



ZV CHAIN: 高安全性、高性能的专业化金融公链

白皮书 v0.4.4

ZV CHAIN 研发团队
2019 年 6 月 21 日

前 言

紫微垣，三垣之一，亦称紫微宫。按《步天歌》，紫微垣为三垣的中垣，位于北天中央位置，故称中宫，以北极为中枢。有十五星，分为左垣与右垣两列，《宋史·天文志》：“紫微垣在北斗北，左右环列，翊卫之象也。”

目录

1 ZV CHAIN 的技术与应用战略	1
1.1 高安全性 Layer1 层	2
1.2 高性能 Layer2 层	3
1.3 区块链金融中间件层	4
1.4 区块链金融场景应用层	5
1.5 智能金融支持模块层	5
2 ZV CHAIN 的创新金融设计	7
2.1 Chiron 共识机制	7
2.1.1 开放型参与机制	9
2.1.2 矿工奖励机制	10
2.1.3 组链模型与块链模型	11
2.1.3.1 组链模型	11
2.1.3.2 块链模型	14
2.1.4 收敛优化与通信优化	17
2.1.5 分叉处理	17
2.1.6 Check Point 机制	18
2.1.7 共识分析与系统安全	19
2.1.7.1 共识分析	19
2.1.7.2 系统安全分析-攻击防御	20
2.2 隐私计算与安全框架	26
2.2.1 数据隐私和监管	26
2.2.2 形式化证明	28
2.2.3 通讯的安全	29
2.3 金融智能合约	29
2.3.1 合约升级	30
2.3.2 重大异常修复（硬分叉）	31
2.3.3 高效 VM 与合约语言-Python	31
2.3.4 金融业务标准组件库和组件市场	31

2.4 跨链技术	32
2.4.1 跨链的主要类型	32
2.4.2 ZV CHAIN 的跨链协议	34
3 ZV CHAIN 性能优化方案	36
3.1 分片并行计算框架	36
3.2 ZLight 闪电网络	37
3.2.1 ZLight 单向闪电网络模式	37
3.2.2 ZLight 双向闪电网络模式	38
3.2.3 ZLight 分支行架构	38
3.3 分布式数据存储	39
3.4 P2P 网络	41
3.4.1 NAT 穿透	42
3.4.2 组播网络	42
3.4.3 RUDP	43
4 ZV CHAIN 的技术架构	44
4.1 ZV CHAIN 核心技术架构	44
4.2 ZV CHAIN 节点架构	44
4.2.1 节点类别	44
4.2.2 节点功能	46
4.2.3 节点关系	48
5 可演进性与场景跃迁	50
5.1 技术扩展与演进	50
5.1.1 基础架构可扩展性	50
5.1.2 核心技术可演进性	50
5.1.2.1 以博弈论为基础的共识机制	50
5.1.2.2 链下计算的趋势	51
5.2 应用场景跃迁	51
5.2.1 基本的清结算体系	51
5.2.1.1 ZV CHAIN 交易支付体系	51
5.2.1.2 ZV CHAIN 跨境清结算体系	52
5.2.1.3 ZV CHAIN 稳定币发行及其跨境结算示例	53
5.2.2 智能金融服务体系	56
5.2.2.1 ZV CHAIN 智能产品与服务生态系统	56

5.2.2.2 ZV CHAIN 智能风控体系	56
6 技术路线与里程碑	59
参考文献	59
A 技术术语表	62
A.1 Chiron 共识术语与符号	62
A.2 结算网络实体名称	63

— ZV CHAIN 的技术与应用战略

ZV CHAIN 提出一种新型的共识机制 Chiron，它采用 VRF 真随机数 [1] 解决去中心化问题，同时，通过组内并行协作方式快速达成共识，目标 TPS 3000。另外，基于我们多年在大型分布式系统的经验，在提案、验证和出块三个环节都保证了无单点设计，进一步提高系统的性能和鲁棒性。通过严格的数学论证和工程分析，我们认为 Chiron 共识机制给出了迄今为止全球范围内不可能三角定律的最优解。下图 1.1 阐述了 ZV CHAIN 的技术及其应用战略。

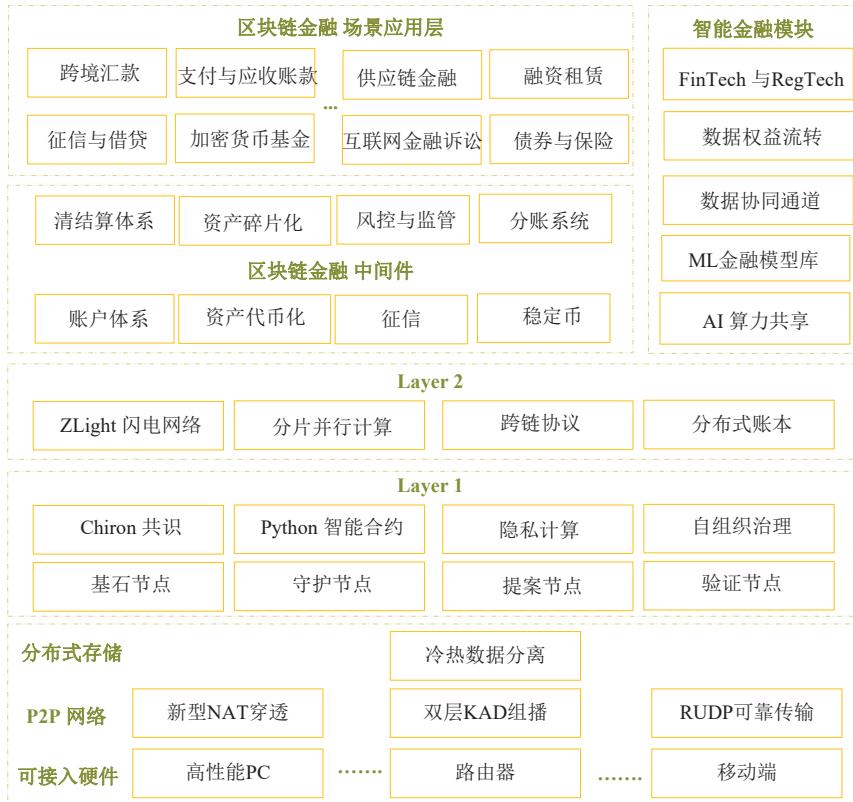


图 1.1: ZV CHAIN 的技术及其应用战略

我们试图构建一个人人可便捷参与的高安全去中心化网络，基于这个网络可以用很低的成本开发可持续发展的商业应用。同时通过一系列数学、密码学和工程技术的引入，让这个网络在保证去中心化和高安全的同时，也能够达到高性能和低能耗。

1.1 高安全性 Layer1 层

在 Layer1 层，我们研发的共识机制 Chiron 采用分组 VRF+BLS 的工作机制，分组 VRF 保证不能私自挖矿，防御长程攻击，并对 51% 攻击的要求提升到需要控制 95% 的节点。同时 POS 权益质押与铸块收益概率线性相关，抵制了女巫攻击，并通过奖惩制度克服了无利害关系。设计应用层对通讯进行分类，需要安全信道的场合均采用 ECDH 算法对通讯信道进行加密，保证通讯的安全性。用户账户安全，我们采用零知识证明技术，确保账户的安全和隐私保护。智能合约执行安全，则在智能合约提交后，系统将对智能合约进行形式化验证，对合约的安全进行审计，确保执行的安全。ZV CHAIN 将不同的设备分为轻节点和重节点两类，并根据矿工对 ZV CHAIN 系统的贡献，提出了矿工健康度指数。

- 嵌入真随机数算法（VRF 与 BLS）的分组共识协议

ZV CHAIN 采用了基于融合技术的共识机制，它结合了 VRF+BLS，并引入了分布式系统中的分片、高并发协作、预处理等技术。其设计思路大致如下：系统必须可以通过增加节点提升吞吐能力，目前来看，分片机制是最佳选择方案。所以共识机制必须支持分片处理，矿工分组是最适配的方式。

分组模式下，最大的风险来源组员联手作恶。我们采用 VRF 秘密抽签方式随机选出提案组，并行发送候选区块到验证组，验证组内最先达成门限签名的候选区块胜出，这样的并行协作机制大幅降低两者联手作恶的可能。验证的效率决定系统的处理性能。从通讯复杂度，签名长度，性能来看，我们认为验证组采用 BLS 门限签名性能强于组内拜占庭容错，即使类似 Zilliqa 对 PBFT 做优化，也只能达到接近门限签名的性能和效果。

- 安全合规的金融智能合约与深度定制 VM

目前，大部分支持智能合约的区块链系统，都采用栈式架构的虚拟机，栈式架构很好的解决了不同物理操作系统间的一致性问题，但同时也导致了运行效率低下。ZV CHAIN 的 TVM 基于 LLVM 路线，在保证一致性和扩展性的基础上，显著地提高了合约的运行效率。

- 隐私计算

隐私计算（Privacy-Preserving Computing）[\[2\]](#) 是通过技术手段实现在保护数据隐私的前提下，完成对数据的安全处理。从密码学角度来看，隐私计算指的是采用以安全多方

计算和同态加密等为代表的现代密码学技术，在保证原始数据安全隐私性的同时，实现对数据的分析计算。

ZV CHAIN 在账户的安全和隐私保护，我们采用零知识证明（ZKPs）技术。证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。公有区块链的隐私将通过使用 ZKPs 技术得到进一步提升，除了声明的有效性，这个验证方法并不会透露出其他的信息。结合该技术应用于区块链上面，可以用来隐匿交易双方和交易金额，保障用户账户安全和隐私保护。对于数据存储安全和隐私保护方面，我们引入同态加密技术。

1.2 高性能 Layer2 层

ZV CHAIN 在设计之初就考虑了系统的效率成本，合理利用全网算力。针对 sharding 机制 [3]，Chiron 共识机制采用分组策略，从底层支持 Layer2 的分片并行计算框架术 [4]。Layer2 层随机选取部分组执行分片并行计算，其他组在闲置时，定期执行 check point，对区块数据的准确性进行验证。同时 ZV CHAIN 采用分级处理的思想，对系统数据（账户，交易，智能合约等）采用冷热备份的思路，大多数节点只需存储热门的数据，提升数据存储的效率成本。

- 分片并行计算

ZV CHAIN 借鉴 Google 的 MapReduce 和阿里云批量计算思想，设计了分片并行交易执行框架，支持数据分片处理，VRF 分组机制保证不同组之间可以并行处理不同任务，可将系统的吞吐量提升一个数量级。

- ZLight 闪电网络

作为专业的金融公链，引入闪电网络技术不但可以提高系统吞吐量，而且是分支行架构必不可少的一部分。因此，我们研发 ZLight 闪电网络，它可以让基金账户里的交易安全地离线进行，只需周期性和主链进行清算同步，而不需要把频繁的小额交易实时上链。闪电网络技术可以快速在 ZV CHAIN 的 B 端商家和 C 端用户建立便捷的轻量连接，并安全的完成交易。

- 分布式账本存储

现有的区块链项目，无论是比特币、还是以太坊，所有挖矿节点都需要存储全量的数据，日积月累，所有节点都耗费了几百 G 甚至上 T 的数据，这造成了极大的存储浪费，同时新节点的冷启动需要等待很长的一段时间。我们认为对于历史数据的访问是一种很低频次的操作。我们借鉴 Cassandra 和 HBase 等一些列存储的分布式存储系统设计思想，以及阿里冷热数据分离的一些工程实践，可以优化区块链的相关存储。我们计划在第一阶段，重节点进行全量账本的存储。在第二阶段重节点实现全量账本的分布式存储。重节点负责出块提案。轻节点仅存储部分账本以及近期高度的账户相关状态，以组协作方式对候选区块进行验证签名。即使手机作为轻节点，在有配套的 APP 情况下也可参与 ZV CHAIN 铸块。

1.3 区块链金融中间件层

基于底层深度定制的金融公链，以及上层的金融业务场景，抽取一些通用的功能模块，我们将分阶段研发多个，以提高安全性与性能为目的的中间件，DApp 开发者通过调用 API 可方便获得相关中间件支持。

- 清结算体系

ZV CHAIN 清结算网络采用分布式账本技术和闪电网络来加强用户端、商户端和企业端的信息交换和结算的效率，并为金融网络活动的安全性和可靠性定义了统一的技术和功能型标准。同时，ZV CHAIN 跨境清结算网络由代理节点和双向闪电网络完成，代理节点需要支持当地商户所接受的与法币勾兑的稳定币和 ZV CHAIN 原生代币作为最后的结算工具。

- 风控体系

风险控制是金融企业的生命线，风控的好与坏决定了金融机构能否盈利。而业界最先进的风控都是基于大量的历史数据和实时数据，构建智能的规则引擎和风控模型，进行风控管控。风控涉及用户的大量的隐私数据以及商业秘密，数据不能直接上链。ZV CHAIN 的链上智能合约使用风控预言机接口得到风控结果，根据风控的不同结果进行对应的业务处理，如同意授权或者拒绝放款等。

1.4 区块链金融场景应用层

针对不同的业务场景与用户需求 [5]，我们将考虑采用两种服务模式提供技术支持，包括 BaaS(区块链即服务)[6] 和 DApp 开发，以满足不同类型用户，以及不同业务规模的需求。采用场景跃迁的理念，我们将陆续提供如下的场景应用：

- 供应链金融
- 融资租赁
- 互联网金融诉讼
- 支付与跨境汇款
- 资产代币化与碎片化
- 征信与借贷
- 债券发行与保险
- 加密数字货币基金

1.5 智能金融支持模块层

人工智能技术实施的三要素包括：机器学习算法或者模型、大数据和高性能算力。近年来，一方面，大部分行业已经实现了大数据化，并开始向智能化转型，尤其是金融领域，智能金融服务潜力，越来越成为业界共识。另一方面，传统的中心化的 IT 架构业也暴漏出很多问题，如个人隐私数据泄露、中心化平台沉淀用户数据进行商业化应用，以及知识创新无法得到有效保护等等。为了解决这些问题，许多行业将目光转向了目前正飞速发展的区块链技术及其应用，并尝试向去中心化的区块链架构迁移。与此同时，区块链技术作为实现金融价值互联的底层网络基础设施，难以满足金融业务智能化的需求，因此，需要接入大数据处理模块、机器学习算法库，以及人工智能的算力支持。我们将在底层公链为智能金融模块的设计提供系统完善的架构支持，并且，在区块链金融中间件部分，为数据、算力和模型的协同调用提供支持。

- 数据协作通道

数据协作通道提供公链内外的大数据交换，一则，可以接入外部不同类型与维度的数据，为我们训练智能模型提供数据支持；二则，为确权后的公链数据提供价值流动创造条件。协作通道功能我们主动适应数据时代的定制化设计。

- AI 算力共享

我们将基于公链底层架构设计高性能设备共享的功能，提高链上计入高性能设备的利用效率，满足公链用户研发智能金融模型的需要。

- ML 金融模型库

通过集体智慧的共享，尤其是公链上机器学习算法专家的智能模型训练“智慧”，我们为各类复杂多样的智能金融服务需求，提供金融模型库，方便同类需求的公链 DApp 用户调用。

- 数据确权与价值流转

首先，通过底层公链隐私计算模块，实现公链用户数据保护与确权；然后，为有偿授权的数据提供交易与使用通道，并使授权用户获取数据共享收益激励；最后，将基于共享数据训练的模型结果输出，完成数据价值的流转过程。

- FinTech 与 RegTech

我们将研发基于上述的不同机器学习金融模型的智能化服务，满足各类传统金融业务以及传统金融监管的智能化升级，从而实现真正意义上的金融科技（FinTech）与监管科技（RegTech）。

二 ZV CHAIN 的创新金融设计

2.1 Chiron 共识机制

从比特币诞生至今，学术界和工业界对区块链的共识机制持续研究，诞生了多种机制、协议与算法，但是这些成果都无法破解一个难题：如何同时满足去中心化、安全、性能的共识三角。POW 机制性能低并且高能耗；POS 机制无法兼顾去中心化与性能；HASH 图与 DAG 更多是解决一致性问题而非准确性问题。这些共识机制一般会取去中心化、安全和性能里的两个点进行强化，而很少从全局考虑最优解。有些共识机制偏向单纯的学术化，在互联网工业界大放异彩的分布式协作、分层处理、预处理和多级缓存等成熟的技术并没有被很好的引入区块链。另外，很少有共识机制对无利害关系、51% 攻击、女巫攻击、长程攻击等安全问题做全面的分析和论证。在 ZV CHAIN 中，我们设计了一种全新的共识机制 Chiron，它结合了 VRF+BLS，并引入了分布式系统中的分片、高并发协作、预处理等技术。Chiron 共识对轻节点矿工随机采样形成若干个验证组，组协作 VRF 算法产生的真随机数来确定每轮的验证组，全网重节点矿工通过 VRF 以秘密抽签的方式给出候选区块提案给到验证组，验证组以组协作方式来完成候选区块验证给出最终出块。

Chiron 共识机制的优点主要包括：在去中心化方面，它比比特币更佳，任何可联网设备均可成为节点。并设计了轻节点和重节点机制兼顾广度和深度。在安全性方面，VRF 真随机数选组，确保某高度上工作组唯一，消除长程攻击和私自挖矿问题，同时需要控制 95% 的节点才能发起类似比特币的 51% 算力攻击。在性能方面，在不做分片等优化的情况下，目标 TPS 3000。Chiron 包含一系列数学理论工具、密码学算法及完备的协议，其核心机制可以精简成如下过程：轻节点矿工节点被分组，通常 100 个节点为一组。每次出块时，全网重节点通过 VRF 算法随机选出提案组，使提案人随机，不可预测，限制了提案与验证联手作恶的情况。在提案时多通道并行发送给验证组。由基于门限签名算法的 VRF 机制选择验证组，保证了验证组的不可预测、不可选择和不可隐藏。在真正出块时，只需在组内达成轻量级验证，以多通道并行流水线方式快速出块。

通过与前沿公链的对比，我们可以看出 Chiron 的全面优势：

与 BTC 相比，Chiron 在去中心化与安全性上更强，且性能大幅提升，能耗大幅降低。与 EOS 相比，Chiron 在性能上大致相当，但在去中心化与安全性上有明显的优势。我们认为，

表 2.1: 与主流及新型公链的对比优势

	对比优势 指标	去中心化	安全性	性能
其他公链				
ZV CHAIN	BTC	√	√	√
	EOS	√	√	
	Dfinity		√	√
	Algorand		√	√
	Cardano		√	√
	Zilliqa		√	√

区块链系统的去中心化 > 安全性 > 性能 [7]。与 Dfinity[8] 相比, Chiron 在去中心化上与之相当, 但是 Chiron 的组内被设计成一个小的分布式协作体, 组员之间通过分工协作极大的提高了性能和鲁棒性。区块提案人由全网重节点 VRF 秘密抽签方式随机产生, 提案人与验证组联手作恶难度从组层面提升全网层面, 大幅限制两者联手作恶的可能。与 Algorand 相比, 分组 VRF 接力模式在每个铸块高度都有唯一确定且无法预测的验证组一一映射; 候选区块定向广播给验证组; 验证时组内 BLS 门限签名达成共识, 在通讯, 签名数据大小, 性能都具有明显的优势。与 Cardano 相比, Chiron 全网节点都可以参与铸块, 且出块的每个环节都做了无单点的镜像设计, 如图2.1所示, 通过提高系统的鲁棒性带来平均性能的显著提升。与 Zilliqa 相

