2017-06

万维链

搭建区块链的互联网

Version 3.0

目 录

摘要 4

1 万维链设计理念 5

1.1 区块链的出现以及革命意义 5

1.2 万维链设计背景 5

1.3 万维链设计目标 6

1.4 万维链的定位 7

2 万维链总体架构及技术特征 7

2.1 万维链总体架构 8

2.1.1 分布式账本及智能合约虚拟机 8

2.1.2 原生币 8

2.1.3 共识机制 8

2.1.4 链内交易 9

2.1.5 跨链连接 9

2.1.6 跨链交易 9

2.2 万维链技术特征 11

2.2.1 完全去中心化，无可信第三方参与 11

2.2.2 无需修改原有链机制，接入门槛低 12

2.2.3 基于密码学算法的安全性保证 12

2.2.4 跨链交易的隐私保护 12

3 万维链跨链通信协议 13

3.1 跨链协议功能模块 13

3.2 跨链交易数据传输流程 13

4 万维链关键技术 16
4.1 万维链验证节点共识机制 16
4.2 万维链权益激励机制 17
4.2.1 验证节点的激励机制 17
4.2.2 普通节点的激励机制 18
4.3 基于安全多方计算和门限密钥共享技术的锁定账户生成方案 18
4.3.1 安全多方计算和门限密钥共享技术介绍 18
4.3.2 锁定账户生成方案 19
4.3.3 锁定账户签名生成方案 20
4.3.4 方案先进性分析 21
4.4 基于环签名和一次性账户的代币交易隐私保护机制 22
4.4.1 一次性账户系统 22
4.4.2 环签名方案 24
4.4.3 代币交易流程 25

5 万维链应用场景 26
5.1 基于公链之间价值传导的应用 26
5.2 基于公有链和联盟链之间价值传导的应用 28
5.3 基于联盟链之间价值传导的应用 28
5.4 基于与传统账本系统对接的价值传导应用 28

6 结论 29

参考文献 30

附录：专业术语 31

摘要

万维链旨在建立一个区块链基础设施，能够以去中心化的方式完成不同区块链网络的连接及价值交换。它应用密码学最新理论，弥补了现有跨链协议的不足，任何区块链网络，无论公有链、私有链还是联盟链，均能低成本的接入万维链，完成数字资产的跨链交易。万维链不仅仅是一个通用的跨链协议，同时是一个记录跨链交易、链内交易的分布式账本。这个账本不但支持智能合约，而且能支持智能合约代币交易的隐私保护。它是区块链“万链互联”“由链变网”的质的飞跃，是先进密码学理论在区块链领域的集中应用，是高效完备的新型区块链网络。

万维链将重塑区块链经济生态。

1 万维链设计理念

1.1 区块链的出现以及革命意义

2008 年 10 月，中本聪（Satoshi Nakamoto）通过密码学小组第一次公布了比特币的白皮书《Bitcoin：A peer-to-peer electronic cash system》。2009 年 1 月，比特币的创世区块被挖出。2009 年 1 月 12 号，Satoshi 给 HalFinney 发起了第一笔比特币转账交易，并记录在第 170 个区块，从此拉开了比特币网络和区块链技术的序幕。狭义来讲，区块链是一种按照时间顺序将数据区块以链条的方式组合成特定的数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账，能够安全存储简单的、有先后关系、能在系统内验证的数据。广义来讲，区块链是利用链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问安全、利用智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

区块链有着划时代的意义，它使用纯数学方法来建立各方信任关系，且信任建立过程中不需要借助第三方，信任的建立成本几乎降低到零，直接促成互联网由信息互联到价值互联的进化。区块链的应用以数字资产为代表, 同时已延伸到金融、物联网、智能制造、供应链管理等多个领域。

1.2 万维链设计背景

从技术角度而言，比特币作为第一个加密数字货币，它的一个显著缺陷就是区块容量太小，造成交易吞吐量瓶颈。一种扩容思路是纵向扩容（vertical scaling solution），如隔离验证和 BitcoinNG，但是这种方式受单机性能的局限；另一种扩容思路是水平扩容（Horizontal scaling solution），而跨链交易就属于这种扩容方式。

从经济角度而言，任何区块链网络（包括但不限于比特币、以太坊），价值上涨的一个重要因素是作为价值载体能够为价值提供很好的流通性，而这种流通性不受国界、地域、组织、时间的限制，但是目前而言这种高流通性仅局限于自身网络中。随着越来越多的基于区块链的数字资产产生，它们都拥有各自独立的基础协议，成为了一个个相对封闭的网络，并不能与其他区块链网络进行价值的传

导。因此，就需要跨链交易将不同的区块链连结为网状，达到信息、资产互融互通的效果。然而已有的跨链交易方案并不能很好的完成区块链之间的互联互通，某种程度上只能在一定限制条件下完成跨链交易，如需可信第三方参与、不支持离线交易、需公证人参与等。

从应用角度而言，到目前为止全球范围内以区块链概念为基础的数字货币共有上千种，到 2017 年 6 月总市值已经超过 1000 亿美金，数字货币的数量和价值仍在不断增长。数字货币正在成为人类新的货币形式，它们之间交易和兑换的需求是显而易见的，而目前主要还是通过中心化的方式（如交易所等）解决去中心化的数字货币的交易兑换问题。同时，在传统资产领域，大量的组织正在探索如何将传统形式的资产映射到区块链上（更多的以联盟链的形式存在），这些资产更大范围的流通也需要将不同的联盟链和私有链互联起来。

综上，跨链交易的技术是极具研究意义和应用价值。万维链正是在这一背景下设计。

1.3 万维链设计目标

跨链交易能力对区块链具有重要意义，它能够将传统的单独运行、机制各异的区块链连接起来，形成一张区块链的网络，达到互联互通、数字资产无障碍转移的效果。根据对跨链交易技术的调研，结合区块链去中心的特点和其应用场景考虑，万维链的设计目标如下：

- 能够连接现存的主要数字货币网络（如比特币、以太坊等），完成资产兑换的同时不改变原有链机制。新产生的数字货币网络也能够以极低的成本接入到万维链中。
- 联盟链性质的区块链网络能够接入万维链，实现资产由原有链转入万维链、由万维链转回原有链、多种资产在万维链上进行交易等功能。
- 保证跨链交易资产的安全性以及跨链交易服务的稳定性。
- 提供跨链交易的隐私保护。
- 具有场景的延展性，能够成为货币兑换、撮合交易、场外交易、竞价交易等资产交易场景的基础平台。

1.4 万维链的定位

从区块链行业发展角度而言，万维链的最终愿景是打造一个区块链的“互联网”，完成区块链“由链变网”的质的飞跃。在万维链的生态环境中，万链互联，价值无障碍传导，将区块链承载价值和传递价值的功能发挥到极致。万维链将重塑区块链经济生态。

从区块链底层技术开发角度而言，万维链应用了安全多方计算、门限密钥共享、基于椭圆曲线的环签名方案、一次性账户生成机制等多项密码学前沿技术，并首次解决了智能合约代币交易隐私保护这一难题。某种程度上，万维链就是先进密码学理论解决区块链领域难题的典型应用，代表着区块链底层技术的发展方向，那就是由条件安全向可证明安全转变、由逻辑控制向算法理论控制转变。万维链有一支专业的密码学研究团队，他们将持续为密码学在区块链领域的应用向整个行业贡献力量。

从区块链技术应用角度而言，万维链不只是一个实现跨链交易和多资产互通的区块链项目，更是一个完备的区块链开发平台。万维链在实现跨链交易功能的同时，也是一个可以独立运行的区块链网络：它包含原生币，支持智能合约，并且拥有智能合约代币交易的隐私保护机制。任何开发者，均可根据应用场景，在万维链上开发出满足需求的应用。

2 万维链总体架构及技术特征

万维链是一个为不同区块链网络提供资产跨链转移通道的基础设施，是一个通过跨链协议实现与不同区块链网络互联互通、完整记录跨链交易、维护链内交易明细的分布式账本。万维链将支持主流公有链间的跨链交易、联盟链间的跨链交易以及公有链与联盟链之间的跨链交易。

