

2017-06

---

# 万维链

## 建立分布式的未来“银行”

Version 0.4.0

---

# 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.....	6
1.3 万维链设计目标.....	7
1.4 万维链的定位.....	8
2 万维链总体架构及技术特征.....	8
2.1 万维链总体架构.....	9
2.1.1 分布式账本及智能合约虚拟机.....	9
2.1.2 原生币.....	9
2.1.3 共识机制.....	9
2.1.4 链内交易.....	10
2.1.5 跨链连接.....	10
2.1.6 跨链交易.....	10
2.2 万维链技术特征.....	12
2.2.1 完全去中心化，无可信第三方参与.....	12
2.2.2 无需修改原有链机制，接入门槛低.....	13
2.2.3 基于密码学算法的安全性保证.....	13
2.2.4 跨链交易的隐私保护.....	13
3 万维链跨链通信协议.....	14
3.1 跨链协议功能模块.....	14
3.2 跨链交易数据传输流程.....	14

4	万维链关键技术 .....	17
4.1	万维链验证节点共识机制 .....	17
4.2	万维链权益激励机制.....	18
4.2.1	验证节点的激励机制 .....	18
4.2.2	普通节点的激励机制 .....	19
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 .....	19
4.3.1	安全多方计算和门限密钥共享技术介绍 .....	19
4.3.2	锁定账户生成方案 .....	20
4.3.3	锁定账户签名生成方案 .....	21
4.3.4	方案先进性分析 .....	22
4.4	基于环签名和一次性账户的代币交易隐私保护机制 .....	23
4.4.1	一次性账户系统 .....	23
4.4.2	环签名方案 .....	25
4.4.3	代币交易流程 .....	26
5	万维链应用场景 .....	27
5.1	数字货币借贷 .....	27
5.2	数字货币支付结算 .....	28
5.3	数字货币交易兑换 .....	28
5.4	数字资产投融资 .....	29
5.5	其他应用场景 .....	29
5.6	与传统银行融合设想 .....	错误!未定义书签。
6	结论 .....	30
	参考文献 .....	31
	附录：专业术语 .....	32

## 摘要

以比特币、以太坊为代表的数字货币的出现正在以燎原之势震动着传统的货币体系和金融体系。区块链技术虽然还处于发展的初期，但其更加透明、开放的理念和机制已经展现出无比的生命力。如何在区块链的时空中连接现在和未来是万维链探索的目标。

万维链旨在建立一个分布式的未来“银行”，正如传统银行是现代金融的基础设施一样，万维链的宏伟目标是建立一个分布式的数字资产金融基础设施。

万维链通过分布式的方式完成不同区块链账本的连接及价值交换。它应用密码学前沿理论，打造通用的跨链协议以及记录跨链交易、链内交易的分布式账本，无论公有链、私有链还是联盟链，均能低成本的接入万维链，实现不同区块链账本的连接及资产的跨账本转移。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。

通过万维链，任何机构和个人，都可以在未来“银行”中开设自己的业务窗口、提供基于数字资产的存贷、兑换、支付、结算等服务。通过“银行”提供的基于区块链的基础设施的保障，更多人能够享受更加丰富的基于数字资产的金融服务。更加准确的描述，万维链是一个基于区块链的分布式超级金融市场。

# 1 万维链设计理念

## 1.1 区块链的出现以及革命意义

奥地利学派著名经济学家哈耶克认为，让货币也像其他商品一样通过市场竞争来优胜劣汰，市场机制能够像提供其他商品一样为我们筛选出最合适的货币。2009 年 1 月，比特币的创世区块被挖出。比特币的出现大大超越了哈耶克理想的状态“控制货币总量的责任将由某些机构承担，这些机构的利己之心会使他们将货币总量控制在用户最能接受的水平上”。区块链将货币的信用基础由某些机构（主权政府或者其他机构）转移到纯数学方法和分布式架构上。

信用授权由机构转向不可侵犯的数学定律是人类历史上对于价值记录和交换的又一次伟大创新。从本质上来说，货币是一种共识，是人类为了方便进行价值交换而达成的协议的记账符号。回顾历史，人类从物物交换到使用牛羊、贝壳作为一般等价物，使用贵金属作为货币，使用信用基础更强的纸币，人类的货币的发展都在更加靠近数学或者更加抽象，符号和账本的性质更加明显。区块链让人类的记账符号更加靠近数学的同时，让整个记账系统脱离了单一机构的控制，朝着更加透明和公平的方向行进。

世界上有 25 亿人无法使用银行，他们开不了储蓄账户，无法获得信用卡，这些无银行账户的人与全球经济隔离；能够通过银行进行跨国汇款的用户也必须承担高昂的手续费；普通投资者只能在银行等金融机构购买收益相对较低的理财产品，却无法在未上市前参与诸如谷歌、阿里巴巴这样的科技公司的早期投资；大量的中小企业即使信用优良，业绩突出，由于不属于传统银行的 80/20 法则下的目标客户，很难从银行获得贷款支持。

“现实是历史的一个进程”，区块链技术的出现正在改变上述局面。在委内瑞拉货币贬值时，比特币成为抢手的避险资产。诸如菲律宾等，在外国打工的劳动者通过区块链网络将收入汇至银行设施薄弱的国内家乡。通过 ICO 形式参与以太坊等著名区块链项目初始投资的投资者获得了成百倍的投资回报。区块链技术正在将普惠金融推向一个全新的高度。