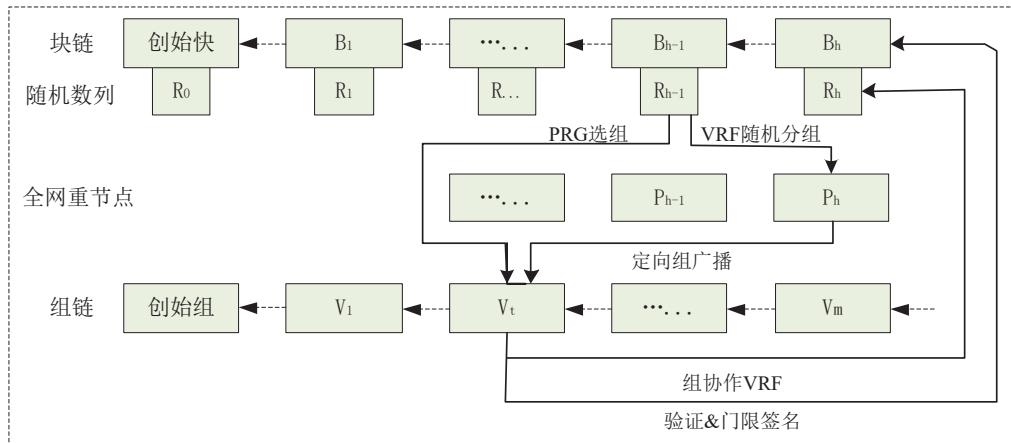


图 2.1: Chiron 铸块流程图

比, Chiron 验证组内所有成员收到门限个签名后均能恢复出最终组签名, 不需选定某位成员成为 Leader, 完成最后的多重签名聚合操作, 系统的鲁棒性以及安全性更好。通过与主流及新兴公链的比对及数学与形式化的论证, 可以得出结论, Chiron 共识机制是迄今为止“不可能共识三角”问题的最优解, 领先于目前所有已知的共识机制。

同时, 为保证系统的正常运行, 我们对全体矿工有一定的假设要求:

1. 系统中存在诚实矿工和恶意矿工
2. 诚实矿工比恶意矿工多
3. 诚实矿工和恶意矿工的行为受经济利益的驱使，诚实矿工通过遵守规则获利，恶意矿工通过破坏规则获取更大的利益

2.1.1 开放型参与机制

Chiron 共识采用开放型的参与机制。在这机制里，普通用户可以通过申请加入系统成为矿工；矿工也可以选择通过申请注销自己的矿工身份，回归为普通用户。对此，我们设计了特殊的智能合约：矿工申请合约和矿工注销合约，并写入创世块中，供用户调用。矿工的注册。普通用户可以提交矿工申请合约来申请成为矿工，申请时用户需指明矿工的类型（Type：提案矿工或验证矿工）。每个矿工都有自己唯一的身份号：

$$ID = transhash(pk)$$

其中 pk 是该矿工作为普通用户的公钥， $transhash$ 现在采用输出 256bit 的哈希函数。普通用户的公钥是与它的矿工 ID 一一对应的，而且在整个系统内也是唯一的。矿工申请合约将 $(pk, Type)$ 写入区块链中。原则上，我们希望重节点上的矿工担任提案矿工，轻节点上的矿工担任验证矿工。矿工的注销。矿工可以提交矿工注销合约来申请退出 Chiron 共识。同样的，矿工注销合约会写入区块链中。在等待一定周期后（大于组存续周期），如图2.2所示，用户可以调用保证金赎回合约，系统将释放保证金给用户。Chiron 共识对轻节点矿工随机采

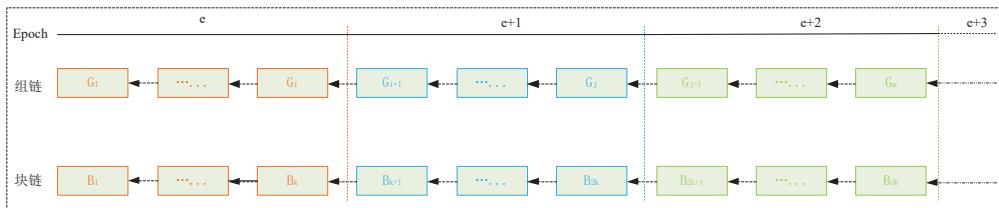


图 2.2: Chiron 组周期划分示意图

样，形成若干个验证组，组协作 VRF 算法产生的真随机数作为 PRG 函数的随机种子，产生的随机数来确定当前 slot 的验证组，全网重节点根据上一块区块的随机数，进行 VRF 分组，随机选出当前 slot 的提案组，提案成员给出若干个候选区块提案定向广播给当前 slot 的验证组，验证组以组协作方式来完成候选区块验证，并通过门限签名方式达成组内共识向组外广播。出于数据的不可篡改性，以及可追溯性，如上图所示，Chiron 机制采用双链模型，区块链和组链，来记录整个数据链产生过程。同时考虑组内矿工可能会形成组内携手作恶，所以

组有存续周期，到期后会解散重新进入随机采样分组流程。所以当系统进入稳定状态，每当进入一个新纪元（epoch）都可能有新组生效，老组解散的情况发生，每个纪元的工作组列表会发生相应变动。

2.1.2 矿工奖励机制

ZV CHAIN 的设计必须实现对矿工的经济激励，让他们的付出有所收益，以此系统才会良性发展。经济激励模型必须做到让所有矿工可根据自身付出的劳动获取相应的报酬，可预期，可审计，可追溯，公平公正却又不可篡改。上述的阐述更像是一个商业的劳动报酬合约的内容，智能合约正是为此而生。自然而然地，智能合约成为实现经济激励模型的最好方法。

ZV CHAIN 系统在每一轮铸块开始启动一个特殊的智能合约，参与铸块（包括提案和验证）的每位矿工，在完成自己对本轮的计算工作后，携带相应工作证明的凭证 call 该合约，合约为其记录工作证明，并计算出奖励份额。在一定时间窗口后，系统自动触发该合约的奖励逻辑，将奖励打入矿工账户。如图2.3所示，

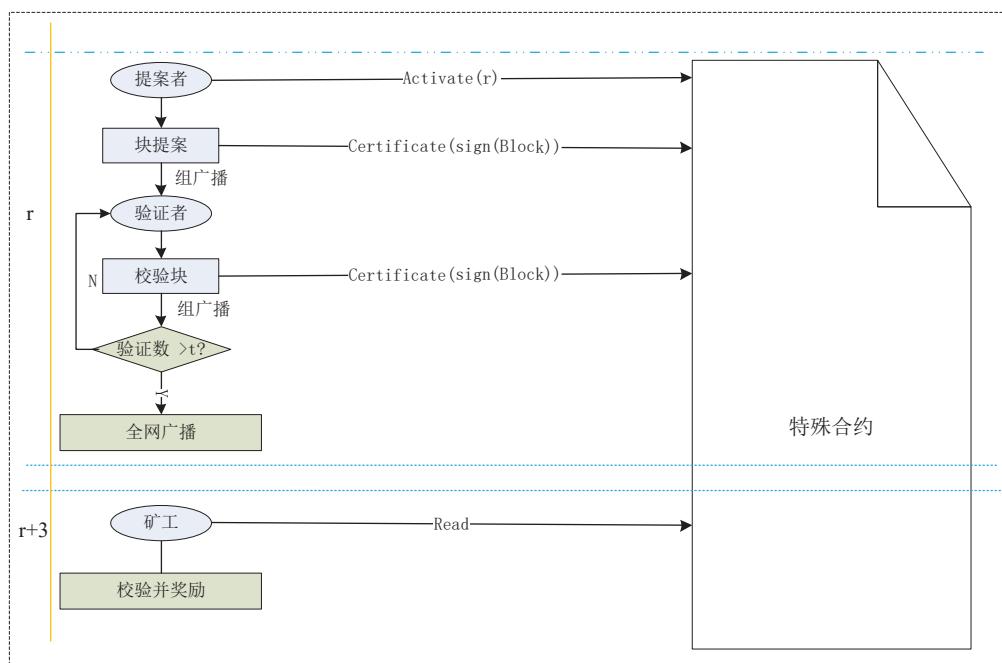


图 2.3: Chiron 经济奖励流程图

ZV CHAIN 采用智能合约实现经济激励的设计，不仅可以实现安全公正的经济激励，同时为评估每个矿工节点的健康指数等参数提供了重要的数据基础，根据这些数据统计，我们可以轻易地识别出系统的积极矿工和消极矿工，而矿工的健康指数可以直接对矿工后续继续参与 Chiron 计算有着正向反馈的功效。

2.1.3 组链模型与块链模型

2.1.3.1 组链模型

1. 组块的数据结构

- Type: 矿工组类型（提案组或者验证组）
- Hash: 组块哈希值
- GIS:parent 组（定义见建组检查章节）指定的信息
 - Activation: 组生效的纪元
 - Deactivation: 组失效的纪元
 - MinerArray[]: 候选矿工数组
 - * pubk: 矿工对应的用户公钥
 - * ID: 矿工的身份号
 - Signature:parent 组对 GIS 的签名
 - Prehash:parent 组块哈希值
 - gpk: 组公钥
- Signature:parent 组对 GIS 的签名
- Prehash:parent 组块哈希值
- gpk: 组公钥

2. 建组检查

ZV CHAIN 系统以 CheckInterval（系统参数）为周期来做建组检查。假设当前第 r 轮 slot，若 r 是 CheckInterval 的倍数，则在铸块完成后，当前工作组需要进行建组检查。考虑链同步的问题，我们假设系统网络广播需要 d 个 slot 的时间，那么可以认为前 d 块之前的区块已经一致。即块高小于等于 $r-d$ 的区块全网已经同步。组成员通过查询区块数据中的矿工申请合约，按一定条件筛选，得到新工作组的矿工候选人数量满足建组要求。则由该工作组作为父亲组，发起新组创建的提案。

3. 新组提案

当前工作组作为父亲组，对新组提案，主要任务是确定新组成员人选。主要策略是根据候选人的健康指数进行排序，以当前区块的真随机数为种子产生伪随机数序列随机挑选，

确保选出的新组成员的健康指数分布与所有候选人的健康指数分布类似。即保证有部分高健康指数的组员的同时会携带一些低健康指数的组员。从分组选人上大幅降低“僵尸攻击”的概率。另外，当前工作组必须为新组指定生效纪元。比如为当前纪元 e 之后的第 2 个纪元 $GIS.Activation = e + 2$ 指定新组的失效纪元时，可以由系统预先设定的参数 $ValidPeriod$ 确定 $GIS.Deactivation = GIS.Activation + ValidPeriod$ 。由于上述候选人序列，选择新组成员策略都是可审计的。所以当前工作组内的诚实矿工，计算出来的组块内容应该都是一样的。所以可以由组内每个矿工分别各自出新组块，对自己的新组块签名，然后发给组内其他成员。组员在收到大于等于门限个的相同 hash 的新块，可以用它们的组员签名恢复出组私钥对该组块进行签名。作为新组的父亲组，需要调用创世块中的分红智能合约模版，为新组创建分红合约，并公布该合约，这些合约最终会写入区块中。

4. 新组创建

由于组成员是去中心化网络上的对等节点，现实中某些时刻，节点因种种原因不在线不可避免，比如网络信号不好，恶意节点故意不作为等等。所以我们设计验证组需要有 (t,n) 门限签名的能力，这里是组成员数，是恢复的门限值，通常 $t \leq n$ 。即有含门限个以上的组员对消息认可签名，就能代表全组个成员对消息的认可，并能恢复出全组对此消息的认可签名。这里我们采用了去中心化的 Shamir 秘密共享算法，来产生各个组员的组内签名私钥 S_i ，组内签名公钥 mpk_i ，以及代表组共识的组公钥对应的组公钥 gpk ，得到上述密钥，并对组公钥 gpk 达成共识，才算完成组创建。

传统的 Shamir 密钥分享技术 [9]，可以看一个需要“中心”的过程。即它首先要有个“分发者”，“分发者”决定采用哪个秘密多项式，然后将秘密分解，发放给其他人。而区块链网络是去中心化的网络，每个节点都是平等，对等的节点，不应产生中心化的“分发者”。另外，分发者是先于其他节点知道秘密的，如果分发者在过程中做恶，是很难预防的，因此我们采用了去中心化的密钥分享算法。其核心思想就是：让每个组员都成为“中心”（即秘密分发者），那结果就是没有物理上的“中心”。但会在组的逻辑层面上形成一个初始秘密（该秘密每个成员均不知晓）。每位组员通过下述步骤的前三步会形成一个组逻辑层面的分享秘密 S_i 。类似传统 Shamir 密钥分享算法，分享秘密集合 S_i 具有门限恢复秘密 SK 的能力，即 S_i 中任意不少于 t 个分享秘密均能恢复组初始秘密 SK，任意少于 t 个分享秘密均无法得到组初始秘密 SK 的任何信息。

具体执行步骤如下：

(a) 每个组员自行选取各自的秘密多项式

$$f_i(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + \cdots + a_{i,t-1}x^{t-1}$$

其中多项式系数 $a_{i,0} a_{i,1} a_{i,2} \cdots a_{i,t-1} \in GF(p)$, 均为每个组员自取的随机数。则每人的初始秘密 $sk_i = f_i(0) = a_{i,0}$, 以 sk_i 作为私钥, 计算对应的公钥 pk_i 。

- (b) 每个组员计算给其他组员的分享秘密并将该分享秘密发给对应的组员。即: 第 i 个组员, 计算 $S_{i,j} = f_i(ID_j)$, 发给第 j 个组员。其中 $i = 1, 2 \cdots, n; j = 1, 2 \cdots, n$; 同时把自己的公钥 pk_i 也发给其他组员。
- (c) 当组员收集齐其他组员发给自己的分享秘密后, 计算所有收到的分享秘密 $S_i = \sum_{j=1}^n S_{i,j} = \sum_{j=1}^n f_j(ID_i)$ 计算 $gpk = \sum_{i=1}^n pk_i$ 。
- (d) 每个组员计算组内签名私钥 S_i 所对应的公钥 mpk_i , 并将组内签名公钥 mpk_i 告知给组内其他组员。

注意, (b) 步的组间成员间通讯, 需要对通讯进行加密, 防止被监听。在新组块信息 MinerArray 里, 记录着组内所有组员的普通用户公钥 pubk, 我们以此作为 ECDH 密钥交换做加密通讯。

经过上述步骤, 每个组员获得了组内签名私钥 S_i , 组内签名公钥 mpk_i , 以及组私钥 SK 对应的组公钥 gpk 。而组逻辑层面还隐含着获得的组私钥 $Sk = \sum_{i=1}^n sk_i$ 因为每个组员只知道自己的初始秘密 sk_i , 故没法知道 SK 的值。

下面对组员的组内签名私钥 S_i 具有门限恢复组私钥 SK 进行证明:

(a) 正确性证明:

对任意 $k \geq t$, 由于组员顺序不影响结果, 不妨假设前 k 个组员。令 $F(x) = \sum_{i=1}^n f_i(x)$, 通过 k 个组员组分享秘密的 Lagrange 插值多项式 $G(x) = \sum_{i=1}^k S_i \prod_{j=1, j \neq i}^k \frac{x-ID_j}{ID_i-ID_j}$, 容易知: 对 $1 \leq i \leq k$, 均成立

$$F(ID_i) = \sum_{j=1}^n f_j(ID_i) = \sum_{j=1}^n S_{j,i} = S_i,$$

$$G(ID_i) = S_i$$

令 $H(x) = F(x) - G(x)$, 容易知道 $H(x)$ 是最高次数不超过 $k-1$ 次的多项式, 而 $H(ID_i) = 0$ 对 $1 \leq i \leq k$ 均成立, 所以 $H(x) \equiv 0$, 即 $F(x) = G(x)$ 。所以通过 k 个组员组分享秘密的 Lagrange 差值多项式即是组的秘密多项式。计算 $F(0) = G(0) = \sum_{j=1}^n f_j(0) = SK$

(b) 安全性证明:

由于 $F(x) = \sum_{i=1}^n f_i(x)$ 是最高次数为 $t-1$ 次的多项式，多项式系数 t 个，而当 $k < t$ 时，只能构建个等式，由线性代数知识可知，方程个数小于未知数个数时，无法求解出未知数（解不唯一）。即无法确定多项式系数，从而无法确定 $F(x)$ 。所以等 $k < t$ 时，无法得到组初始秘密 SK 的任何信息。

全网节点（包括新组成员节点）在收到相同的新组组公钥，达到门限 t 个以上时，才认为新组创建成功，组公钥为真，将新组块写到本地的组链上。

5. 组异步创建

每次创建新工作组，均需要由父亲组协商决定新组的候选人列表，并通知新组成员，由新组成员自行达成组内密钥创建。而申请加入组和真正执行组创建这两种行为是异步的，由上述知道新工作组创建时，要求所有组员同时开始发送分享秘密，但在实际情况下，这个条件变得很苛刻，因为只要有一个成员不在线，就无法完成建组工作，因而会大大降低建组成功的概率。为了解决这个问题，Chiron 共识从工程上实现支持新组创建的异步模式。即组创建时，允许有成员不在线，但只要在合理的时间内上线，并发现自己被指定加入新组，则自行发起上述建组步骤的第 1, 2 步，将自己的分享秘密分发给其他组员，其他组员收到它的分享秘密后，反馈自己的分享秘密给该组员。这样能异步收齐所有组员分发的分享秘密即可新组创建成功。

2.1.3.2 块链模型

1. 区块的数据结构

- BlockHeader: block 块头信息
 - Hash: 当前块 hash
 - Height: 当前块高
 - CurTime: 当前块铸块时间
 - PreHash: 上一块 hash
 - PreTime: 上一块铸块时间
 - Castor: 提案人 ID
 - GroupId: 工作组 ID
 - Signature: 随机数

- Rand: 工作组 ID
- Transactions[]: 交易集 hash 列表
- Nonce

2. 结合 ECDLP 的 Shamir 秘密共享方案

我们采用的 Barreto-Naehrig 椭圆曲线 $E : y^2 = x^3 + b$ $b \in GF(p)$

其中，有限素域 $GF(p)$:

$$p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$

$$p = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

这里 x 是 63 bit 的数，p, r 均为 bit 长度在 256 左右的素数。

两个有限群 $G_1 = E(GF(p))[r]$ $G_2 = E[r] \cap Ker(\pi_p - [p])$

我们采用近年来论文中 bn 椭圆曲线上最优线性对算子 $e : G_1 \times G_2 \longrightarrow GF(p^{12})$ 定义为：

$$e(Q, P) = (f_{6x+2}(P) \cdot H)^{(p^{12}-1)/r}$$

这里 $H = l_{Q_3, -Q_2}(P) \cdot l_{Q_2 + Q_3, Q_1}(P) \cdot l_{Q_1 - Q_2 + Q_3, [6x+2]Q}(P) f_{6x+2, Q}(P)$ 是可以通过 Miller 算法计算的。

由双线性算子的特性：对任意 $P_1, P_2 \in G_1, Q \in G_2$, 成立 $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$

对任意 $P \in G_1, Q_1, Q_2 \in G_2$, 成立 $e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$

对任意 $p \in G_1, Q \in G_2, a, b \in Z$, 成立 $e([a]P, [b]Q) = e(P \cdot Q)^{ab}$

这里，记 $[.]$ 为椭圆曲线上的倍乘。如 $[a]P$ 是椭圆曲线上点 P 的 a 倍乘积。基于椭圆曲线的签名算法：

- $m \in \{0, 1\}^*$: 需要签名的消息（二进制表示）
- 计算 $R = H(m) \in G_1$
- 计算 $\sigma = [x]R$, 其中 x 是用户签名私钥, σ 即为所得签名