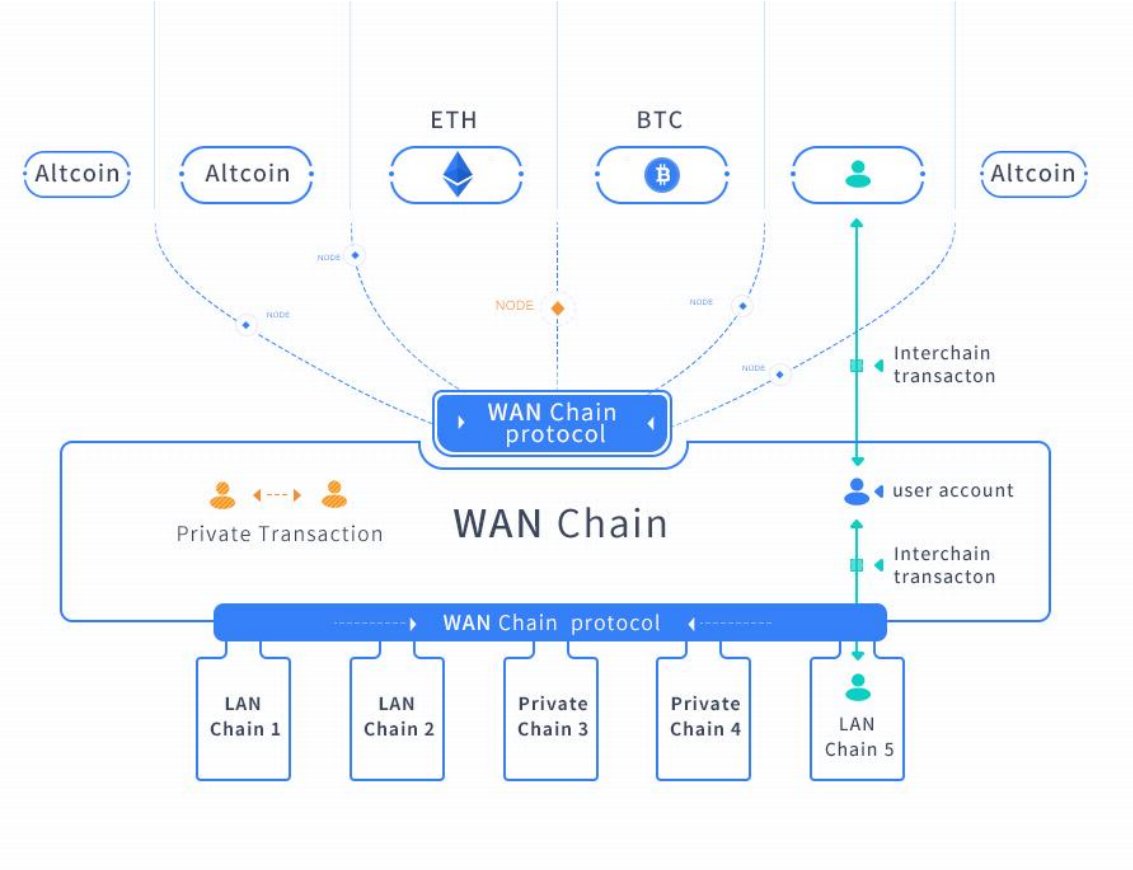

图 2. 1 万维链模型图

2.1 万维链总体架构

2.1.1 分布式账本及智能合约虚拟机

万维链是一个基于以太坊开发的通用账本，可以独立运行应用，保留账户模式和智能合约，可以完整实现以太坊原有的各项功能。在此之上，我们加入了跨链交易机制，并且实现了智能合约代币交易的隐私保护。

2.1.2 原生币

万维币（WANCoin）是万维链的原生币，链内的普通交易以及跨链交易都将消耗一定量的万维币，同时万维币还会被用作跨链交易验证节点的保证金。

2.1.3 共识机制

对于万维链上普通交易的共识机制，我们采用 POS 共识。同时，在传统 POS

共识基础上，我们引入跨链交易的共识和激励机制。对于这部分内容的初步设想和规划在后文中有相应论述。

2.1.4 链内交易

万维链上的普通交易与以太坊相同，同时我们增加了智能合约代币交易的隐私保护机制，该机制通过环签名和一次性账户实现。

2.1.5 跨链连接

其他链接入万维链，首先需要完成在万维链上的注册，确保万维链能够对该链进行唯一识别；不同资产转入万维链，首先也需要完成在万维链上的注册，确保万维链可以对该资产进行唯一识别。这两部分功能分别通过链注册和资产注册协议完成。

对于跨链交易，我们利用多方计算和门限密钥共享方案进行联合锚定，在不改变原有链机制的基础上通过跨链通信协议实现最小代价接入。万维链本身也是一个完备的开发平台，利用万维链开发的公有链、联盟链和私有链具备智能合约代币交易的隐私保护功能，可以适用于广泛的金融应用场景，更为重要的是基于万维链开发的其他链相当于万维链的同构链，与万维链有相同的跨链机制，可与万维链无缝衔接。

2.1.6 跨链交易

当一种未注册资产由原有链转移到万维链上时，万维链节点会使用一个基于协议的内置资产模板，根据跨链交易信息部署新的智能合约创建新的资产。当一种已注册资产由原有链转移到万维链上时，万维链节点会为用户在已有合约中发放相应等值代币，确保了原有链资产在万维链上仍然可以相互交易流通。

为描述公有链与万维链之间资产的转入转回，我们以以太坊为例详细说明如下：

转入过程：Alice 和 Bob 分别在以太坊和万维链上拥有账户，当 Alice 需要向 Bob 转移 10 ether。Alice 使用万维链钱包发出跨链交易请求，并在以太坊中发起一笔转账交易，接收方为万维链在以太坊上的跨链锁定账户（Locked Account）；万

维链验证节点收到跨链交易请求并验证以太坊上该交易已完成记账，然后在万维链上创建一个新的智能合约代币资产 ether’， ether’是 Alice 需要跨链转移的 ether 在万维链上的代表，并将该资产链内转移到 Bob 在万维链的账户中。

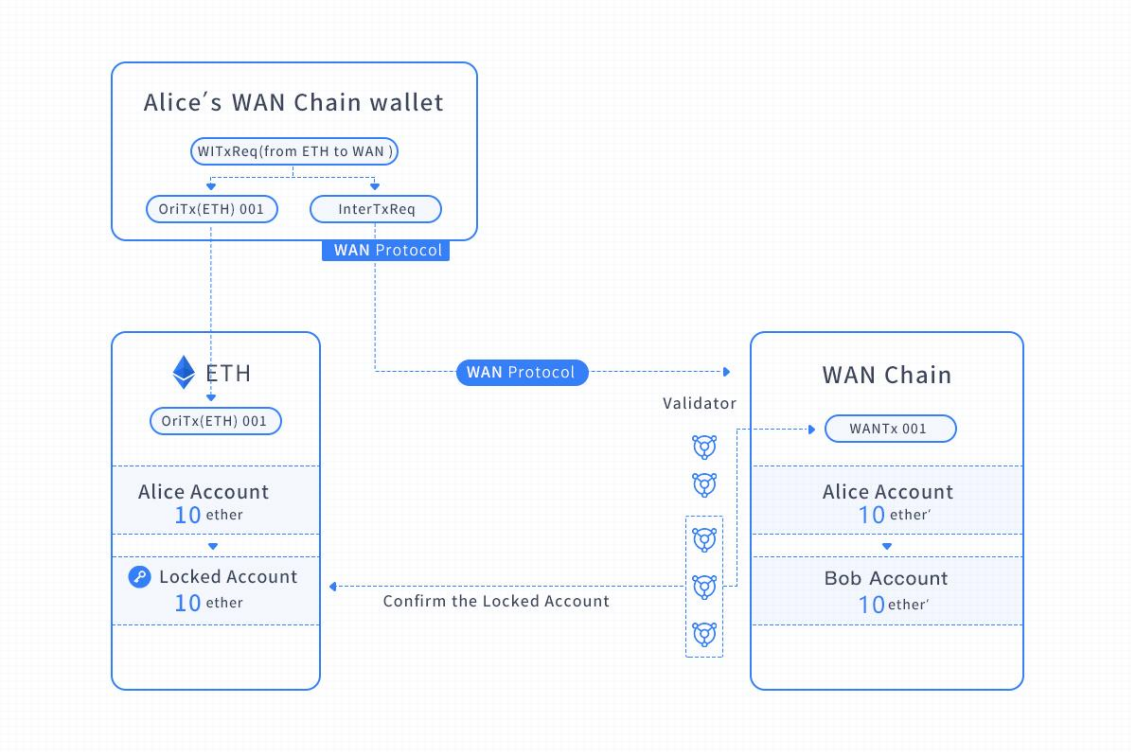

图 2. 2 跨链交易——以太坊到万维链

转回过程：Bob 将从 Alice 处收到的 10 ether 转给 Cris。Bob 使用万维链钱包向 ether’资产合约发起一笔跨链交易，验证节点收到交易后将 Bob 的该笔资产对应的价值 10 ether’转为锁定状态；锁定完成后，验证节点利用门限密钥共享机制构造出一笔以太坊交易，交易的转出方是之前锁定 Alice 资产的跨链锁定账户（Locked Account），转入方是 Cris 在以太坊上的账户；验证节点验证以太坊上的交易确认后，将 Bob 账号下锁定的 10 ether’清空，意味着等值的资产已经回到原有链。

