DAGkor

白皮书

DAZZLE MAGNET

V 1.0

目录

免责申明

该文文档只用于传达信息之用途，本文档不构成任何投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。

1.DAGkor

1.1 DAGkor 简介

DAGkor 是一种新型底层公有链分布式账本系统。它采用新型的 DAG(Directed Acyclic Graph)存储和共识方案，以及基于 DAG 的智能合约方案设计。不仅可以实现在 DAGkor 网络上交易的快速落账以及数据的及时共享，而且可以在该平台上灵活地开发去中心化的应用程序(DApp)。此外，DAGkor 还实现了公有链和联盟链之间的跨链技术，打通了链之间价值交换的通道。

DAGkor 致力于打造全球交易的生态系统，目标是为全球市场提供低成本，高效率的去中心化服务。

1.2 公有链的现状和挑战

区块链与分布式账本是当今互联网金融领域备受关注的热门话题，近几年这一领域的研究和应用呈现出蓬勃发展态势。区块链与分布式账本是密码技术、分布式存储、共识协议、点对点传输、智能合约、经济博弈技术在互联网时代的融合创新，是传统信息互联网向价值互联网演变的关键技术，并有望像互联网一样革命性地重塑经济与社会生活方式。

区块链与分布式账本技术解决了传统支付方式中过于依赖第三方机构的问题，可以在较弱的信任环境下建立很强的信任效果，让那些对彼此互不信任的人在无中心机构（或多中心机构）的情况下很好地合作。区块链与分布式账本技术具有分布式共识一致性、难以篡改、不可否认等特性，可被广泛用于加密货币、金融支付与清算、数字资产管理、去中心化交易、征信和权属管理、资源共享、物联网与供应链等众多领

域，目前已引起了各国政府、各大行业、众多金融科技公司以及研究机构的高度关注。到目前为止，已经涌现出众多区块链与分布式账本系统，在不同的系统上、技术上、架构上、应用场景上，或是商业逻辑上有所创新。从技术架构层面来讲，这些系统大致可分为三类：基于区块链技术的分布式账本系统，例如：比特币、以太坊、Hyperledger Fabric，等等；基于 DAG 结构的分布式账本系统，例如： IOTA、Byteball、 Raiblocks，等等；基于公证人机制的分布式账本系统，例如： Corda、Ripple，等等。这些区块链或分布式账本系统可视为一个个相互独立、互不相连的信息与价值孤岛（或视为一个个局域网）。

从参与记账节点的开放程度来看，这些系统大致可以分为两类：公有链和联盟链。其中，公有链(Public Blockchain)具有去中心化的特性，完全向任何个人和团体开放，任何参与者均可发送交易，任何人都可以参与其共识过程，从而有可能获取到某次记账权。

公有链的特点是对任何人开放交易验证及记账资格，其典型代表是比特币和以太坊等加密货币，可通过各类智能合约，提供众筹募资、跨境支付、数字资产管理、域名系统、交易市场、身份与征信管理等业务。联盟链(Consortium Blockchain)指定多个预选的节点记账（即具有多中心化的特性），每个区块的生成由所有的预选节点共同决定，这些节点参与共识过程，其他接入点可以参与交易，但不参与记账过程，他们可以通过该联盟链提供的服务进行限定查询。联盟链的记账方一般为可确认身份的可信方，因此，可采用更为快速、高效的共识算法，如 PBFT 算法、 RAFT 算法等。联盟链的特点是对交易验证及记账节点执行授权准入机制，是当前政府、金融行业应用较为集中的方向。国际科技行业和金融行业巨头已取得联盟链平台建设的显著成果。Linux 基金会发起并由 IBM 等提供技术支持的开源区块链项目超级账本(Hyperledger)，由英特尔、ING、微软、摩根大通等共同推出的企业以太坊联盟(EEA)是目前联盟链建设的典型代表。此外，由 R3CEV 推出的 Corda 是针对金融领域的业务形态而专门设计的、基于公证人的分布式账本平台，与联盟链有异曲同工之妙。

然而，目前区块链与分布式账本技术还处于发展初期，在系统性能效率、可扩展性、安全性、隐私保护和审计监管等方面还有诸多不足，需要深入研究并提出相应的解决方案。其中尤为突出的三大关键问题是：性能效率低（系统吞吐量较低、共识一致性收敛较慢）、安全问题（自私挖矿、51%算力攻击、未来的量子计算攻击等）以

及跨链互通问题（如何将相互独立的“信息与价值孤岛”打通，构建价值互联网）。

1.3 DAGkor 的特性

1.3.1 高可扩展性和性能效率

基于区块的单链存储模型（例如比特币，以太坊）由于设计上块的高度只能线性增长（软分叉的块最终也只有一个块被确认），使得交易的打包受制于区块的大小和区块产生的速度。而基于 DAG 存储模型的公有链技术，在安全可靠的前提下，可以并行的产生区块，实现交易的高并发。与此同时，DAGkor 采用新型共识算法在高并发的基础上实现交易的快速确认（算法详细请参考技术概述模块）。

1.3.2 面向未来的安全机制

DAGkor 里不仅支持传统的 ECDSA 签名算法，而且还提供了抗量子签名方法，可以根据需求灵活切换。即使传统的签名算法被量子计算机攻破，用户仍可以通过抗量子算法生成新的公私钥地址来实现财产的安全转移。

1.3.3 打通公有链和联盟链的价值通道

到目前为止，已经涌现出各种各样的区块链或分布式账本系统，这些系统分别对应于不同的信息与价值生态圈，它们相互独立、互不相连，从而形成一个个信息与价值孤岛。其中，联盟链系统主要对接现有应用场景或商业模式中的需求或痛点问题，公有链系统主要承载去中心化的新型业务创新。本系统致力于打通公有链与联盟链的价值通道，构建价值互联(Internet of Value)，实现从现有商业模式到未来创新业务的价值流通。为此，我们将基于跨链机制的研究积累，设计新型、安全、高效的跨链协议，实现公有链与联盟链的无缝连接。

2.关键技术

2.1 基于 DAG 的新型去中心化共识模型

区块链技术在共识机制、可扩展性与性能效率、系统的安全性分析评估、安全与隐私保护等方面已经有较多的研究成果，且该技术在主流加密货币或公有链的应用实现已经经受了时间与市场的考验。然而，到目前为止，主流区块链系统在共识协议方面基本采用 PoW 机制（如比特币、以太坊、莱特币、门罗币等）、PoS/DPoS 机制（如以太坊:以太坊将由 PoW 机制逐步切换到 PoS 机制、EOS 等）或 PoW+PoS 混合共识机制（如 Decred、DASH）。这些区块链系统在性能效率方面有较大的局限性（包括系统吞吐量较低、共识收敛速度较慢等）。