那么结合上述的组创建（去中心化 Shamir 秘密共享），对组员签名私钥 S_i 与组私钥 SK，存在如下关系：

$$SK = \sum_{i=1}^k S_i \prod_{j=1, j \neq i}^k \frac{x - ID_j}{ID_i - ID_j}, k \geq t$$

则对消息 $m \in 0,1^*$, 每位组员的签名为 $V_i = [S_i]R$, 由双线性椭圆曲线的上述特性, 可得:

$$[SK]R = [\sum_{i=1}^k S_i \prod_{j=1, j \neq i}^k \frac{x-ID_j}{ID_i-ID_j}]R = \sum_{i=1}^k \prod_{j=1, j \neq i}^k \frac{x-ID_j}{ID_i-ID_j} V_i$$

简而言之就是, 在双线性椭圆曲线上, 上述的构组方式所得组员签名私钥对消息签名后, 当得到 k 条组内成员的消息签名, 可以用 Lagrange 插值多项式得到组私钥 SK 对该消息的签名。

在 Shamir 秘密共享算法中, 恢复组私钥 SK, 是要泄露 S_i 的。利用双线性映射 e 的性质, 在不泄露 S_i 的情况下完成组私钥的签名, 保证了组员签名私钥可以不断复用。通过使用该技术, 可以通过门限签名来实现组内共识, 而且效率比拜占庭算法 (BFT) 更高。

3. 组协作 VRF 随机数

由于组私钥 SK 无人知晓, 所以该签名 $[SK]R$ 具有不可选择, 不可预测, 不可改变, 却可以通过组公钥 gpk 来验证签名 $[SK]R$ 是否由该组签出的。它是一种组协作 VRF 随机数生成方法。

Chiron 系统采用的随机数生成方法, 就是采用上述组协作的 VRF 方法。记 $B^r.Rand$ 是第 i 轮 slot 出的区块的 Rand 值。对于第 r 轮 slot, 使用的随机数 $R_r = \text{hash}(B^{r-1}.Rand)$ 按选组策略可以确定第 r 轮 slot 的工作组, 由当前工作组对做签名, 收集组内门限个以上的签名后, 恢复的组私钥对 $(r|R_r)$ 签名作为当前 slot 生成随机数, 写入第 r 轮 slot 所出的区块的 $B^r.Rand$ 。

$$B^r.Rand = \text{recover}(\text{sig}_1(r|R_r), \text{sig}_1(r|R_r), \text{sig}_2(r|R_r), \dots, \text{sig}_t(r|R_r),)$$

前一块的 Rand 确定当前块的工作组, 当前工作组以上述公式产生当前块的 Rand, 确定下一块的工作组。其中 RR 是创世块中的 Rand, 由系统初始设定。若第 r 轮 slot 的工作组没能完成出块, 则第 $r + 1$ 轮使用的随机数

$$R_{r+1} = \text{hash}(\text{hash}(B^{r-1}.Rand))$$

按选组策略可以确定第 $r + 1$ 轮 slot 的工作组, 对 $(r + 1|R_{r+1})$ 做门限签名, 产生当前块的 Rand。若第 $r + 1$ 轮仍未出块, 当前 slot 使用的随机数, 以及当前块随机数生成准则, 以此类推。

4. 验证选组策略

假设当前进入第 r 轮 slot，计算：当前纪元 $e = r/epoSlots$

随机数 $R_r = \text{hash}(B^{r-1}.\text{Rand})$ ，从组链中获取当前存续的工作组列表 gB

$gB^i | gB^i.\text{GIS}.\text{Activation } e < gB^i.\text{GIS}.\text{Deactivation}$

以该随机数 R_r 作为随机种子，用伪随机数生成函数 PRG 可以随机在上述存续工作组列表 gB 里确定当前工作组。这些选择都是其他节点可审计验证。后期我们可能会考虑拿组的健康指数（组员健康指数和），利用追随中本聪算法（FTS）来作为选组的依据。

2.1.4 收敛优化与通信优化

由于提案组规模动态，可能会同时出多个候选区块。所以算法必须对候选区块快速收敛。这里我们规定的两个策略：

- 验证组会优先提案组获得上轮的公证区块（完成组签名的区块，可能会多个），验证组会对上轮区块的权重进行优先处理；
- 验证组签名时，当某个候选区块达成组共识被广播时，就不再对该轮的其他候选区块签名

参考比特币的 P2P 网络的传播性能：1KB 消息，在 1 秒钟内完成全网 95% 的传播，而 1MB 消息需要 1.5 分钟完成全网 95% 的传播。我们考虑到组成员散布在世界各地，而且工作组会以多个区块的方式提出候选区块，所以必须对通讯做相应的优化。我们考虑采用组内以 Block header 传给验证组。组内对 block header 的 Hash 达成强一致，仅仅保证了 block 内容以及时序。用户账户是否存在 double-spending 没法验证。所以我们是在快速对 hash 达成一致后，等交易同步到本地后，由上链时的账户状态验证来保证交易的有效性。这样可以达到更高的共识效率。如果提案矿工是诚实的，这样的流程效率比传统的以整个 block（包含区块内所有交易内容）为消息传输的方式要高。如果提案矿工是恶意的，这区块在上链时会验证失败，由上述的组外验证保证不会被传播，这样也保证了安全。另外，如果提案矿工是恶意的，该块的验证组验证后会发起该块的分红合约，但上链验证失败使该区块上链失败。块链中分红合约与块链的不一致，可以作为作恶凭证，对作恶的提案矿工给出相应的惩罚。比如降低出块矿工的健康指数，保证金扣除等。

2.1.5 分叉处理

1. 分叉选择

由于共识机制的特性和 P2P 网络状况的不确定性，软分叉在区块链中无法避免，在出现软分叉之后，ZV CHAIN 链的各节点以优先级最高的分叉 $totalG = \sum G_i$ ，其中， G_i 是各个区块的优先级。如图2.4所示，

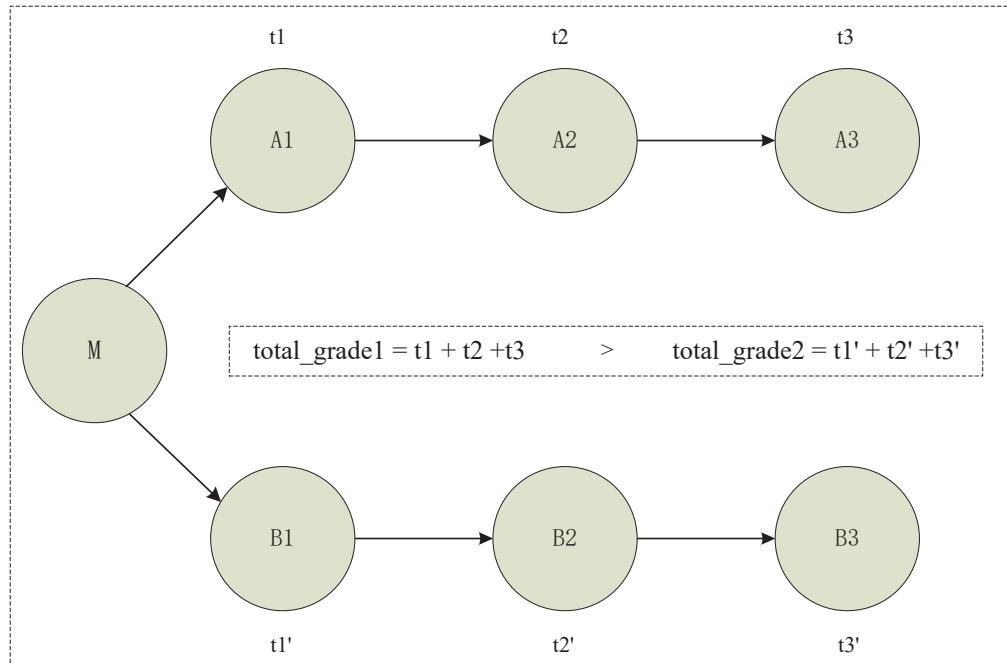


图 2.4: Chiron 分叉处理示意图

作为规范链，分叉节点会通过分叉调整简单快速地将本地链调整至规范链，从而保证链的一致性。

2. 分叉调整

节点遇到分叉之后，首先找到分叉点，然后比较分叉点到当前高度的总优先级做出选择。在寻找分叉点的过程中，采取局部比较的方式，每次请求一定步长的目标链片段进行二分比较，然后根据比较结果调整步长，从而快速定位到分叉点进行分叉调整。

2.1.6 Check Point 机制

确定性 (Finality)，从一个非常宽松的意义上来说，意味着一旦一个特定的操作完成，它将永远被蚀刻在历史上，没有任何东西可以逆转这个操作。在处理金融事务的领域，这是非常重要的。ZV CHAIN 作为一个承担银行业务的公链，数据确定性是至关重要的一个安全因素。需要强调：确定数据的明确最终共识，而不是概率上最终共识（类似 Bitcoin 的 6 块确认）。

Chiron 共识提供了周期性检查点（Check point）机制，检查周期为 epoch 周期（系统设定参数，例如 epoch 周期为 100 块区块时间）。由上述 Chiron 建组机制可知，在一个 epoch 周期内，验证组的组数是固定的。我们采用类似 Hashgraph 寻找“强”可见连接的思路（本质是达成拜占庭容错条件， $2/3$ 成员认可），可以利用已有信息，确定出“检查点”的状态。

Check point 机制：假设当前铸块高度进入第 $n+2$ 个 epoch 周期，则回溯第 n 个 epoch 周期内，在 epoch n 期间产生的区块链区间内如果能找到其中一段子链区块是由当前 epoch 验证组集合中的 $2/3$ 组验证通过的。Chiron 的 check point 机制不会像 DAG 或者 Hashgraph 这样确定时间不可预测。原因在于：前面关于 VRF 选组时论证了每个 slot 上都仅有唯一的，随机的，不可预测的验证组担任验证工作。即对每个组来说，承担验证区块的概率是公平的，所以每个 epoch 周期内找到“经过” $2/3$ 组的子链，这件事是平凡的，大概率发生的。ZV CHAIN 最终化区块链可以防止长程攻击，就算是控制 51% 或者更多的全网节点意图重写最新检查点之外的历史也会被阻止。

2.1.7 共识分析与系统安全

如果一个系统对双花攻击、长程攻击（私自挖矿）、无利害关系、女巫攻击和 51% 攻击都有数学可证明或经济博弈的解决方案，则我们认为这个系统是高安全的。因为所有的攻击最终都会汇总到这几种方式永久或临时的伤害系统和个体。上述的周期性 Check point 机制保障了 ZV CHAIN 区块链数据具有确定性（Finality），即使攻击者控制 51% 或者更多的全网节点意图重写最新检查点之外的历史也会被阻止。所以攻击者控制超过半数的网络节点仅仅可能修改近期的区块（当前块到最新检查点之间的区块）。但除了 check point 机制之外，针对最严重的 51% 攻击，ZV CHAIN 引入系统健康度概念，交易用户可以通过简单观察即可发现系统是否处于被攻击状态，并通过暂停交易或延迟交易的最终确认块来保证交易的安全性。

2.1.7.1 共识分析

1. 去中心化分析

POW 共识是高度去中心化的算法，但是随着矿机，矿池出现，它们成为 POW 共识的隐性中心。用户使用普通算力设备参与铸块，几乎无法收益。Chiron 共识将节点分为重节点和轻节点，重节点每轮 VRF 秘密抽签随机获得提案权，单个重节点的提案概率和它的权益质押线性相关；轻节点随机分组，具体轮次由真随机数确定工作组，保证了每组有相同概率获得验证机会。最终区块的提案人以及验证组中参与验证的组员会有铸块

奖励。

2. 一致性与准确性分析

Chiron 设计了 check point 机制，每 100 块（5 分钟左右）一个 CP。出块组的验证阶段做一致性检查，提案和出块阶段做准确性检查。全网非出块组在收到一个新块时，对内容做准确性检查，如果发现有问题，则先组内投票，当组内超过门限数量节点认为该块有问题，则以组为单位投票到一个特殊的智能合约。投票节点共享该投票的收益和惩罚。每个新 CP 开始的组，需要检查该智能合约，如发现超过 N 个组在前一个 CP 内投票有异常的出块，则进行准确性检查。验证发现异常，回退到异常之前的 CP 重新开始。反之则继续当前 CP。对于大多数中小金额的交易，观察到 90% 的邻居节点已经在包含交易的块之后又新增了 3 个一致的出块，即可确认交易。对于大额交易，我们建议观察 90% 的邻居节点已经进入一个新的 CP 后确认交易。

2.1.7.2 系统安全分析-攻击防御

- 无利害攻击 (nothing at stake)

在纯 POS 算法中，只为创造区块提供奖励，恶意出块或者基于错误的分叉出块都没有惩罚措施，这就出现在多链竞争条件下，理智的矿工的最佳策略是在每条链上进行“挖矿”。这意味着在该机制下，不管哪条链胜出，矿工都会得到奖励，由于他们没有花费物质上的算力，所以矿工以很低的成本就可以使得自身利益最大化。如图2.5所示，

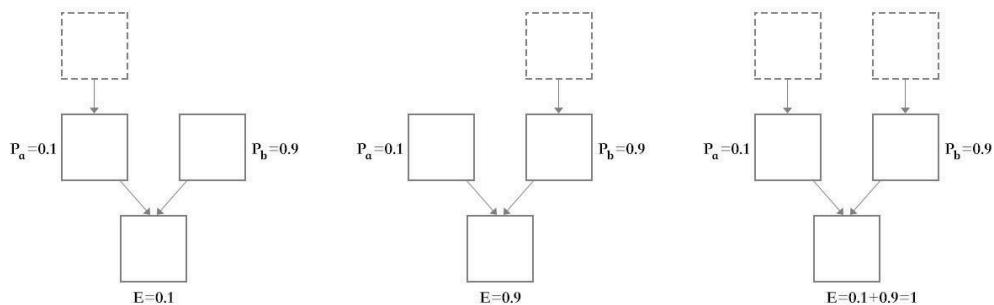


图 2.5: 无利害攻击示意图

P_a, P_b 分别为两个分叉的胜出概率，当矿工在两个分叉上均投票时, E (收益期望) 得到最大化. 在极端情况下，全网矿工唯利是图，即使没有攻击者，也有可能无法达成共识。

在传统的 POW 算法中，所有矿工进行实时算力竞赛，要实施无利害攻击必须分散算力到两个分叉中，这样会大大降低自己的竞争力，因此传统 POW 天然抗无利害攻击。

实际上，在 Chiron 体系中，每个块高度 VRF 选择与之对应的工作组，这决定了每一轮在多条分叉上具有出块权的组只有一个，同时收益也只有一份，剩余无权出块的组均没有经济动力保留两条分叉，他们会在两条分叉中作出选择并最终达成一致。另外，区块提案者和验证者在出块结束后需调用分红合约来获得自己的铸块奖励。系统对同一高度出多区块的行为设置了惩罚机制，这些分红合约在打包加入块时，相应的矿工即会发现该行为，并以此作为作恶证据提交系统，系统会对该高度的出块人进行惩罚。所以我们认为 Chiron 算法机制消除了无利害攻击的问题。

- **女巫攻击 (sybil attack)**

女巫攻击的一种形式是攻击者注册大量的账号，并且使用这些账号进行挖矿，以提高自己的收益。ZV CHAIN 采用传统的权益质押的方式参与铸块，重节点提案概率和权益质押的数量线性相关。所以将手头权益分到多个账户来参与系统，并不能提升自己的收益。同样的，轻节点入选验证组时，选中的概率与其权益的质押线性相关，女巫攻击也是无利可图的。

另外一种攻击形式是攻击者围绕在诚实者周围，通过一定手段与诚实者交互企图窃取利益。在 ZV CHAIN 系统中，节点之间交互类型主要有三种，第一种是单向交互，即接收者接收消息后通过合法性验证并进行存储即可，如数据同步消息，由于单向交互性使得攻击者基于此种交互并不能获取任何利益。第二种是双向交互，即接收者接收消息并通过合法性验证后向发送者（或组内其他成员）进行相关反馈，如块验证消息，建组消息；攻击者可以试图伪装成组员和被攻击者进行建组流程或者共同参与块验证，企图获取利益。由于 ZV CHAIN 的建组流程是由指定的父亲组发起的，建组的成员经过父亲组门限值以上的节点签名，具有不可篡改，可审计的特性，因此被攻击者可以轻易的判断与之交互的节点是否属于组内成员。第三种是链式交互，即接收者接收消息后只做简单的转发。显然这种简单转发不会让攻击者收益。最后值得强调的是，上述攻击无效的前提是矿工的私钥不泄露，ZV CHAIN 系统所有的交互都不涉及私钥的传递。

综上所述，ZVCHAIN 系统采用铸块参与度与设备健康指数相互反馈相互促进的机制使得攻击者无法作恶。安全可验证的消息通讯机制使得攻击者无法通过任何手段窃取被攻击者的利益。

- 51% 攻击 在纯 POW 的系统中, 51% 攻击是致命的不可恢复的。因为攻击者拥有足够的算力挖出一条难度更大的更长的链去淘汰主链, 而诚实者会渐渐接纳攻击者链, 攻击者永久胜出。

ZV CHAIN 系统将矿工随机分配到不同的组, 51% 攻击可能导致攻击者控制了绝大部分工作组。在这种情况下, 主链将缓慢延长, 攻击者链由于拥有更多的组而延长速度更快, 但是诚实者会拒绝接受攻击者链, 他们会一直坚持延长主链。此时绝大部分用户能轻易感知系统存在两条不同的链而不敢轻易交易, 从而导致攻击者收益甚微, 这与其发动 51% 攻击的成本完全不成比例。

如果一个普通用户随机连接的所有节点都被攻击者控制, 则此用户由于无法感知异常而继续信任网络, 我们认为这个用户是能给攻击者带来收益的, 暂且称此类用户为受害用户。显然受害用户越多, 攻击者收益越大。下面简单分析一下攻击者和受害用户的比例关系。

假设每个用户都随机连接的 n 个节点中有 90% 的节点都被攻击者控制, 则该用户成为受害用户。假设全网节点数 W , 攻击者控制比例为 x , 则受害者比例为:

$$V = \frac{\sum_{i \geq 0.9n}^n \binom{W \cdot x}{i} \binom{W \cdot (1-x)}{n-i}}{\binom{W}{n}} i \in N$$

更普遍的, 设 $W = 10000$, $n=10$, v 和 x 的曲线如下图2.6所示,

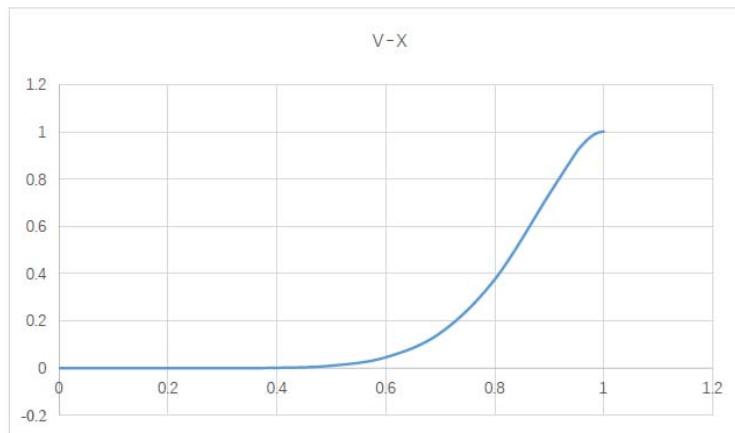


图 2.6: 攻击者比例与受害者比例关系图

由此可知, 当攻击者控制 50% 的节点时, 受害者比例仅为 1.07%; 而理论上只有当攻击者控制了 100% 的节点时, 攻击者才可以控制整个网络。如果受害者比例超过 90% 后, 攻击者就有利可图, 那么攻击者需要控制 95% 以上的节点。这个攻击的成本非常巨大。