到 2017 年 6 月以区块链技术为基础的数字货币共有上千种，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。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，如商业票据、会员积分等记录到区块链上（更多的以联盟链的形式存在）。

与传统金融机构类似的数字资产金融模式已经出现，完成数字货币的兑换的交易所执行类似银行货币兑换的职能，购买和交易首次发行代币的平台执行类似证券交易所的职能，进行跨境转账的平台执行类似银行的跨境汇款职能。

而这些平台不同程度上都以中心化的方式在运行，这不但带来了中心化的安全和道德风险，也阻碍了区块链技术更大范围的应用。

基于此我们需要一个分布式的未来“银行”，在这里不同的数字货币和数字资产可以以区块链的方式转入转出并完成交易，在这里基于数字货币和数字资产的金融产品和合约可以被创建和执行，在这里相关的交易都能得到有效的隐私保护。当然这样的“银行”除了借贷、汇款、结算、销售金融产品等功能与传统银行类似外，会是完全不同的模式。任何机构和个人如果有相应的能力和资金实力，都可以在其中开设自己的业务窗口、提供不同的服务，通过区块链的分布式网络基础设施的保障，为更多人提供更加丰富的金融服务。或者更加准确的描述，这是一个未来基于数字资产的金融基础设施，是一个分布式的金融市场。

万维链正是要建立这样一个分布式的未来“银行”。

## 1.2 万维链设计背景

传统的银行在诞生初期是以货币兑换为主要职能，逐渐发展了货币保管、支付、结算、汇款等功能，最后诞生了以存贷业务为主要模式的现代银行。可以说银行是一个记录债权债务关系的账本，每一次资金的进出和转移，实际上是银行账本中对应资产账户的变动。并且银行的账本是一个支持多资产的账本。不同银行间的汇兑结算，实际上是不同账本间资产记录变动的过程。无论是同一账本中资产的变动还是不同账本中资产的变动，都必须确保资产不可被双花。简单来说某个资产在一个账户或账本中的增加或者减少必然对应另一个账户或账本中等值的减少或者增加。目前区块链已经很好的解决了在同一个账本不同账户中的双花问题。解决资产在不同区块链账本中的转移问题是区块链技术更大范围应用的关键。万维链需要以分布式的方式支持不同区块链的接入和资产的转移，也就是支持跨链交易。

有效的保护用户的隐私是传统银行赖以生存的根基之一，任何的金融交易都需要让无关第三方无法知晓。万维链需要具备同样的能力。

万维链是一个分布式的金融市场，原则上任何的机构或个人都可以基于万维链开发和提供自己的金融服务，这就需要万维链这一区块链设施能够支持可编程的智能合约功能。

综上，万维链正是在这一背景和考虑下设计。

### 1.3 万维链设计目标

为了打造分布式未来“银行”，让区块链技术和数字资产应用能够更大范围的普及。根据对已有技术的调研，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：

#### **跨链资产转移：**

- 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。

#### **提供交易的隐私保护：**

- 交易双方可以选择带隐私保护的交易所，选择该种交易所双方地址不可被追踪。

#### **具有场景的延展性：**

- 能够成为多种数字货币兑换的分布式平台。
- 能够开展不同数字货币的存贷业务。
- 能够以数字货币为媒介完成数字资产的交易。
- 能够发行和交易全新的数字金融资产。

## 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分布式的未来“银行”，通过建立不同区块链账本之间的连接，实现资产的跨账本转移，为基于数字货币和数字资产的金融应用提供一个基础设施。将区块链承载价值和传递价值的功能发挥到极致，将区块链的平等、开放的理念发挥到极致。