虽然 PoW 共识机制存在一些优点，例如:稳定性好(经过充分的实践证明)、具有较强的容错性、拥有不错的激励机制、支持用户动态加入与退出等。然而，PoW 存在诸如资源浪费、矿力集中、系统吞吐量过低等诸多为人诟病的问题，因此需要对 PoW 机制进行改进扩展。

已有的改进方法包括：(1)缩短区块的产生间隔；(2)增加区块大小；(3)采用双层链结构；(4)引入闪电网络。

方法(1)牺牲了一定的安全性，以太坊的实践（其区块产生间隔为 15 秒）证明了缩短区块产生时间间隔会影响到系统的安全性和稳定性，为此以太坊采用了颇受争议的 GHOST 协议来抑制因缩短区块产生时间间隔所带来的不良影响。

方法(2)会增加系统的通信开销。

Bitcoin-NG 采用了方法(3)，其主要思想是:矿工解决哈希难题并由此创建的区块称为 keyBlock，创建 keyBlock 的矿工在下一个 keyBlock 出现之前每隔一小段时间可以发布一个 microBlock。系统的安全性和健壮性建立在 keyBlock 的 PoW 机制上，而系统的交易吞吐量则通过 microBlock 的频繁发布得以显著提高。然而，在 Bitcoin-NG 中存在两个安全隐患：一是不能有效阻止自私挖矿，二是当某个恶意矿工创建 keyBlock 之后，他可以在短时间内发布大量的 microBlock，从而大大加重了系统的通信负荷。

方法(4)是一种链下交易机制，用于支持小额高频交易。此外，新型共识机制不断涌现，其中主流的代表为 PoS、DPoS，这两种共识机制与算力无关，从而有效避免了

资源浪费问题，然而这些共识机制的效率、稳定性、安全性需进一步论证，尤为重要的是，它们的共识收敛速度与安全性的平衡需进一步探究。而对于目前已有的 PoW+PoS 混合共识机制，其安全性很大程度上依赖于 PoW 机制，从而基本继承了 PoW 机制存在的问题。

与区块链技术相比，基于 DAG 结构的分布式账本技术存在如下特性:无区块大小限制，易扩容，支持的消息格式较为灵活等使得该技术有非常广泛的应用场景，且 DAG 网络结构的特性使得支持高并发量交易成为可能。因此，基于 DAG 结构的新型共识模型（要求:共识安全稳定 -- 理论模型可证明安全，收敛速度快，且具有良好的去中心化特性）就成为本系统的关键技术之一。

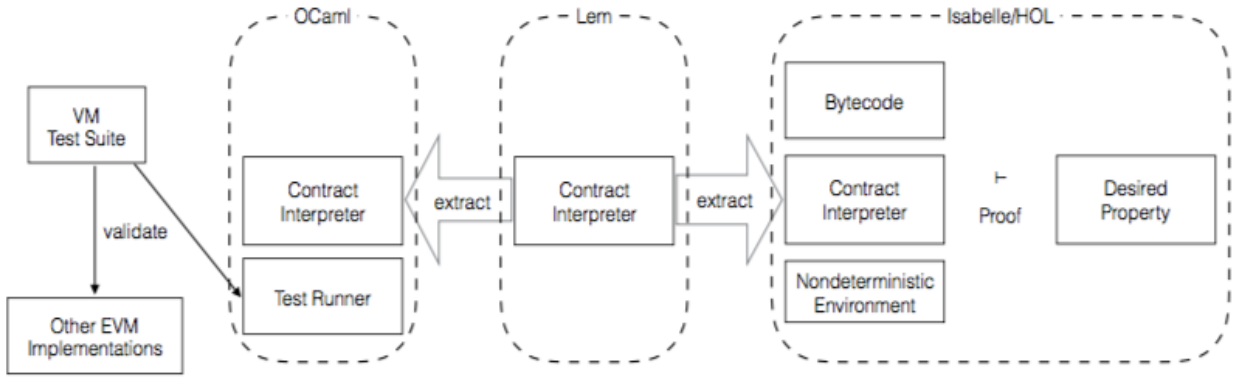
目前主流的、基于 DAG 结构的分布式账本系统包括 IOTA、Byteball 以及 Raiblocks。但是，Byteball 系统过于依赖少量的 Witness 节点；此外，在 IOTA 系统中，其安全性较大程度依赖于交易频率，且其共识确认机制依赖于单一的、中心化的 Coordinator 节点，等等。为此，在本系统中，我们将在深入研究 IOTA、Byteball 以及 Raiblocks 等基于 DAG 结构的主流分布式账本系统的共识模型基础上进行融合创新，设计并实现安全稳定、支持高并发、快速收敛、且具有良好去中心化特性的新型双层链共识模型（共识模型详细参考架构概述模块）。

2.2 新型智能合约

在本系统中我们希望通过智能合约机制来支持各种创新业务，实现基于 DAG 结构的下一代公有链基础架构与智能合约机制的有机融合。智能合约(Smart Contract)是区块链技术催生的一项新技术，本质上它是一种电脑程序，保证当合约所需的前提条件满足时，合约就会自动执行。区块链上智能合约技术的去中心化特性，解决了传统合约中存在的各种问题，使得人们在进行交易时无需寻找可靠的第三方担保，无需信任对方，无需办理繁杂的手续，也无需担心交易失败带来财产上的损失，交易可以公开透明，避免了冲突的可能。传统合约是由法律强制保证合约上的规定得到实现或执行，智能合约则通过密码学技术、共识一致性技术等来保证其被安全可靠地执行。目前主流的智能合约机制包括以太坊、Qtum 以及 Hyperledger 系统中实现的智能合约机制。以太坊 (Ethereum)为例，简要介绍一下智能合约的实现原理。

从技术原理方面来看，以太坊采用以太坊虚拟机(Ethereum Virtual Machine, EVM)

来运行智能合约。以太坊虚拟机是和外界几乎完全隔离的沙盒，没有任何访问文件或者网络的权限，能读取调用时传递给它的参数，以及在严格的条件限制下调用其他智能合约。这种严格的沙盒隔离最大限度地保证了执行智能合约节点的安全。下图为 EVM 的智能合约语言解释器的实现原理图。



EVM 被设计为基于栈的机器，类似于 Java 虚拟机(JVM)。EVM 最大存储 1024 字，每个字为 256 比特。单个指令对栈的访问限制在栈顶的 16 个字。一个指令最多只能拷贝栈顶的 16 个字，或者将最顶端的字和栈顶的 16 个字之一交换。一个指令可以将栈顶若干个元素弹出 (pop)栈并存在内存(memory)中，或者将若干元素压(push)入栈中。之前已经提及，CALL 指令可以用来调用其他智能合约。一个调用被称为一个 Message Call，调用参数为一个 message，包括发送方(sender)，接收方，数据，以太币和最大 GAS 限制等。为了让被调用的合约能够顺利执行完毕，调用者需要将剩余的 GAS 中的一部分传递给被调用合约。被调用的合约会在一块全新的内存空间上执行。调用结束后，被调用合约的返回值会存储在调用者的栈顶。EVM 对合约调用的深度限制为 1024 层，因此复杂的操作一般选择用循环而减少对合约的深层调用。