表 2.2: 两者比例的几个特殊点

0.5	0.01071
0.8	0.3757
0.9	0.7361
0.95	0.914
1	1

相反，当攻击者由于无利可图而渐渐退去，诚实者比例大于 95% 后，系统就能恢复正常。

综上所述并结合最近发生的多起针对低算力 POW 公链的 51% 攻击，我们认为 ZV CHAIN 系统能抗 95% 甚至更高的攻击（在系统冷启动和低算力状态进一步提高系统健康度阈值），因而具有更高的安全级别。

- **长程攻击 (Long-range attack)**

在 POS 算法中，出块的速度没有限制，在系统初期，矿工不多，如果这些矿工联合起来，回到系统初期的状态开始铸块，在短时间内铸出一条更长的链，这时候用户无法辨认哪条链是主链，甚至攻击者发布的链有可能战胜主链。当前很多 POS 实现是通过限定区块能回滚的数量加大攻击的难度。

在 ZV CHAIN 系统中，所有区块难度设定了上下限，记为 D_{max} 和 D_{min} ，并且有 $D_{max} = k \cdot D_{min}$ ，每个 epoch 宽度为 H_{epoch} ，每个工作组的工作周期为 n 个 epoch，工作周期过后组会自动解散进入重建流程。假设攻击者选择回退 H 块实施长程攻击，并且攻击者控制的组占比为 x ，那么在攻击过程中，由于 VRF 的不可选择性，攻击者每次只能在被选中的时间窗口出块，而未被选中的时间窗口出空块。长期来看，攻击者链的有效区块比例与攻击者组占比正相关。 n 个 epoch 后链状态如下图2.7所示，

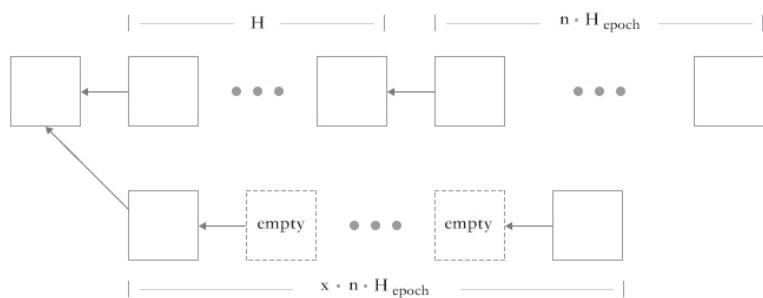


图 2.7: 长程攻击示意图

表 2.3: 攻击者至少需要控制组的比例

k 取值	x 范围
1	大于无解
2	大于 50%
3	大于 33%
5	大于 20%

攻击者在工作周期内能算出的最大链累积难度为:

$$D_{attack} = x \cdot n \cdot H_{epoch} \cdot D_{max} = x \cdot n \cdot H_{epoch} \cdot k \cdot D_{min}$$

此时主链累积的最低难度为:

$$D_{main} = (H + n \cdot H_{epoch}) \cdot D_{min}$$

攻击者得逞的条件为:

$$D_{attack} > D_{main}$$

$$\text{简化后得: } n \cdot H_{epoch} \cdot (k \cdot x - 1) > H$$

由此可见，攻击者只能回退到有限高度去实施长程攻击。尤其是，当 $k \cdot x \leq 1$ 时，攻击成功的概率将为 0。意味着攻击者必须控制更多的组来降低攻击的难度。如下表 2.3 所示，不同 k 值条件下，攻击者至少需要控制组的比例。

事实上，上述推论成立的条件非常苛刻。首先，攻击者控制的所有组必须处在相同的存续周期中，这样才能保持攻击者的攻击力，但这在随机建组模型上，攻击者很难实现。其次，推论假设攻击者每次出块都能算出区块难度上限，并且诚实者都只算出难度下限，只要两个条件的一个不满足，都将大大减小 H 可选的范围。最后，诚实者会拒绝接受过期 (n 个区块以前) 的区块，即系统限制了能回滚的区块数量。

简而言之，难度区间的设定和区块时效限制了系统能回滚的块数量；随机分组策略和组定期重建机制使得攻击者无法长期保持高强度攻击，因此长程攻击在 ZV CHAIN 系统变得几乎不可能。

- DDOS 攻击

DDOS 攻击主要是攻击者通过组织一批计算机，对服务节点发起大量的请求，从而使得服务节点忙于处理请求而耗尽资源，无法继续对外提供服务的攻击方式。比特币和以太坊全网节点进行 POW 计算，没有任何中心节点，因此天然地抗 DDOS。我们认为去中心化程度将决定抗 DDOS 的安全程度。

Chiron 算法通过 VRF 在全网工作组中随机选择每一轮的验证组，表面上验证组成为了某一刻系统的中心，实际上由于 VRF 的随机不可预测性，这个中心每一轮都在变化，这是一个动态变化的中心，本质上也是去中心化的。

- **最后操作者攻击**

ZV CHAIN 系统中所有节点通过分组协作方式参与记账，每个区块由组内门限个以上成员签名，组外节点可通过组公钥进行验证，因此具有不可篡改的特性。最后操作者若企图修改数据，则会导致最终校验失败，攻击者无利可图。

另外，最后操作者选择不作为也是攻击的一种手段。然而，在 ZV CHAIN 系统中，任何组内节点都可以是最后操作者，不存在单点，只要有诚实节点，攻击者就不会得逞。极端情况下，攻击者控制了某个组所有成员，在最后出块时，选择不出，则系统会跳过本轮继续下一轮。攻击者同样无利可图。

- **双花攻击**

双花攻击的常见手段是制造另一个能战胜主链的分叉。攻击者首先需要在某个组中控制超过一半以上的节点，并在轮到攻击者所控制的组出块时，提前将自己的一笔交易广播出去，同时自己也开始在另一个分叉铸块并把该交易打进块中，等待该笔交易在主链中被确认（ZV CHAIN 的确认时间很短）后，再把自己的分叉广播出去，若攻击者的分叉链难度大于当前主链新增的累积难度，就会被矿工作为新的主链，如此一来，先前的交易就像不存在一样，以此达到攻击目的。此类攻击者的攻击策略和长程攻击类似，具体分析请参考长程攻击防御章节。

- **私自挖矿攻击**

在比特币系统中，由于所有矿工可以在每个高度上进行 POW 挖矿，因此算力强的节点可以在挖到某块后，先藏着，并私自开始下一轮挖矿，以此获得先机。ZV CHAIN 系统中所有矿工通过分组协作方式进行挖矿，每个矿工挖出的块必须经过组内大多数矿工的签名才能广播出去，因此私自挖矿对单个矿工并不成立。而组间的轮换完全由 VRF 决定，私自挖矿并不能使组获得下一轮挖矿权，因此私自挖矿对组亦不成立。

Chiron 共识机制的单链性能达到 3000TPS，并且保证了共识机制的高安全性，高去中心化，是至今为止的所有共识机制中给出去中心化、安全、性能三角不可能问题的最佳方案。Chiron 共识机制从设计之初就考虑了系统的效率成本，充分利用了组闲置时间，设计了定期 check point 机制。

2.2 隐私计算与安全框架

2.2.1 数据隐私和监管

区块链技术具有“去中心化”和“可信任化”等特点，能够不依赖第三方可信机构在陌生节点之间建立点对点的可信任价值传递，有助于降低交易成本，提升交互效率，有非常广阔的应用前景，被认为是引领信息互联网向价值互联网转变的关键技术。然而随着区块链技术不断发展与应用，其面临的数据隐私问题越来越突出。

1. 交易隐私性

中本聪创造性地提出了比特币并且构建了一个去中心化的交易平台，从而去除了长久以来对第三方交易平台的信任依赖，但是与此同时，比特币又需要将所有的交易广播到网络上并通过所有节点达成共识来保证整个系统的安全性，也就是说所有的人都可以看到网络上所有的交易，而原始的比特币协议又并没有对交易发送者和接收者的地址作任何处理，这就导致某些细心的攻击者通过分析一个地址的交易特征并结合一些实际信息，就有可能分析出地址与实际人的对应关系，从而给使用者的隐私带来极大的隐患。基于此，研究者提出了关于货币隐私的两个基本属性：

(a) 不可链接性 (Unlinkability)

无法证明两个交易是发送给同一个人的，也就是无法知道交易的接收者是谁；

(b) 不可追踪性 (Untraceability)

无法知道交易的发送者是谁。ZV CHAIN 作为一条承载银行业务的公链，数据隐私保护是极其至关重要的环节。

2. 隐私保护理论

账户的安全和隐私保护，我们采用零知识证明 (ZKPs) 技术。同时，对于数据存储安全和隐私保护方面，我们引入同态加密技术。其中，同态加密 (Homomorphic Encryption) 是一种特殊的加密方法，允许对密文进行处理得到仍然是加密的结果。即对密文直接进行处理，跟对明文进行处理后再对处理结果加密，得到的结果相同。从抽象代数的角度讲，保持了同态性。同态加密可以保证实现处理器无法访问到数据自身的信息。它提供了一种急需的方法，能够在原有基础上使用区块链技术。通过使用同态加密技术在区块链上存储数据可以达到一种完美的平衡，不会对区块链属性造成任何重大的改变。也就

是说，区块链仍旧是公有区块链。然而，区块链上的数据将会被加密，因此照顾到了公有区块链的隐私问题，同态加密技术使公有区块链具有私有区块链的隐私效果。同态加密技术不仅提供了隐私保护，它同样会允许随时访问公用区块链上的加密数据进行审计或其他目的。换句话说，使用同态加密在公用区块链上存储数据将能够同时提供公有和私有区块链的最好的部分。另一方面，使用同态加密技术，运行在区块链上的智能合约可以处理密文，而无法获知真实数据，极大的提高了隐私安全性。

3. 隐私保护方案

(a) 蒲公英中继协议

加密货币面临的主要隐私挑战之一是，可以跟踪交易，因为它们被添加到 mempool 并通过网络传播并将这些交易链接到其原始 IP 地址。即使在具有强大交易隐私的网络上，此信息也可用于对用户进行去匿名化。为了在交易传播到网络期间改善隐私，提出了蒲公英网络传播方案。在此方案中，交易分两个阶段传播，即匿名阶段和传播阶段，如下图所示。在匿名阶段，交易仅传播到单个阶段从当前节点对等列表中随机选择对等体。在沿着网络的随机跳数之后，每个跳仅传播到单个随机对等体，传播过程进入第二阶段。在传播阶段期间，然后使用在大多数网络中发现的完全泛洪/扩散方法来传播交易。这种方法意味着在洪泛网络之前，交易首先传播到网络中的随机点，因此跟踪其来源变得更加困难。；

(b) I2P 匿名网络

I2P 是一项混合授权的匿名网络项目，I2P 网络是由 I2P 路由器以大蒜路由方式组成的表层网络，创建于其上的应用程序可以安全匿名的相互通信。它可以同时使用 UDP 及 TCP 协议，支持 UPnP 映射。

对于想使用 Tor 匿名网络的用户，ZV CHAIN 支持使用 SOCKET 代理连接到本地 Tor 客户端，后期根据需要可以选择直接在节点、或者钱包中植入 orchid 库，另外 I2P 也作为 ZV CHAIN 的可选匿名网络支持，可在本地启用代理或植入 SAM，I2P 原生工具接入匿名网络，保护用户网络接入隐私，用户不必担心 ip 地址被跟踪。对于第二阶段，则采用成熟的 P2P 网络技术即可。

(c) MimbleWimble 协议

MimbleWimble 数 [10] 最早是被定义作为比特币的一种改进，在该协议中，隐去交易地址、交易金额，合并中间交易部分。每次转账，参与交易的各方创建一个可以

验证交易的公共多重签名密钥。系统中没有地址，因为参与交易的两方分享所谓的“盲因子”（一种用于电子货币的加密技术），其中只有那两方知道他们正在进行交易，从而保护网络隐私。

MimbleWimble 协议使用一种 Pedersen 承诺方案，在该方案中，完整节点从事务接收端加密的数量（输出）减去事务发送端加密的数量（输入）。加入盲因子产生平衡等式，则节点永远不需要知道交易金额是多少。合并中间交易部分指的是，A 给 B 一笔钱，B 又全数给了 C，这个时候 B 就等于没有参与交易，因此，B 的数据不会被记录在链上。从而显著减少区块存储所需空间可选的审计功能拥抱监管，ZV CHAIN 提供可审计的钱包，可以为审计对象生成额外的公钥/私钥对，这些签名用于标签交易，只有获得公钥的审计机构才能识别块链上的那些交易，但不能自己创建具有此标签的交易。这允许企业向指定的权威机构提供其交易的可见性，而不会损害他们对公众的隐私。

2.2.2 形式化证明

以太坊将智能合约引入区块链，极大地扩展了区块链的功能。今年以来有数个基于 ERC-20 的 ICO 项目因为智能合约代码出现漏洞而遭到黑客攻击，导致投资者巨额的损失，这给数字货币的各方参与者敲响了警钟。如何保障智能合约的安全，对各个公链开发者来说，是要重点考虑的问题。对此 ZV CHAIN 引入智能合约形式化证明。在用户上传自己的智能合约后，ZV CHAIN 系统针对该智能合约构造形式化证明进行验证，同时结合传统的“测试 + 审计”方式相结合，将会是保证智能合约安全强有力手段。

目前针对智能合约安全问题的应对方式主要有两种：合约代码的测试和审计。这两种方式能够在一定程度上有效的规避大部分的安全问题，是保证合约安全的必要手段，但是同时也存在着一定的局限性。合约测试安全团队开发自动化测试工具，自动生成大量的测试用例执行合约来进行测试，检测在尽量多的条件下，合约是否能够正确执行。但由于测试用例无法保证 100% 覆盖所有的情况，所以，即使测试结果没有发现问题，也不能保证合约的实现一定没有漏洞。合约审计安全审计人员对合约源码从代码实现和业务逻辑等多个角度进行审计。安全团队通过专业的手段检查出大部分的合约漏洞和隐患，并在业务逻辑的实现上给与项目方指导或者建议。尽管安全审计可以发现并规避大部分常见的漏洞和风险，但由于审计工作在一定程度上依赖于审计人员的自身经验和主观判断，并不能 100% 完全杜绝安全风险和漏洞。

形式化证明是通过形式化逻辑的方式来表示合约代码，并加以严格地推理证明。这个过

程依赖于数学逻辑推理的严密性，保证 100% 覆盖到到代码的运行期行为，可以明确保证在一定范围内的绝对正确，能弥补以上两种传统方式的局限。

形式化验证指的是用数学中的形式化方法对算法的性质进行证明或证伪。方法有两种：

1. 模型检验

即把系统所有可能的状态列出并进行一一检验，此种方法全自动化但只适合小型系统；

2. 演绎验证

首先把系统代码标记成抽象数学模型，然后对定理进行证明，此种方法适合大型系统，但是需要首先人工将系统的运作方法转换成验证系统可以理解的语言。

在区块链应用中，由于区块链的不可篡改性，智能合约一旦上线并出现安全隐患，对用户造成的损失是巨大且不可挽回的。一旦出现黑客事件，需要整个社区的共识才能回滚交易，所以每次遭受攻击都回滚交易也是不现实的。因此，区块链应用开发的过程需要用大量的测试和检验以获取足够的安全性，而反过来牺牲迭代的速度。由于区块链开发人员的稀缺，远远无法赶上智能合约数量的增长，人工审计智能合约是成本非常高昂的，因此机器辅助验证是目前的必然趋势。规则、语义验证的实现，相对较为容易，技术门槛也较低，但是只能进行一些浅层的纠错，不能深入程式的逻辑。因此，只有形式化验证方法有希望真正提高智能合约审计的自动化程度。

2.2.3 通讯的安全

网络的通讯安全由系统应用层的逻辑保证。我们在系统应用层会对网络通讯信息进行分类，对于有信道安全要求的通讯，将会采用 ECDH 加密的安全信道进行点对点通讯，保证通讯的安全。

2.3 金融智能合约

在 DAPP 快速发展的过程中，正面临着和传统 APP 发展一样甚至更多的由去中心化带来的问题。ZV CHAIN 希望在保证契约性、安全性、公平性的前提下，为 DAPP 开发者打造一个完整和高效的开发生态环境，以帮助 DAPP 的快速实施和落地。

2.3.1 合约升级

在传统的 APP 开发领域，功能升级一直是流程里重要的一环。DAPP 的前身来自于交易，且由于“代码即法律”的区块链精神，功能升级一直没有从系统化角度得到有力支撑。考虑到 ZV CHAIN 的最终目标是构建强大的商用 DAPP 平台，我们将建立一套完整的合约升级方案，从平台层面让合约构建者和使用者可以协调功能升级方案。合约创建者通过发起合约升级邀约，合约使用者在得到邀约通知后，可以全面评估升级方案对自身利益的影响，并自由选择是否升级到新合约。具体如图 2.8 所示。

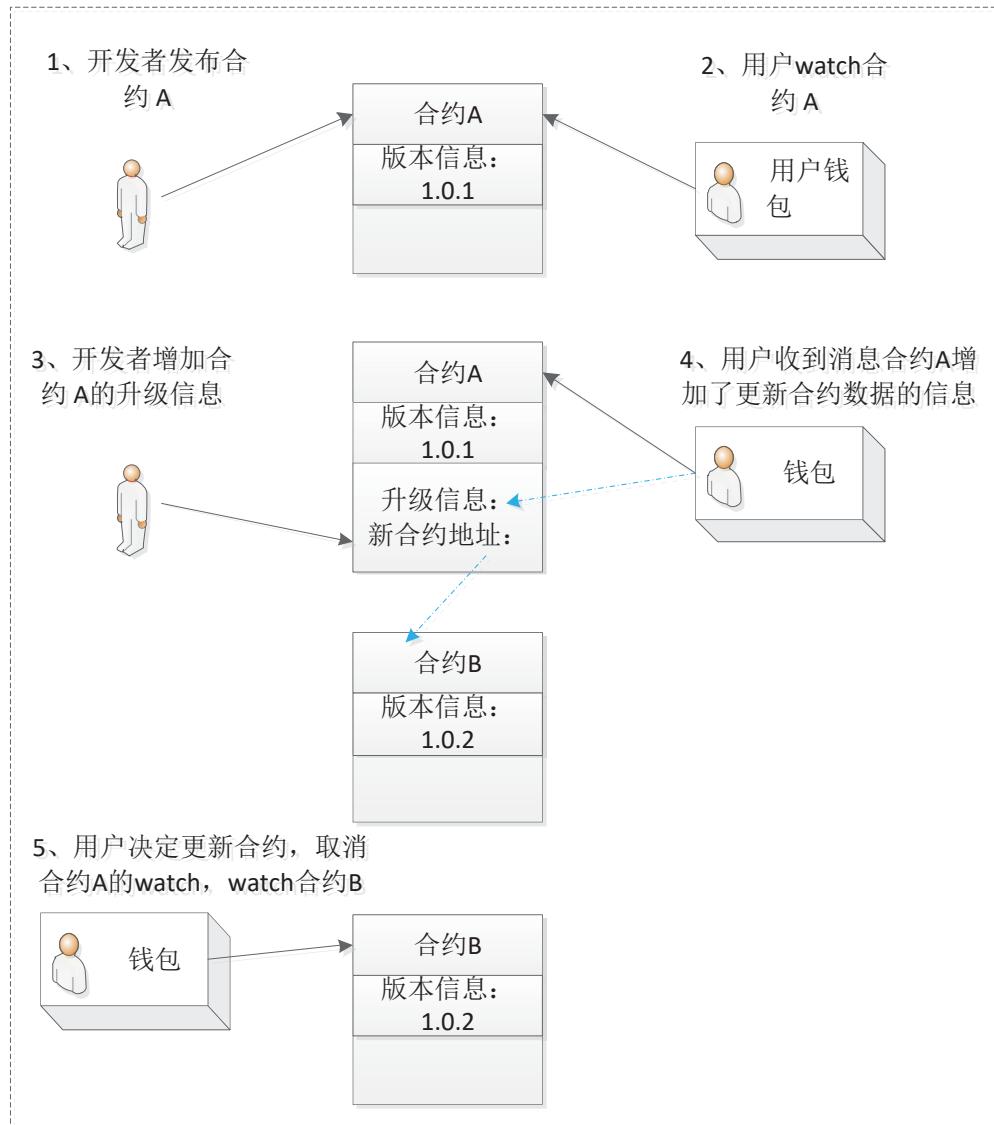


图 2.8: 智能合约升级示意图

2.3.2 重大异常修复（硬分叉）

在传统的 APP 开发过程中，除了 APP 的日常功能性升级和 bug 修复升级外，还有重大 bug 触发的应用强制升级和数据回滚。在以智能合约为基础的 DAPP 迭代过程中，不能单方面由研发人员决定是否进行强制升级和数据回滚，平台层面的支持有助于快速修复和解决 DAPP 运行过程中的严重问题，做到最小粒度的硬分叉。