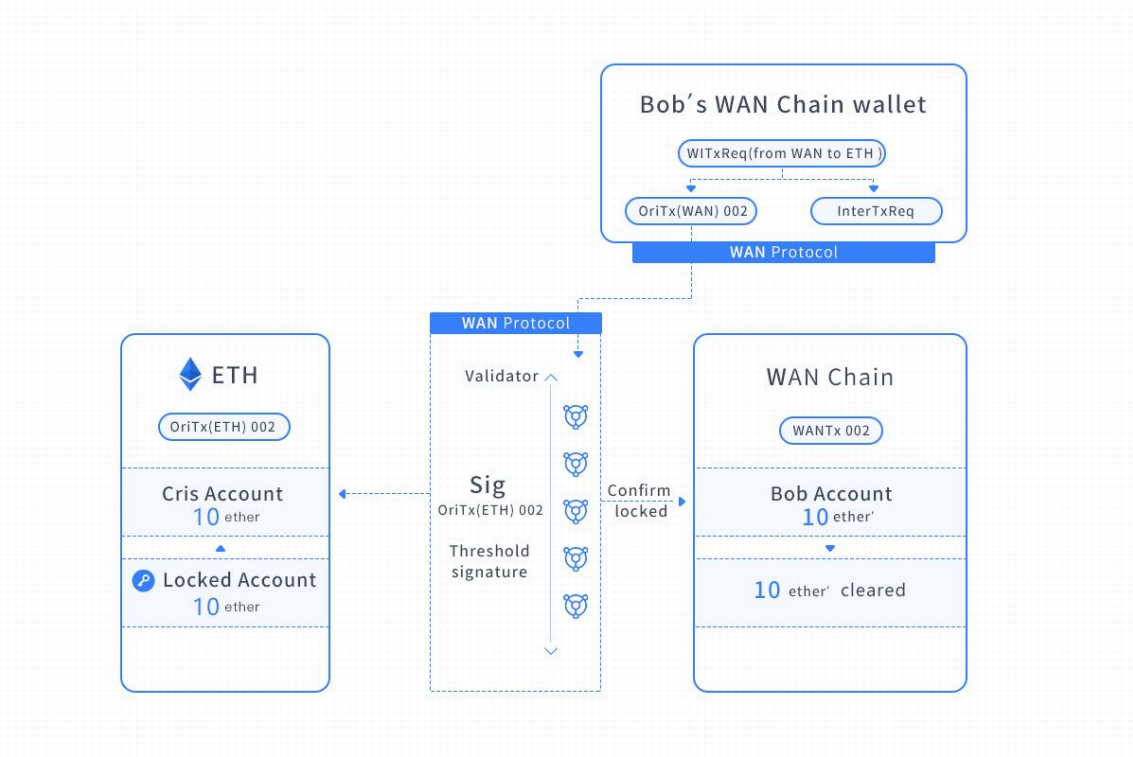

图 2. 3 跨链交易——万维链到以太坊

以上描述了万维链与公有链之间完成资产的转入和转回过程，万维链与联盟链之间的资产转移本质上与之相同。资产转移的详细流程及数据传输过程请参考后续章节 3.2 跨链交易数据传输流程。

2.2 万维链技术特征

2.2.1 完全去中心化，无可信第三方参与

目前跨链交易大部分是交易所和第三方交易平台在承担，区块链跨链交易平台也往往需要第三方托管账户参与，这就将整个交易能安全顺利完成的基础依托在第三方参与者的可靠性上。而万维链的锁定账户机制采用多方计算和门限密钥共享技术，完全去中心化，实现了无需可信第三方参与的账户管理功能，不需要任何实体机构信用背书，消除了第三方参与者信用问题带来的隐患。

2.2.2 无需修改原有链机制，接入门槛低

跨链交易方案中，我们的账户锁定机制没有采用双向锚定方法，不需要在原有链上添加识别和验证 SPV 证明的脚本扩展，所有交易数据都是在万维链验证节点上重构合成后传入原有链节点网络，都是符合其交易类型要求的合法格式，这就将跨连交易的特定操作和计算完全归结于万维链网络中完成，无需对原有链的各项机制进行任何修改，使得无论已有公有链还是基于其他平台开发的私有链、联盟链都可以低门槛自由接入万维链，降低跨链交易合作成本，实现各链间资产的自由流通。

2.2.3 基于密码学算法的安全性保证

已有的很多跨链交易所使用的机制常立足于逻辑上的安全性，需要依靠跨链交易参与者基于自身利益推动，即参与者不会以损害自身利益为代价破坏跨链交易进行，这就引入了参与者理智假设。而万维链中，除了使用原有椭圆曲线密码体制以保证原有签名方案安全的基础上，使用了基于多方计算和门限密钥共享技术的锁定账户管理方案和基于环签名和一次性账户的智能合约代币交易隐私保护机制，去除了参与者理智假设，跨链交易发起后，后续所有操作都无需交易参与者配合，将在万维链验证节点间自动完成，使得整个系统的顺利运行依托于密码学算法的安全性，在逻辑安全之上提高到了算法理论安全。

2.2.4 跨链交易的隐私保护

万维链的跨链交易方案中，原有链上的资产在转移到万维链上后以智能合约中代币的形式存在，我们一方面通过环签名技术将智能合约代币交易的发起者隐匿在一个账户集合之中，令发起者对于任何人都是不可追踪的，另一方面通过一次性账户系统使得智能合约中的账户一次性使用，且与万维链上原生账户无法建立对应关系，令合约内账户与原生账户隔离。综合两方面，实现了智能合约代币交易的隐私性，也就是让资产跨链后的交易受到隐私保护，为用户提供更好体验的同时扩展了应用场景。

3 万维链跨链通信协议

万维链跨链通信协议是其他链与万维链之间数据传输的规范，实现链与链之间数据流转和互联互通。下面按照模块功能和数据传输流程描述。

3.1 跨链协议功能模块

万维链跨链通信协议按功能划分主要包括三个模块：

注册模块：该模块主要实现两项功能。一是对参与跨链交易的原有链进行注册，通过特定算法规则为原有链生成唯一标识，维护原有链标识注册表，避免虚假链造成欺骗；二是对请求转移的资产进行注册，通过特定算法规则为资产生成唯一标识，以确定资产的唯一性，保证同一种资产在万维链上的流通性。

跨链交易数据传输模块：该模块主要实现三项功能。一是原有链上用户向万维链提出跨链交易请求，是万维链资产转入交易的起点；二是万维链验证节点针对跨链交易请求为用户返回操作成功与否的回执；三是万维链验证节点向原有链发送合法交易，以实现原有链资产转回过程。

交易状态查询模块：该模块主要实现查询原有链状态数据的功能，以确认原有链上用户向万维链锁定账户转入资产的交易是否已被确认、万维链锁定账户向原有链上用户转回资产的交易是否已被确认，是跨链交易进程的控制标志。

3.2 跨链交易数据传输流程

以原有链上用户 Alice 将$value$资产转移到万维链上为例说明万维链资产转入数据传输流程：

Step1：Alice 在原有链上用账户$OriAccount$发起一笔交易$OriTx$，将需要转移的资产$OriAssetID$发送至万维链锁定账户$Locked\ Account$，并以交易数据为参数通过跨链交易数据传输模块向万维链网络广播跨连交易请求$InterTxReq$：

$$OriTxInfo = (OriBlockNum, OriTx)$$

$$InterTxReq = (OriAccount, OriChainID, OriAssetID, value, OriTxInfo, sig)$$

Step2：万维链上跨链交易证明节点(Voucher)接收到跨链交易请求$InterTxReq$，以$OriTxInfo$、$OriChainID$和$OriAssetID$为参数通过交易状态查询模块在原有链上

查询交易$OriTx$是否已被确认：

$$TLF = CheckCommitment(OriChainID, OriAssetID, OriTxInfo)$$

Step3：跨链交易证明节点(Voucher)对TLF结果进行共识，若$TLF = true$，说明$OriTx$已被确认，则验证节点(Validator)收到$TLF = true$数据，查询原有链资产注册表，若为新资产，则为此资产注册并加入注册表，由 Validator 维护的公共账户$WANAccount$发起一笔交易$WANTx$部署新资产合约并在其中为$OriAccount$分发价值$value$的代币资产；若为已注册资产，则发起一笔交易$WANTx$直接在已有资产合约中为$OriAccount$分发价值$value$的代币资产。若$WANTx$被确认，则 Validator 使用跨链交易数据传输模块给 Alice 回复跨链交易成功回执：