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金融应用。

## 2 万维链总体架构及技术特征

万维链在技术上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。



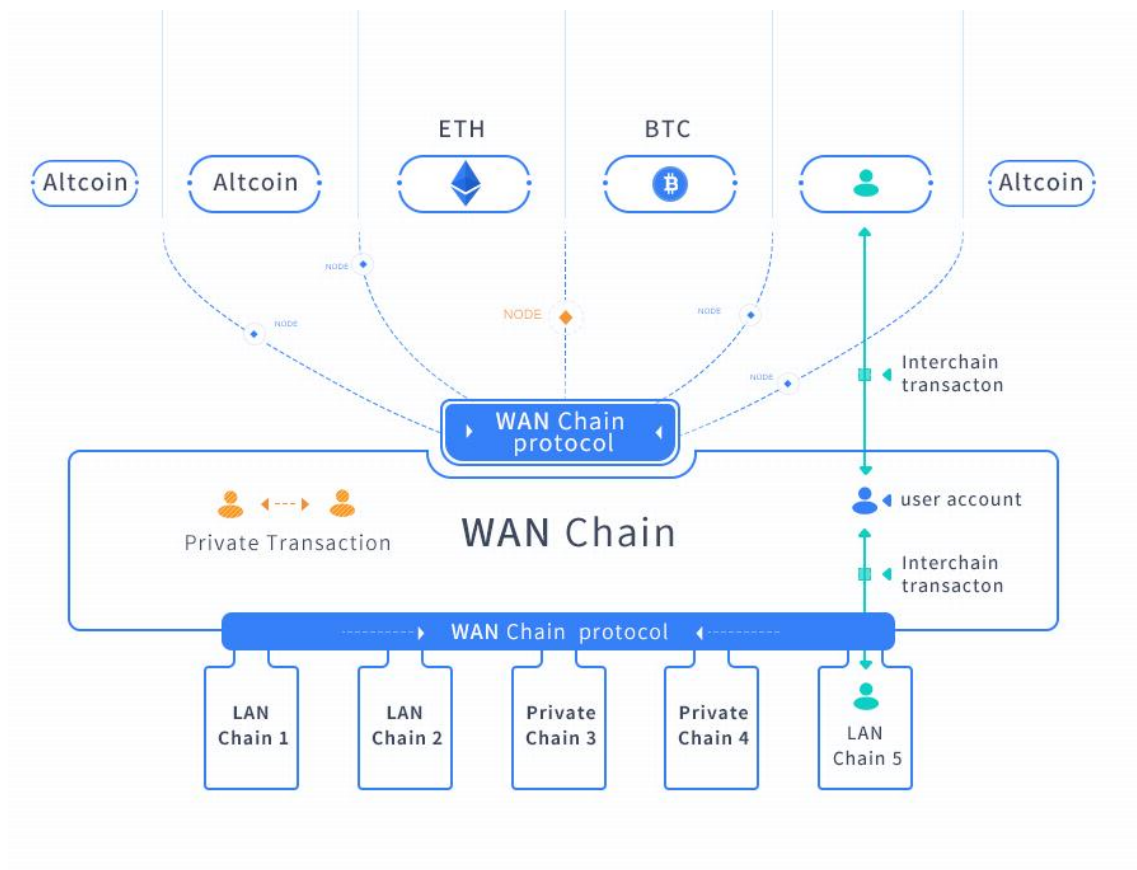


图 2.1 万维链模型图

## 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。

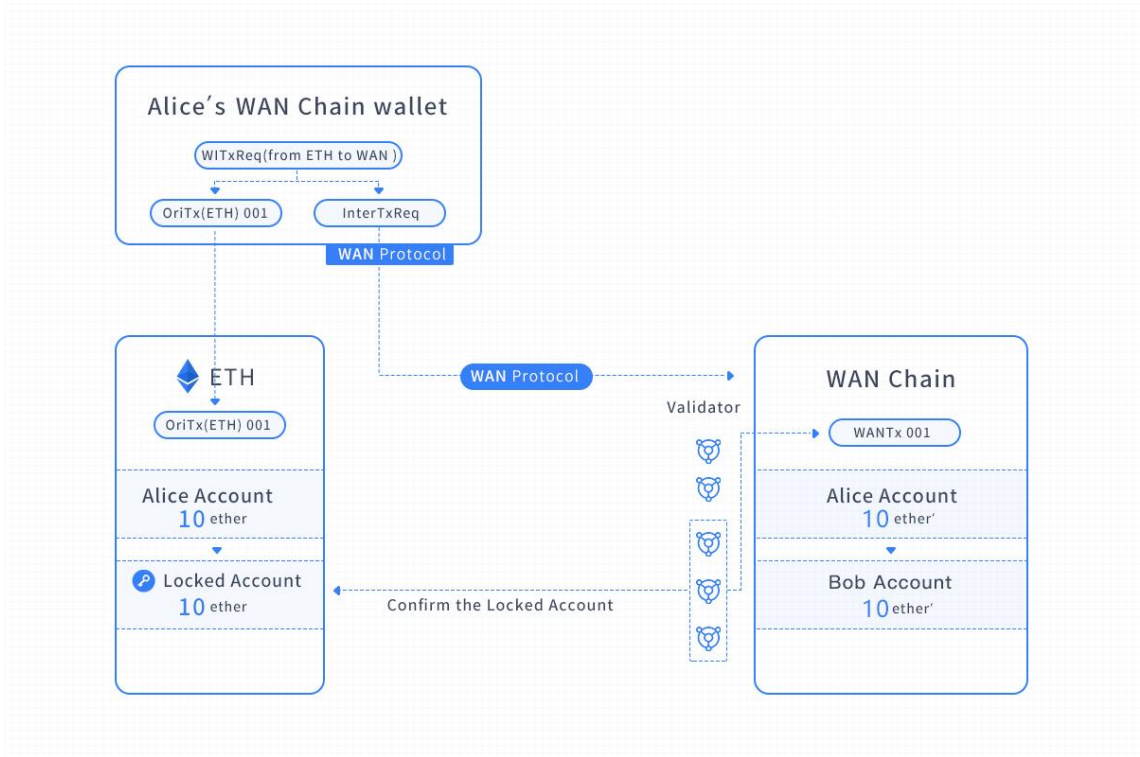