ZV CHAIN 将提供一套完善的接口和工具链，在 DAPP 发现严重问题时可以让开发者快速便捷的对运行中的 DAPP 进行分叉处理，包括合约的镜像拷贝、数据拷贝和指定高度回滚，并通知所有 DAPP 的参与者。

2.3.3 高效 VM 与合约语言-Python

ZV CHAIN 采用自己研发的 TVM，支持扩展行业原语作为智能合约关键词，支持多种用户友好的编程语言，如 python, go 等。并且对一些常用应用提供多个智能合约模版，用户仅需少量的设置即可调用。

python 是一门简单易学的编程语言，学习曲线非常平缓，可以直接通过命令行交互环境来学习 Python 编程；Python 的语法非常优雅，代表了一种极简主义的设计思想，代码可读性强，拥有高效的代码审计的特点；python 拥有十分成熟的语言生态，Python 本身具有丰富而且强大的库，而且由于 Python 的开源特性，第三方库也非常丰富；上述的几个优点决定了 python 是一门开发效率高的语言，语法简单，类库丰富可以显著提高开发者的效率，同时脚本语言的特性使得调试成本更低；正是因为 Python 语言简单易学，已经有越来越多的初学者选择 Python 语言作为编程的入门语言，作为合约语言能被更多的大众所接受并使用。

2.3.4 金融业务标准组件库和组件市场

TVM 推出了一系列常用基础组件库，组件具有高效且低 GAS 消耗特性，在提供高解耦性和可复用的基础上，极大的降低了 DAPP 的上链存储成本。准对各行业的常见需求，制定了标准化协议，便于钱包对一个需求的标准化接入。同时，TVM 会建立一个标准化的组件市场，鼓励开发者开发三方组件库，在通过严格的审计和上链后，这些三方库会向 DAPP 开发人员开放，进一步降低 DAPP 开发人员的研发成本和存储成本。调用这些组件本身不需要付费，平台根据组件被调用的次数，支付相应的奖励代币。通过单次奖励代币数量小于对应的 GAS 消耗机制，避免恶意调用。通过平台奖励开发者的机制，大大提高了开发者的积极性，组件市场中的组件库得到大量得丰富，开发者开发一个 DAPP 的难度大大降低。随着三方库

的广泛使用，开发者会收到代币激励以鼓励他们优化和创造更多的高可用和可信赖的三方库。我们认为这样的基础组件库和应用组件库模式有利于构建良好的 ZV CHAIN 生态联盟。

具体如图 2.9 所示。



图 2.9: 区块链金融业务标准组件库和组件市场

2.4 跨链技术

跨链是利用一种能让价值跨过链和链之间的障碍，进行直接流通的技术。具体来讲，区块链是分布式总账的一种，一条区块链就是一个独立的账本，两个不同的独立的账本并没有关联。本质上价值没有办法在账本间转移，但是对于具体的某个用户，用户在一条区块链上存储的价值，能够变成另一条链上的价值，这就是价值的流通。目前有多条被广为使用的区块链，包括公有链、联盟链和私有链，通常认为，私有链朝着联盟链发展，联盟链朝着公有链推进，不同区跨链的演进，也使跨链互操作成为一种显而易见的需求。

2.4.1 跨链的主要类型

在区块链所面临的诸多问题中，区块链之间互通性极大的限制了区块链的应用空间。不论对于公有链还是私有链来看，跨链技术就是实现价值互联网的关键，它是把区块链从分散的孤岛中拯救出来的良药，是区块链向外拓展和连接的桥梁。目前主流的跨链技术，除了以太坊创始人 Vitalik 为银行联盟链 R3 写了一份关于跨链互操作的报告 [11] 提到三种跨链方式，还有一种是分布式私钥控制技术。具体的类似跨链方式如下所述。

1. 公证人机制 (Notary schemes)

公证人模式在许可分账领域受到很多关注，因为其既可以提供灵活共识的主要竞争者，也无需进行昂贵的工作证明或关于利益机制的复杂证明。假设 A 和 B 是不能进行互相信任的，那就引入 A 和 B 都能够共同信任的第三方充当公证人作为中介。这样的话，A 和 B 就间接可以互相信任。具有代表性的方案是 Interledger Protocol (2012 年 Ripple 实验室主导发起的互联账目协议)，简称 ILP，它本身不是一个账本，不寻求任何的共识。相反它提供了一个顶层加密托管系统称之为“连接器”或“验证器”，在这个中介机构的帮助下，让资金在各账本间流动。公证人是交易双方共同选择出来的，具有高度可信的特征。公证人负责验证数据的有效性和数据的唯一性。Interledger 适用于所有记账系统，能够包容所有记账系统的差异性，该协议的目标是要打造全球统一的支付标准，创建统一的网络金融传输的协议。

2. 侧链/中继 (Sidechains/Relays)

侧链 (Sidechain) 协议允许资产在比特币区块链和其他区块链之间互转。它是以锚定原生数字资产为基础和其他账本资产在多个区块链间的转移的新型区块链技术，如法币对黄金的锚定一样。该技术一般是为了解决主链扩展性问题而想出来的扩容技术，侧链技术进一步扩展了区块链技术的应用范围和创新空间，是传统区块链可以支持多种资产类型，以及小微支付、智能合约、安全处理机制、真实世界财产注册等，并可以增加区块链的隐私保护。比较著名的比特币侧链是 Consensys 的 BTC-Relay、Rootstock 和 BlockStream 的元素链，非比特币的侧链如 Lisk 和国内的 Asch。

中继 (relays) 是链与链之间的通道，如果通道本身是区块链，那就是中继链。中继器模式比较有代表性的是 polkadot 和 Cosmos HUB。其中，Polkadot 计划将私有链/联盟链融入到公有链的共识网络中，同时又能保有私有链/联盟链的原有的数据隐私和许可使用的特性。它可以将多个区块链互相连接。在 Polkadot 看来，其它区块链都是平行链，Polkadot 为通过中继链 (relay-chain) 技术能够将原有链上的代币转入类似多重签名控制的原链地址中，对其进行暂时锁定，在中继链上的交易结果将由这些签名人投票决定其是否生效。它还引入了钓鱼人角色对交易进行举报监督。通过 Polkadot 可以将比特币、以太币等都链接到 Polkadot 上，从而实现跨链通信。。

3. 哈希锁定 (Ash-locking)

哈希锁定起源于闪电网络的 HTLC，Lightning network 闪电网络提供了一个可扩展的 bitcoin 微支付通道网络，它极大提升了比特币网络链外的交易处理能力。闪电网络的关键技术是 HTLC 哈希锁定技术，基本原理如下：Alice 和 Bob 可以达成这样一个协议：协议将锁定 Alice 的 0.1 BTC，在时刻 T 到来之前（T 以未来的某个区块链高度表述），如果 Bob 能够向 Alice 出示一个适当的 R（称为秘密），使得 R 的哈希值等于事先约定的值 H(R)，Bob 就能获得这 0.1 BTC；如果直到时刻 T 过去 Bob 仍然未能提供一个正确的 R，这 0.1 BTC 将自动解冻并归还 Alice。。

4. 分布式私钥控制 (Distributed private key control)

分布式私钥控制协议代表性的基础设施包括 WanChain 和 FUSION，其中，万维链利用多方计算和门限密钥共享方案。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。通过多层共识机制和记账节点分组，实现了一定的并行计算。多层机制使合约计算与计算结果的记账分步完成，记账节点分组使不同的智能合约由不同的记账节点分组完成。。

目前这四类跨链技术从不同角度来讲各有利弊，需要根据具体的业务场景的需要和技术实力进行综合评估，选择适合自己的跨链方式。可以参考的评价维度包括互操作性、信任模型、使用跨链交换与否、适用跨链 oracles 与否、适合跨链资产抵押与否、实现难度和多币种智能合约等。

2.4.2 ZV CHAIN 的跨链协议

区块链的特性是不可篡改性，可追溯性。我们认为 DAPP 最有可能在数字资产领域率先爆发，比如供应链金融、数字版权、电子票据、游戏等等。ZV CHAIN 支持用户将线下资产映射上链，用户之间的交易，可以用登记在 ZV CHAIN 链上的资产实现价值的转移。通过链下资产与链上资产映射，甚至一些链下的商业交易，可以通过智能合约进行锁定交易并完成事务管理。

目前区块链项目不能很好服务于商业应用，除了存储容量有限和交易性能限制等原因之外，还有很重要的原因是：单个区块链项目是个独立的价值网络。要求所有商业项目落户在同一个区块链上是不现实的，可以预见多链多生态会是个大概率事件。不同区块链项目之间的协同操作难度大，极大地限制了区块链项目的发挥空间。为此，ZV CHAIN 提出跨链协议，

支持不同链之间的价值交换与价值传递。

ZV CHAIN 不仅是一个独立运行的区块链网络，支持跨链协议后，能实现跨链资产的交换，以及价值转移等跨链通信功能。ZV CHAIN 的跨链协议会有三类角色：

- **侦听节点**

执行原链的全节点矿工功能，可以铸原链新块并执行交易。在原链中收集有效的跨链通信交易信息传给验证节点

- **验证节点**

原链的公证节点兼 ZV CHAIN 链中的矿工节点，验证来自原链数据的合法性，并将此打包到 ZV CHAIN 链的新块内。

- **网关节点**

同时运行原链钱包节点和 ZV CHAIN 链，相当于原链与 ZVCHAIN 链之间的网关。记录并处理跨链进入的交易和出去的交易。该类节点需要配置原链对应的代币，能够实现跨链 Oracle。

ZV CHAIN 定位未来区块链世界的中转器，用户友好的智能合约支持方便接入新型的业务场景，更将为传统商业进行流通，实现区块链连接一切商业，为未来的商业提供信任与价值互换的基础。

三 ZV CHAIN 性能优化方案

3.1 分片并行计算框架

Chiron 在保证去中心化和安全的前提下, 达到了 POS 的性能, 3000+TPS 足够支撑大多数的商业化应用。考虑到对超大规模应用的扩展性支持, ZV CHAIN 借鉴 Google 的 MapReduce 和阿里云批量计算思想, 设计了分片并行交易执行框架, 进一步提高吞吐量。

在并行计算框架中, 我们将重节点逻辑上分为计算节点和提案节点。也就是说, 在一个铸块周期里, 根据上一区块产生的随机数可以选定多个提案节点 (详见 Chiron 共识机制), 而根据签名与交易发起人的地址的运算, 选定的节点称之为计算节点。计算节点负责执行交易, 提案节点负责块的生成。如下图 3.1 所示, 分片计算的具体流程:

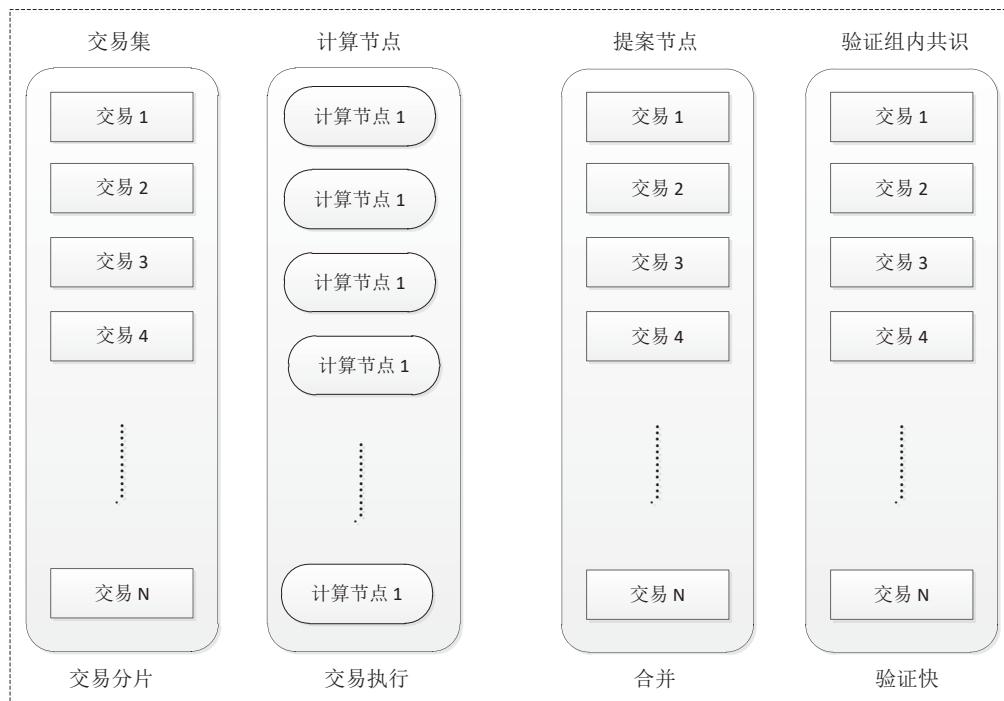


图 3.1: 分片计算流程图

- **交易分片**

根据交易发起人的地址和上一块的签名, 将交易发送到不同的计算节点。在这里, 我们并没有限制交易目标账户地址, 比起状态通道模式具有更好的灵活性。相同的交易发起

人发起的多笔交易，都将落到同一个计算节点，用最短时间窗口即可验证双花问题。同时在分发交易的策略中采用了 Chiron 共识的 VRF 输出随机选择计算节点，通过计算节点复用和计算节点的不可预测提高了系统的健壮性和安全性。

- **交易执行**

计算节点会根据当前账户状态执行交易，同时记录账户状态变化等情况。对于交易的执行往往需要依赖状态数据，例如账户余额、合约内保存的用户数据等。在我们的设计中，计算节点保存了完整的状态信息，一旦接受到一个新块，就会更新本地状态。所以计算节点本地即可完成交易的执行，无需进行跨链等复杂交互。

- **合并**

对于每一笔交易的执行结果，计算节点提交给提案节点的内容包括账户状态树根 hash（简称根 hash）、交易影响的账户、账户状态的差值。提案节点遍历收到的所有结果，对比本地根 hash 与结果中的根 hash，筛选出交易结果，称之为候选集。提案节点将候选集中的账户状态差值，合并到本地账户之上，生成最终的账户状态。

- **验证块**

验证组内验证交易执行结果，生成组签名，最终出块上链，参见 Chiron 共识机制的验证组共识出块部分。

3.2 ZLight 闪电网络

对 ZV CHAIN 而言，引入闪电网络技术不但可以提高系统吞吐量，而且是分支行架构必不可少的一部分。闪电网络可以让基金账户里的交易安全地离线进行，只需周期性和主链进行清算同步，而不需要把频繁的小额交易实时上链。闪电网络技术可以快速在 ZV CHAIN 的 B 端商家和 C 端用户建立便捷的轻量连接，并安全的完成交易。ZV CHAIN 设计了单向闪电网络和双向闪电网络，用于不同的业务场景。

3.2.1 ZLight 单向闪电网络模式

单向闪电网络简单易用，B 端商家不需要预存资金即可完成和 C 端用户的高频小额交易，适用于小卖部、小超市、小餐馆等快消业务。如图 3.2，描述了单向闪电网络的流程示例。

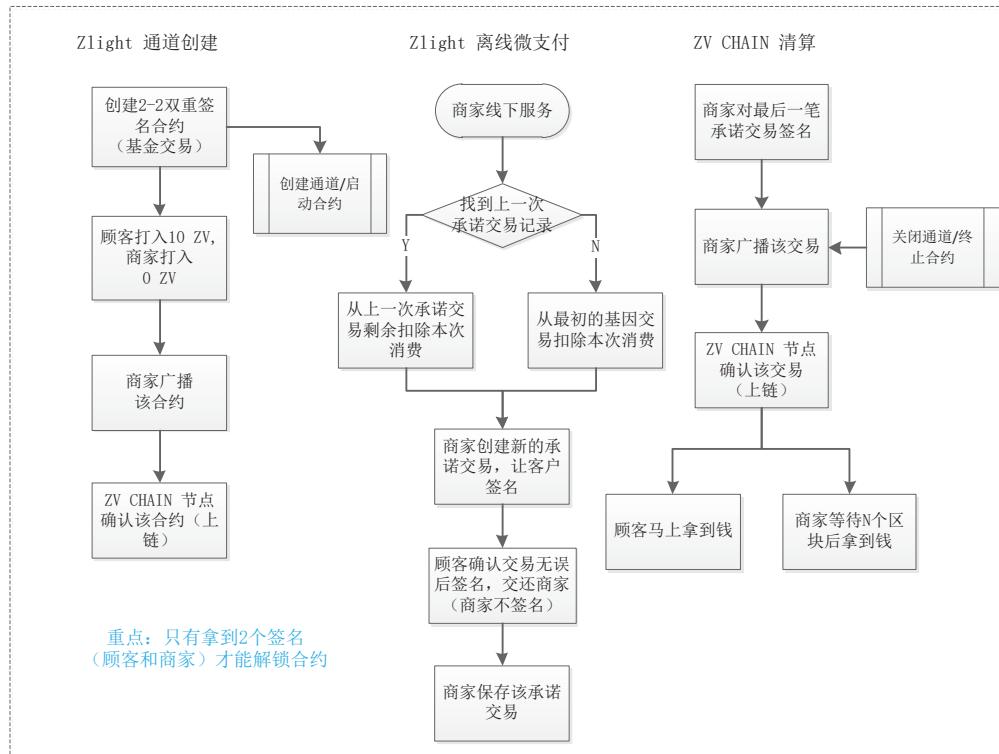


图 3.2: ZV CHAIN 单向闪电网络流程图

3.2.2 ZLight 双向闪电网络模式

双向闪电网络适用于有较多往来资金的 B 端商家之间，例如，供应链金融和产业上下游，商家之间的资金通道支持双向离线流转，并保证了高安全性。双向闪电网络是标准化闪电网络通道，支持全双工工作。

