmod p$ 形式的等式定义，其中 $a, b \in \mathbb{F}_p$。椭圆曲线组 $\mathbb{G} = E(\mathbb{F}_p)$ 由满足此等式的所有点 $(x, y) \in \mathbb{F}_p$ 组成，并且有一个群组操作可插入任意两个点以找到在该曲线上的第三个点。Findora 使用名为 Curve25519 的曲线，它使用素数 $p = 2^{255} - 19$ 和曲线方程 $y^2 = x^3 + 486662x^2 + x$。

商群 另一种类型的群组称为*商群*，可以构建在现有群组 $\mathbb{G}$ 之上，该群组具有一种特殊类型的子群 $N \subset \mathbb{G}$，称为*正规*子群。子群 N 是 $\mathbb{G}$ 的子集，也是同一操作下的一个群组。如果对所有 $g \in \mathbb{G}$ 和 $h \in N$，元素 $g + h + (-g)$ 被包含在 N 中，则 N 是正规的。在可交换群组中，操作顺序无关紧要，每个子群都是正规的。给定正规的子群 N 和 $\mathbb{G}$，商群 $\mathbb{G}/N$ 是通过形成 $\mathbb{G}$ 的分区而产生名为*等价类*的一些子集来构建的。这里有两个元素 $a, b \in \mathbb{G}$ 放在同一个等价类中，当且仅当 $a - b \in N$。这些等价类是 $\mathbb{G}/N$ 群的新元素，通过从每个等价类中挑选一个元素来“代表”该类来表示。如果 $\bar{a}$ 和 $\bar{b}$ 是两个代表性元

素，则群操作会为 $c \in \mathbb{G}$ 查找代表元素 $\bar{c}$，其中 $c == \bar{a} + \bar{b}$。如果 $\mathbb{G}$ 拥有阶 m 而且 N 拥有阶 n，则 $\mathbb{G}/N$ 拥有阶 m/n，该阶总是一个整数。

Ristretto 群 Findora 使用 Ristretto 群，这是一个由 Curve25519 上的椭圆曲线组构建的商群。Curve25519 上的椭圆曲线群的素数阶为 $8p$:

$$p = 2^{252} + 27742317777372353535851937790883648493$$

Ristretto 商群是从阶 8 的正规子群构建的，因此具有素数阶 p[6].

抽象符号 为描述加密学协议目的，我们将在 Ristretto 群中使用以下符号进行操作。我们使用 $\mathbb{G}_p$ 来表示 Ristretto 群。$\mathbb{G}_p$ 中的元素（由 Curve25519 上的点表示）用大写字母表示，例如 $A, B \in \mathbb{G}_p$。小写字母用于表示 $\mathbb{F}_p$ 中的元素，也称为 “标量”。

- 群加法: $C \leftarrow A + B$ 是 $\mathbb{G}_p$ 中的组操作，取两个代表性曲线点 A B 并返回第三个代表性曲线点 C。
- 标量乘法: aC 表示 $\mathbb{G}_p$ 的一个元素，通过使用群添加操作将 a 个 C 加在一起获得，其中 $a \in \mathbb{F}_p$ 被解释为小于 p 的正整数。

离散对数问题（DLP） 在 $\mathbb{G}_p$ 群中解算 DLP 的一个算法是给出 $G \in \mathbb{G}_p$ 中的一个非零元素和随机元素 $H \leftarrow_R \mathbb{G}_p$ 并继续输出 $a \in \mathbb{F}_p$，这样得出 $aG = H$，概率不可忽略。人们普遍认为 DLP 在 Ristretto 群中计算难度很大，即目前的计算能力不存在 DLP 的有效算法。[7]

决策性 Diffie Hellman (DDH) 如果计算上难以将元组 (aC, bC, abC) 与元组 (aC, bC, rC) 通过随机选择的 $a, b, r \in \mathbb{F}_p$ 和任意元素 $C \neq 0$ 区分开来，则该素数阶群具有 DDH 安全属性。众所周知，Ristretto 群拥有当前计算能力下的 DDH 属性。DDH 属性是一个比 DLP 更强的安全假设，因为解决 $\mathbb{G}_p$ 中的 DLP 破解 DDH 属性。

2.4.2 Pedersen 承诺

Pedersen 承诺是一个群元素 $C \in \mathbb{G}_p$，它以加密方式绑定到标量 $m \in \mathbb{F}_p$，但完全隐藏了 m。标量 m 可以使用任何合适的加密抗冲突哈希函数 $\mathsf{Hash} : \{0,1\}^* \rightarrow \mathbb{F}_p$ 来编码任意的消息。该哈希函数将数据字符串映射到字段 $\mathbb{F}_p$

[6]关于 Ristretto 群的更多信息请参看`https://ristretto.group/`

[7]但是，如果量子计算变得实用，DLP 将在任何数群（包括 Ristretto 群）中被有效解决

元素 C 是使用 m 以及一个额外的随机标量盲因子 r 以独特的方式生成。因此，给定 m 和 r，很容易验证 Pedersen 承诺 C 是否是正确生成的输出。只要 DLP 在 $\mathbb{G}_p$ 中很难破解，m 和 r 生成的 Pedersen 承诺就会在计算学意义上绑定消息 m。找到替代输入值 m' 和 r' 以让 Pedersen 承诺产生相同的点 C，难度等同于在 $\mathbb{G}_p$ 中有效解决 DLP。

Pedersen 承诺具有如下组成部分:

- PedersenSetup: G, H are randomly generated “base points" in the group $\mathbb{G}_p$.
- PedersenCommit$(m) \to (C, r)$: The input is $m \in \mathbb{F}_p$ and the output is $mG + rH$ for a random $r \leftarrow_R \mathbb{F}_p$.
- PedersenOpen$(C, r, m) \to (r, m)$: The opening of a commitment C are a pair of values m, r for which it can be verified that $mG + rH = C$.