EVM 同时支持弱调用(Delegate Call)指令。这类调用不改变执行环境，即内存和栈仍然使用调用者自己的，只是将被调用合约的代码拷贝过来执行而已。这类调用实现了代码的可重用性，使得在以太坊中建立代码库成为可能。智能合约可以记录日志，一条日志以一个事件(Event)的形式记录在区块链上。能够访问区块数据的用户（比如全节点）可以直接从区块链中读到日志。但智能合约本身没有读日志的权限，只能对日志进行记录。日志用布隆过滤器(bloom filter)算法存储在区块链上，可以用高效并且密码学安全的方式在链上对日志进行搜索，因此即使是没有下载区块数据的轻客户

端也能够访问日志。

在本系统中实现智能合约机制的技术创新是如何将 DAG 网络结构的特性与智能合约机制有机地结合在一起，使得系统能够安全、稳定、高效地支持各种应用。为此，我们将在充分研究主流智能合约机制的技术原理的基础上，选取能够与我们设计的、基于 DAG 结构的新型共识模型很好融合的 go-lisp 智能合约技术架构，并在其上进一步细化及优化创新。同时，后期我们也将开发出基于以太坊虚拟机 EVM 的智能合约系统，使得 DAGkor 兼容性更好。

2.3 高效、灵活的抗量子特性

在分布式账本系统中，密码技术是用于保障系统安全可靠、不可篡改、不可否认等关键特性的核心底层技术，例如，现有公有链系统均采用了 Hash 算法及数字签名算法（基本上为传统的公钥签名算法）。然而，随着量子理论、量子技术的不断发展与成熟，量子计算机将有可能逐步取代现有的电子计算机，目前可用于密码破译的量子计主要有 Grover 算法和 Shor 算法，其中 Grover 算法的作用相当于把需破译的密钥长度减少一半，而 Shor 算法则适用于解决大整数分解、离散对数求逆等数学困难问题，对目前广泛使用的 RSA、EIGamal、ECC 公钥密码和 DH 密钥协商协议等传统公钥密码体制可以进行有效攻击，这就意味着在量子计算环境下，基于传统公钥密码的分布式账本系统将不再安全。例如:对于 Bitcoin, Ethereum 等，在量子计算环境下，它们所使用的数字签名方案将不再安全，攻击者可以根据公钥很容易计算出私钥，这就意味着交易的不可伪造、不可否认等特性将不复存在，个人用户的数字钱包将变成公共钱包。

量子计算机到底离我们有多遥远？2017 年 11 月 11 日，IBM 宣布:成功研制出了量子计算机原型机，量子计算机商业化正在加速！2017 年 12 月 18 日，消息传来，摩根大通将与 IBM 进行量子计算试验。这个试验的应用重点，将放在金融行业中，包括交易策略、投资组合优化、资产定价和风险分析等。摩根大通只是 IBM 量子计算机商业化的一个合作伙伴而已。随后，奔驰戴姆勒、本田、三星、化学品公司 JSR 也纷纷宣布，将与 IBM 开始量子计算机合作。可以预见，量子计算机离我们已不再遥远! 为此，抗量子计算已经成为分布式账本系统的必要特性之一。

通过深入研究我们发现，构建抗量子计算的分布式账本系统可以通过如下两种方

案。

a. 基于量子密码技术实现安全高效的密钥分配，并在此基础上实现高效的共识机制。然而，该方案存在一些关键问题，例如：需构建大规模的、安全可靠的量子通信网络，需有效抵抗各种量子攻击技术，特别地，对于窃听攻击，虽然通信双方能够感知窃听者的存在，从而舍弃当前密钥信息，但是，若窃听者一直存在，通信双方就无法获得安全的密钥，等等。

b. 基于后量子密码技术来实现数字签名、隐私保护等。量子计算机的超强并发计算能力，使得基于某些数学难题的传统公钥密码安全受到挑战，然而，量子计算机并不能解决电子计算机难于求解的所有数学问题。基于量子计算机不擅长计算的那些数学问题构造密码，就可以抵抗量子计算的攻击。我们称能够抵抗量子计算机攻击的密码为抗量子计算密码，或后量子密码。目前主流的四大类后量子密码包括 Hash-based cryptography 、 Multivariate-quadratic-equations cryptography 、 Code-based cryptography 以及 Lattice-based cryptography。

基于量子密码技术的分布式账本系统很大程度依赖于量子通信技术的发展，并需要解决量子通信网络中高效共识问题。而更为可行的、抗量子计算的分布式账本解决方案是使用后量子密码技术，为此，在本系统中我们将采用后量子密码技术。我们致力于研究、分析、比较各类后量子签名方案的安全性、实现代价、性能效率等，积极关注美国 NIST 发起的后量子密码标准化工作并参与到相关候选算法的分析评估中，在此基础上，对已有算法进行优化创新并将其用于本系统中。

通过对如下抗量子签名方案（包括 Hash-based signature schemes:MSS, LMS, XMSS, SPHINCS, NSW; Lattice-based signature schemes:GVP, LYU, GLP, BLISS, DILITHIUM, NTRU; Code-based signature schemes: CFS, QUARTZ; Multivariate-polynomial-based signature schemes:RAINBOW, 等等）进行了深入地安全性及性能效率分析评估，发现与传统的签名方案(如现有密码货币系统中使用的 ECDSA 算法)相比，抗量子签名方案的公钥、签名长度大幅增长。若在已有加密货币或区块链系统中简单引入抗量子签名方案，将会造成已有系统的 TPS 大幅降低，以比特币系统为例，目前其 TPS 至多为 7 笔/秒，若引入抗量子签名方案（如 DILITHIUM），其 TPS 将降至 0.389 笔/秒。