$$response = (WANAccount, InterTxReq, True, address_{SC}, sig_{validator})$$

若$WANTx$失效，则锁定账户管理节点（Storeman）在原有链上发起一笔交易，将 Alice 锁定资产转回其账户$OriAccount$。

若 Voucher 对TLF共识结果为$false$，则认为跨链交易无效。

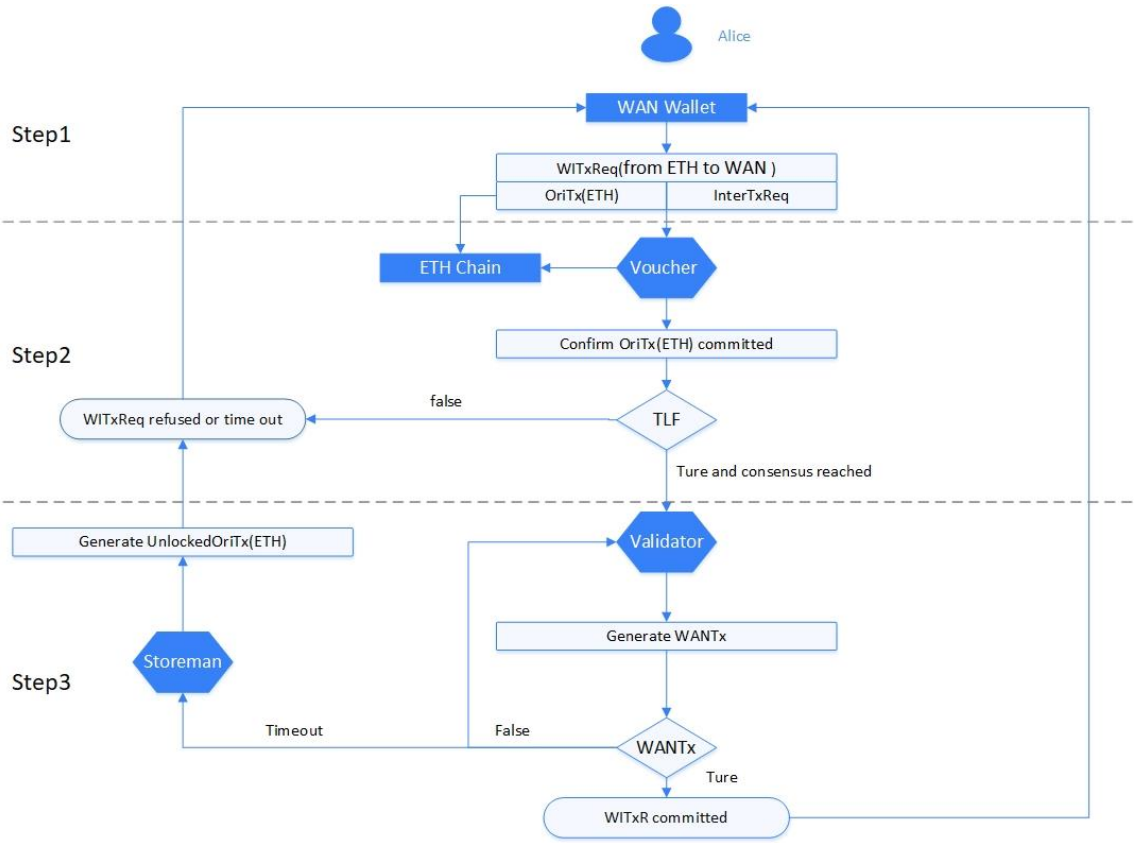

图 3.1 跨链数据流程——以太坊到万维链

以万维链上用户 Bob 将$value$资产转回到原有链上为例说明资产转回数据传输

流程：

Step1：Bob 在万维链上使用账户$BobAccount$发送一笔交易$WANTx$调用原有链资产对应智能合约的资产转回函数。

Step2：Validator 接收到交易后调用智能合约，Voucher 检测合约执行结果，对结果正确标志TLF进行共识，若$TLF = true$说明 Bob 在合约中的$value$代币资产已被锁定，则 Storeman 通过跨链交易数据传输模块在原有链中广播一笔由$Locked\ Account$向$BobAccount$转账$value$的交易：

$$OriTx = (LockedAccount, BobAccount, value, sig_{storeman})$$

Voucher 通过交易状态查询模块检测该笔转账是否被确认，对确认标记TUF进行共识。

Step3：若$TUF = true$，则 Validator 将智能合约中锁定的资产清除；若$TUF = false$，则原有链交易未被确认，Storeman 重新发起交易。

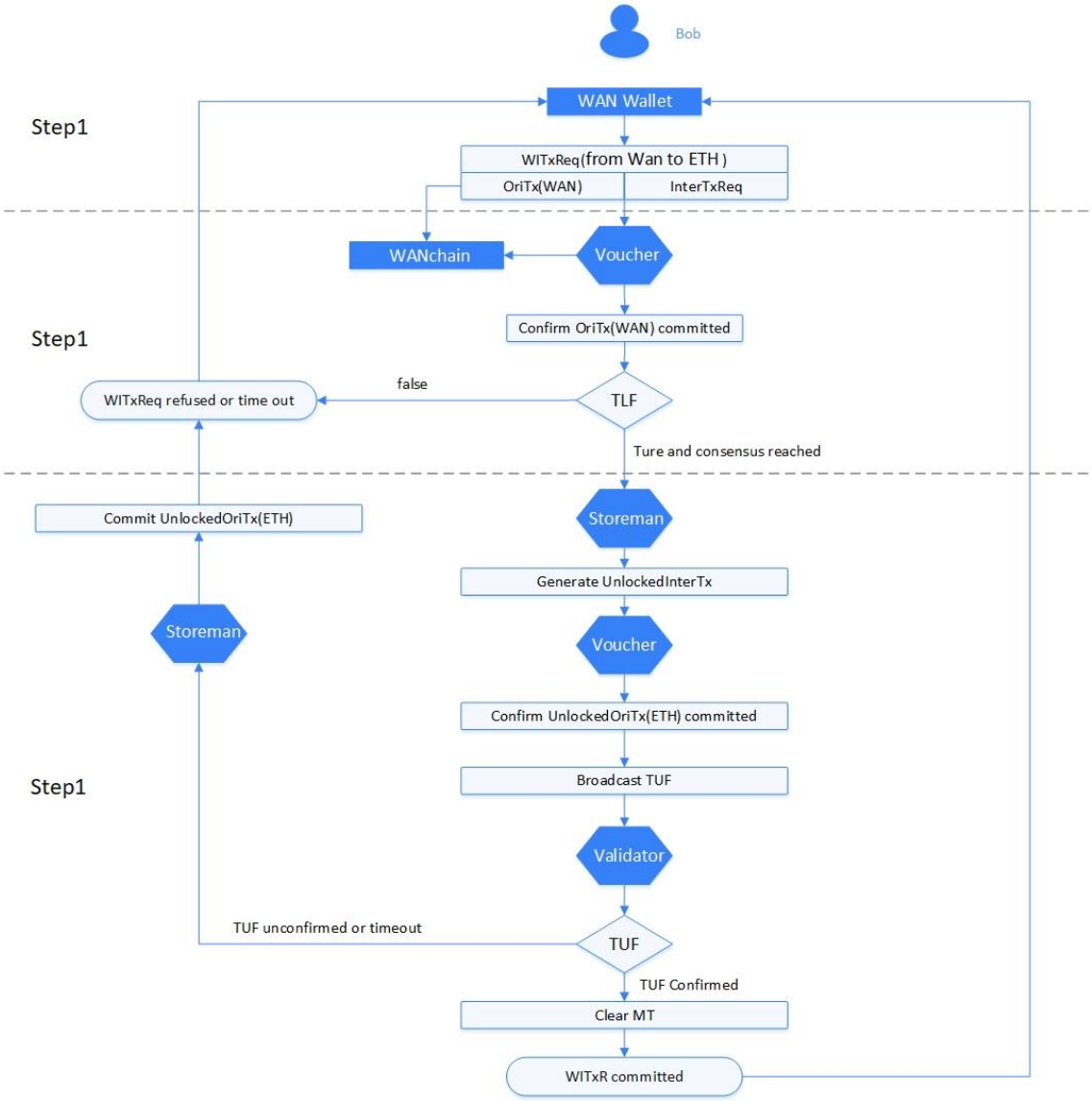

图 3. 2 跨链数据流程——万维链到以太坊

4 万维链关键技术

4.1 万维链验证节点共识机制

万维链将采用 POS 共识机制，这一共识机制的通用描述在以太坊的一系列论文中均可找到，这里不再详述。POW 共识算法理论上存在 51%算力攻击的威胁，同样 POS 共识算法理论上也存在参与者合谋攻击的威胁。因此万维链将引入以下机制去提高验证节点合谋的机会成本，使得万维链能够真实的记录跨链交易和客观的完成跨链流程。

微观上考虑，万维链上验证节点设计为三类——普通验证节点（Validator）、跨链交易证明节点（Voucher）和锁定账户管理节点（Storeman）。Voucher 负责在跨链交易过程中提供原有链账户与锁定账户之间交易的证明，同时它也需要缴纳一定的保证金，保证金越多，它所提供的证明被采纳的概率也越高，如果提供虚假证明，它的保证金将会被扣除并剥夺跨链交易证明节点的身份。Validator 负责在收到达成共识的交易证明后，通知 Storeman 对锁定账户进行相关操作并完成万维链账本的记账操作。Storeman 负责在接到通知后，通过自己所持的密钥份额计算出签名份额并最终合并为锁定账户完整签名，以便进行锁定账户的相关操作（具体流程见 4.3 部分）。也就是说，万维链将验证节点分为三类，将跨链交易的验证权限进行了一个分离。一方面，每一类节点内部需要达成共识；另一方面，单独一类验证节点即使合谋也无法完成跨链交易的伪造。这种分离机制能够最大限度的降低验证节点合谋的可能性。

宏观上考虑，万维链的安全取决于自身的总体价值。当跨链交易承担的价值远远大于万维链网络的总体价值时，即合谋的收益大于合谋的机会成本，那么验证节点合谋的风险将会变高；反之，当万维链网络的总价值足够大以后，验证节点合谋意味着要放弃自身持有的保证金和万维链上代币的权益，合谋的机会成本大大增加，节点不会为小于自己已有利益和长远收益的跨链资产而合谋破坏整个网络，合谋的风险会降低。因此越多的跨链交易参与到万维链中，万维链承载的价值就越大。验证节点合谋的机会成本就越高，整个网络就更加安全，而更加安全的万维链会吸引越来越多的跨链交易参与进来。这是一个相互作用的过程，随着价值在万维链网络中传导，万维链势必会变得越来越健壮。