图 2.2 跨链交易——以太坊到万维链

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。

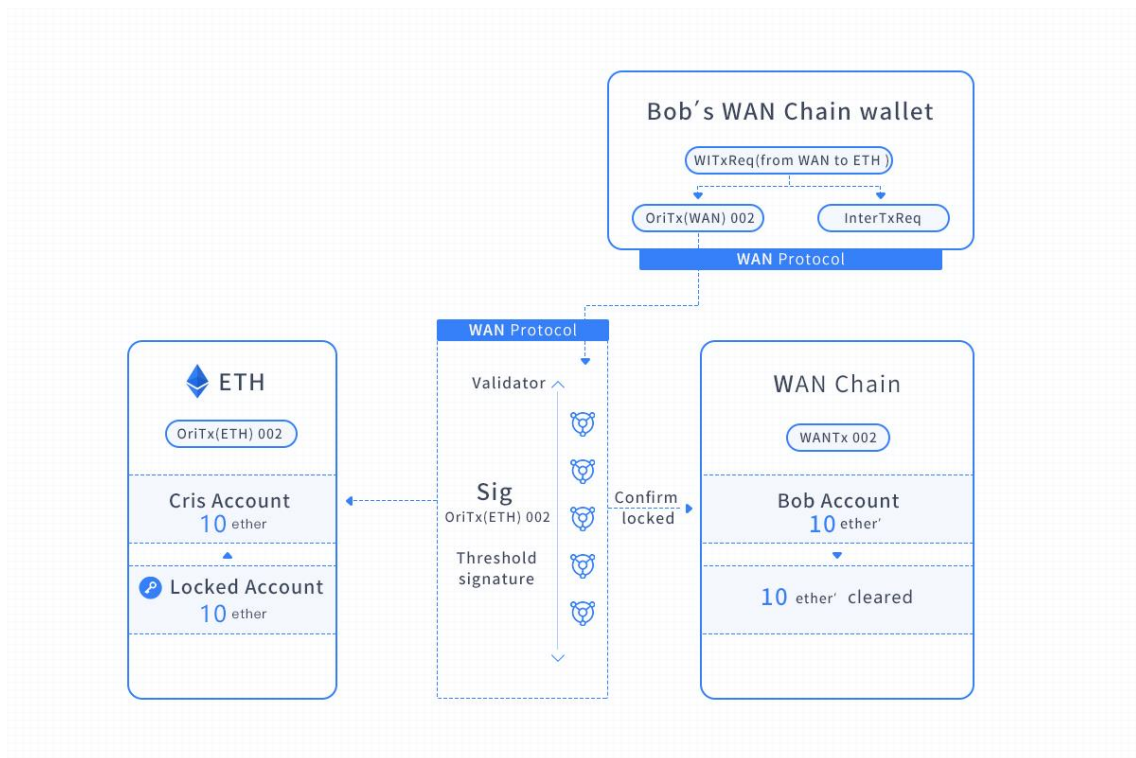


图 2.3 跨链交易——万维链到以太坊

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，这就将跨链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链交易请求 *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。