我们对抗量子签名方案进行了技术选型。

a. 从安全性角度出发，我们选取了基于 Hash 函数的抗量子签名方案(LMS)，这个方案的安全假设很弱，其安全性仅依赖于所采用的 Hash 函数的安全性，换句话说，若其采用的 Hash 函数是安全的，那么该方案就是安全的。在我们的方案中，我们将采用 NIST 国际标准 SHA-3（即 Keccak，2012 年 10 月， Keccak 被 NIST 遴选为 Hash 函数国际标准）函数，根据到目前为止国际密码学界对 Keccak 进行的非常充分的、安全性分析评估结果，可以预见 Keccak 在未来很长一段时间内有非常强的安全界。而相比传统的电子计算机，量子计算机对 Hash 函数的攻击效果（碰撞攻击、原像攻击及第二原像攻击）并没有太大的优势，这就意味着采用了基于 Keccak 函数的 LMS 方案的分布式账本系统在未来很长一段时间内将有非常强的安全界，且基于 Keccak 函数的 LMS 方案实现具有抗旁路攻击的特性。

b. 从性能效率（包括签名/验签效率，公钥/签名长度）角度出发，尤其是公钥、签名长度会极大地影响密码货币或区块链系统的吞吐量(TPS)，为此，我们选取了目前性能效率综合来说最优的抗量子签名方案(Bliss)，该方案的安全性是基于 LWE 上的困难数学问题，目前来看量子计算机对求解 Bliss 算法所依赖的、LWE 上的困难数学问题没有非常有效的算法。由于 Bliss 算法的签名、验签效率高，公钥、签名长度之和是目前所有已知的抗量子签名算法中最优的，支持 Bliss 算法对于本系统的吞吐量来说是非常有优势的。

c. 需要说明的是：LMS、Bliss 算法均为经过国际密码学界充分分析、评估、论证过的、同时在安全性或性能效率方面非常突出的抗量子签名方案（LMS 与 Bliss 算法的安全假设不同，理论上均可证明安全）。

基于上述技术选型，在本系统中我们将支持基于 Keccak 函数的 LMS 方案（理论安全性极强，其方案实现抗旁路攻击），以及基于 LWE 的 Bliss 算法（理论安全性依赖于 LWE 上的困难数学问题，其性能效率是已有抗量子签名方案中最优的）。但是，对于这两种抗量子签名算法，我们仍然需要解决如下关键问题：

1)公钥、签名长度远大于传统数字签名算法 ECDSA 的公钥、签名长度，在密码货币或区块链系统中实现这些签名算法将带来交易大小显著增加，从而引发系统吞吐量明显下降。

2)Bliss 算法中的离散高斯采样(DGS)模块在实现中存在旁路攻击的风险。

针对问题 1)我们创新性地提出了一种新型隔离见证方案，该方案能很好地解决抗

量子签名算法中签名较长带来的吞吐量明显下降的问题。

针对问题 2) 目前存在一些针对 Bliss 算法实现的旁路攻击，需要指出的是，这些旁路攻击方法在实际实现时都有较大的困难性。例如：在针对乘法运算的攻击中，作者自己也指出这种利用马尔科夫模型的攻击方法在获得的汉明重量噪声较高的情况下不能成功，而实际获得的汉明重量总是有噪声的；在使用功耗、电磁信息攻击采样函数时，首先采集质量可能会影响对于分支语句的判断，其次，在能获得质量较好的曲线的情况下，准确的定位泄漏点在整体曲线上的位置也是一件很有工程难度的工作；同理，在使用 branch trace 分析运行在操作系统上的应用时，虽然每个分支语句都可以被准确记录（无噪声），但是在大量的 branch 记录中定位攻击位置依然很有难度；至于 Cache 攻击，如何在时序上保持 flush 和 reload 交错进行，在不修改源码的条件下是很难实现的。

尽管这些旁路攻击方法在实现上有较大的困难性，但是 Bliss 算法的旁路泄露问题依然需要引起我们足够的重视。为此，通过深入分析 Bliss 算法可能存在的旁路信息泄露点，我们设计了有效的防护方案，该防护方案依然能够保持 Bliss 算法的高效性（尤为重要的是:防护方案丝毫不影响签名算法的公钥、签名长度）。上述创新研究成果为本系统中安全、高效地实现抗量子特性提供了有力保障。

总体而言，本系统中抗量子方案的亮点主要体现在以下几个方面:

1)兼容性：在目前抗量子计算机还没有真正出现之前，密码货币或区块链系统仍然可以使用 ECDSA 签名方案。我们的方案兼容已有系统的 ECDSA 签名方案，从而能够很好地与目前各大主流区块链系统平台进行对接，并为后续支持跨链互通特性提供基础。

2)灵活性：我们的方案支持两种经过国际密码学界充分分析、评估、论证过的、同时在安全性或性能效率方面非常突出的抗量子签名方案，这为本系统提供了更大的灵活性与更好的安全性。

3)安全性：我们的方案支持两种抗量子签名算法：LMS 以及 Bliss。对于 LMS，其安全假设很弱(即安全性很强，安全性仅依赖于我们所采用的 SHA- 3 函数的安全性，在该安全假设下 LMS 是可证明安全的)，即若 SHA-3 函数是安全的，那么该方案就是安全的。

对于 Bliss 算法，其安全性是基于 LWE 上的困难数学问题（在该安全假设下 Bliss

是可证明安全的）。目前来看量子计算机对求解 Bliss 算法所依赖的、LWE 上的困难数学问题没有非常有效的算法。进一步地，我们通过深入分析 Bliss 算法可能存在的旁路信息泄露点，创新性地提出了有效的防护方案，使得 Bliss 算法实现在保持高效性的前提下能有效抵抗旁路攻击。