4.2 万维链权益激励机制

4.2.1 验证节点的激励机制

万维链上验证节点分为三类——普通验证节点、跨链交易证明节点和锁定账户管理节点。对于跨链交易证明节点，正确的提供原有链账户与锁定账户之间交易的证明，将会根据其保证金获得相应份额的交易费用；如果提供虚假的交易证明，将会被扣除保证金并取消节点资格。普通验证节点完成万维链上的记账，并获取所记账交易的部分交易费。锁定账户管理节点根据其所持权益获得对应数量

的密钥份额，计算相应的签名份额附在交易中，它根据密钥份额比例获取参与验证交易的交易费。如果离线或者丢失密钥份额，则无法参与验证交易，也就不能获得交易费。同样这些节点如果对错误交易签名，也会被取消锁定账户管理节点的身份。综上，验证节点激励机制会激励跨链交易证明节点提供正确的交易证明，激励普通验证节点如实的完成万维链记账，激励锁定账户管理节点保持在线并安全保管自身密钥份额。

4.2.2 普通节点的激励机制

只有在万维链上掌握足够的权益才能够成为验证节点，未成为验证节点的其他节点称为普通节点。普通节点无法参与跨链交易的验证，它们可以将所掌握的权益委托给信任的验证节点，受委托的验证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。如果受委托验证节点受到惩罚，普通节点也会承担相应损失。这一激励机制保证了万维链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权益委托给可信的验证节点，从而提高万维链的安全性与稳定性。

4.3 基于安全多方计算和门限密钥共享技术的锁定账户生成方案

4.3.1 安全多方计算和门限密钥共享技术介绍

安全多方计算（Secure Multi-party Computation）是分布式密码学的理论基础，也是分布式计算研究的一个基本问题，最早由姚期智于 1982 年通过姚氏百万富翁问题提出。简单的说，安全多方计算是指一组人，比如$P_1 \cdots\cdots P_n$，共同安全的计算函数$f(x_1, \ldots\ldots, x_n) = (y_1, \ldots\ldots, y_n)$。函数的$n$个输入分别由$n$个参与者秘密掌握，设$P_i$的秘密输入是$x_i$，并且在计算结束后，$P_i$得到输出$y_i$。这里的安全性是要求即使在某些参与者有欺骗行为的情况下保证计算结果的正确性，即计算结束后每个诚实的参与者P_i都能得到正确的输出y_i，同时还要求保证每个参与者输入的保密性，即每个参与者P_i除了(x_i, y_i)外，得不到任何其他信息。

门限密钥共享技术（Threshold Key Sharing Scheme）解决的是密钥安全管理问题。现代密码学体制的设计是使得密码体制的安全性取决于密钥安全，密钥的泄露就意味着体制失去了安全性，因此密钥管理在密码体制的安全性研究和设计中

占有重要的地位。特别是多方利益体共同管理一个账户时，账户的密钥如何可信安全的分配给多方参与者就变得非常棘手。针对这一问题，以色列密码学家 Shamir 提出了 Shamir(k,n)门限密钥共享方案。方案中，密钥被分为n份分配给n个参与者，每个参与者掌握一个密钥份额（key share），只有集齐超过k个密钥份额，才能够将密钥恢复。因此，账户的任何操作都至少需要n位参与者中的k位参与才能够实施，这样便保证了账户的安全可信。

4.3.2 锁定账户生成方案

我们基于安全多方计算和门限密钥共享技术设计了锁定账户（Locked Account）生成方案。生成的锁定账户密钥由万维链上的锁定账户管理节点（Storeman）共同维护与管理，保证了账户的安全可信、降低了密钥丢失的风险，同时对没有固定拓扑结构的 ad-hoc 网络也有较强适应性和稳定性。具体方案如下：

Step1：万维链n个验证节点（编号为$P_1 \cdots\cdots P_n$），各自选取随机数d_i和k次多项式$f_i(x) = d_i + a_{i,1}x + \cdots + a_{i,k-1}x^{k-1}$，将$f_i(j)$通过安全信道发送给其他验证节点，并将$d_iG$广播全网，其中$G$是椭圆曲线上的基点。

Step2：节点P_j收到其他节点信息后，验证收到信息的正确性：

$$flag = Check(f_1(j), \ldots\ldots, f_n(j))$$

如果$flag = Ture$，则接受并本地保存；如果$flag = False$，则拒收并请求其他节点重新发送消息。

Step3: 待所有信息都发送完毕且验证通过后，每个验证节点计算所得到的密钥份额为：

$$key\_share_k = \sum_{j=1}^{n} f_j(k)，\ k = 1, \ldots\ldots, n$$

Step4: 计算锁定账户地址：

$$Locked\_Account\_Address = GenerateAddress(d_1G, \ldots\ldots, d_nG)$$

以上便生成了锁定账户，并将它的密钥分为n个密钥份额分配给n个万维链验证节点，锁定账户的任何操作都至少需要n个验证节点中的k个参与才能够完成。

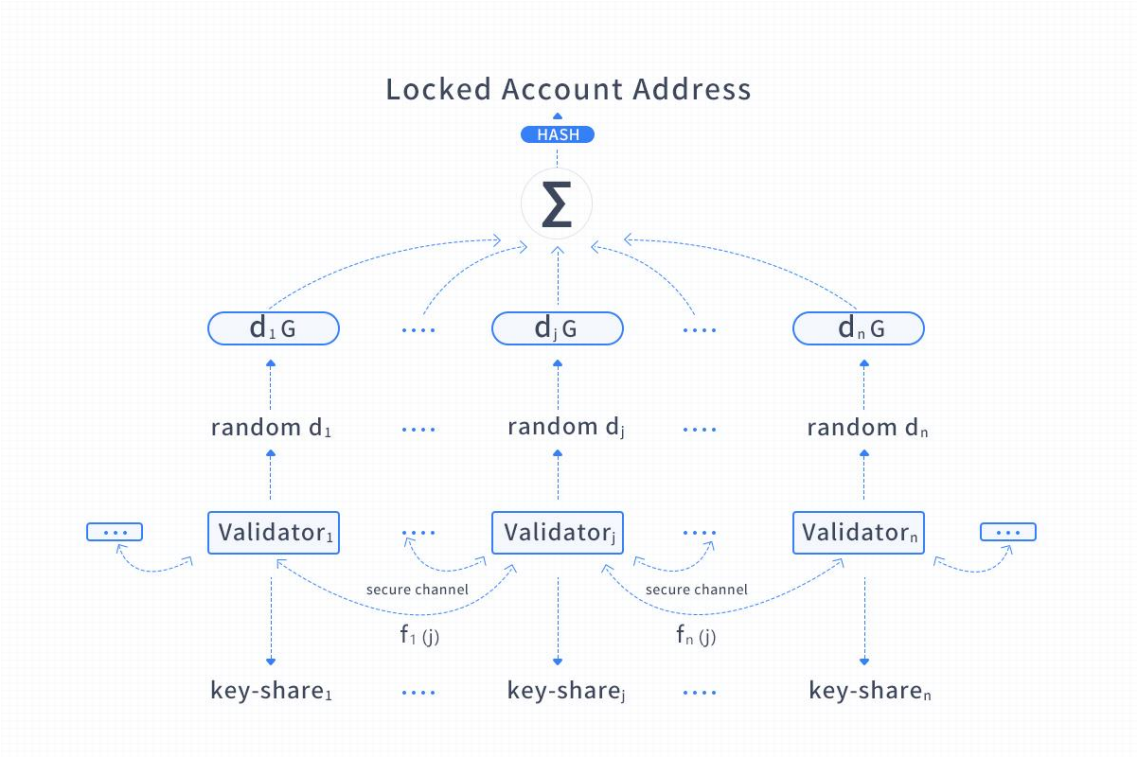

图 4.1 锁定账户地址生成

4.3.3 锁定账户签名生成方案

锁定账户生成过程中并不会产生对应私钥，并且它的私钥不会在任何过程中重构出来。要生成锁定账户的签名，需要至少k个验证节点参与，它们通过自身掌握的密钥份额计算得到对应的签名份额（signature share），最终重构出对应于锁定账户的完整签名。具体过程如下：

Step1：万维链上n个验证节点使用自身掌握的密钥份额计算消息签名份额：

$$signature\_share_j = Generate\_Sig(m, key\_share_j)$$

Step2：验证节点将产生的签名份额发送给其他所有验证节点。

Step3：某一验证节点收到大于k个签名份额之后，重构出完整签名，并公布：

$$signature = Construct\_Sig(signature\_share_1, \ldots\ldots, signature\_share_k)$$