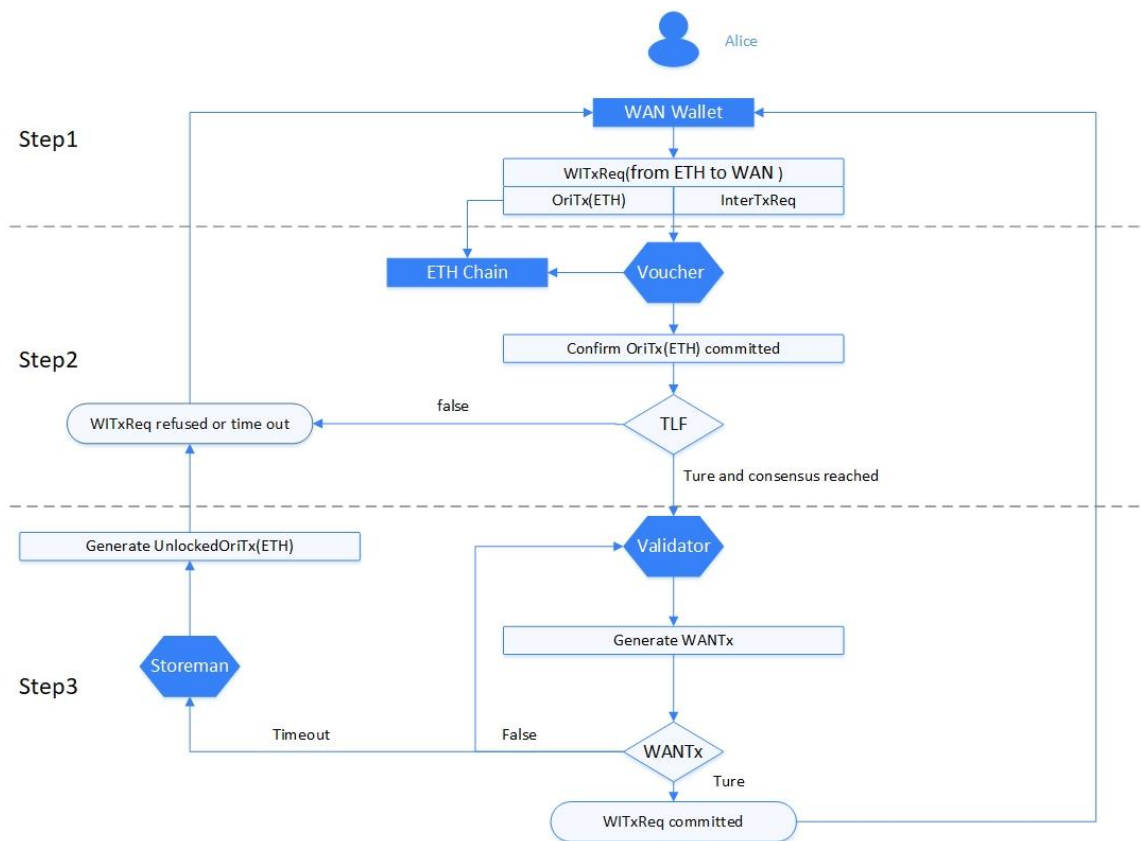


图 3.1 跨链数据流程——以太坊到万维链

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。



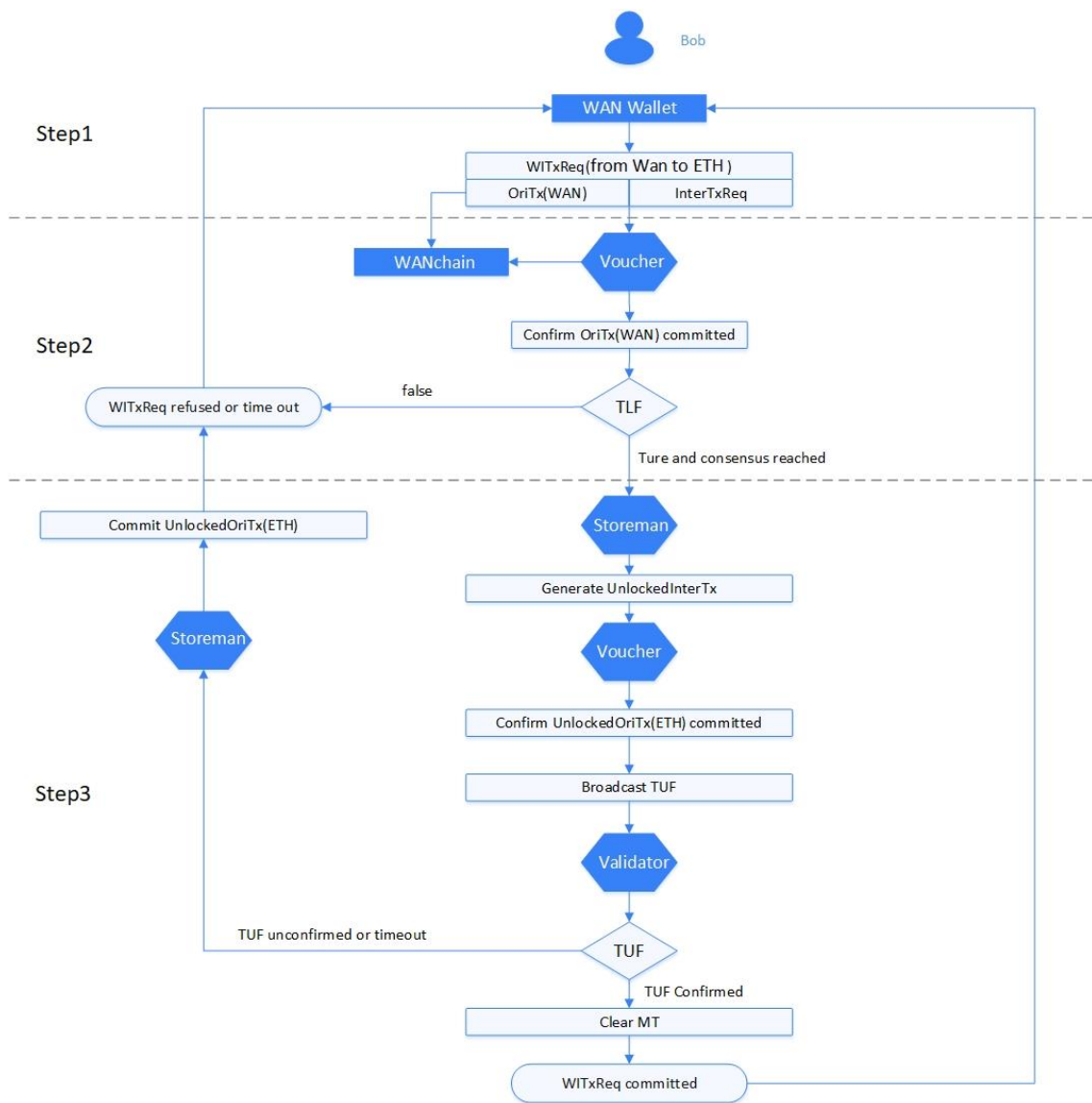


图 3.2 跨链数据流程——万维链到以太坊

## 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地完成万维链记账，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 $P_1 \cdots P_n$ ，共同安全的计算函数 $f(x_1, \dots, x_n) = (y_1, \dots, y_n)$ 。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 $P_1 \cdots P_n$ ），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：