双向闪电网络的安全关键，在于如果有一方广播了一个对其有利的中间承诺交易，如何发现并进行惩罚。如图 3.3 展示了密码学相关的 RSMC 安全保障原理图。

ZLight 设计了延迟到账窗口，并在某方向 ZV CHAIN 主链发起承诺交易广播时，周期性向另一方发送交易通知，并对广播中间承诺交易的一方实施全额罚没给对方进行惩罚。

3.2.3 ZLight 分支行架构

闪电网络的 RSMC 可以极大的提高主链吞吐量，但如果在 100 万用户和 10 万商家之间建立离线通道，则需要在主链上构建 $100 \text{ 万} * 10 \text{ 万} = 1000 \text{ 万个基金合约}$ 。一旦有更多的用户和商家参与到 ZV CHAIN 的生态，这个基数呈笛卡尔积放大。考虑到不同地域不同行业的可扩展性，ZV CHAIN 引入了 HTLC 技术构建分支机构。传统的 HTLC 一旦链路上有节点

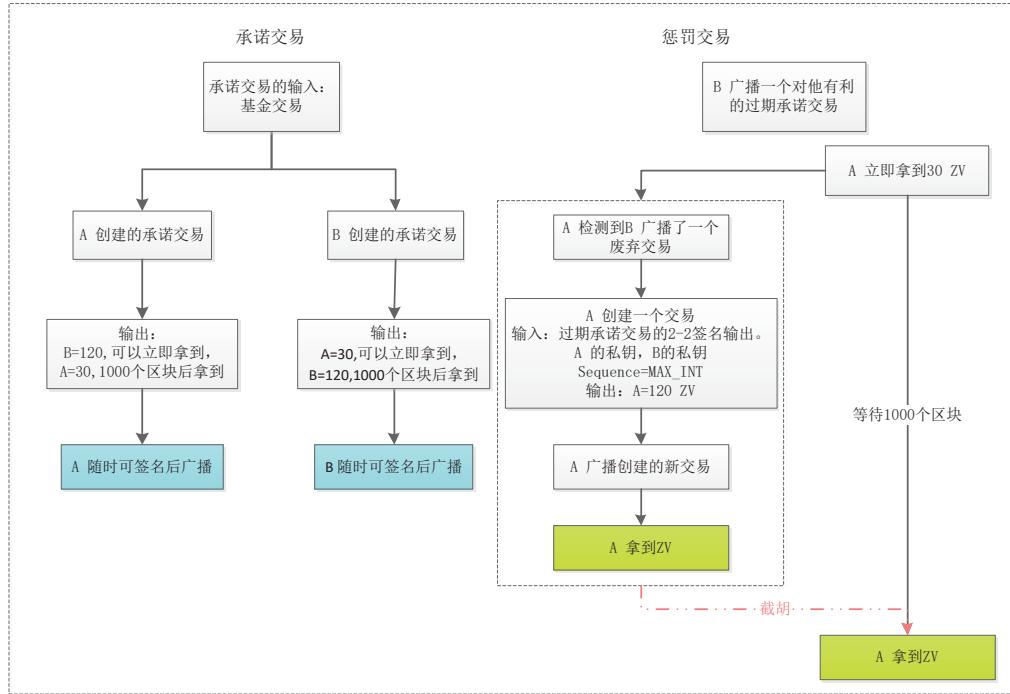


图 3.3: ZV CHAIN 双向闪电网络安全保障结构

掉网或临时性不在线，会导致整个交易锁死，交易中的资金会被锁定一个较长的周期才释放，这样的模式很难构建高效稳定的交易网络。ZV CHAIN 创新的把 HTLC 深度设定在最多两层，且纳入分支行结构，只有通过 ZV CHAIN 认证的 HTLC 节点才能成为 ZV CHAIN 的分支行节点，在提供稳定 HTLC 服务的同时，获取节点收益。具体的设计架构，如下图 3.4 所示：

3.3 分布式数据存储

分布式数据不仅仅指的是区块数据，也包含账户余额数据、合约代码、合约内部数据等。我们对数据 D 设定一个过期时间 T1，在 T1 之前所有提案节点都会保存这份数据，我们称之为热数据，具体如图 3.5 所示。

在超过 T1 之后，根据数据哈希值对节点 ID 进行取模，确定 D 所处在的分片（例如节点 ID 是一个十六进制数，取第一个十六进制位，就能分成 0 到 F 十六组）。对于处在 D 所在分片的提案节点，数据 D 将继续被保存。而其他提案节点将只保留 D 的 hash，而不再保留数据 D。这部分数据我们称之为温数据。

类似的算法，我们对温数据设定一个过期时间 T2，在 T2 之后温数据被切换到访问数据更慢但成本更低的存储节点上。这样的数据我们称之为冷数据。当提案节点构建区块，执行

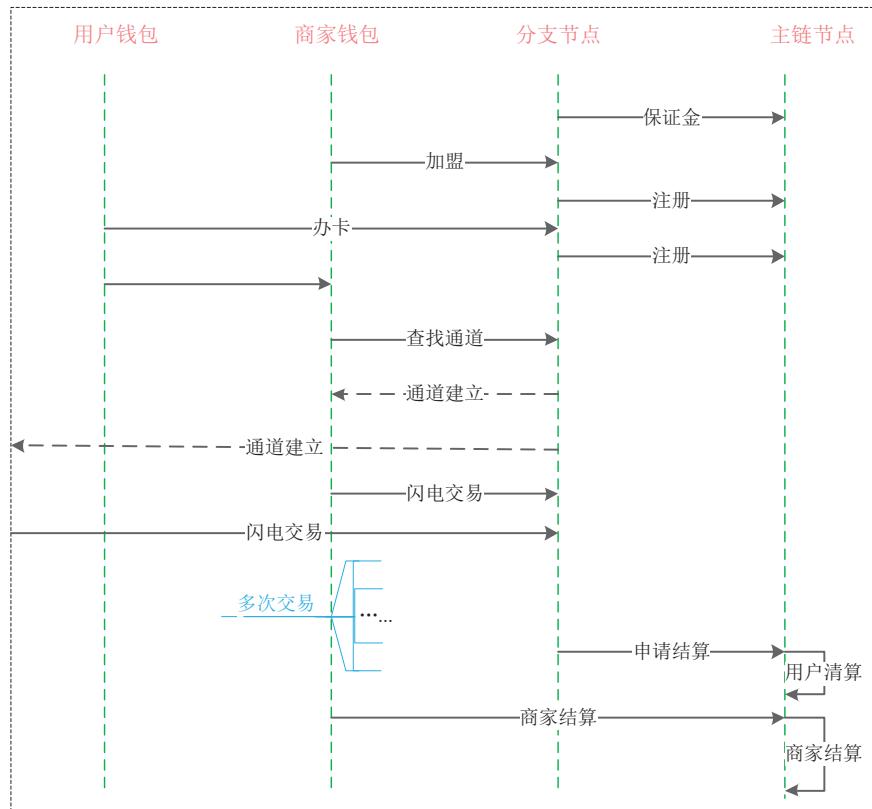


图 3.4: ZLight 分支行架构

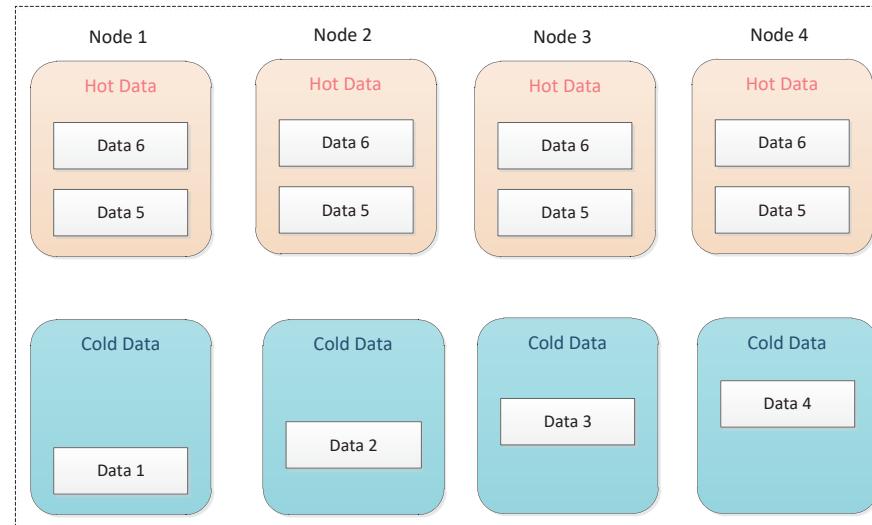


图 3.5: 数据分布式存储与管理-冷热数据存放示意图

交易需要历史数据时，首先在本地读取。当本地没有时，将依次从温数据存储节点、冷数据存储节点读取。当读取到数据时，根据本地保存的 hash 校验存储节点提供的数据。若数据校验通过，则奖励存储节点。若超时或数据校验失败，则本区块中不能打入此交易。

3.4 P2P 网络

对于商业应用来看，交易吞吐量和延时是企业最关心的交易性能指标。主要影响区块链的交易性能包括广播通信、信息加解密、共识机制、交易验证机制等等几个环节。由于区块链的核心技术之一就是 P2P 网络，因此 P2P 网络通信的效率是对性能的影响非常重要。Chiron 共识机制的轻节点验证和组内、组间通讯极为依赖高性能的 P2P 网络实现。ZV CHAIN P2P 对传统的 P2P 技术做了较大的技术升级，如图 3.6 所示 ZV CHAIN P2P 架构。

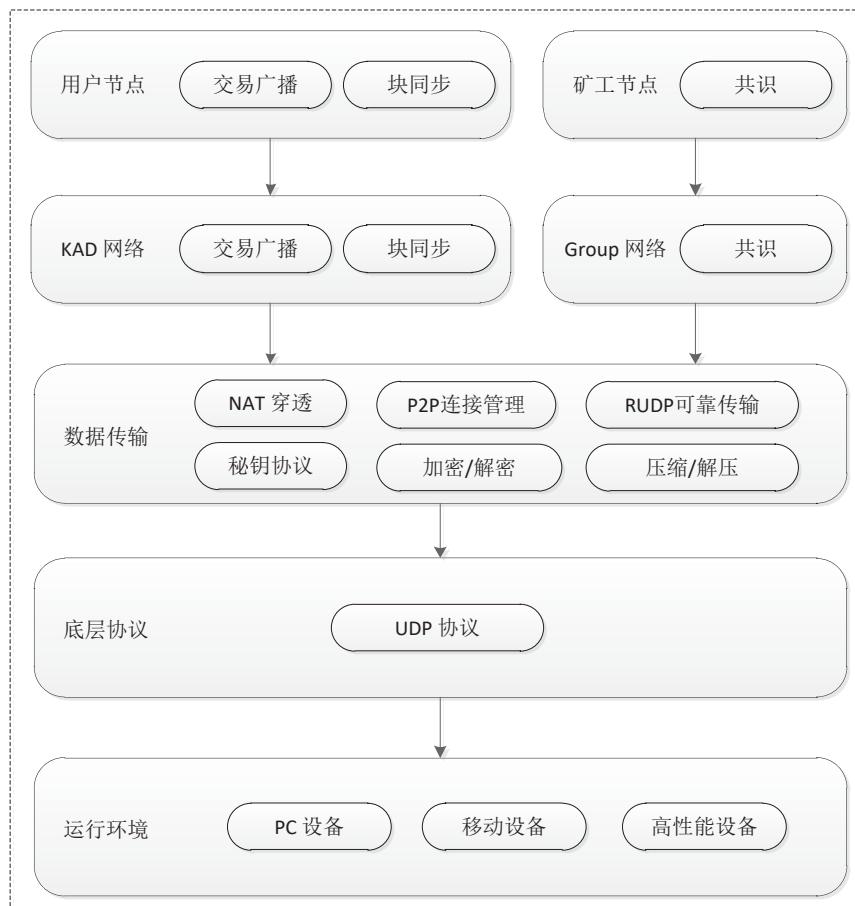


图 3.6: ZV CHAIN P2P 网络框架

主要改建策略包括：

- 使用新型的 NAT 穿透技术（专利申请中）大幅提高节点在线率；

表 3.1: 内网穿透技术对比

内网穿透	STUN	ZV CHAIN P2P
原理	RFC3489	Linux 内核协议栈
穿透率	30%	96%
设备分类	全锥型/限制锥型/端口限制锥型/对称型	主机端口/固定端口/对称端口
防火墙穿透	不支持	支持

- 针对 Chiron 以组为单位出块的方式，设计了双层 KAD 网络提高通讯效率；
- 使用 RUDP 代替 TCP，通讯延时降低 35% 左右。

3.4.1 NAT 穿透

主流的 NAT 穿透使用标准 STUN[13] 作为解决方案，STUN 将 NAT 设备分为四类，全锥型、限制锥型、端口限制锥型、对称型。我们对中国六万个网吧 NAT 设备进行了统计，其中全锥型 5%，限制锥型 7%，端口限制锥型 58%，对称型 30%，得到的理论穿透率为 56% ($5\% \times 100\% + 7\% \times 100\% + 58\% \times 70\% + 30\% \times 12\% = 56.20\%$)。另外，由于 NAT 防火墙的存在，被动的 UDP 包到达 NAT 设备时，在连接跟踪模块会产生相应的记录，引起的副作用会导致随后的端口预测失败进而使整个穿透流程失败。STUN 并没有考虑 NAT 防火墙的因素，按标准实现的穿透率仅在 30%-40% 左右。

通过对 linux 内核协议栈的分析，我们从端口映射规律重新定义了 NAT 设备类型，并将之分为三类：主机端口、固定端口和对称端口。用这种分类法重新对六万个 NAT 设备进行统计，其中主机端口占比为 75%，固定端口为 23%，对称端口为 2%，得到的理论穿透率为 96% ($75\% \times 98\% + 23\% \times 98\% + 2\% \times 0\% = 96.04\%$)。针对路由器防火墙在接收到无相关性的被动数据包后会更改映射端口而导致随后的穿透失败，ZV CHAIN P2P 设计了 TTL 动态调整算法，最终使实际穿透率基本达到了理论值的水平。

3.4.2 组播网络

ZV CHAIN 的所有节点都会加入到全局的 KAD 网络中，某个节点都将和 8-16 个邻居节点建立连接，由邻居节点间的通讯完成交易广播、块链同步和组链同步。针对分组的 Chiron 共识机制，ZV CHAIN 构建了二层子 KAD 网络定位组成员节点，保证组成员间提案和验证的高效通讯。相比全局的 KAD 网络，二层组播网络保证了组内消息更快速的投递，同时减轻了对整个节点网络的负载。

表 3.2: 通讯协议对比

底层协议	TCP	RUDP
内网节点穿透	难	易
高质量网络传输速度	高	高
中质量网络传输速度	中	高 (ARQ 快速重传)
低质量网络传输速度	低	高 (FEC 冗余传输)

3.4.3 RUDP

对于高在线率节点网络和大量碎片验证数据交互的场景，RUDP 相比 TCP 有着明显的优势。宏观来看，用 RUDP 代替 TCP 已是工业界的趋势，如谷歌提出的 QUIC 框架可以看做 RUDP 的超集，考虑到 ZV CHAIN 要求的高连通性和组内协作出块，ZV CHAIN 在通讯层用开源且成熟的 RUDP 代替 TCP。

四 ZV CHAIN 的技术架构

4.1 ZV CHAIN 核心技术架构

ZV CHAIN 是一个通用型区块链金融服务提供商，底层是一条区块链的公链，保证业务的去中心化、数据不可篡改。ZV CHAIN 上运行的核心业务都是基于智能合约的去中心应用。为了完成 ZV CHAIN 金融业务正常运行，除了区块链技术外，还需要额外的技术。一方面，为保障用户的隐私以及商业机密，比如，风控服务需要云技术和大数据技术，以及清算服务需要分布式计算集群等等；另一方面，为提供更好的用户体验，在直接面对用户体验的部分，需要集成现有分布式服务集群、CDN 等技术。具体的 ZV CHAIN 核心技术框架，如下图 4.1 所示。

4.2 ZV CHAIN 节点架构

4.2.1 节点类别

ZV CHAIN 节点是对所有 ZV CHAIN 生态的参与者的称呼，从生态参与角色上划分，可以有基石节点、用户节点、矿工节点、守护节点。节点功能包括提案、验证、存储、风控和检测。依照对节点设备的最低要求可以分为轻节点、重节点和超级节点。随着主链网络账本的增加，项目中期主链提供分布式账本存储功能后，重节点将细分成存储节点和算力节点。

- **用户节点（轻节点）**

用户节点为 ZV CHAIN 生态提供了数字资产的流动性，在 ZV CHAIN 网络中的实际载体倾向于移动端钱包。用户节点通过参与提案获得激励，在线时长越长获得激励越多。

表 4.1: ZV CHAIN 节点角色划分与功能设定

角色维度	设备维度	验证	提案	存储	风控	监测
基金会节点	基石节点	√ (初期)	√ (初期)	√	√	√
用户节点	轻节点	√				
矿工节点	算力节点	√	√			
	存储节点	√		√		
守护节点	超级节点			√	√	

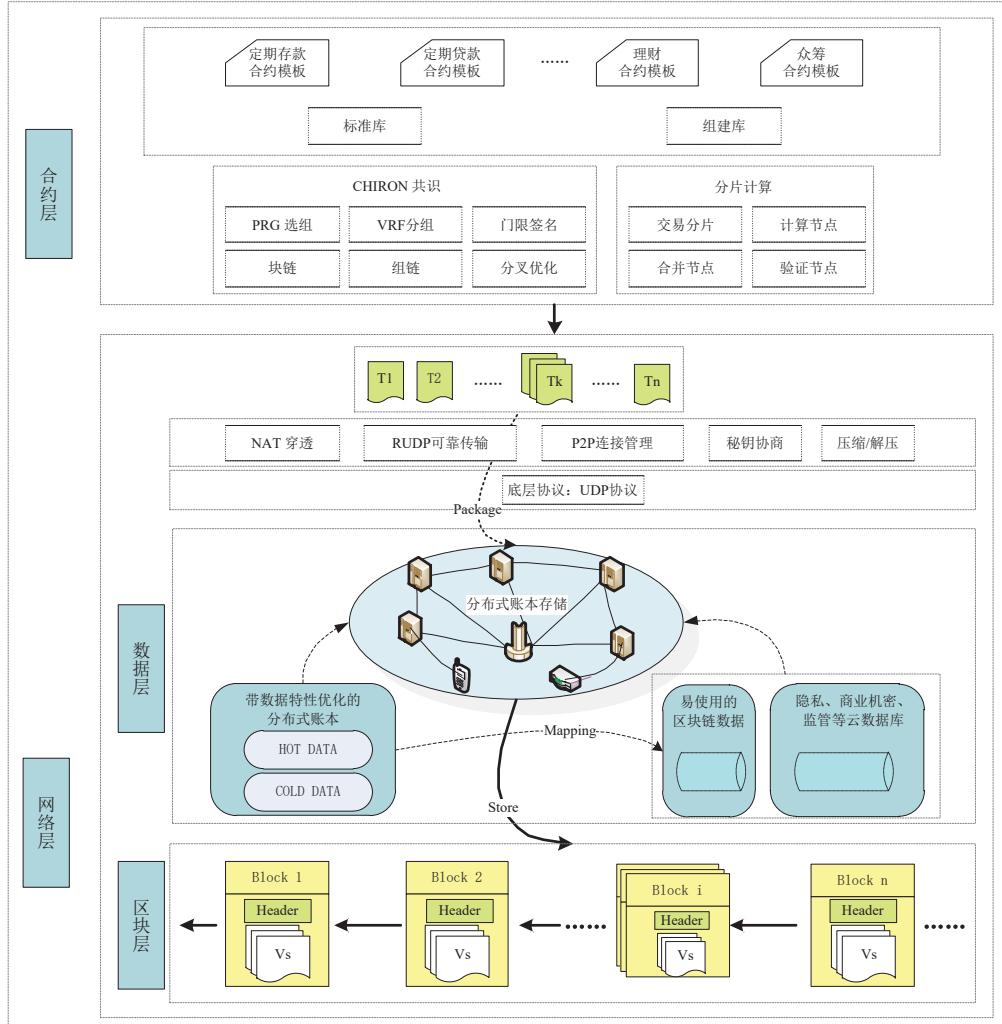


图 4.1: ZV CHAIN 核心技术框架

- **矿工节点（算力节点与存储节点）**

矿工节点为 ZV CHAIN 生态提供基础建设支撑。在 ZV CHAIN 网络中的实际载体倾向于低能耗的网络设备，比如家用 NAS 或 AP 等。通过参与验证出块及账本存储获得激励。