此时 Locked Account 的完整签名便重构出来了。

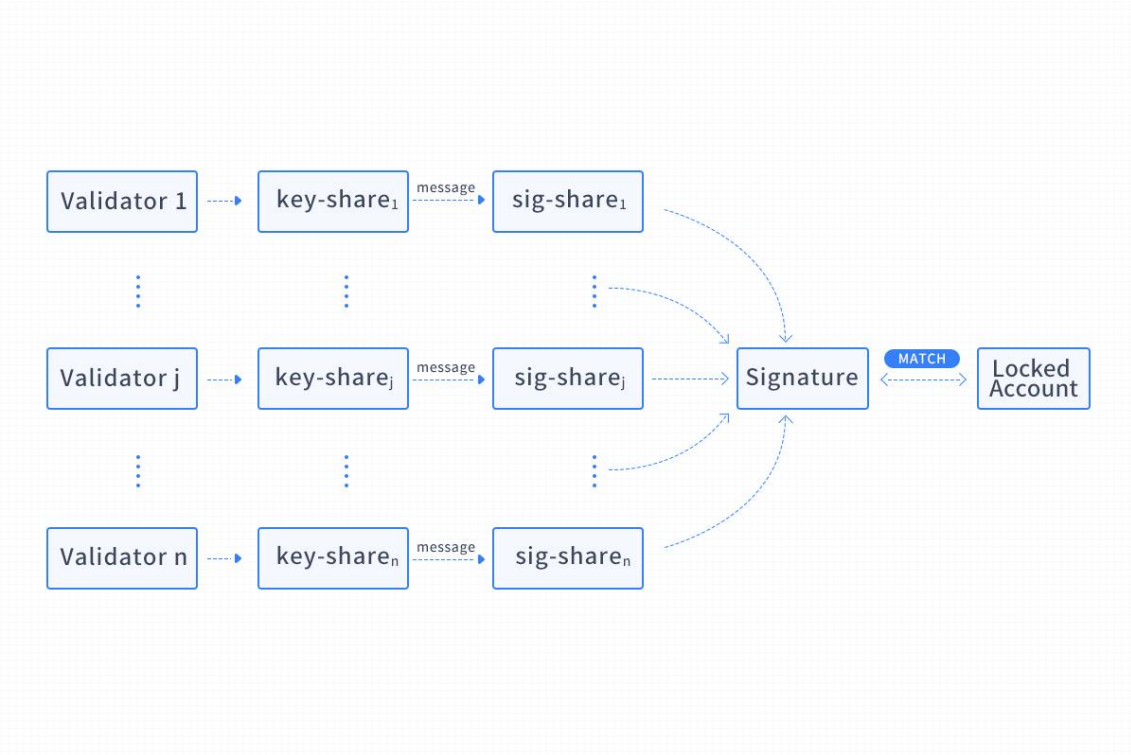

图 4. 2 锁定账户签名生成

4.3.4 方案先进性分析

跨链交易方案都需要一种机制去将用户原有链上的资金进行锁定，只有触发条件达到之后才可以解锁退还到原始账户或者转移到其他账户。目前的实现机制有 HTLC（Hashed TimeLock Contract）、可信第三方托管账户（Escrow）、多方签名账户等。相较于已有方案，锁定账户生成方案有以下先进性：

- **去中心化，无需可信第三方参与**

锁定账户由多方计算得到，生成环节不需要任何可信第三方参与，也不需要任何可信机构背书，只需要万维链上节点通过安全信道进行信息交互与计算即可。相比可信第三方托管账户机制，锁定账户生成方案成本更低且相对灵活。

- **安全稳定**

锁定账户的密钥通过 Shamir(k,n)门限密钥共享方案分配给万维链的验证节点，每个验证节点掌握一个密钥份额。即使个别验证节点离线或者密钥份额丢失，只要有k个以上节点正常参与交易，那么锁定账户的签名仍然能生成，从而保证交易

正常执行。因此，锁定账户生成方案能够保证即使出现个别节点网络瘫痪或者密钥份额丢失等意外情况，整个系统的安全稳定运行。同时，也通过周期式或者触发式的机制对每个验证节点的密钥份额进行更新，消除密钥份额泄露对系统带来的安全威胁。

- **易接入，存储空间低**

锁定账户进行的任何操作，均为原有链上的原生交易，不需要对原有链添加新的交易类型和验证机制，因此任何链理论上均可接入万维链，且接入成本很低。同时，相比多方签名账户机制依赖智能合约逻辑实现账户的多方管理，锁定账户生成方案使用密码学原理达成账户的多方管理，最终交易结构中只存在一个签名，而不是多个签名，因此交易所占空间低，存储空间利用率更高。

4.4 基于环签名和一次性账户的代币交易隐私保护机制

万维链采用环签名和一次性账户技术实现智能合约代币交易隐私保护，具体方式为通过环签名技术使智能合约代币交易发起方匿名不可追溯，通过一次性账户技术使得合约内账户与链上原生账户隔离并不可对应，最终实现万维链上智能合约代币交易的隐私保护功能。

4.4.1 一次性账户系统

账户体系是整个隐私交易的基础，我们采用一次性账户机制，每个用户拥有唯一主账户和多个子账户，子账户也可以看作智能合约中的账户。为此，我们要求如果用户需要使用具有隐私保护功能的代币交易机制，就需要在已有账户基础上添加伴生账户，构成一次性账户系统所需账户形式。

万维链上 Alice 的原生账户(A, a)，其中A为公钥，a为私钥，为构成一次性账户系统所需形式，Alice 生成新账户(B, b)作为伴生账户，添加到原有账户后，在一次性账户系统中，(A, B)作为 Alice 的主账户，(a, b)作为 Alice 的主账户私钥，(A, b)作为 Alice 的扫描密钥。一次性账户系统中用户的子账户通常不是自己生成，而是由交易对方为用户生成。如 Bob 要为 Alice 生成一次性账户，则将 Alice 的主账户(A, B)作为输入，通过$OTA_GenerateAccount(\,)$函数生成 Alice 的一次性账户(A_1, S_1):

$$(A_1, S_1) = OTA\_GenerateAccount((A, B))$$

Alice 利用扫描密钥(A, b)通过$OTA_ScanAccount(\,)$函数检测所有一次性账户(A_i, S_i):

$$flag = OTA\_ScanAccount((A_i, S_i), (A, b))$$

当检测到(A_1, S_1)时$flag = true$，说明(A_1, S_1)为 Alice 的一次性账户，再利用主账户私钥(a, b)通过$OTA_GetPrivateKey(\,)$函数得到一次性账户(A_1, S_1)对应私钥sk：

$$sk = OTA\_GetPrivateKey((A_1, S_1), (a, b))$$

在一次性账户系统中，Alice 拥有扫描密钥(A, b)才能确定某个一次性账户属于自己，拥有主账户私钥(a, b)才能得到一次性账户私钥，因此，任何其他用户在没有扫描密钥(A, b)时无法建立一次性账户与 Alice 主账户的对应关系，保证了主账户和一次性账户的隔离不可追溯，而在没有主账户私钥(a, b)时无法得到一次性账户私钥，保证了一次性账户安全。

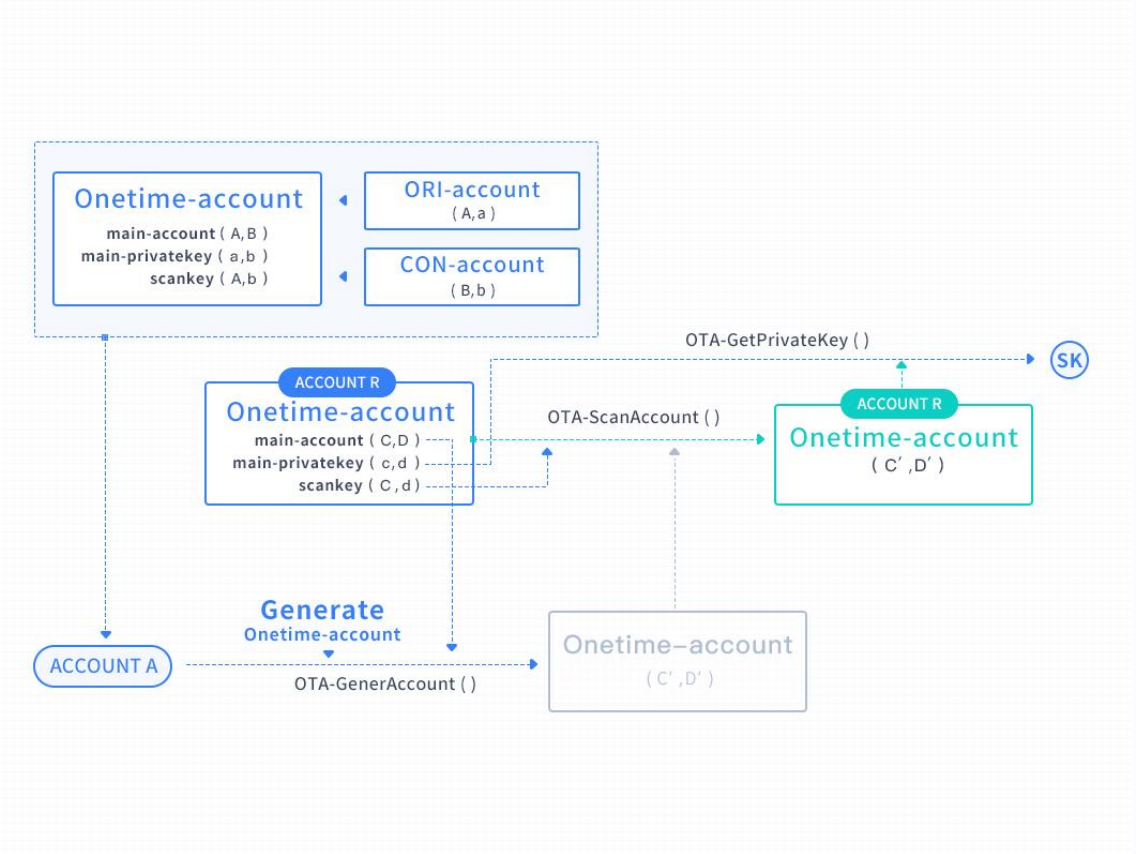

图 4. 3 一次性地址系统

4.4.2 环签名方案

2001年，Rivest等人在如何匿名泄露秘密的背景下提出了一种新型签名技术，称为环签名（Ring Signature）。环签名可以被视为一种特殊的群签名（Group Signature），由于群签名需要可信中心和安全的建立过程，往往在匿名保护上存在漏洞（签名者对于可信中心是可追溯的），而环签名在群签名基础上去除了可信中心和安全建立过程，对于验证者来说，签名者是完全匿名的，所以环签名更具实用价值。自环签名提出后，大量学者发现其重要的价值，基于椭圆曲线、门限等多种环签名方案被设计开发，总体概括可分为门限环签名、关联环签名、可撤销匿名性环签名、可否认环签名四类。为实现区块链上智能合约代币交易隐私保护，我们使用一种基于椭圆曲线的环签名方案。