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

如果 $flag = True$ ，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：

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

**Step4:** 计算锁定账户地址：

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

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。

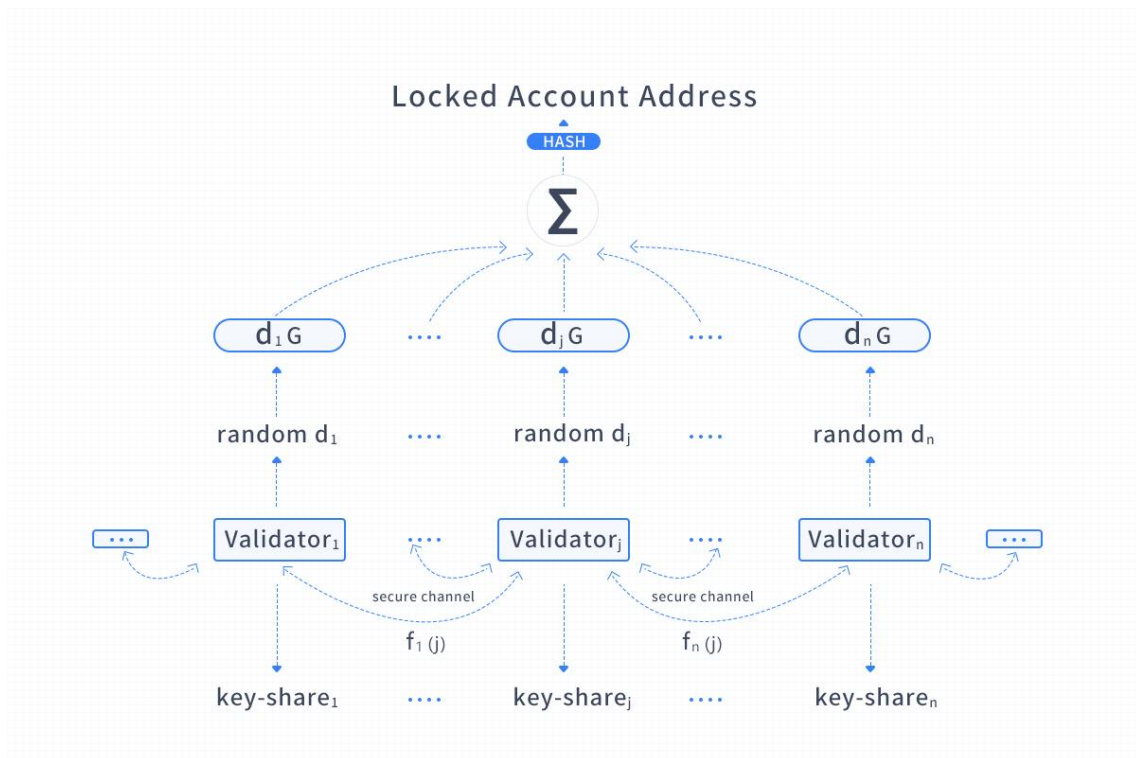


图 4.1 锁定账户地址生成

### 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：

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

此时 Locked Account 的完整签名便重构出来了。

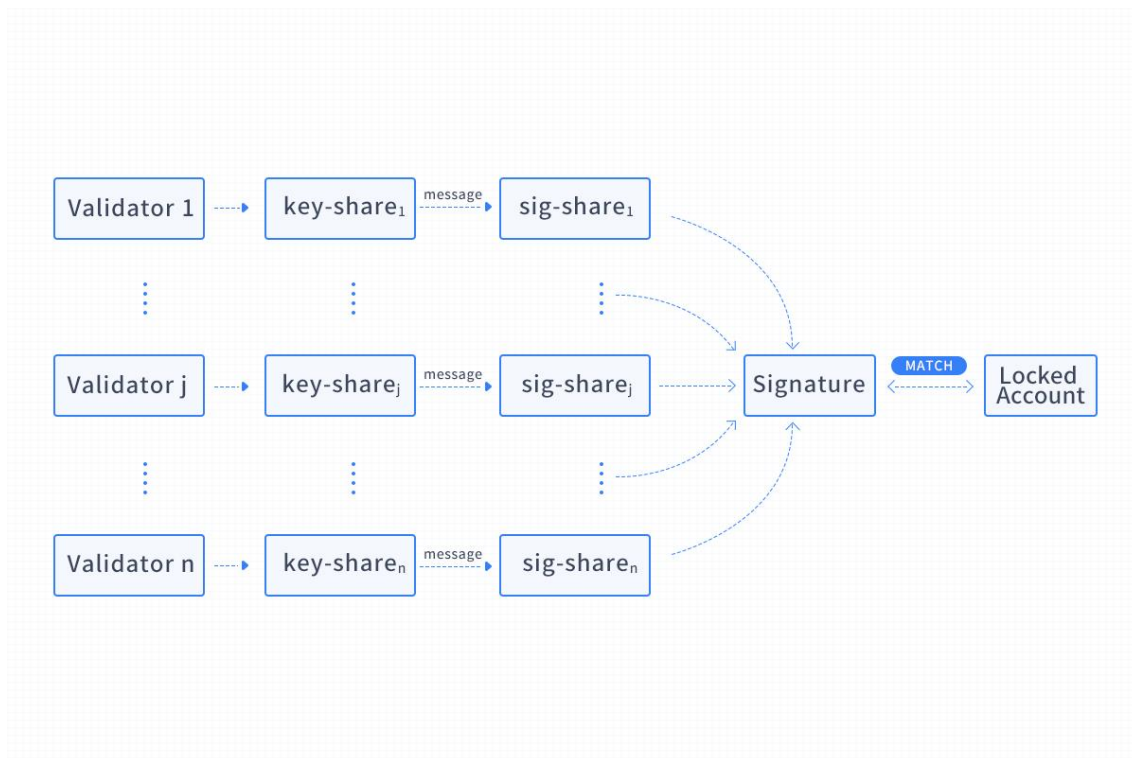


图 4.2 锁定账户签名生成

#### 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  $(A_1, S_1)$ ：

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

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

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

当检测到 $(A_1, S_1)$ 时 $\text{flag} = \text{true}$ ，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 $\text{OTA\_GetPrivateKey}()$ 函数得到一次性账户 $(A_1, S_1)$ 对应私钥 $sk$ :