- **守护节点（超级节点）**

守护节点为 ZV CHAIN 生态的用户提供安全风控服务，是通过用户节点及矿工节点参与的社区授权的 ZV CHAIN 网络守护者，也是监管节点。在 ZV CHAIN 网络中的实际载体倾向于高性能分布式集群。守护节点在 ZV CHAIN 生态中通过风控的实时计算、全量账本存储等获得激励。

- **基金会节点（基石节点）**

基石节点是 ZV CHAIN 基金会委托部署的节点，是系统运行的最小配置。当系统初始或者没有太多外部矿工参与的情况下，基石节点会承担提案节点，验证节点，存储节点，超级节点的功能，保证系统运作的。随着外部矿工加入数量的增加，提案节点或验证节点超过阈值后，基石节点不再履行对应提案，验证等功能，做好系统旁观监测的工作（还需保留部分存储，风控功能）。当外部矿工节点不够时，又可转化承担提案，验证等职责。

4.2.2 节点功能

ZV CHAIN 的节点架构，如下图 4.2 所示，包括五大类节点：

1. **提案节点**

承担候选区块的提案职责

2. **验证节点**

承担候选区块的验证职责

3. **存储节点**

承担系统分布式数据的存储职责

4. **超级节点**

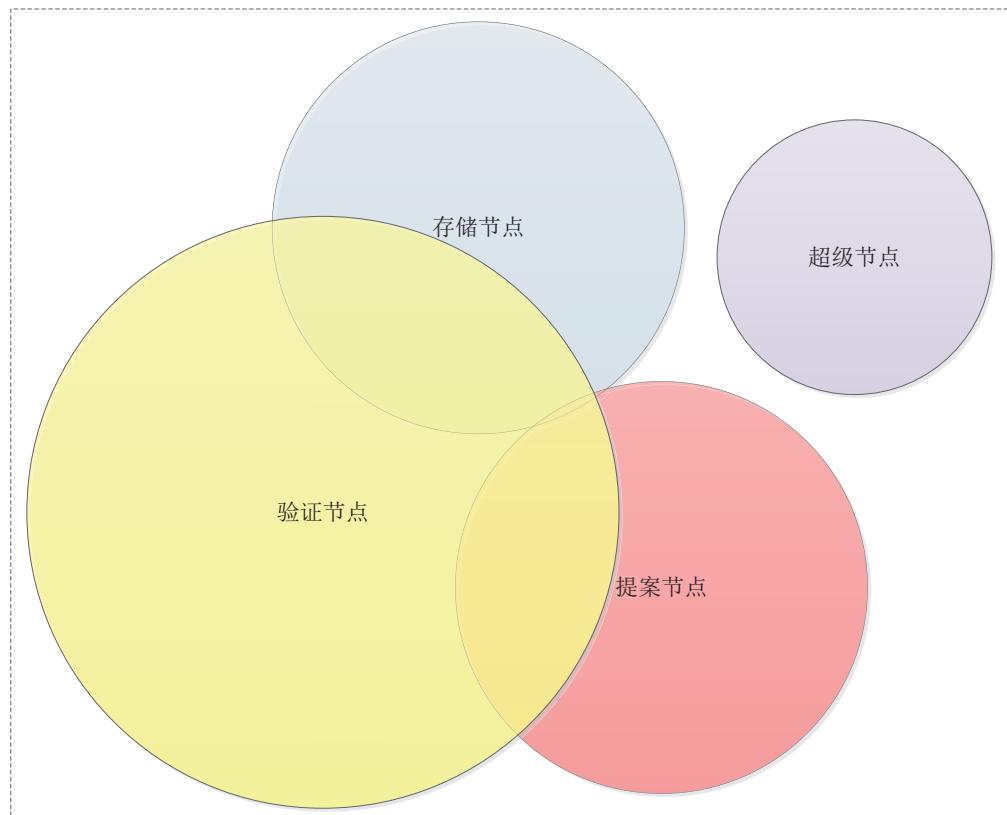


图 4.2: ZV CHAIN 节点功能示意图

存储系统的风控数据，提供用户的风控管理。ZV CHAIN 的超级节点是指为了完成 ZV CHAIN 银行的业务正常运行，除了区块链的节点外，额外提供的服务的节点，例如提供智能风控服务的节点、提供清算服务的弱中心化节点等等。

5. 基石节点

开发团队自行部署的节点，是系统运行的最小配置

当系统初始或者没有太多外部矿工参与的情况下，基石节点会承担提案节点，验证节点，存储节点，超级节点的功能，保证系统运作的。随着外部矿工加入数量的增加，当提案节点数或验证组数高于系统设置的阈值后，基石节点停止履行相应的提案或验证功能，做好系统见证监测的工作（还需保留部分存储，超级节点）。当外部矿工节点不够时，提案节点数或验证组数低于于系统设置的阈值，基石节点又会重新开启提案，验证等职责，保障系统正常有序的运行。

4.2.3 节点关系

用户节点是 ZV CHAIN 网络的流动性贡献者也是网络的实际使用者，用户节点需向矿工节点支付费用方能使用网络。同时，用户节点会依据流动性贡献得到矿工节点挖矿分配。此外，用户节点可定期投票授权守护节点。如图 4.3 描述了节点经济生态的关系：

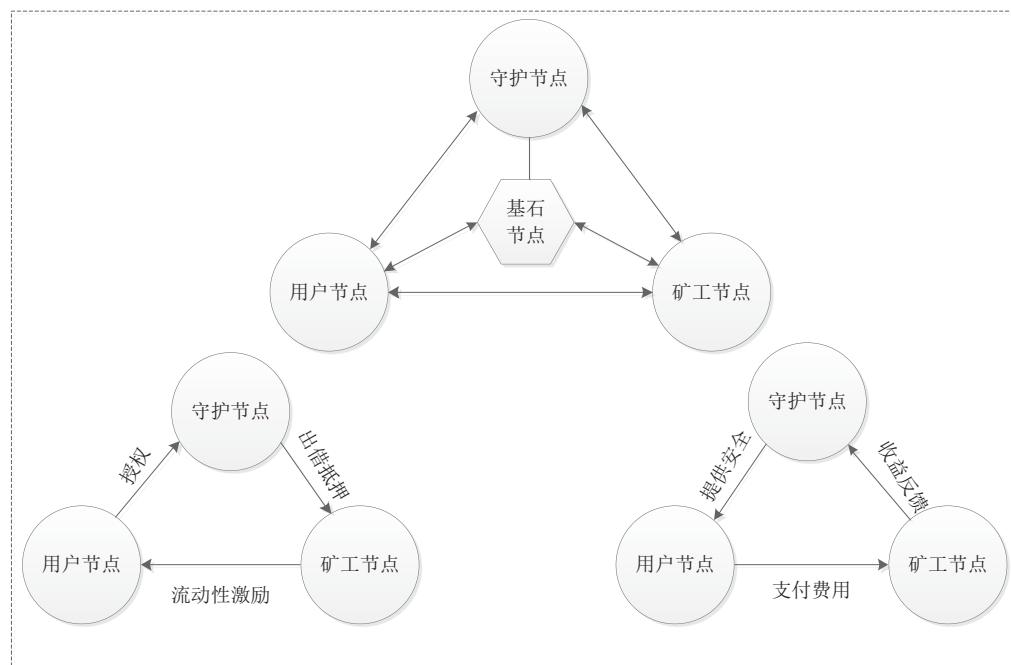


图 4.3: ZV CHAIN 节点经济生态关系

矿工节点是 ZV CHAIN 网络的基础建设者，为了防止潜在作弊等有害 ZV CHAIN 生态建设的行为，Chiron 共识挖矿需要评估矿工节点的可信度及其对网络的贡献，在很大程度上取决于锁定的 ZV 数量及其持续在线时长等。如果矿工节点需要锁定的 ZV 不足，可以向守护节点租用足额 ZV 获得最大奖励。守护节点是 ZV CHAIN 网络的安全守护者，用户节点的多少决定了守护节点的多少。他们为用户节点提供安全风控、为矿工节点提供出借抵押服务。

五 可演进性与场景跃迁

5.1 技术扩展与演进

基础架构的可扩展性与核心技术的演进，直接决定了我们金融公链发展的张力与活力。因此，我们在研发之初，就从底层架构到上层应用层面，全面系统地融合了金融公链的技术未来 [12, 15]。

5.1.1 基础架构可扩展性

除了前述的 ZLight 闪电网络和分片并行计算，未来我们将更多关注提升区块链金融在智能服务方面的扩展，比如，引入外部数据与算力，以及智能模型，以及跨链的实现，比如，接入外部公链 Token，解锁公链资产整体的价值潜力，加速不同公链 Token 的价值流转。

5.1.2 核心技术可演进性

由于当前业内区块链公链项目都还处于技术早期阶段，随着不断的深入探索与研发，若要实现核心技术实时的迭代升级，就需要提前把握公链技术的发展趋势，尽早实现先进的设计理念。

5.1.2.1 以博弈论为基础的共识机制

博弈论用来帮助我们理解所观察到的决策主体相互作用时的现象，在区块链的机制设计方面，无论是从链内到链外，或是链的边界，都是博弈论在发挥作用，甚至区块链的出现和产生其实都可以用博弈论来思考解释。

区块链上共识机制的设计与博弈论机制设计最为相似，机制设计通常被称作反向博弈论，因为我们是从一个期望的结果开始，反向推导来设计一个完整的游戏，下文是随机博弈模型的应用示例。

- 随机博弈模型与网络安全

我们将采用随机博弈模型，构建网络攻防实验整体架构，它由网络连接关系、脆弱性信息等输入数据到网络攻防博弈模型的快速建模方法，基于最终生成的攻防模型可以对目标网络的攻击成功率、平均攻击时间、脆弱节点以及潜在攻击路径等方面进行安全分析与评价。从而，解决网络攻防过程中无法有效应对攻击意图与策略变化的问题。

5.1.2.2 链下计算的趋势

目前业界倾向于链下计算的考量越来越多，我们考虑，未来若链下计算花费低廉，将一部分复杂且对硬件性能要求高的智能合约在链下运行或许可以解决处理速度下降和资源占用等问题。另外，鉴于我们是区块链金融公链，对隐私要求更高，一定程度上，可以解决链上数据与计算公开透明的问题，提升智能合约数据和运行的隐私性。

5.2 应用场景跃迁

ZV CHAIN 的应用场景跃迁一方面是指在研发的不同阶段，将提高可服务场景的覆盖率，不断接入推出新的业务应用；另一方面是指，针对某一场景，将不断提升服务的质量和深度，比如，提升自动化、智能化服务的比率等 [13, 14]。

5.2.1 基本的清结算体系

尽管 GCMS (Global Clearing Management System) 和 S.A.M (Settlement Account Management System) 等清结算系统已经显著地提高了支付的结算效率，但银行间的跨境清结算体系仍然主要依赖于代理银行、往来账户或者第三方结算行等传统结算方式。大量的人力工作、会计处理和过多的中间单位使得银行间的结算工作（尤其指跨境结算）有较长的处理时间、昂贵费率汇率和繁琐冗杂的处理过程。

5.2.1.1 ZV CHAIN 交易支付体系

各个交易实体参与到一笔 ZV CHAIN 支付的流程如下：

1. 消费者选择一个代理节点，并将一笔预付资金存入双重签名（消费者签名与代理节点签名）合约。并将该合约广播至区块链中；
2. 代理节点与其负责的商户开通双重签名（代理节点签名与商户签名）合约，（代理节点）存入预付资金。并将该合约广播至区块链中；

3. 消费者刷卡（扫码）支付，商户端将用户交易信息发送至代理节点并生成承诺交易（商户-代理节点）询问代理节点签名，代理节点生成承诺交易（代理节点-消费者）询问用户授权；
4. 代理节点获得用户授权后，检查双重签名合约（消费者与代理节点）余额：如果在扣除累计承诺交易（代理节点-消费者）后余额充足则签名承诺交易（商户-代理节点）并返回给商户（代理节点签名，商户不签名）；
5. 商户获得代理节点签名的承诺交易后，检查双重签名合约（代理节点与商户）余额：如果在扣除累计承诺交易（商户-代理节点）后余额充足则为消费者提供商品及服务。

具体交易流程如图 5.1 所示。

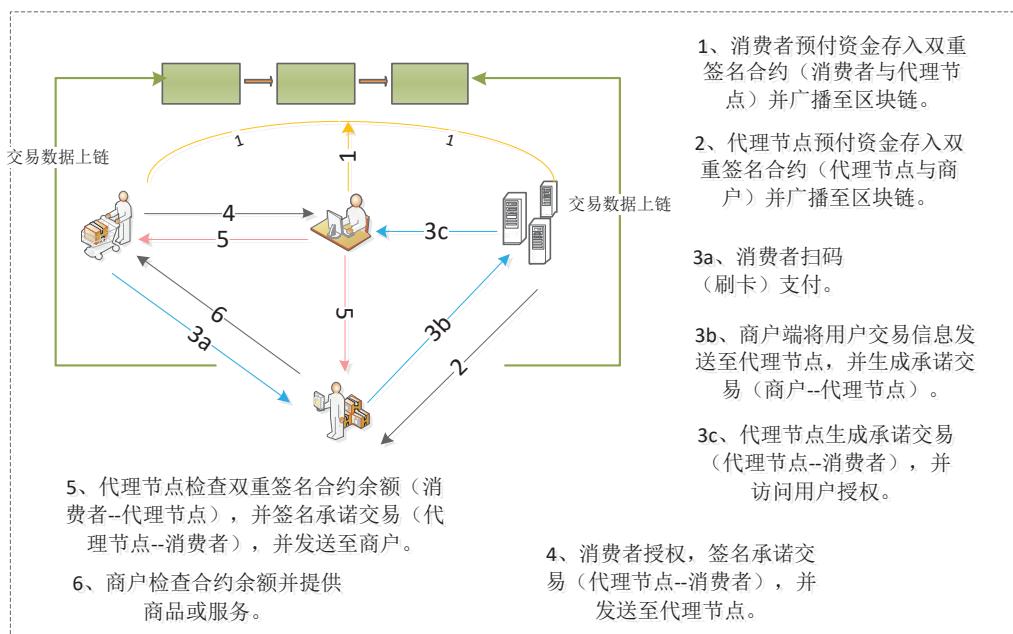


图 5.1: ZV CHAIN 交易支付流程

5.2.1.2 ZV CHAIN 跨境清结算体系

ZV CHAIN 清结算网络主要包含以下几个阶段：开通闪电网络（预付）、交易单方签名（授权与清算）、交易双方签名并广播至区块链（交易结算）。开通闪电网络（预付）指代理节点需要双向开通与商户和消费者之间的单向闪电网络，其中与消费者之间的单向闪电网络由消费者进行预付，与商户之间的单向闪电网络由代理节点进行预付。这让消费者和商户仅需要开通少量的闪电网络就可以实现在所有商户和用户之间闪电支付。

交易单方签名（授权与清算）指一笔承诺交易由单方进行签名并发送至另一方，即在链下完成交易的授权和清算。消费者授权并签名承诺交易后发送至代理节点（代理节点可以选择签名并链上广播进行结算），代理节点授权并签名承诺交易后发送至商户（商户可以选择签名并链上广播进行结算）。

图 5.2 是 ZV CHAIN 跨境清算结算体系。

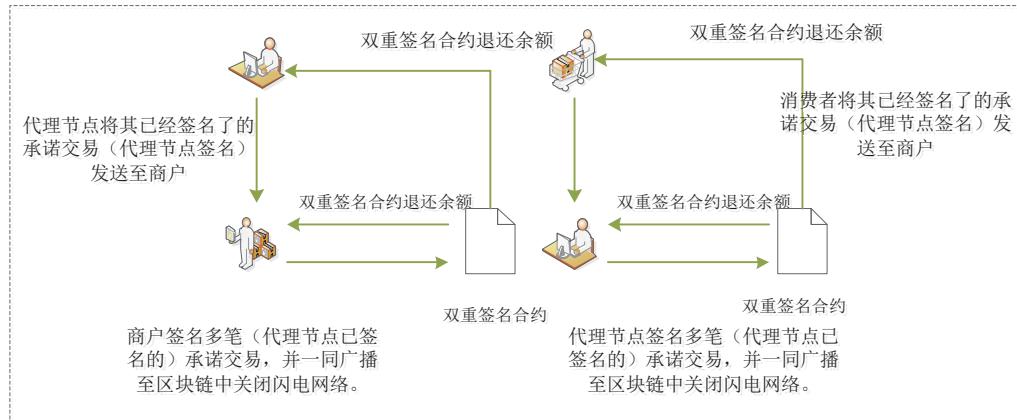


图 5.2: ZV CHAIN 跨境清算结算体系

交易双方签名并广播至区块链指交易一方在收到有另一方签名的多笔承诺交易后，将其进行签名并广播至区块链的过程，即为交易结算。结算后双方的闪电网络将关闭并将对应余额返回至双方的钱包地址。由于交易单方签名（清算）在链下完成，交易的效率得到了极大的提高，最终结算仅需要单方签名和广播，与传统的结算方式在复杂度和效率相比有着显著的优势。

5.2.1.3 ZV CHAIN 稳定币发行及其跨境结算示例

“代币入金”成为加密货币越来越重要的一项应用，可以有效提升现阶段加密货币在跨境汇款方面的实际价值，同时，有效增强加密数字货币价值尺度属性，从而，提升其信用度，并进一步扩展其应用价值。

我们将提供发行稳定币的“一站式”服务中间件，配合清算体系发挥更大的实际功能。下文是基于稳定币的一个跨境结算示例。本例中，法币缩写符号如“JPY”均代表与其对应的数字资产。以 JPY 购买以 USD 计价的商品为例，其跨境支付流程有如下几种情形：