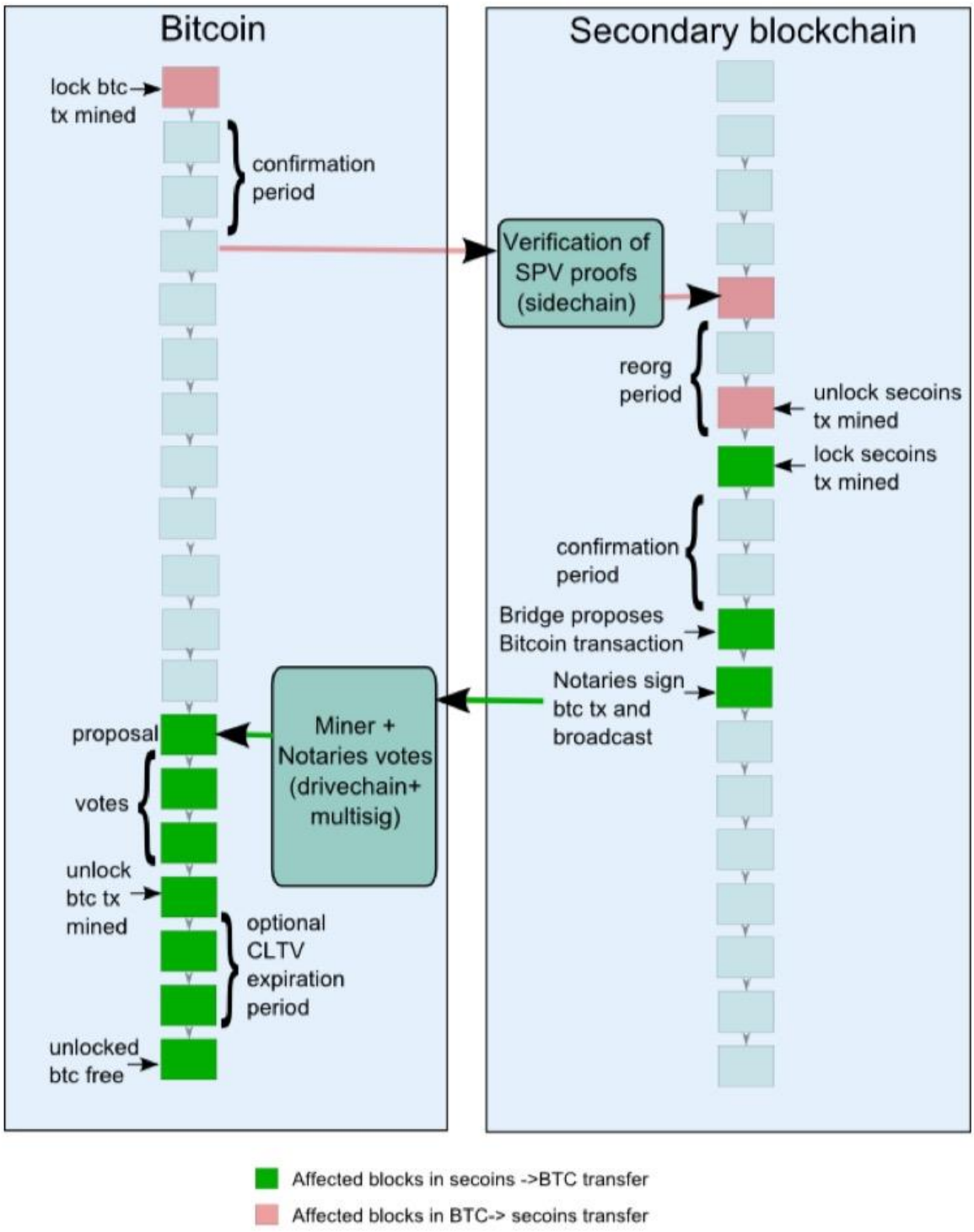
4)高效性：在现有的抗量子签名方案中，我们的方案支持的两种抗量子签名算法在签名/验签效率、公钥/签名长度等特性方面具有非常突出的综合优势。进一步地，考虑到抗量子签名方案的公钥、签名长度远大于传统数字签名算法 ECDSA 的公钥、签名长度，这将引起交易大小显著增加，从而造成每个区块包含的交易数量显著减少，并最终引发系统吞吐量明显下降。为此，我们创新性地提出了一种新型隔离见证机制，该机制能很好地解决抗量子签名算法中签名较长带来的吞吐量明显下降的问题。

5)适用性：我们的抗量子签名方案可以广泛适用于现有的区块链或分布式账本系统。进一步地，未来本系统还将支持抗量子计算的隐私保护机制（例如:抗量子计算的零知识证明方案或抗量子计算的环签名方案）。

2.4 高效、安全的跨链协议

由于不同区块链之间架构的差异，使得链与链之间进行交互变得十分困难。但区块链之间不会彼此之间成为孤岛，链与链之间价值的转移是必不可少的。本章介绍几种现有的跨链解决方案。

2.4.1 双向锚定



双向锚定(two-way peg)允许比特币从比特币区块链转移到第二层区块链，反之亦然。“转移”其实是一个错觉：比特币是不能被转移的。但我们可以暂时锁定比特币，同时释放在另一条区块链上释放等价的代币；反之，当代币在另一条区块链上被锁定时，则解锁等价值的比特币。这就是双向锚定的本质。

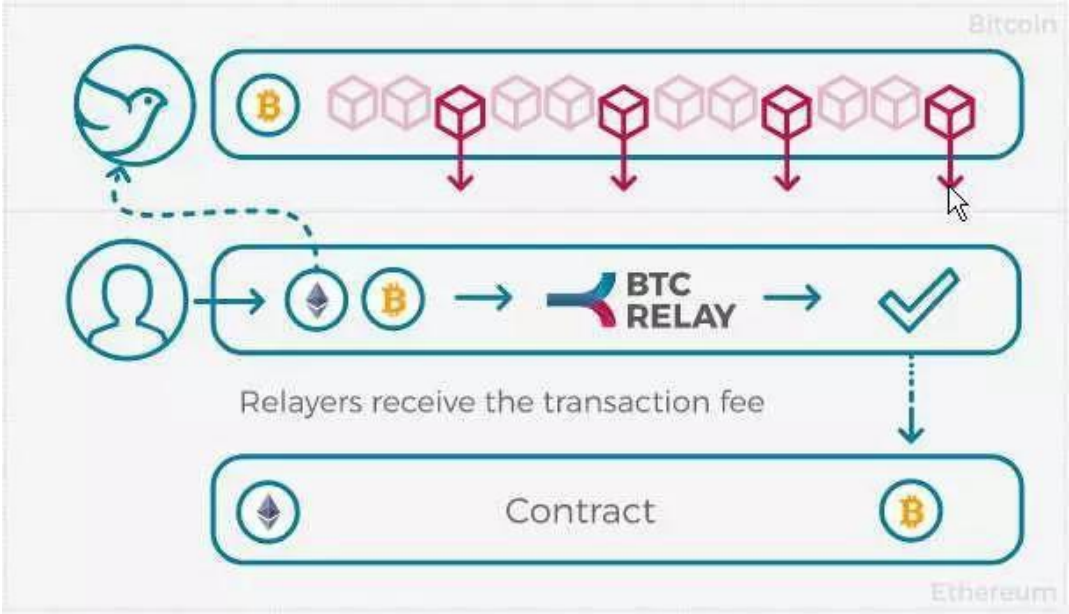
2.4.2 链中继

链中继技术，简称 X-Relay，是在以太坊智能合约中实施和维护区块链轻客户端的一种方式。合约主要存储所有的区块头数据，这些区块头数据的大小比整条区块链的完整数据信息小得多，故名轻客户端。只要拥有区块头数据，节点便能够验证交易是否已被打包，且可以在区块头存储数据支持的前提下，验证区块链的状态。因此，X-Relay 允许以太坊上的任意合约来验证交易，甚至可以通过使用轻客户端来验证区块链上的账户状态。

例如：BTC Relay。 BTC Relay 它是基于以太坊的智能合约，合约内部存储着比特币的区块头，把以太坊网络与比特币网络以一种安全去中心化的方式连接起来。通过使用以太坊的智能合约功能，BTC Relay 允许用户在以太坊区块链上验证比特币交易。BTC Relay 使用区块头创建一种小型版本的比特币区块链，以太坊 DApp 开发者可以通过智能合约调动 BTC Relay 的 API，来验证比特币网络活动。

一种被名为 Relayer 的角色会不断地为 BTC Relay 提供新的比特币区块头。当交易在以太坊区块链进行验证或者区块头被检索的时候，Relayer 会获得一笔手续费(ETH)作为奖励。