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

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。

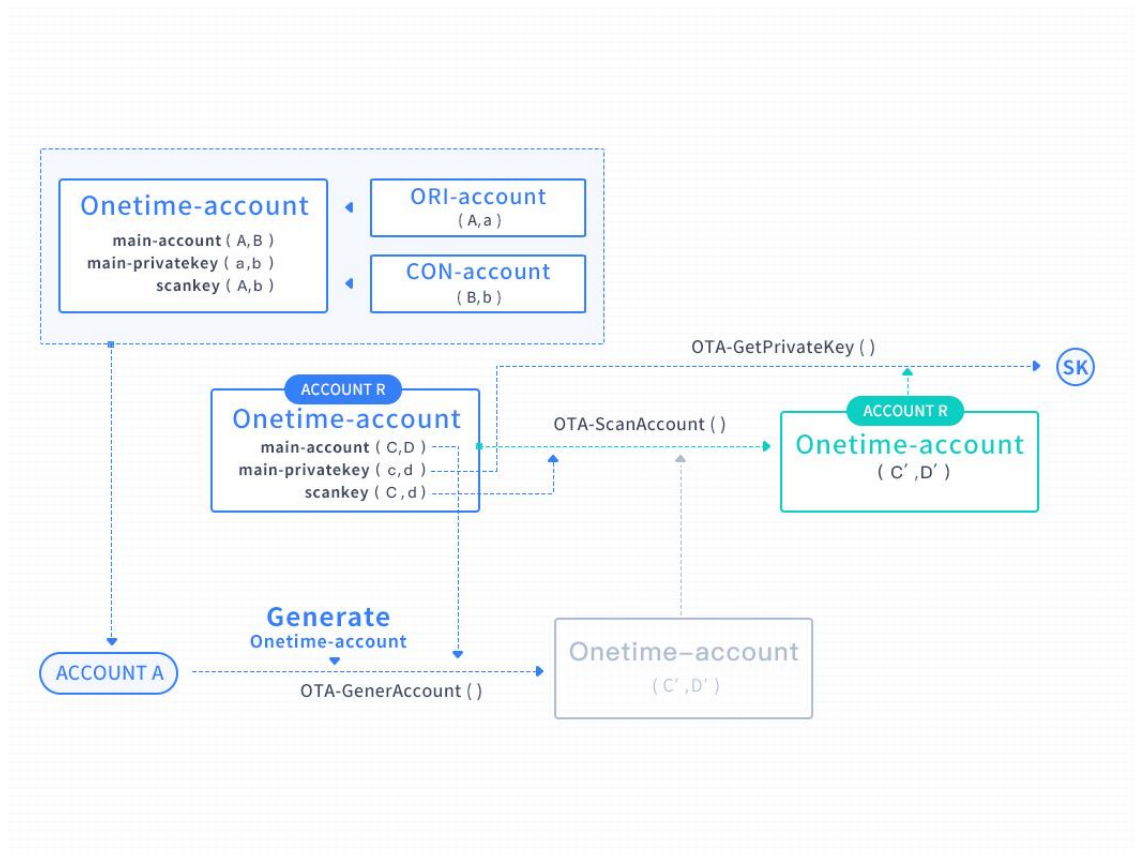


图 4.3 一次性地址系统



#### 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的建立过程, 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。

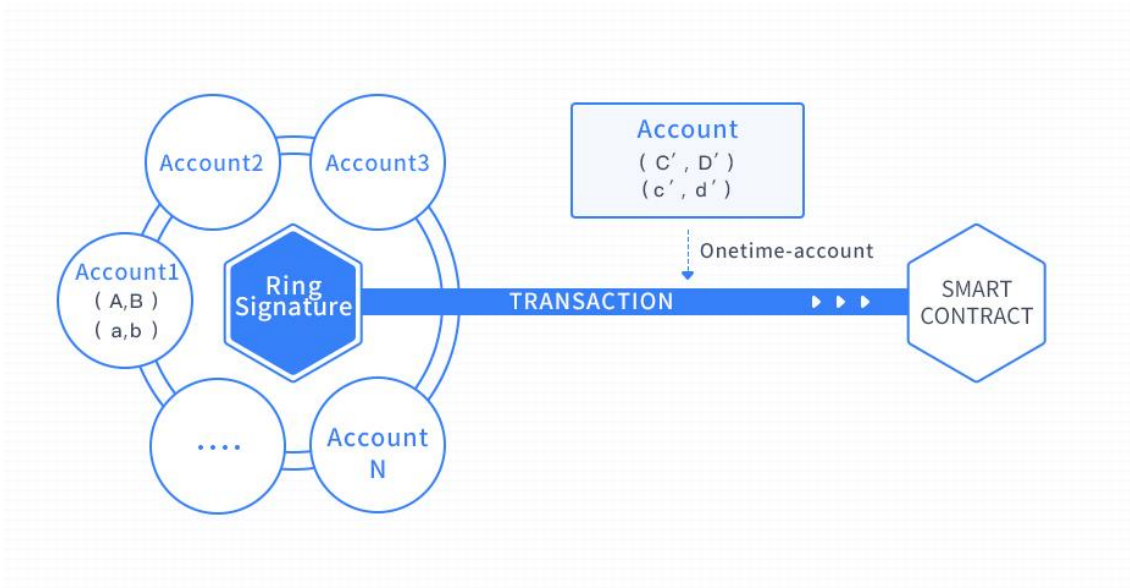


图 4.4 环签名

#### 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 数字货币借贷

随着数字货币成为更加广泛的交易媒介及更加重要的价值储藏载体，利用数字货币创造新的价值并获得相应收益是必然趋势，正如将比特币投资于“挖矿”，投资于其他区块链项目 ICO 类似。随着数字货币应用范围的不断增加，利用数字货币直接(不需要转换为法币，投资的收益也以数字货币计价)进行投资的领域和机