同态加法 可以使用 $\mathbb{G}_p$ 中的群操作添加两个 Pedersen 承诺 $C_1 = m_1G + r_1H$ 和 $C_2 = m_2G + r_2H$ 以形成新承诺 $C_3 = C_1 + C_2$。元素 C_3 是对 $m_1 + m_2 \bmod p$ 的承诺，其盲因子为 $r_1 + r_2 \bmod p$。

证明承诺等效 为了证明两个 Pedersen 承诺 C_1 和 C_2 提交至相同的标量值 $m \in \mathbb{F}_p$，我们可以使用所谓的 Schnorr 证明。Schnorr 证明是一个离散对数知识的零知识证明。鉴于 $C = aG$，一个 Scnorr 证明能证明证明者（即生成证明的算法）必须具有 a，使得 $aG = C$，但证明并未显示有关 C 的任何其他信息。

需要注意的是，如果 $C_1 = mG + rH$ 和 $C_2 = mG + r'H$ 那么 $C_1 - C_2 = (r - r')H$。C_1 和 C_2 承诺相同值的零知识证明仅仅是 $C_1 - C_2$ 基数为 H 的离散对数的 Schnorr 证明，即它证明了知道值 r^* 而 $C_1 - C_2 = r^*H$。如果证明者知道值 (m, r, r') 开 C_1 和 C_2 到 m 那么它就知道 $r^* = r - r'$ 并且能够成功创建这个证明。另一方面，如果证明者能够开 C_2 到 (m', r') 那么 $m' \neq m$ 并且仍然成功创建这个零知识证明中，那么它必然知道值 $z = (m - m')(r^* - r + r')^{-1}$ 这样 $zG = H$。换句话说，这个证明者可以有效地解决 $\mathbb{G}_p$ 中的 DLP。因此，只要 DLP 在 $\mathbb{G}_p$ 中计算难度很高，就不会发生这种情况。

公开输入 $A = aH$ 和 H 含私密输入 $a \in \mathbb{F}_p$ 的 Schnorr 证明包含两个标量 (z, c)，形式如下:

1. Randomly sample $r \leftarrow_R \mathbb{F}_p$
2. $c \leftarrow \mathsf{Hash}(A, H, rH)$

3. $z \leftarrow ac + r \bmod p$

证明 $\pi = (z, c)$ 是通过检查 $c = \mathsf{Hash}(A, H, zH - cA)$ 来验证的。

批量等式证明 给出承诺 $C_1, ..., C_n$，证明每个 C_i 提交到相同的标量值 m 相当于证明每个 C_i 提交到相同的值 C_1。这样减少工作量为证明知道每个 $D_i = C_1 - C_i$ 基数为 H 的离散日志。有一个优化，用来避免为每个 D_i 生成 n 个单独的 Schnorr 证明。假设 $D_i = a_i H$。给出标量 $\beta_1, ..., \beta_n$，证明者知道 $D = \sum_{i=1}^{n} \beta_i D_i$ 基数为 H 的离散日志，这就是值 $a = \sum_{i=1}^{n} \beta_i a_i$。此外，如果在承诺 $C_1, ..., C_n$ 给出之后随机选择这些标量，那么不知道至少一个 D_i 基数为 H 的离散日志的证明者将无法解决 D 基数为 H 的离散日志除非概率可以忽略不计。重要的是 β_i 是独立随机的，不能是任意的。例如，如果 $D_0 = m_0 G + r_0 H$ 和 $D_1 = m_1 G + r_1 H$ 使得 $\beta_0 m_0 + \beta_1 m_1 = 0$ 那么证明者知道 $\beta_0 D_0 + \beta_1 D_1 = (\beta_0 r_0 + \beta_1 r_1) H$。[8]

批量等式证明使用 Fiat-Shamir 启发式算法并使用散列函数导出系数 β_i。假设证明者知道 $C_i = m_i G + r_i H$，则生成批量等式证明的步骤是:

1. Set $\beta_i = \mathsf{Hash}(C_1, ..., C_n, i)$.
2. Compute $D = \sum_{i=1}^{n} \beta_i (C_i - C_1)$
3. Provide a Schnorr proof for D base H, i.e. $D = aH$, using knowledge of $a = \sum_i \beta_i (r_i - r_1) \bmod p$.

证明的大小尺寸是一个单个 Schnorr 证明，即两个标量。此证明的验证者还执行上面的前两个步骤，使用定义的散列函数从输入中导出 D，然后验证 Schnorr 证明。

范围证明 (Bulletproof) 范围证明是零知识证明，Pedersen 承诺 C 提交到标量 m，该标量是整数，范围为 $[L, R]$，即 $L \leq m \leq R$。Findora 的保密转账需要 $m \in [0, 2^{64}]$ 的范围证明。我们的范围证明使用 Bulletproofs [9]，一个专门的零知识证明系统。与 zk-SNARKs 不同，Bulletproofs 不依赖于可信和复杂的设置。Bulletproofs 特别适用于范围小的范围的证明：64 位范围的证明小于 $1KB$ 并且创建和验证只需几毫秒。Bulletproofs 具有批处理模式，其中 m 点的范围证明仅比单点范围证明大 $64\log(m)$ 字节（例如，100 点的批量证明仅大了不到 500 字节）。Bulletproofs 还具有批量验证模式，其中验证许多范围证明的摊销时间约为每个 0.34 毫秒。

[8]此非正式描述仅提供了协议为何安全的直觉判断。本协议有一个正式的安全证明。

[9]Benedikt Bünz，Jonathan Bootle，Dan Boneh，Andrew Poelstra，Pieter Wuille 和 Greg Maxwell。*Bulletproofs*：保密交易的简短证明及其他。 In Bulletproofs：保密交易的简短证明，p. 0，IEEE，2018.