BTC Relay 进行了跨区块链通信的有意义的尝试，打开了不同区块链交流的通道。



2.4.3 原子交易

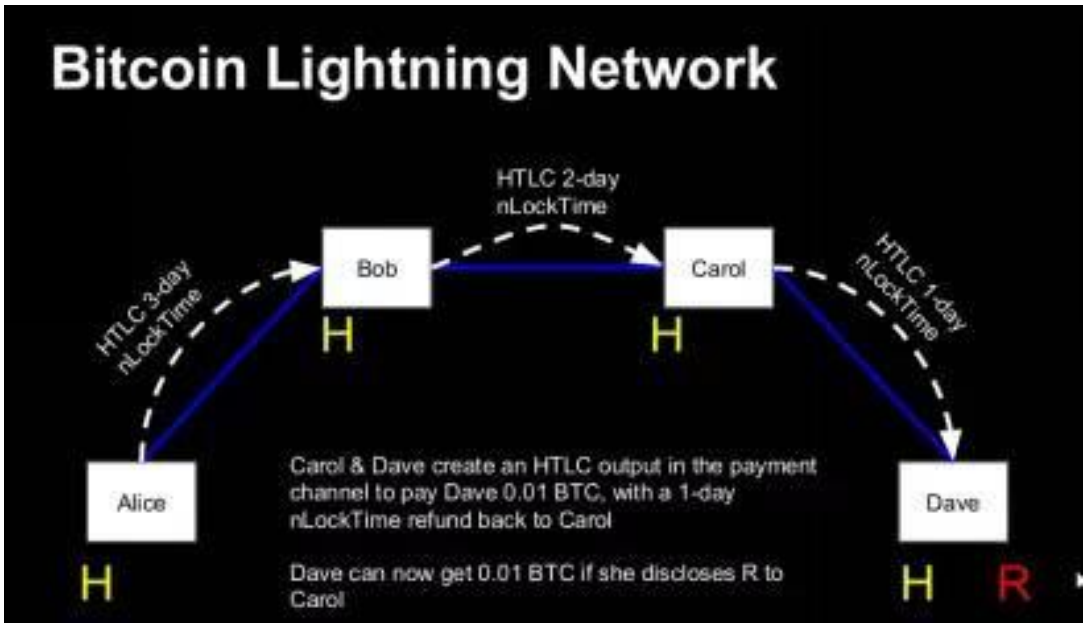
原子交换(Atomic Swap)是在无可信第三方的参与下，双方实现原子性的跨链公平交易的协议。原子交换的概念早在 2013 年 Bitcointalk 上就有人提出。它的实现使用了 HTLC 和博弈论思想。比特币上很早就实现了 HTLC，而在支持智能合约的区块链上就更容易实现了。

HTLC 的全称是 Hashed Timelock Contracts，原子交换基本是依赖它构建的。可以把 HTLC 理解成一种条件输出，只要满足这个条件你就能花这笔钱。它有两种类型：

a. Hashlock：当给出某个哈希值的原像时，就可以解锁该输出。

b. Timelock：在到达某个时间点之后，才可以解锁该输出。

除了原子交换，闪电网络也用到了 HTLC。



原子交换只需要交易双方参与，无需第三方介入这是一种十分去中心化的跨链交易方式。且原子交易十分安全且公平，结果要么交易成功，要么交易失败，双方都不会从中损失或受益。然而在效率上，原子交易还是存在不少缺陷的。

a. 不管交换成功或失败，总会有 4 个交易被上链，手续费较高。而且交易上链的时间顺序是串行的，因此无法做到即时交易。如果网络一拥堵，交易确认时间和手续费都会增加，则原子交易会存在无法在指定时间内上链的不确定性，会大大增加风险。

b. 如果考虑到外部交易所，原子交易中会存在对手风险。在交易锁定的事件里，

一方可以根据交易所的汇率是否对自己有利，来决定要不要选择去交易所交易。若放弃原子交换，风险全部转嫁给了另一方。这个风险无法通过缩短锁定事件参数 24h 和 48h 来解决，无法根本消除，只能将参数调节至与网络环境相适应，来减少该风险。

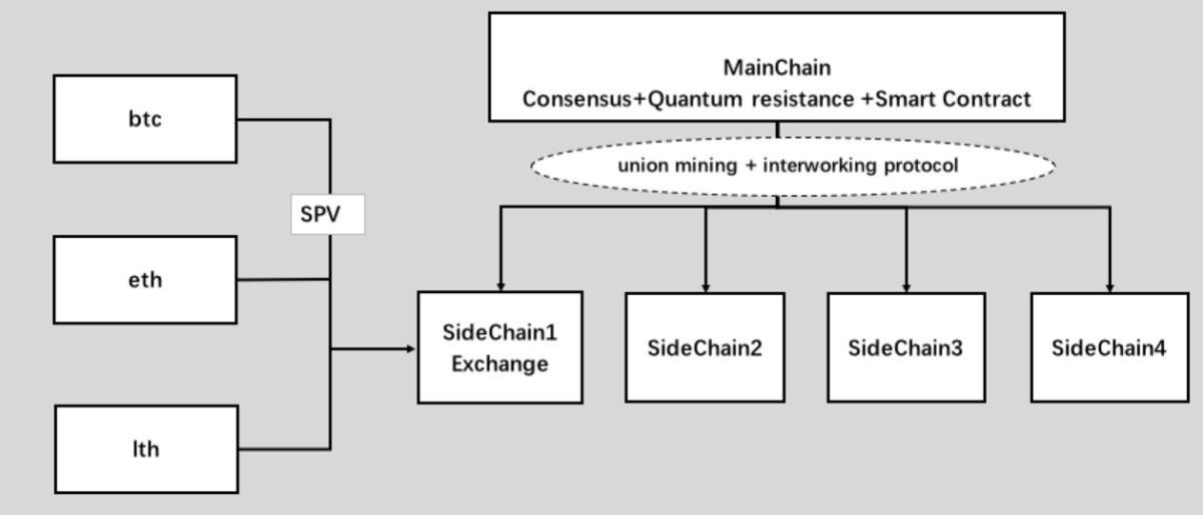
综合以上分析，我们在设计全新的侧链架构和协议时，遵从以下设计原则：

a.侧链设计的目的是为了分散主链的业务功能，使主链协议清晰简单。

b. 侧链与主链共享币源，即侧链不铸币，仅从主链中转移币。

c. 侧链的安全性与稳定性可以借力于主链，但侧链协议出现漏洞时，不会影响主链的安全性与稳定性。

结合以上设计原则，我们设计的侧链架构如下图所示。



主链上只包含混合共识、抗量子签名以及智能合约等核心功能。针对每一种新的扩展业务或功能，需要通过一条新的侧链来实现。然后利用基于联合挖矿的主侧链互通协议，将主链与侧链进行联通，从而实现主链的功能扩展。这种架构的优势在于结构简单、层次清晰。并且通过将扩展功能与主链分割开来，使得主链较为简洁精炼，可靠性增加。同时，为主链增加新功能只需要改变或另起一条新的侧链，可扩展性强。