会逐渐增多。

利用数字货币创造价值的人需要更多的数字货币，手中持有数字货币的人需要保值增值，数字货币的借贷业务需求会越来越多。万维链支持具有信用和资金能力的机构或者个人作为数字货币的供需中介，完成存贷业务。以以太坊举例，实现方式是中介方在万维链上利用智能合约创建存款应用并设定利息，以太坊存入方通过跨链机制将以太坊上的以太坊转入万维链上的智能合约对应的地址，万维链上的存款智能合约发放对应该笔存款的凭证（万维链上的 **token**，类似银行的存单）到万维链上该用户的账户中，智能合约自动计算利息。当用户需要提取该笔以太坊存款时，将凭证转移回中介地址，合约执行跨链交易将凭证对应的以太坊在原链上解锁转移回原有用户的账号中。该场景优于传统模式的重要一点是，作为存贷中介方的存款准备金（该中介地址对应的被锁定的原链资产）是透明的，作为存款人能时刻知晓存款准备金情况。

## 5.2 数字货币支付结算

越来越多的商户正在接收比特币等数字资产作为支付手段，未来会有更多的商业场景将多种数字货币作为支付媒介。对于用户来说无论在电脑和手机上安装多个钱包进行支付都是不方便的，正如目前的支付需要 **VISA**，**Papal**，支付宝这样的中介机构进行支付结算的统一整合。万维链本身是一个分布式的多币种平台。从本质上说正如第三方支付将不同银行的账本接入在自己的统一账本下一样，万维链实现数字货币领域的类似功能。任何商户和用户都可以安装万维链钱包完成多币种的支付结算功能，而不需要安装多个数字货币钱包。

## 5.3 数字货币交易兑换

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。多币接入万维链后，交易所或者中间人可以通过智能合约实现多币种的竞价交易和一对一的场外交易。万维链上提供隐私保护的机制，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。

## 5.4 数字资产投融资

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，例如商业票据、商业积分、未来收益权、应收账款等。未来会有更多的金融资产以基于联盟链的分布式账本形式记录。当这些联盟链接入万维链后，联盟链成为金融资产的提供方，数字货币的持有者可以利用手中的数字货币购买这些资产进行投资。类比传统银行业务，这类似于在银行购买理财产品。区别在于更多的中介机构可以参与进来，或者资产持有人可以直接进行资产融资。

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。越来越多的项目，尤其是基于以太坊的项目，直接使用智能合约进行 ICO，整个过程更加透明公平，但是只能使用以太币进行众筹，给持有其他数字货币的投资者造成了不便。基于万维链开发的 ICO 平台，或者单独的 ICO 项目，发行方以智能合约进行发行的同时，可以支持多币种进行投资。投资人能够更加方便的用以太坊、比特币或者其他任何与万维链连接的区块链代币进行投资，发起方可以更加便利的管理自己募集的资金。更进一步，当项目上线时，新的区块链只要接入万维链，通过跨链机制就可以方便的完成众筹份额与原生币的转换。利用万维链，我们将进入一个全流程基于区块链的数字权益发行时代。

## 5.5 其他应用场景

上面描述的是最基本的应用场景，目的在于让读者更好的理解万维链的运行逻辑和价值。举一反三可以想到，通过万维链，可以发行基于数字货币的多币种信用卡；可以将多种资产打包进行资产证券化操作；可以进行基于多种数字货币的 P2P 业务，众筹业务等。

区块链技术在银行中的应用已经被各大银行视为重要战略，但出发点多是基于如何利用区块链技术改造传统业务；而数字货币领域货币兑换等类银行的业务已经在蓬勃发展。区块链在这两个领域的进展，如同两条平行线。随着数字资产在经济中的比重日益提升，与现实经济的融合不断增强。这两条平行线同样会走向融

合：数字资产进入银行的资产负债表（银行支持数字资产的存贷），银行的资产负债表部分转移到区块链上（法币以区块链 token 的形式表示和记账）。万维链跨账本资产转移的特性将能够支持未来的融合。

## 6 结论

在本文中我们试图构想未来“银行”，我们采用“银行”一词是为了让更多的读者能够有一个直观的理解，是一种类比的表述。将区块链技术从比特币概念中抽象出来，变成一项中性的技术从很大程度上推动了区块链在全球范围的推广应用。但目前也同样面临着巨大的障碍，传统的银行尝试用区块链解决现有的业务问题，就需要评估成本与风险，决策者难以在财务报表的压力面前去冒如此大的风险，更何况这不是一个银行改变就足够的。

万维链构想的未来“银行”是一种基于数字货币的金融形态，在纯业务层面与目前传统银行业务很相似，在本质与组织形式上却不同。正如互联网和移动互联网产业并没有从传统产业内部发芽一样，而是诞生了全新的产业和商业模式反过来影响和改变了传统产业。当数字货币在经济中的比重不断增加，基于数字货币本身和数字货币理念的新的金融业态将蓬勃发展。当然传统银行在一定时间也将以自己的方式加入到数字货币经济中来，逐渐发展出一个传统资产与数字资产融合的金融生态。

我们旨在设计并论证一个未来的分布式金融基础设施——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。基于该设施，更多的中介机构能够开发自己的金融服务，通过万维链打造分布式未来“银行”。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，是普惠金融的未来。

## 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
- [15] Paul Vigna & Michael J. Casey: Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order

## 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。

**ICO (Initial Coin Offering):** 是数字货币和区块链社区的产物, 一般称之为原始币发行。ICO 源自于 IPO (Initial Public Offering), 即“首次公开发行”, 指股份公司首次向社会公众公开招股的发行方式, ICO 与之非常类似, 只不过发行的不是股票而是数字币, 一般称之为代币 (Token)。