2.4.3 `BlindAssetRecord` and `XfrProofs`

现在我们已经介绍了构建块，我们将更详细地描述 `BlindAssetRecord` 中的承诺和 `XfrProofs` 中的零知识证明。

`amount_commitment` 和 `asset_type_commitment` 是对 Ristretto 群 $\mathbb{G}_p$ 的 Pedersen 承诺。接收人的公钥也是元素 $P \in \mathbb{G}$，其中包含相应的私钥标量 s，使得 $P = sG$。元素 G 与 Pedersen 承诺设置参数中指定的公共基础相同。

当用户在交易中创建盲化资产记录时，用户会对名为 *blinding key* 的随机标量 $k \in \mathbb{F}_p$ 进行采样，并导出盲因子 $r_0 \leftarrow \mathsf{Hash}(kP, 0)$ and $r_1 \leftarrow \mathsf{Hash}(kP, 1)$。`blind_share` 是元素 kG。接收人 (即资产记录所有者) 可以使用密钥 s 和 `blind_share` 导出 $kP = skG$，因此可以恢复盲因子。

`XfrProofs` 的结构如下:

```
pub struct XfrProofs{
  pub(crate) range_proofs: Option<BatchRangeProof>,
  pub(crate) equality_proof: EqualityProof,
  pub(crate) asset_proof: Option<BatchEqualityProof>
}
```

输出的范围证明 `range_proofs` 是一个 Bulletproofs 批量化范围证明，转移交易的输出盲化资产记录中的所有金额承诺都是对 64 位整数的 Pedersen 承诺。使用 m 输出此证明的大小约为 $700 + 64\log(m)$ bytes).

等式证明 给定所有输入盲化资产记录的资产金额承诺 $C_1, ..., C_n$ 以及所有输出盲资产记录的资产金额承诺 $C'_1, ..., C'_n$，定义 $C = \sum_{i=1}^{n} C_i$ 和 $C' = \sum_{i=1}^{m} C'_i$。设 $T_1, ..., T_n$ 表示输入的资产类型承诺，$T'_1, ..., T'_m$ 表示输出的资产类型承诺。`equality_proof` 包含一个 Pedersen 等式证明，C 和 C' 提交到相同的标量值。`asset_proof` 包含批处理 Pedersen 等式证明所有 T_i 和 T'_i 提交到相同的值。

2.5 智能合约

智能合约是由分布式分类帐本上的交易驱动的动态程序。智能合约的状态也存储在分类帐本中。特别是，智能合约可用于编码交易对手之间复杂的金融关系，其寿命超过单次一次性交易。从本质上讲，智能合约定义的规则决定了智能合约的状态如何受到分类账本上交易的影响，以及这种状态如何反过来触发交易。对于编程智能合约，基本操作码指令集解决了软件共识问题：用任意代码编写的合约可能导致歧义，并且不同的验

证者节点可能主张不同的解释。在一组基本操作码上同步的验证者网络被用作编写更复杂合约的“虚拟机”。这在以太网中尤其重要，网络中的任何人都可能是验证者。以太坊拥有“图灵完备”操作码集，意味着可以从操作码集构建任意程序。

但是，金融合约通常是专门的程序，不需要图灵完备语言来编码。此外，当合约仅由相对较小的验证者网络子集强制执行时，自定义的软件共识更加可行。Findora 认为，特定合约的自定义操作码只需要分发给该合同的一组自定义验证者节点。合约的参与者将能够自己确定他们是否信任合约验证者的某个多数阈值。此合约的自定义验证者集根据其独立验证协议的结果发出多签名交易。这使得“图灵完备”合约能够在仅支持基本多签名合约的基础分布式分类账本上运行。[10]

智能合约和智能账户 *智能资产*是智能合约的特殊案例，它将条款附加到特定资产通证上，并通过资产制度规范这些资产的转移。有关证券通证术语在下一节将进行更详细的讨论。*智能帐户*是有状态帐户，即保留不同资产和其他动态数据的余额，但另外还有限制交易更新帐户状态的制度。帐户制度是布尔函数，采用帐户的当前状态和新交易作为输入。验证者节点检查帐户制度确保任何更新给定帐户状态的交易须返回 true，并在制度返回 false 时拒绝该交易。

由于交易可以将多个操作捆绑在一起（例如，同时影响多个帐户），因此仅通过批准将适当操作捆绑在一起的交易（例如，要求更新帐户余额与向运营者节点自动付费捆绑），帐户制度可用于“触发”其他交易以响应帐户更新。*智能合约*进一步通用化智能帐户，因为它们是存储在分类帐本上的动态有状态程序，并运行任意代码来确定状态转换。如上所述，智能合约可以指定一组目标托管人，其以阈值多签名的形式批准对合约的状态改变。这些多签名合约可以运行任意代码，因为主要网络验证者节点只需要验证签名。最后，Findora 具有*原生智能合约*，它不指定托管人并由整个验证者节点网络处理。

2.5.1 原生智能合约

Findora 中的一个重要特色产生在*有状态*和*无状态*智能合约之间。有状态合约比无状态合约更具表现力，但存在给网络验证者节点带来高计算量和存储负担的风险。无状态合约是一种特殊的智能合约，没有任何动态状态。相反，智能合约程序定义了一个在一组交易捆绑输入上运行的布尔函数。如果程序返回 true，那么交易捆绑输入组将以原子方式执行并附加到分类帐本的交易日志中。资产通证和智能资产的制度是无状态智能合约的例子。最终交易组还引用了智能合约程序，它是 Findora 分类帐本上的内容可寻址静态数据对象。验证交易捆绑组需要在捆绑组上运行合约程序并检查合约程序的结果。

[10]在 Hyperledger 和 Corda 中使用了类似的概念。

在正常的交易操作中，使用变量和前提条件也可以实现无状态智能合约功能。对于许多用例，在交易上放置变量和前置条件足以完全通过原生交易操作来模拟所需的智能合约行为。无状态合约在可扩展性方面要好得多，并且在可以避免使用有状态合约时应鼓励使用。

变量地址和前提条件 可以在交易中定义变量和前提条件。一项操作可以指定变量目标地址 $[x]$，例如 “从地址 A 转移 100RMB 到 $[x]$”，然后是变量 $[x]$ 必须满足的令该操作有效的前提条件列表。前提条件可能包括：