2.5 高效的系统调度模块设计

考虑到系统的可插拔性和可扩展性，本系统秉承着软件设计的模块内高内聚，模块间松耦合的设计理念，遵守开放-封闭原则（模块可扩展开放，对修改封闭），这样

的设计不管从开发的分工还是后期的维护都将非常有效率。例如，如果后期从 PoW 共识改为 PoS 共识，只需要开发一个 PoS 共识模块来替换当前的 PoW 模块即可。

为此，为了解决模块之间的调度和依赖产生的耦合问题，参考操作系统的系统总线调度设计，开发了 EventBus 组件来负责各个模块之间的调度和任务分配。使得各个模块之间可以实现高并发调用。与此同时，我们还对系统里的线程进行统一管理，一方面可以减少进程的开始和结束时分配资源的时间；另一方面可以避免线程数太多导致系统出现崩溃的状况。

EventBus 和各个模块的架构具体设计请参考架构 3.架构设计篇。

2.6 高兼容性的抗量子分层确定性(HD)钱包

钱包是用于发送和接受代币的客户端，就像我们使用邮箱来管理自己的邮件，我们需要一个客户端来管理自己的代币。钱包的本质是保管私钥的工具，私钥就是一串很长的数字和字母组合的字符串，这个字符串让你有权力把自己的加密货币送给别人。换句话说，无论谁知道你的私钥，都可以控制你的加密货币。私钥也用于生成你的代币地址，这就像邮箱地址，只有知道地址才能给别人发送代币。然而，尽管代币地址是通过私钥生成的，但是没有办法通过检查加密货币地址来确定私钥是什么。总而言之，钱包的核心功能是私钥的创建、存储和使用。

1) 钱包的分类

私钥不同的生成方法，也对应着不同的钱包结构，通常可以分为非确定性钱包和确定性钱包。比特币最早的客户端(Satoshi client)就是非确定性钱包，钱包是一堆随机生成的私钥的集合。客户端会预先生成 100 个随机私钥，并且每个私钥只使用一次。每个交易使用一个地址的概念是中本聪提出的。如果交易比较频繁，私钥可能会用光，然后再产生一批私钥，所以每次完成 100 个交易后，你必须备份新的 wallet.dat 文件，否则可能会丢失资产。这种钱包难以管理和备份。如果你生成很多私钥，你必须保存它们所有的副本。这就意味着这个钱包必须被经常性地备份。而且每个私钥都必须备份，否则一旦钱包不可访问时，无法找回钱包。

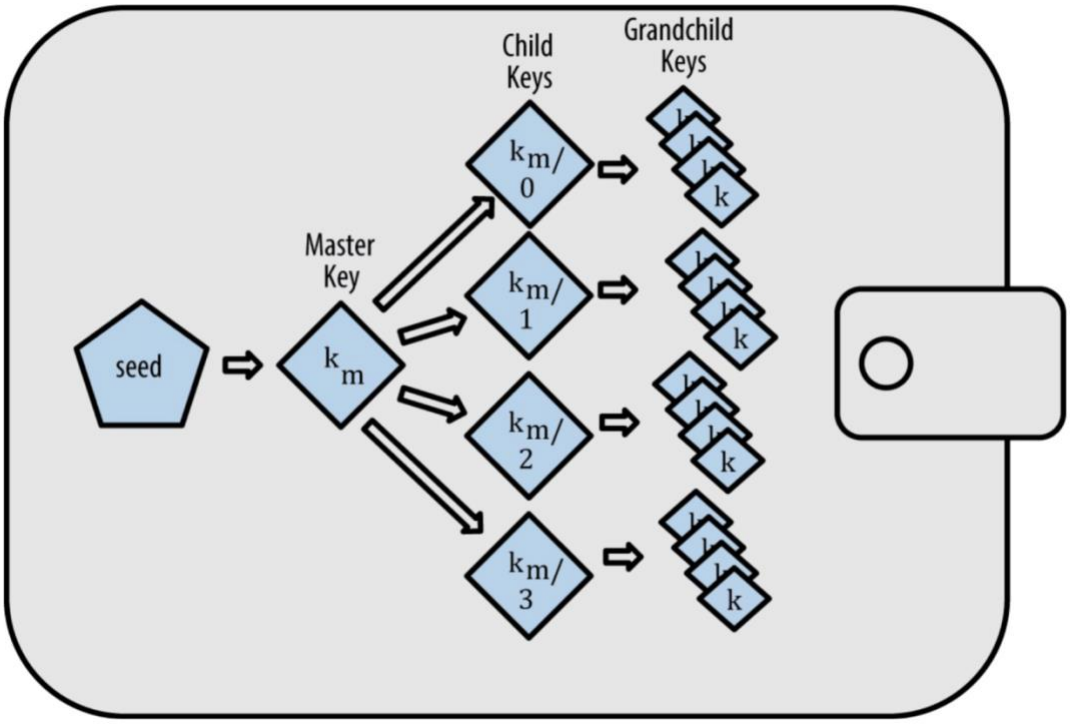
确定性钱包则不需要每次转账都要备份。确定性钱包的私钥是对种子进行单向哈希运算生成的，种子是一串由随机数生成器生成的随机数。在确定性钱包中，只要有这个种子，就可以找回所有私钥，只需备份种子就相当于备份所有钱包，所以这个种

子也相当重要，一定要备份到安全的地方。

2) HD 钱包（分层确定性钱包）

HD 是 Hierarchical Deterministic（分层确定性）的缩写。包含以树状结构衍生的密钥，使得父密钥可以衍生一系列子密钥，每个子密钥又可以衍生出一系列孙密钥，以此类推，无限衍生。如下图所示。

相比较随机（不确定性）密钥，HD 钱包有两个主要的优势。第一，树状结构可以表达组织的含义。可以有一个密钥负责接收而另一个分支的子密钥负责支付花费。第二，HD 钱包可以允许使用者建立一个公钥的序列而不需要访问相对应的私钥。这可以允许 HD 钱包在不安全的服务器中使用或者在每笔交易中发行不同的公钥。公钥不需要被预先加载或者提前衍生，而在服务器中不需要可用来支付的私钥。



3) 抗量子 HD 钱包的优缺点

抗量子 HD 钱包不仅集成了一般 HD 钱包的所有优点，具有一般 HD 钱包的所有功能。而且抗量子钱包还追加了具有抗量子特性的签名算法（bliss 等），使得用户可以根据资产的重要程度选择是否使用抗量子签名算法来保护自己的资产。