环签名可分为三个部分：**GEN，SIG，VER**，以签名者账户公私钥对(P,x)为例说明三个过程：

GEN：采集公共参数，签名者利用$GeneratePublicKeySet()$函数在万维链账户系统中随机选取$n-1$个账户，与签名账户共同构成环签名公钥集$publickeyset$：

$$publickeyset = GeneratePublicKeySet(P)$$

签名者利用公私钥对(P,x)，通过$GenerateKeyImage()$函数生成公钥镜像I：

$$I = GenerateKeyImage((P,x))$$

SIG：完成环签名。针对所需签名消息m，利用环签名公钥集$publickeyset$，公钥镜像I和签名账户私钥x通过$GenerateRingSignature()$函数生成环签名$ringsig$：

$$ringsig = GenerateRingSignature(m, publickeyset, I, x)$$

VER：验证环签名。基于消息m，利用环签名公钥集$publickeyset$，公钥镜像I和环签名$ringsig$，通过$VerifyRingSignature()$验证签名合法性：

$$flag = VerifyRingSignature(m, publickeyset, I, ringsig)$$

$flag = true$则签名合法；$flag = false$则签名不合法。

环签名设计方案中，由于环签名公钥集$publickeyset$中公钥账户真实存在，公钥镜像I和环签名$ringsig$均与签名账户无法对应，使得签名账户的匿名隐私性得以保证。交易验证者只能确定签名合法，且签名者是$publickeyset$中某一账户，却无法进行准确定位。

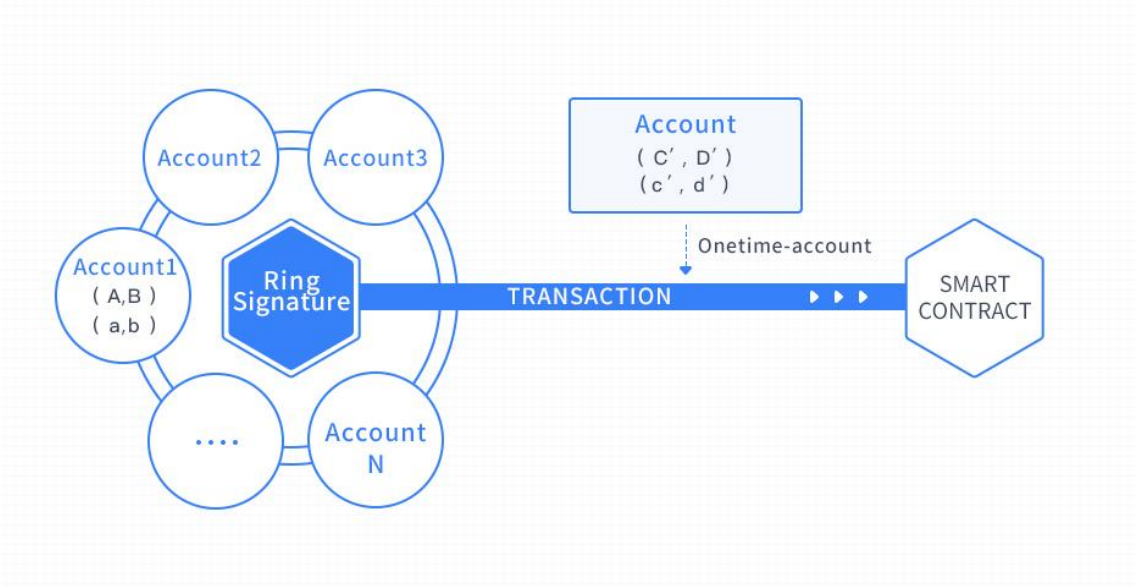

图 4. 4 环签名

4.4.3 代币交易流程

对于智能合约代币隐私交易流程具体描述如下：

用户 1 主账户为(A, B)，主私钥为(a, b)；用户 2 主账户为(C, D)，主私钥为(c, d)。用户 1 在智能合约SC（合约地址记为$SC_{Address}$）中一次性账户为$Onetime_account1$，对应私钥为sk_1，想要从这个账户中为用户 2 转移价值为$value$的代币。

- 用户 1 发起交易流程：

Step1：用户 1 利用用户 2 主账户(C, D)为用户 2 生成一次性账户$Onetime_account2$:

$$Onetime\_account2 = OTA\_GenerateAccount((C, D))$$

Step2：用户 1 使用$Onetime_account1$对应私钥sk_1通过 $GenerateSignature()$函数构造智能合约内交易签名sig，并构造合约使用数据$Payload$：

$$sig = GenerateSignature(Onetime\_account1, Onetime\_account2, value, nonce)$$

$$Payload = (Onetime\_account1, Onetime\_account2, value, nonce, sig)$$

Step3：用户 1 利用$GeneratePublicKeySet()$函数在万维链账户系统中随机选取$n-1$个账户，构成环签名公钥集$publickeyset$：

$$publickeyset = GeneratePublicKeySet(A)$$

Step4：用户 1 计算公钥镜像I并构造交易内容m：

$$I = GenerateKeyImage((A, a))$$

$$m = (publickeyset, SC_{Address}, Payload)$$

Step5：用户 1 计算环签名并构造最终合法交易$transaction$：

$$ringsig = GenerateRingSignature(m, publickeyset, I, a)$$

$$transaction = (publickeyset, SC_{Address}, Payload, I, ringsig)$$

Step6：用户 1 将合法交易$transaction$全网广播。

- 验证节点（Validator）流程：

Step1：验证节点接收到交易$transaction$，构造交易内容m并验证环签名合法性：

$$m = (publickeyset, SC_{Address}, Payload)$$

$$flag = VerifyRingSignature(m, publickeyset, I, ringsig)$$

Step2：若$flag = true$，执行 Step3；若$flag = false$，认为交易不合法，将其丢掉。

Step3：以$Payload$为参数调用智能合约，智能合约内部检测一次性账户签名合法性并进行相应操作。

上述过程完成后，则交易被确认，用户 2 使用其扫描秘钥检测合约内一次性账户信息，发现$Onetime_accunt2$属于自己，利用主私钥计算得到相应一次性私钥，进而获得$Onetime_account2$的使用权限，得到$value$代币。

5 万维链应用场景

5.1 基于公链之间价值传导的应用

按设计初衷，对于某一公有链来说，万维链首先类似于这条公有链的侧链，具备提升公有链拓展性的能力。万维链同时是一条支持智能合约的可编程链。当万维链连接多条公有链时，万维链的作用就能更好的体现出来。

- **众筹平台**

ICO 现已成为区块链领域众筹融资的重要手段，且这一趋势正向非区块链领域蔓延。以区块链技术为基础的代币作为权益体现是人类的重大创新。目前的 ICO

过程中，对价数字货币的支付，ICO 份额的记录等基本操作还是采用中心化的方式在处理，只有等到 ICO 项目的区块链代币正式上线，代币持有人才能以区块链的形式拥有自己的资产。这一过程不仅存在中心化风险，更造成购买人兑换可支付数字货币的不便利和 ICO 发起方管理资金的风险。

基于万维链开发的 ICO 众筹平台，或者单独的 ICO 项目，发行方可以以智能合约进行发行，使得整个众筹过程更加公正透明。持有不同数字货币的购买者可以将自己持有的数字货币（BTC、ETH 等）直接用万维链钱包转移到万维链上进行购买。ICO 发起方可以更加便利的管理自己募集的资金。以智能合约发行的 ICO 份额本身也是以代币的形式存在，在 ICO 对应的链和代币正式上线前，ICO 的份额具备了更好的流通性，可以直接进行交易。更进一步，当 ICO 项目上线时，将 ICO 链的代币接入万维链，用户可以自行完成 ICO 份额代币与 ICO 链代币的转换。

可以说利用万维链，我们将进入一个全流程完全基于区块链的数字权益发行时代。

- **博彩平台**

以太坊的白皮书中提到，基于区块链的智能合约能够很好的实现博彩应用，简单理解就是通过智能合约实现博彩的游戏规则，并通过代币进行博彩的投注。除了游戏规则和投注外，博彩很重要的一个环节是筹码的兑换，如果将代币看作筹码，随着更多数字货币的广泛应用，参与者希望更便捷的利用自己持有的任何一种数字货币兑换为筹码，万维链就提供了这样一个平台，除了具有利用智能合约实现游戏规则和筹码外，还是一个支持多种数字货币的筹码兑换平台。