- Ops: 涉及相同地址 [x] 的其他操作。这些操作必须包含在同一交易的操作列表中。
- Records: 包含在交易输入中的资产记录。前提条件可能需要特定的资产记录并完全指定此记录的内容，或者更通用化的将一些资产记录字段保留为变量，并指定资产记录输入必须满足的资产制度。
- Policy: 资产制度适用于操作或输入记录中引用的变量。支持的原生本机制度包括操作或记录中的地址变量的资质凭证要求，以及转账额变量的算术表达式。评估资产制度可能需要辅助输入，例如资质凭证证明或其他保护隐私的合规性证明。

在伪代码中，具有可变地址 $[x]$，可变金额 $[y]$ 和前提条件的示例操作是:

```
Operation A {
Transfer from addrA to [x] 300 RMB tokens
preconditioned on
  Op: Transfer from [x] to addrA [y] TCEHY tokens
  Policy: A credential proof that [x] is accredited
  Policy: y >= 1
}
```

验证者节点通过扫描操作列表并替换变量来处理具有变量和前提条件的交易，直到每个交易的所有前提条件得到满足。对于上面的示例，假设已将新操作 B 添加到交易操作列表中:

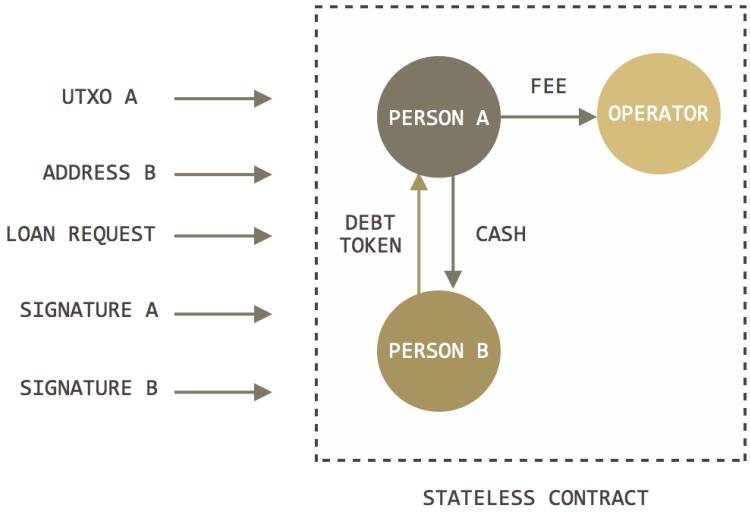
```
Operation B  {
Transfer from addrB to [x] 1 TCEHY tokens
preconditioned on
  Op: Transfer from [x] to addrB [y] RMB tokens
  Policy: y > 275
```

```
<proof of addrB accreditation>
}
```

当一个验证者节点一起处理操作 A 和操作 B 时，替换变量，这解析为:

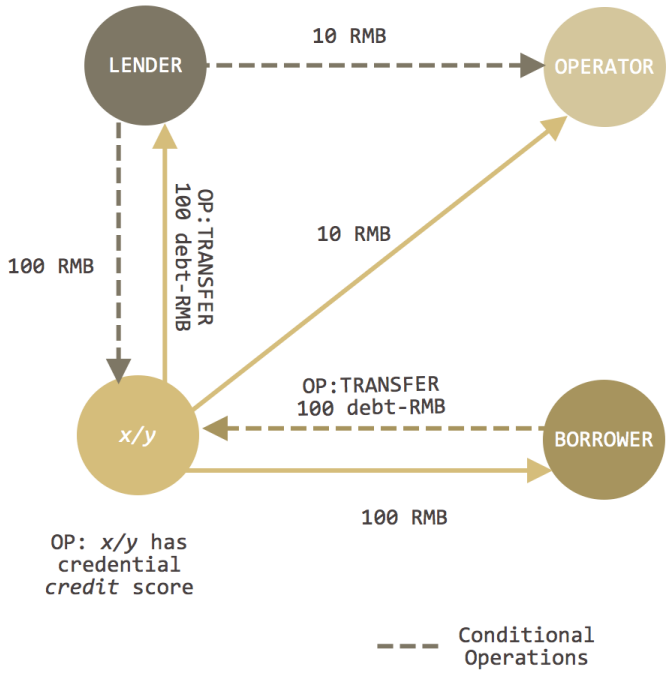
```
Transfer from addrA to addrB 300 RMB
Transfer from addrB to addrA 1 TCEHY
```

案例 1: 用于贷款匹配的无状态智能合约 一个无状态智能合约可用于执行贷款平台的基本功能。



合同首先检查贷款请求是否与贷款质押相匹配，签名是否有效，输入记录（即 UTXO A）是否有足够的资金来支付贷款。如果满足所有条件，则（1）从地址 A 支付到地址 B，（2）向运营商支付 1% 的费用，以及（3）从 B 到 A 发行债务通证。与正常交易不同，因为最终交易是由智能合约本身“发行”的。验证其中一个交易需要检查合约程序的结果。最终交易包括合约输入，合约输出和智能合约程序的引用，智能合约程序是可以在分类帐本上查找的内容可寻址数据对象。由于没有中间状态，只有最终的智能合约发布的交易会影响永久分类帐本存储。验证流程只检查输入，运行程序，并检查输出的有效性。

案例 2: 含变量和前提条件的贷款匹配 具有变量和前提条件的交易可用于实现贷款平台的简单贷款匹配功能。这些交易避免了定义任何智能合约程序的需要。

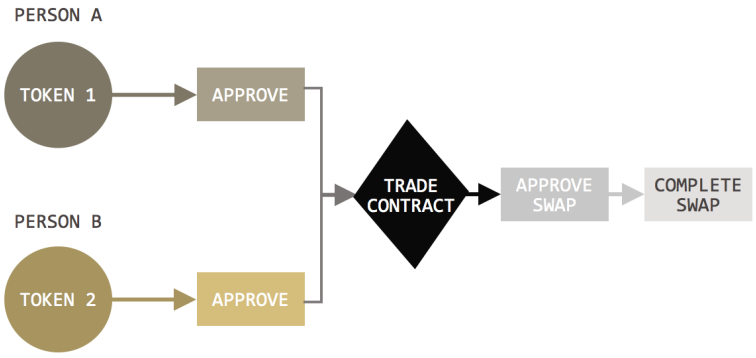


贷款要约是已签署的转让操作，其中包含从地址 A 到可变地址 [x] 的 100 元人民币的转账以及向运营商地址 C 转账 10 元人民币的转账，这两项转账都是以第二个操作为前提条件下进行的，第二个操作包含从地址 [x] 到地址 A 转移 100 RMB 债务通证，以及地址 [x] 具有足够信用评分的凭证证明。上述人民币债务通证包含有关贷款偿还时间表和利息的条款。