1. 单个双向闪电通道

如图 5.3 所示，JPY 代理节点 A 与接受 JPY 的 USD 代理节点 B 开通双向闪电通道，

JPY 代理节点向双重签名合约转入一定的 JPY, USD 代理节点向双重签名合约转入一定的 USD。

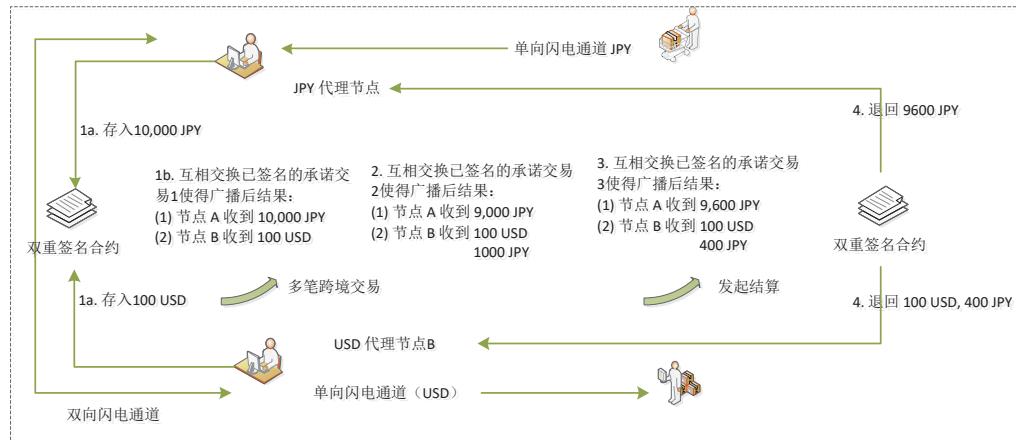


图 5.3: ZV CHAIN 单个双向闪电通道

双方各自生成承诺交易 1 (该交易结算后, 使得 JPY 代理节点收回其存入额的 JPY, USD 代理节点收回其存入额的 USD, 各自签名后发送给对方, 即节点互相持有对方已签名的承诺交易, 可以由一方发起结算)。在一笔跨境交易中, 双方各自生成承诺交易 2 (该交易结算后, 使得节点各自取得累计交易后的余额, 废除承诺交易 1)。重复步骤 3, 在跨境交易中, 不断生成新的承诺交易并刷新待结算状态, 使得承诺交易反映实时余额。关闭闪电通道, 代理节点 A 与代理 B 进行结算;

2. 链式双向闪电通道

基于单个双向闪电通道的跨境支付需要与代理节点 A 开通闪电通道的代理节点 B 接受 JPY, 如果用户授权的代理节点 A 无法直接建立与接受 JPY 的代理节点 B 的闪电通道, 跨境支付可由链式双向闪电通道完成。ZV CHAIN 跨境结算网络会自动匹配最优费、汇率的链式闪电通道并完成跨境清、结算。链式双向闪电通道如下图 5.4 所示:

3. 最后的结算工具

ZV CHAIN 系统代币 ZV 在上述的链式闪电网络无法联通时将充当最后的结算工具, 如图 5.5 所示,

JPY 代理节点 A 在与 USD 代理节点 B 的闪电通道中将使用 ZV 作为支付工具。

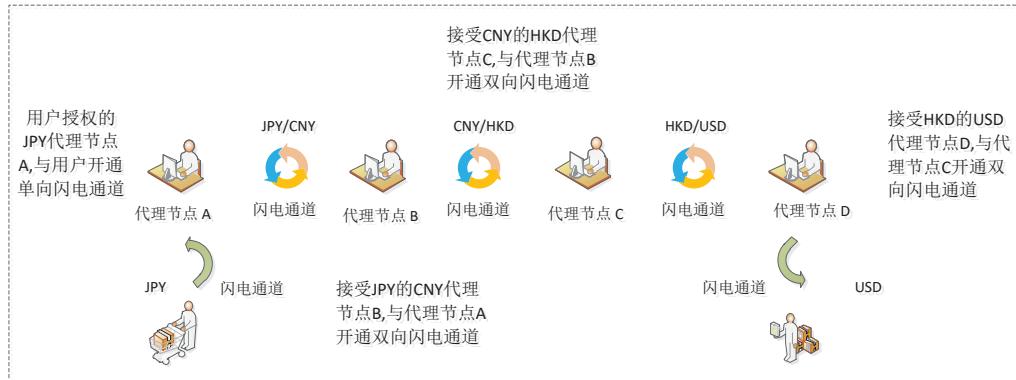


图 5.4: ZV CHAIN 链式双向闪电通道

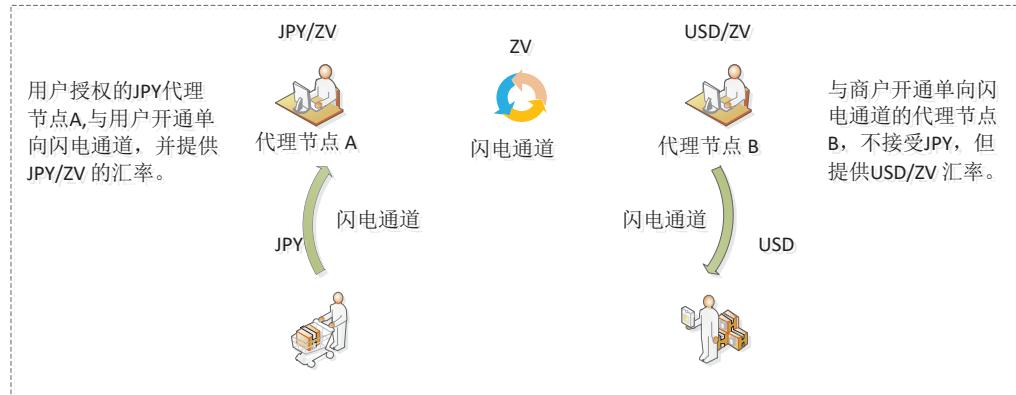


图 5.5: ZV CHAIN 最后结算工具

5.2.2 智能金融服务体系

5.2.2.1 ZV CHAIN 智能产品与服务生态系统

作为专业化的金融公链，我们可以更容易形成产品与服务的生态系统。同时，融合人工智能技术在金融领域的应用实践成果，更方便提升金融产品与服务的质量，比如，业务的自动化与智能化等。这也就充分发挥了区块链技术在构建金融基础设施方面的优势，以及人工智能技术在提升分布式账本价值方面的优势，最终，形成相得益彰的智能化生态系统。如下图 5.6 所示，描述了我们研发的智能产品与服务生态系统框架。

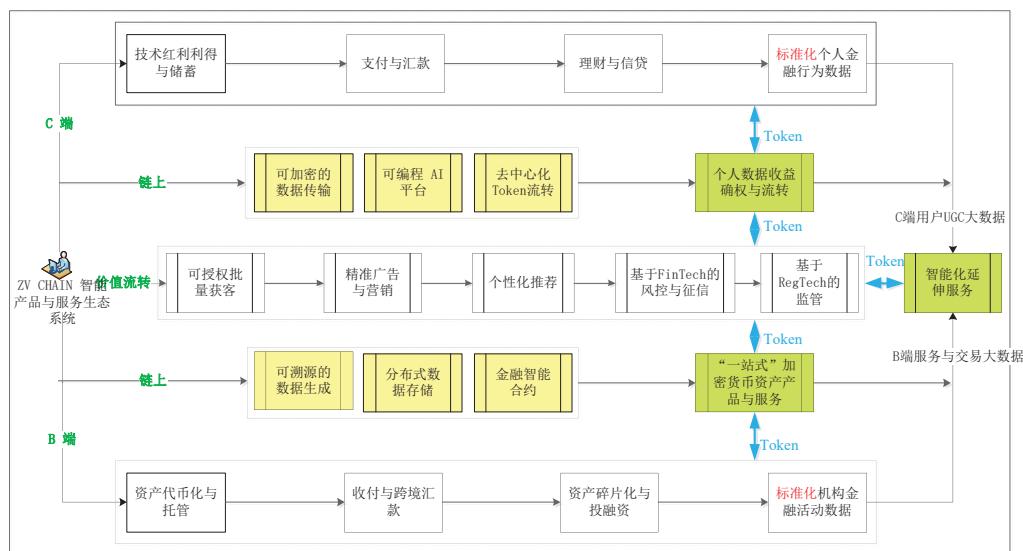


图 5.6: ZV CHAIN 智能产品与服务生态系统

- C 端产品生态
- B 端产品生态
- 价值流转产品生态
- 智能化延伸服务产品生态

5.2.2.2 ZV CHAIN 智能风控体系

针对金融业务的特色，风控体系是贯彻始终的全生命周期需求，我们在风控中间件的基础上，经过功能深度扩展与延伸，我们研发了融合区块链技术与人工智能技术的高性能风控系统，ZV CHAIN 智能风控的设计框架将包括如下几个主要模块：

1. 超级节点

超级节点或者传统分布式中心化集群，采用大数据以及云计算技术，根据历史和实时的行为数据，进行规则引擎和风控模型计算，输出风控控制结果；

2. 风控预言机（Oracle）

把链下的风控结果，进行加密和 Hash 处理，提供接口给链上使用；

3. 智能合约

链上智能合约使用风控预言机接口得到风控结果，根据风控的不同结果进行对应的业务处理，如同意授权或者拒绝放款等。

如图 5.7 是 ZV CHAIN 智能风控系统的框架，其中，预言机技术是一个提供外部信息的平台，提供了智能合约在合约条款得到满足时运行的必要条件。

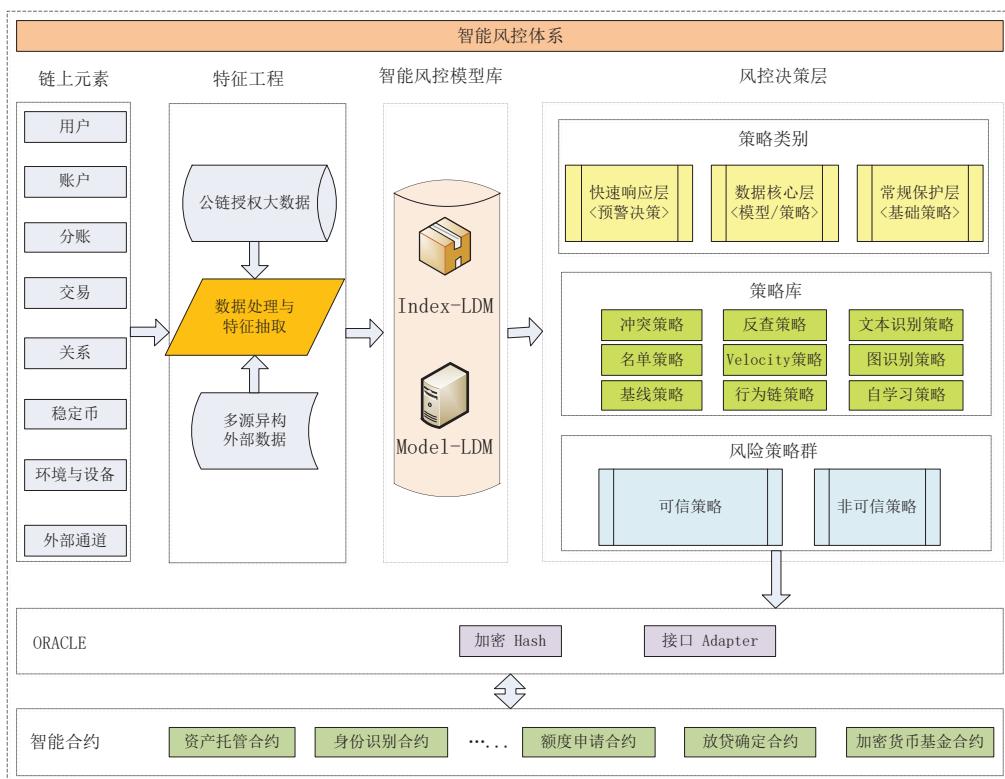


图 5.7: ZV CHAIN 智能风控框架

这些预言机是智能合约与外部进行数据交互的唯一途径。其目的是在区块链和互联网之间建立一道可信的数据网关，其目标是打破智能合约获取数据的束缚，在保证可信的情况下，

使其具有访问互联网数据的能力；为保证所获数据的真实可信，预言机需要提供多种加密证明方法，构建可信环境。

六 技术路线与里程碑

1. Phase I (2018-09 至 2019-08) - 主网上线

我们使用极具前瞻性的 chiron 共识算法，专注于 ZV 链的性能优化和稳定性测试，和适用于金融服务的账户体系；同时紫微宝 APP 上线，为用户提供数字资产的管理服务；我们会在金融服务、跨链及隐私计算等方向与生态合作伙伴展开合作。在第一阶段最后，紫微链会完成主网上线；

2. Phase II (2019-09 至 2020-02) - 生态跨链

我们为开发者准备了 beta 版的 ZV SDK；紫微链将在第二阶段完成和 Cosmos Hub 的链接，打通 BTC 生态与 ETH 生态；紫微宝将与紫微链完全接通，利用闪电网络技术，进入 DAPP 状态；

3. Phase III (2020-03 至 2020-08) - 分布式存储

紫微链进一步升级，正式版本的 ZV SDK 及各类金融服务方向的官方中间件将上线；紫微宝也将不断迭代，一方面增加用户的安全性，另一方面为公链对接更多落地场景；随着生态的形成，全量账本和金融隐私数据的增量将促使我们不断完善分布式存储的解决方案；

4. Phase IV (2020-09 之后) - 隐私计算与智慧金融

我们将在这一阶段为隐私计算寻找真正的区块链解决方案；随着数据价值流转生态的逐步形成，我们将嵌入智能金融模块，将整个生态系统升级为完善的智能化自治社区。同时整个生态，也将进入一个全新的世界。

参考文献

- [1] S. Micali, M. Rabin and S. Vadhan. Verifiable Random Functions. 40th Foundations of Computer Science (FOCS), New York, Oct 1999.
- [2] Wang C, Wang Q, Ren K, et al. Privacy-preserving public auditing for data storage security in cloud computing[C]//2010 proceedings ieee infocom. Ieee, 2010: 1-9.
- [3] Sharding FAQs In URL <https://github.com/ethereum/wiki/wiki/Sharding-FAQs>.
- [4] Jeffrey Dean and Sanjay Ghemawat. MapReduce: Simplified Data Processing on Large Clusters. OSDI 2004.
- [5] Zhao J L, Fan S, Yan J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue[J]. 2016.
- [6] Kastelein, R. "IBM Fuses Blockchain, AI and Cloud Computing into One Unit."
- [7] Dhillon, Vikram, David Metcalf, and Max Hooper. "Recent Developments in Blockchain." Blockchain Enabled Applications. Apress, Berkeley, CA, 2017. 151-181.
- [8] DFINITY White Paper: Consensus System. In URL <https://dfinity.org/pdf-viewer/pdfs/viewer?file=..../library/dfinity-consensus.pdf>. 2017.
- [9] McEliece R J, Sarwate D V. On sharing secrets and Reed-Solomon codes[J]. Communications of the ACM, 1981, 24(9): 583-584.
- [10] 2018 Deloitte Millennial Survey Millennials disappointed in business,unprepared for Industry 4.0. 2018.
- [11] Buterin V. Chain interoperability[J]. 2016.
- [12] Underwood, Sarah. "Blockchain beyond bitcoin." Communications of the ACM 59.11 (2016): 15-17.
- [13] Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard Business Review 95.1 (2017): 118-127.
- [14] Batsaikhan U. Cryptoeconomics—the opportunities and challenges of blockchain[R]. 2017.

- [15] Atwood, Mark. "Blockchain Technology Explained:(2018)." (2018).
- [16] Pittenger, David J. "The utility of the Myers-Briggs type indicator." *Review of Educational Research* 63.4 (1993): 467-488.
- [17] Samaniego, Mayra, and Ralph Deters. "Blockchain as a Service for IoT." *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016 IEEE International Conference on. IEEE, 2016.
- [18] Middleton, Stuart E., Nigel R. Shadbolt, and David C. De Roure. "Ontological user profiling in recommender systems." *ACM Transactions on Information Systems (TOIS)* 22.1 (2004): 54-88.
- [19] NIST, "Sha-3 standard: Permutation-based hash and extendable-output functions," 2015.
- [20] B. David, P. Gaži, A. Kiayias, A. Russell, Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. *EUROCRYPT* 2018.
- [21] F. Vercauteren, Optimal pairings, *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 455-461, 2010.

附录 A 技术术语表

A.1 Chiron 共识术语与符号

p: 大素数，密码学参数。如 256bit 的素数。

GF(p): 基于 p 的有限素域。

节点: 我们把用户设备上运行的一个客户端进程称为节点。根据设备的算力情况，用户可以将节点的属性设置为轻节点和重节点两种。

重节点: 计算型 PC，专业设备（矿机）等。

轻节点: 普通 PC，手机，机顶盒，移动设备，嵌入式设备等。

矿工: 普通用户通过注册，可以加入参与分布式记账。设 M 为所有矿工的集合，把它们分别添加标记 $1, 2, \dots \in |M|$ 。根据职能分类为提案矿工和验证矿工。

提案矿工 (proposer): 全量账本节点，负责给出区块提案 (proposal)。

验证矿工 (verifier): 以组协作方式工作，对提案矿工所给出的区块做有效性验证，并在组内达成出块共识。

组: 在任何给定时间，一些或所有 $i \in M$ 被排列成一个或多个子集 $G_1, G_2, \dots \in |M|$ ，称为组。我们将提案矿工和验证矿工按系统预设的比例组成一个工作组。每个工作组具有相同的组规模 $n = |G_4|$ 。

槽 (slot): 区块铸块时间。Slot 轮数与区块高度对应：第 r 轮 slot 铸出块高 (height) 为 r 的区块。若第 r 轮 slot 铸块失败，则块高为 r 的区块不存在 ($r + 1$ 区块 prehash 指向 $r - 1$ 区块)。

纪元 (epoch): 一个纪元包含若干个槽 (slot)，由相应的系统参数设定。

父亲组: 当申请成为矿工的候选者数量上满足建组条件后，需要由一个工作组发起组建新组操作，该工作组称为新组的父亲组。父亲组可以为新组指定一些特殊属性，比如新组的生效纪元等等。

组存续周期: 是指工作组的生效纪元至失效纪元之间的时间。由系统参数设定。当时间到达工作组失效纪元后，工作组将被解散。

矿工健康指数: 这个指数是多因素的函数，目前我们暂时考虑以下几个因素（权重从高到低排列）：

- 参与铸块（提案或验证）个数

- 参与率 (实际参与次数/理论参与次数)
- 设备健康度 (通过设备指纹获得)
- 曾加入过的组个数 (在线时长))
- 权益证明

A.2 结算网络实体名称

以下各个实体（网络节点或技术名词）将参与到 ZV CHAIN 的结算网络：

1. 消费者 (ZV CHAIN 钱包用户或持卡用户)

得到授权的 ZV CHAIN 用户

2. 商户

通过终端 POS 机或钱包接入 ZV CHAIN 结算网络的实体，接受 ZV CHAIN 支付并提供相应商品或服务

3. 代理节点

代理消费者与商户进行交易的网络节点，在用户端、商户端双向开通单向闪电网络，并在跨境支付场景中为货币兑换提供流动性

4. 单向闪电网络

允许消费者和商户进行高频、低额转账的技术（清算）网络

5. 双向闪电网络

允许代理节点之间进行高频交易、汇兑的技术（清算）网络

6. 双重签名合约

由一方或者双方进行预付的合约，交易的转出需要双方共同签名

7. 承诺交易

在双重签名合约中，由一方对交易进行签名，并将结果签名后的交易发送至另一方，可视作完成交易清算；另一方对交易进行签名并广播至区块链网络即完成交易结算

8. ZV CHAIN 结算网络

ZV CHAIN 分布式账本，交易最终确认结果（即结算结果）将广播到该区块链中