- **去中心化的数字货币交易平台**

数字货币种类和价值的增加，使得数字货币的兑换成为重要的需求。目前完成数字货币的兑换主要依赖于中心化的交易所和场外交易中间人。所有交易都基于对交易所和中间人的信任。多币种接入万维链后，万维链成为了一条多资产的链，可以通过智能合约实现多币种的相互竞价交易和一对一的场外交易。万维链上提供隐私保护的交易机制，为有隐私保护需求的交易提供支持。将没有隐私保护的数字货币导入万维链，并在万维链中发起隐私交易，最终再将数字货币转回原有链，一定程度上通过切断资金追踪路径实现了原有链的隐私保护。这一使用场景类似于较早出现过的混币模式。

5.2 基于公有链和联盟链之间价值传导的应用

我们已经看到传统的资产以联盟链的形式映射到区块链上的趋势，例如银行的票据、商业积分等。但在很多场景下，未来会有更多的资产以基于联盟链的分布式账本形式记录。资产之间的交易、变现、贴现等业务意味着两种价值要完成转换。数字货币逐渐称为通用的交易媒介，意味着传统资产需要与数字货币进行交易。也就是说，联盟链和公有链之间需要进行连接和资产的交易。

- **商业积分等数字资产与数字货币的交易**

多个商家成立联盟链将通用的商业积分放到区块链上，商业积分成为客户持有的资产。客户除了使用积分进行消费，也需要将多余的积分变现。变现成法币是一种选择，当联盟链与公链链接后，变现成数字货币同样是一种选择。同理，例如社区代金券、游戏代币等基于联盟链的数字资产同样可以通过与万维链连接，实现不同数字资产、不同数字货币之间的相互交易。

5.3 基于联盟链之间价值传导的应用

- **供应链金融资产交易网络**

商业企业的供应链中有大量需要流动的资产，针对这些资产产生的金融业务被称为供应链金融。目前这一业务会被供应链中的强势方所主导，例如核心企业、大型物流企业，他们主导了一个个相对封闭的供应链金融网络，随着区块链技术的发展，更多这样的网络会利用区块链技术来实现多方信任，以达到资产更易流动的目的。不同联盟链网络如果需要进行跨网络的资产交易，使用万维链进行连接和中继，能更有效的扩大网络效应，增大资产和资金的利用效率。

当然在这种场景下，万维链除了可以发挥连接的作用外，还可以成为资产登记和公示的平台。通过将资产进行登记，避免同一个实体资产被重复上链进行交易或者融资。

5.4 基于与传统账本系统对接的价值传导应用

- **法币与数字资产进行链上交易的设想**

法币无法在链上与数字资产进行交易，关键的问题不在于法定数字货币的诞生。基于目前的银行体系，商业银行如果允许将用户的部分资产账本转移到区块

链上，同样可以实现法币与数字资产的链上交易。这样的前提是商业银行的中心化账本与联盟链的区块链账本相互连接，或者直接与公有链连接。用户可以申请开立资产的区块链账号，并将一定金额的资金转入区块链账号。这样用户通过万维链就可以实现法币与其他数字资产的交易。这种实现方法从本质上类似于第三方支付，区块链是一部分现金资产的记录账本，只不过这个账本原来是存在于第三方支付的中心化系统里，现在这个账本存在于一个更加透明和开放的区块链网络中。

6 结论

我们旨在设计并论证一个未来的区块链基础设施——万维链，以去中心化的方式完成不同区块链网络的连接及价值的交换。它能够为不同的区块链提供一个通用的资产跨链转移协议；同时万维链还是一个分布式账本，这个账本不但支持智能合约，而且支持智能合约代币交易的隐私保护。这样的设计能够支撑丰富的业务场景，尤其是金融应用场景。我们相信一个可以灵活开发的、满足多场景需求的、去中心化的价值交换系统是金融基础设施的未来。

万维链将重塑区块链经济生态。

参考文献

［1］NAKAMOTO.S, Bitcoin: A Peer-to-Peer electronic cash system

［2］Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper

［3］Stefan.Thomas, Evan.Schwartz, A Protocol for Interledger Payments

［4］Jae.Kwon,Ethan.Buchman, A Network of Distributed Ledgers

［5］Shamir A. How to share a secret. Communications of the ACM, 1979, 24(11): 612~613

［6］Blakley G.R. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies, V.48, 1979:313~317

［7］B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. In Proceeding 26th Annual Symposium on the Foundations of Computer Science, IEEE, 1985:383~395

［8］Desmedt Y. Society and group oriented cryptography: a new concept Advances in Cryptology-Crypto’87, 1987:120~127

［9］Ronald L. Rivest, Adi Shamir, and Yael Tauman, How to Leak a Secret: Theory and Applications of Ring Signatures, Springer Berlin Heidelberg, 2006,22(11):164-186

［10］Man Ho Au, Sherman S.M. Chow, Willy Susilo, and Patrick P. Tsang, Short Linkable Ring Signatures Revisited, EuroPKI 2006: Public Key Infrastructure pp101-115

［11］MONERO: Nicolas.van.Saberhagen, CryptoNote v 2.0

［12］Melanie Swan，Blockchain: Blueprint for a New Economy

［13］Adam Back, Matt Corallo, Luke Dashjr,Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille:Enabling Blockchain Innovations with Pegged Sidechains

［14］Stefan Thomas & Evan Schwartz: A Protocol for Interledger Payments

附录：专业术语

万维链（WAN Chain）：本白皮书所指的公共区块链，包含分布式账本、智能合约、跨链协议等内容，能够实现跨链交易、代币交易隐私保护等功能。

公有链（Public Chain）：完全开放、去中心化的区块链网络，任何参与者（节点、用户等）只要遵循公有链的协议都可以参与和加入网络。

私有链和联盟链（Private Chain）：与公有链相比，是开放性和去中心化受限的区块链网络，节点和用户的加入需要经过特定规则下的授权。

同构链（Homogeneous Chain）：基于万维链开发的公有链、联盟链或私有链，包含了相同的跨链协议、相同的资产跨链映射方法，可以与万维链无缝对接，并能实现资产的相互转移。为了形象的理解，我们把同构链称为 LAN Chain。

跨链交易（Inter-chain Transaction）：两条不同区块链之间资产的相互转移（对于原有链来说意味着转入或转出），其中一条链上的资产向另一条链转移时，该资产在两个账本中的可流动总额保持不变，不会造成资产的通胀或紧缩。

万维链跨链协议（WAN Chain Inter-chain Protocol）：基于万维链进行跨链交易时，钱包与节点、万维链节点之间、联盟链节点与万维链节点进行相关通信的规范，简称 WIP。其中至少包括：

- **万维链跨链交易请求**（WAN Chain Inter-chain Transaction Request）：简称 WITxReq，是一个打包的信息组合，其中包括两个部分的信息——跨链交易请求（Inter-chain Transaction Request，简称 InterTxReq）和原有链交易（Origin Chain Transaction，简称 OriTx）。如果原有链是 BTC 则表示为 OriTx(BTC)，原有链是万维链则表示为 OriTx(WAN),对于公有链 OriTx 遵循公有链的交易数据格式进行构造，钱包利用 OriTx 发起向原有链上万维链锁定账号的转账。万维链及万维链的同构联盟链可以按照原有链交易数据格式构造 UnlockedOriTx。OriTx 用于锁定原有链资产，与之相反 UnlockedOriTx 用于解锁原有链资产。
- **资产锁定标记（Token Locked Flag）：**简写 TLF，资产锁定过程中，万维

链节点根据 OriTx 对原有链是否完成该交易的成块进行校验并向其他节点公布 TLF 共识结果。

- **资产解锁标记（Token Unlocked Flag）**：简写 TUF, 资产解锁过程中，万维链节点根据 OriTx 对原有链是否完成该交易的成块进行校验并向其他节点公布 TUF 共识结果。
- **映射资产（Mapping Token）**：简写 MT，指万维链上对应于原有链资产的代币。

链标识（Chain ID）：万维链注册表中链的标识。交易中用 OriChainID 标记原有链。

万维链公共账户（WAN Account）：万维链上由验证节点（Validator）共同维护的账户，用于 Validator 发起万维链上的交易，进行智能合约的部署或调用操作等。

原有链账户（OriAccount）：原有链需要发起跨链交易的账户，Alice 的原有链账户表示为 OriAccount(Alice)。

原有链锁定账户（Locked Account）：表示用于锁定转出该链的资产的账户。

验证节点（Validator）：是指区块链中打包交易并进行交易验证的节点。在万维链中，我们把验证节点分为普通验证节点 Validator、跨链交易证明节点 Voucher、锁定账号管理节点 Storeman。

跨链交易证明节点（Voucher）：该类节点主要负责验证跨链交易时，原有链资产是否被原有链锁定账号锁定或解锁。

锁定账号管理节点（Storeman）：该类节点掌握锁定账号私钥的份额，在跨链交易过程中，使用掌握的密钥份额生成签名份额并合成完整签名，进而对锁定账户进行相关操作。