贷款请求是提交给网络的已签名转移操作，从地址 B 转移到变量地址 [y]100RMB 债务通证，以第二个操作为前提条件，该操作将 100 元 RMB 转移到地址 B。在转移操作的备忘录 (memo) 字段中包含一个证明，证明地址 B 属于一个具有足够信用评分的借款人。

贷款平台运营商收集贷款请求和贷款要约已签署的操作，并将它们一起打包成有效的交易。当打包在一起时，两个操作的前提条件相互满足。经网络验证后，本次交易将从地址 A 向地址 B 发送 100 元人民币，向运营商发送 10 元人民币，并从地址 B 向地址 A 发送 100 人民币的债务通证。

案例 3: 原子交换 原子交换是一种分类账本交易，允许双方同时交易两个不同的通证，这样就不存在一方违约的风险。



在此交易中，A 和 B 的通证被批准并用作交易合约的输入项，该交易合约从 A 转移到 B 类型 1 的通证（A 保证有），从 B 转移到 A 类型 2 的通证（B 保证有）。A 和 B 使用签名作为他们拥有这些通证的证明。执行合约时，会发生原子交换，因为合同中的两个交易都被执行（通证类型 1 的 A 到 B，通证类型 2 的 B 到 A），允许双方以最小的违约风险交换两个不同的通证。

2.6 证券通证条款

限制证券通证转移的条款可以在通证的定义中普遍化编码，也可以通过智能合约在自定义的基础上强制执行。第一类条款由基础层分类账本协议的验证者节点处理。例如，证券通证发行者可以在通证的定义中放置资质凭证要求，规定所有通证持有者必须具有来自指定的一组 KYC 权威的认可批准。将此通证从一方转移到另一方的任何交易都需要来自接收人的特殊签名来证明该资质凭证。

定制化执行条款更适合投资基金中的资产组合，这些资产根据投资条款进行管理。这些条款显然取决于基金的类型，同一基金的投资者也可能有不同的条款。例如，在私人投资基金中，条款可以规范和限制转移，管理锁定或将被授权投资者列入白名单。在共同基金中，条款可以限制对特定资产类别的投资，限制风险或规定最低现金余额。

2.7 合规

通过利用零知识证明，选择性身份证明披露和隐私保护计算，Findora 能够同时提供隐私和透明度. 这些加密技术为以前无法实现的更有效的监管提供了新的可能性，而不会影响用户隐私。从功能上讲，这意味着基金可以通过加密方式向监管机构证明他们的合规运作（例如通过使用偿付能力证明），而无需披露其行为或投资的细节。

2.8 隐私保护合规工具

Findora 设计的基石价值之一是允许各种级别的透明度，同时保持机密性。例如，Findora 赋能智能投资基金向监管机构提供对一般基金信息（资产，持股，投资者资质凭证）的可见性，同时保密其他选定的基金相关数据（投资活动，投资者，条款等）。高级加密技术精确地完成了同时实现透明度和机密性的任务。

我们使用的两种最相关的加密技术是*零知识证明*和*多方计算*。零知识（ZK）证明是一种技术，用于表明陈述是真实的，而不会泄露除陈述有效性之外的任何其他信息。ZK 证明也可用于证明秘密的*知识*，例如解锁帐户的密码，而不会泄露密码本身。与 ZK 证明类似，安全多方计算（MPC）支持一组参与方共同学习输入计算的输出，而不会相互揭示有关私密输入的任何其他信息。例如，MPC 可用于进行秘密投标拍卖，而不依赖于受信任方来收集投标。

通常，MPC 要么需要多轮交互，要么要求进行成本昂贵的计算，例如完全同态加密，因此对于智能合约的实施是不切实际的。但是，SIF 将使用足以满足 Findora 用例的专用高效 MPC 协议（例如，保持基金的资产负债表保密）。

保密支付 基本保密支付是在一个以某种通证单位计价的交易中，该交易将隐藏金额从一个地址/账户转移到另一个地址/账户，但整个系统仍然可以公开验证交易的有效性。

保密资产转移 保密资产转移使用加密承诺隐藏发送和接收账户中持有的资产的详细信息（例如类型和余额），并使用零知识证明来证明这些承诺是根据资产转移规则正确更新的，例如新余额的总和等于旧余额的总和，两者的余额都没有出现负数。当资产类型保密时，证明还必须证实在相同资产类型标识符下的两个帐户中更新了余额，而不显示此标识符。我们的实施使用了 Pedersen 承诺，ElGamal 加密，Bulletproofs 等技术组合[11], and Σ-Bullets[12]. 这些密码学证明在 Findora 技术实现下的生成和验证是毫秒级的。

偿付能力证明 一个偿付能力证明[13] 表明由基金或交易所等实体拥有的资产支持通证的价值超过其负债 (例如对投资者的总负债)。当产生证据的实体持有的资产是保密的，即

[11]B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell.*Bulletproofs: Short Proofs for Confidential Transactions and More.* https://eprint.iacr.org/2017/1066.pdf.

[12]B. Bünz, S. Agrawal, M. Zamani, and D. Boneh. *Zether: Towards Privacy In a Smart Contract World.* 2018.

[13] Dagher, Bünz, Bonneau, Clark, and Boneh. *Provisions: Privacy-Preserving Proofs of Solvency for Bitcoin Exchanges*, 2015. http://www.jbonneau.com/doc/DBBCB15-CCS-provisions.pdf.

以加密承诺方式隐藏时，该工具尤其重要。偿付能力证明背后的通用技术采用一组标记为负债的账户或交易以及一组标记为资产的账户，并生成了解控制资产账户的密钥的零知识证明，以及证明这些资产余额的总和（按类型加权）超过负债余额总和。

白名单资产的证明 这证明了交易中涉及的保密资产的标识符包含在不显示标识符本身的白名单集中。例如，白名单可以保存在 Merkle 树中，并且证明该标识符包含在树中的零知识证明。

余额范围证明 该工具使用 Bulletproofs 来证明账户或交易中包含的余额的范围，例如投资账户的最低余额或交易中转移金额的上限范围。

权限特定的查看密钥 监管机构可以被授予解密用户帐户或交易内容的密钥，这些密钥不能用来代表用户发布交易 (即只读密钥而不是启用写入的签名密钥)。查看密钥也可以附加到合规性证明，例如偿付能力证明或列入白名单资产证明。这些密钥可以向授权监管机构披露比零知识证明结果更详细的信息，但仍然没有透露个人账户的所有细节。如果有可信的硬件执行环境可用，那么这些工具也可用于实现高度细粒度的特定功能的查看密钥。[14]

保密多源支付 虽然保密转账对公众隐藏交易中转移的金额，但此金额始终会向接收人显示。考虑从多个独立来源向收件人的多方付款。从收件人隐藏从每个来源转移的金额并仅显示总金额可以通过来自*线性秘密共享*[15]。这是一个两轮协议，在第一轮中，每个源将其输入分成线性秘密共享，每个源一个。在第二轮中，来源计算他们从其他来源收到的分享的总和，并公开发布其本地计算的结果。最终的总和可以从这些输入中得出。为了使最终的总和对公众保密，接收者也可以参与秘密共享方案，以便只有接收者才能揭露最终总和。此外，如果基础保密支付使用同*态承诺方案* (例如 Pedersen 承诺)，则可以有效地修改 MPC，以便保证接收方知道它所获知的最终总和是否正确。

保密资产追踪 此工具使资产发行人能够跟踪其资产并查看涉及这些资产的所有交易的详细信息，即使这些资产对公众是保密的。例如，对于希望能够在任何给定时间点看到公司所有股东的股权公司而言，这可能很重要。证券通证转移条款与零知识证明相结合，

[14]Ben A Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. *Iron: Functional encryption using Intel SGX.* CCS 2017.

[15]A k-of-n linear secret sharing of a value x splits it into n parts [x]1,...,[x]n such that any k - 1 shares reveal no information at all, yet any k shares are sufficient to reconstruct the value x.

可以创建保留此跟踪器的资产，而无需与发行方进行交互。发行人可以在任何时间点上线并解密具有此跟踪器的所有转账交易的详细信息。

隐私保护计算 可以使用 MPC 实现的隐私保护计算的其他示例包括密封投标拍卖和订单簿匹配，其中出价和要价的值被隐藏直到匹配以防止提前交易 (Front Running)。这些计算需要的可不仅仅是上面描述的极轻量级的两轮秘密共享技术。

用于一般功能的最先进的 MPC 协议采用若干方法来减少限制实际部署的计算成本和轮次交互。一种方法是将大部分计算和交互提前到“预处理阶段”，该“预处理阶段”在所涉及的各方之间分配设置信息，以准备“在线阶段”，其中各方重复地对私人输入执行有效的隐私保护计算。另一种方法是将维护隐私的责任转移到分布式的“第三方”服务器上，只要存在至少一个“诚实”的非串通服务器，就可以保持隐私。

3 Findora 基础层

基础层是 Findora 的核心功能层，支持 Findora 的公共金融分类账本。Findora 基础层中的主要运营代理是验证者节点，网关，归档节点和数据提供节点。网关为用户提供了发送交易的入口点。（交易是 Findora 分类账本上的任何已请求的修改，使用 Findora 的交易 API 发布）。验证者收集并验证从网关广播的交易，并通过基础共识协议就确认的交易达成一致。数据提供者确保公共用户具有对分类帐本的经过身份验证的查询访问权限。归档节点确保永远不会遗失历史分类帐数据。

Findora 主分类账本的验证者节点运行 Finsense 共识算法来向分类账本提出并确认交易。分类帐本本身是财务记录的公共数据库，可由网络中的所有节点访问。记录可以包括加密和未加密的内容，并且不同的方（例如监管者或消费者）可以具有关于分类帐本内容的不对称信息，例如用于解密分类帐上的某些内容的密钥。更新这些记录的所有交易都是不可改变的记录。Findora 平台还提供帐户信息的链下可验证存储功能。分类帐数据存储具有容错性和永久性。

3.1 经验证的分布式账本

基础层的核心是共享的*经验证的数据结构*（*ADS*）[16]用来存储一组帐户，每个帐户的当前状态以及分类帐本的更新历史记录。每个帐户都引用一个类型余额对列表，其中

[16]Andrew Miller, Michael Hicks, Jonathan Katz 和 Elaine Shi。*Authenticated Data Structures, Generically*。POPL，2014。https://www.cs.umd.edu/ mwh/papers/gpads.pdf。

“类型”是资产描述，“余额”描述帐户中的资产余额。此分类帐本上的每个帐户都与公钥相关联。ADS 具有表示其当前状态的标签以及每次更新的标签历史。有一个生成可验证证据的程序，称为成员见证，分类帐本历史的任意部分与此标签一致。ADS 对分布式设置具有多种效率优势：

1. 验证网络中的所有节点是否就分类帐本的状态/历史记录达成一致只需要比较短数据标签。
2. 用户（不存储整个分类帐本的数据）可以从网络中的单个节点检索分类帐本的一部分以及验证证明它是正确的并且与在网络中的每个其他节点上复制的相同分类帐本一致。
3. 用户可以向分类帐本提交更新（即一个交易），并从网络中的任何节点获取一个短证书，该证书证明更新已被合并到分类帐本的新状态中。

有许多方法可以构建 ADS，每种方法都有自己的细微差别和优势。Findora 的基础层使用基于加密累加器的新 ADS [17] 这消除了存储和内存瓶颈，并通过完全解耦共识和存储来提高吞吐量。

3.2 保密交易

提交给分类帐协议的交易一般以原子交易方式批处理执行一个或多个帐户操作。交易中每个操作所需的签名还必须签署整个交易的摘要。这保证了事务中的各个操作不能单独重放（非原子地）。

交易还可以包括前提条件，一个逻辑表达式，其输入取决于分类帐的状态。例如，前提条件可以评估交易之间是否已经过了一定的时间。前提条件必须解析为 true 才能使交易有效。相同的交易可以多次广播直到满足前提条件。这使得相互不信任的用户能够以原子交易方式链接他们的交易。

基本的保密交易隐藏了交易中交换的值。保密性是与匿名性非常不同的隐私性目标，匿名性也隐藏了交易中涉及的帐户的身份。使用 Pedersen 承诺和零知识证明的组合，保密支付被引入了比特币分类账本模型。[18] Findora 为隐私目标（保密性和匿名性）实现了可扩展的解决方案。重要的是，Findora 将身份证明与保密交易集成在一起，这样即使

[17] Dan Boneh, Benedikt B u nz 和 Ben Fisch。应用于 *IOP* 和无状态区块链的累加器批处理技术。Crypto, 2018。

[18] G.Maxwell。保密交易。https://people.xiph.org/ greg/ confidential $_v alues.txt$ 2016

匿名地址也可以唯一地绑定到身份/资质凭证上，这可以被选择性地显示出来。这样，分类账本的审计者（例如，监管者与公共用户）可以根据他们已经获得的访问密钥对交易方的身份具有不同程度的可见度。

3.3 多签名账户

一个多签名帐户是由一组分布式存在的所有者控制的帐户。每一次帐户的更新，是否存款或提款，需要从业主获得阈值多签名（TMS）。TMS 是区块链智能合约常用的技术。如果有 n 个代理管理帐户，则每个代理都持有一个秘密密钥，能成为 TMS 的一个贡献部分同时不泄露秘密。当且仅当 n 个代理中的至少 k 个对签名有贡献时，基本 k-of-n TMS 才有效。更复杂的 TMS 验证逻辑也是可能的。加权 TMS 为每个代理的签名分配权重，并要求签名的加权和超过阈值。更一般地，任何逻辑谓词都可用于定义签名有效性。虽然大多数的 TMS 签名规模与该组的代理人数的多少成比例，某些 TMS 签名（例如，基于 BLS 的签名）可以做得紧凑，即使该组代理人值 n 很大[19]

4 Findora 网络

Findora 是一个全球性的公共金融基础设施。Findora 由公开和公共的验证者节点组成，由 Finsense 保障，Finsense 是一种新颖的共识机制，结合了机构信任和经济利益，以保证诚实行为。预计验证者节点将来自不同的地理区域，金融机构和行业。Findora 的参与者和用户将托管、管理和使用可以相互无缝交互的各种应用程序集。

Findora 也是枢纽网络，提供私有和联盟链之间的互操作性，就像互联网连接各组织的内部网一样。管理 Findora 和此类侧链之间的资产和数据传输的 Findora 验证者节点称为侧链接口。侧链接口明确定义了允许跨越其侧链的资产，交易，身份提供商等类型的限制。

Findora 是一个强大的系统，可赋能:

- 高效跨境支付
- 开放金融开放银行
- 针对任何资本市场的全球入口
- 透明化金融服务

[19]Dan Boneh, Manu Drijvers, and Gregory Neven. *Compact Multi-signatures for Smaller Blockchains.* https://eprint.iacr.org/2018/483.pdf

4.1 金融基础设网络单位

在 Findora 上，网络利益相关者持有并使用金融基础设施网络单位（FIN）。在 Finsense 共识的权益加权领导者选择模式中按比例选择押注 FIN 的验证者节点。FIN 押注者因诚实地执行交易被网络奖励，包括交易费用以及新创建区块的 FIN 的奖励。FIN 的押注模式还为诚实行为提供经济安全保障，因为在报告不诚实行为时，罚没条件会导致权益损失。最后，FIN 还必须由侧链接口节点进行押注，这些节点希望在 FIN 和私有/联盟侧链之间移动资产。

4.2 Finsense

Finsense 是 Findora 的共识算法，它可以赋能一个稳定、高吞吐量和公共开放的网络-由现实世界的信任锚点和权益押注同时来保障。Finsense 使用 FIN 通证来代表共识席位。FIN 通证的总供应量足够大，因此理论上世界上任何人都可以参与共识，但是，个别验证者可能拥有多个席位。验证者对协议的影响与其持有的席位数成正比。

鉴于 FIN 通证的固定分配，该协议的运行方式与其他权益证明（PoS）协议非常相似。随机选择一个小型席位委员会来提议和确认新的交易块。选择的随机性是加密保证的，而不是依赖于可信运营者。该技术方法基于使用加密 VRF 以固定间隔选择随机委员会，如在其他[20]权益加权共识协议中那样。然后，每个委员会运行一个快速 BFT 协议，旨在在弱同步网络中工作。

在委员会中担任席位的验证者节点通过收取交易费来获得奖励。一个验证者节点被选择参与一个委员会，其频率与其拥有的 FIN 通证的数量成比例，因此 FIN 通证的价值应与交易费用成比例。FIN 通证可以在验证者之间交换; 然而，在验证者参与委员会之后，将有一个锁定期，锁定该部分帮助节点当选的通证。

只要基于 FIN 的共识协议是可操作且安全的，诚实的[21]验证者利用协议本身来处理所有 FIN 转移。但是，如果诚实的验证者检测到网络安全中断或基于 FIN 的共识运营被卡住，那么这些验证者将回退到 FBA 共识系统以帮助解决该故障。在这个意义上，共识协议由两个“通道”组成：一个主 PoS 通道和一个辅助 FBA 通道-只有在 PoS 通道发生故障时才会激活。

[20] Algorand,PiLi

[21] 诚实的验证者就是指正确遵循协议规定的验证者。

4.2.1 一致性，活跃性，和最终确定性

Finsense 倾向于保持一致性 (Consistency) 而不是活跃性 (Liveness)。一致性最终会比活跃性对网络中资产的安全性有更大的影响。Finsense 并不认为网络将始终是 Δ-同步的，因为这对于 Δ 的任何实际值都是不切实际的假设。因此，该协议倾向于异步网络中的最大容错。

如果 Finsense 被设计为在弱同步条件下容忍超过 1/3 的节点腐败，这将降低异步条件下的容错度。因此，即使在网络异步条件下，Finsense 也只采纳一条容错性高达 1/3 的快速共识路径。除了在节点腐败率不超过 1/3 全部押注情况下保持网络异步条件下的一致性，协议还将引入在超过阈值的情况下的恢复过程。恢复过程无法预防在节点故障超过阈值时可能发生的不可避免的一致性错误，但是将有助于请除腐败的验证者节点并使诚实的验证器能够重新获得超过 2/3 的权益控制。

Finsense 在 *2/3-弱-同步的*网络条件下保持活跃性。这是一个至少 2/3 的验证者节点（按照押注额加权）是在线的、诚实的、并且能够在很短的网络延时内相互通信的网络。当保持活跃性时，该协议将是完全响应的。换句话说，除非网络条件太不安全，否则它会立即确认交易最终性。

4.2.2 主动安全，问责，和恢复

主动安全 Finsense 采用一种与其他对共识协议不同的方式阻止自适应攻击。在我们的协议中，我们使用加密学机制来确保在投票回合中使用相同的选定公共押注密钥签署两个相互冲突的消息的验者者在该过程中泄漏相应的私有押注密钥。这允许网络中的任何人提交交易来窃取该验证者的押注密钥控制的所有 FIN 通证。腐败的验证者可能会尝试立即将该部分 FIN 通证转移到新的公钥，但仍有可能因为在转移竞赛中不够快而失去这些通证[22]这使验证者有强烈的动机不愿意接受来自主动性对手的贿赂以提交相互冲突的投票。对手贿赂腐败押注密钥的价值必须至少超过押注密钥当前控制的所有 FIN 通证的价值。

我们使用的加密机制称为*一次性签名*。假设验证者有一个押注密钥 mpk 和相应的私钥 msk，它控制分类账本上的 FIN 通证。在给定的投票轮次 i 中，验证者使用其押注私钥 msk 和特殊的生成过程来创建一次性签名密钥 opk_i，以及 opk_i 是被正确导出的证明。该证明可以针对 mpk 被验证。对于每个 mpk，只有一个唯一的 opk_i 可以在投票轮

[22]此外，在其他诚实的验证者能接受来自在一轮投票中参于押注的密钥的转帐之前，设计存在一个重大延时，即该资金在转帐后马上被锁定一段时间。

次 i 中生成。使用 opk_i 对消息进行签名需要私钥 msk。不同消息上的两个 opk_i 签名会泄漏 msk。

问责和恢复 共识中断只有两种：一致性错误会导致诚实的验证者无法同意，而活跃性错误则会阻碍系统的进度。诚实的验证者最终会检测到任何类型的中断并激活 FBA（联邦拜占庭协议）通道来解决它。特别是，验证者使用 FBA 通道就 FIN 余额的手动更改达成一致，以试图清除腐败节点和行为。对共识协议提交可检测违规行为的验证者将被追究责任。当腐败验证者批准无效交易或签署相互冲突的共识投票时，会发生可检测的违规。只有可检测的违规行为才会导致一致性错误。诚实的验证者将清除提交可检测违规的验证者的 FIN 余额。为了确保可检测的违规行为成本高昂，协议对每个验证器者钥帐户实行最低押注余额要求。这可以防止验证者在许多不同的公钥账户上分配他们的股权益，以便只为每次违规行为支付小额罚款。最后，验证者必须在重新激活 PoS 通道之前在 FBA 通道上达成一致共识。

法定人数知识证明 Finsense 将使用法定人数投票的知识证明来降低通信复杂性。减少通信的尺寸大小有助于使同步更容易实现。另一方面，该过程必须仔细进行，以便网络仍然能够检测到可问责的违规行为（即当对手签署两条相互冲突的消息时）。

4.3 侧链界面接口押注

除了为公共金融服务提供基础设施外，Findora 还可以连接到私有分类账本。通过这种方式，Findora 可以被视为连接独立（但可互操作）的金融网络的互联网，每个网络都有自己的资产和财务协议。与帐户可以在 Findora 上发行资产的方式相同，侧链（私有和联盟分类帐本）可以设置自己的资产发行、转移、批准身份证明提供商等规则。侧链也可以指定智能帐户作为本地分类帐本和 Findora 之间的网关节点。此智能帐户以及操作帐户的关联节点称为侧链界面接口。从本质上讲，寻求连接 Findora 以获得资产互操作性和流动性的侧链是 Findora 公共基础设施枢纽的轮辐。侧链界面接口账户必须持有并押注 FIN。与 Findora 上任何其他交易一样，在侧链和 Findora 之间转移资产的交易也会产生费用（也是以 Findora 上发行的任何资产组合为计价单位）。

在 Findora 和侧链之间进行互操作时，在侧链和 Findora 上发布的资产表现如下:

1. 希望在 Findora 上运营的侧链上发行的资产只是抽象为 Findora 的侧链界面接口账户发行的资产。侧链账户必须配置已发行资产以启用所需属性（例如免费发行额外单位）

2. Findora 上发行的希望在侧链上运行的资产只需发送到侧链界面接口账户。如果侧链上的金融服务试图根据 Findora 上的基本事实来验证侧链上的某资产的总供应量，则该账户可以用作托管账户。侧链界面接口帐户可以指定资产类型、身份证明提供商以及转帐到侧链界面接口帐户的其他任意规则。

* * *