抗量子钱包在增加安全性的同时，对交易的签名的数据量也会增大，会带来交易手续费的增加。建议在大额资产保护的时候使用。

3.架构概述

3.1 双层链架构设计

作为区块链技术的典型代表，比特币自 2009 年诞生以来已经稳定运行 9 年。它采用的 PoW 的共识模型也成为区块链技术的典范，由此衍生出多种加密货币解决方案。

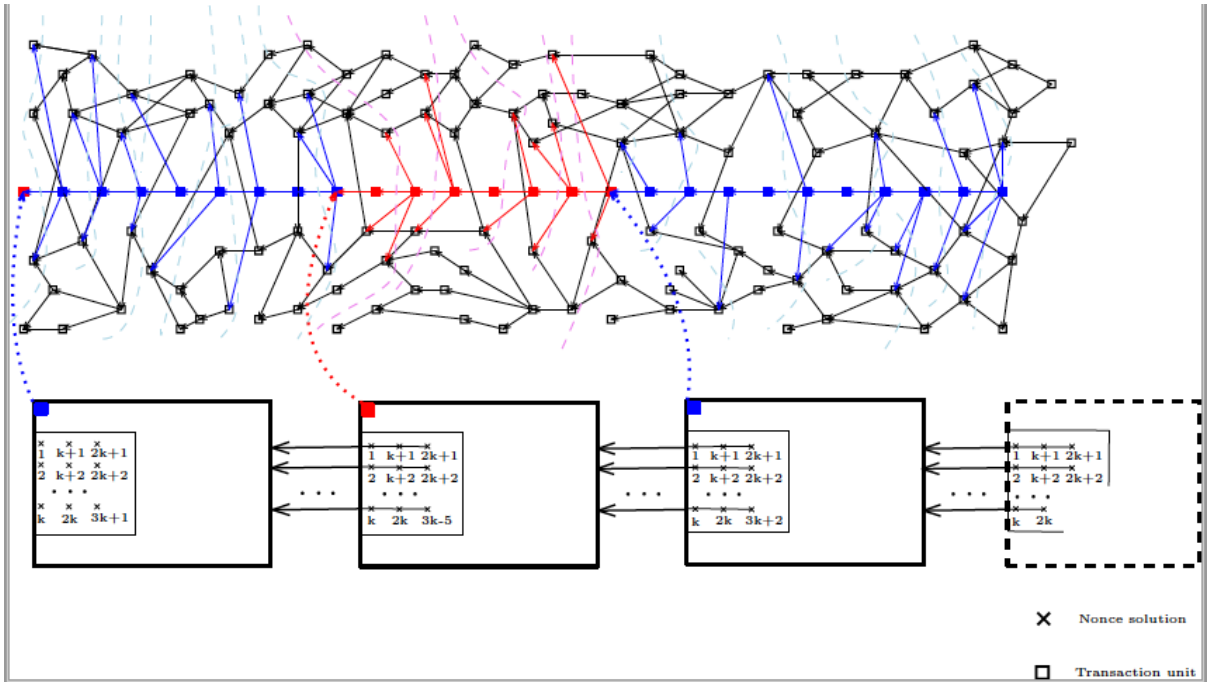
随着越来越多的用户了解并参与其中，系统固有的一些问题也逐渐显现出来。比特币中区块大小限制为 1MB，平均每 10 分钟产生一个区块，最大 TPS 为 7，网络的吞吐量非常有限。表面上看，增加区块大小或者缩短区块的产生间隔可以带来扩展性的改善，但随之而来的是区块在 P2P 网络传播延时和区块链分叉等问题，进而影响整个系统的安全运行。

本质上来说，区块链是一个两级体制。用户产生交易将其广播，矿工收集这些交易并打包上链。矿工的打包上链构成区块链的准入，因此矿工处理能力称为区块链的性能瓶颈。区块链的单链结构是其扩展性的天然限制。

为了解决扩展性问题，近年来有向无环图(Directed Acyclic Graph, DAG)成为分布式账本结构新的发展方向，Byteball 和 IOTA 是其中的典型例子。在 DAG 中，一个节点可以同时引用多个父节点，也可以同时被多个子节点引用，这种特性使得高并发和高吞吐量成为可能，天然解决了区块链的扩容问题。但与之同时，如何在 DAG 中达成共识变成了更为突出的问题。

Byteball 引入 witness 这些荣誉节点作为系统见证人，由他们发出的 unit 确定 DAG 的主链，最后通过主链给所有 DAG 节点定全序，达成交易确认。IOTA 中每个交易在网络中的累积权重随着新节点的加入和对其确认不断增加，根据累积权重是否达到某一阈值判定交易是否进入稳定状态。

但两者都存在严重的中心化问题。Byteball 虽声称 witness 是由普通用户选定，但由于其机制的设计，普通用户几乎没有太多自主选定 witness 的自由，导致它自运行以来，12 个 witnesses 从未变过。IOTA 由于无法明确给出稳态阈值，且目前由于其网络参与用户有限，无法有效抵抗恶意攻击。基金会引入 Coordinator 这一中心节点用于交易确认，背离区块链去中心化的初衷。



为了解决扩容问题，DAGkor 采用了 DAG 的账本结构。同时为了避免 DAG 中心化的问题，DAGkor 以 gPoW +PBFT 的方式产生权威 unit（即 key unit），完成对 DAG 中新来交易的即时确认。

矿工通过挖矿进入 PBFT 共识发出的 key unit，它们前后相继，构成 DAG 的主链。根据被 key unit 引用的先后顺序，对普通 unit 进行编号，以此确定在整个 DAG 中的全序。全序一旦确定，unit 的合法性（是否双花等）便唯一确定。

DAGkor 独特的双层链设计，使得该系统既具备有向无环图系统的高吞吐率和交易即时确认的特点，又兼顾了区块链的去中心化特性，具有高可靠性和高安全性。

3.2 高性能的上层 DAG

3.2.1 介绍

与区块链的链式结构不同，DAGkor 采用有向无环图(Directed Acyclic Graph, DAG)的账本结构。

区块链是一个两级体制：用户创建自己的交易并向全网广播，但这些交易不能直

接上链；矿工收集用户的交易并进行挖矿，竞争求解 hash 谜题以获得提议区块的权利。只有用户的交易被矿工打包进入区块并最终上链，且等待几个区块的间隔以保证自己的交易较大概率不会被篡改，这笔交易才算真正完成。在这种两级体制中，矿工是交易收集者，以平均时间期望产生区块，交易数量只能线性增长。区块大小和产生间隔构成区块链的性能瓶颈。

在 DAG 中，unit 是基本单元，构成 DAG 的顶点；unit 之间通过 hash 连接，构成 DAG 的边。unit 相当于区块链中用户发送的一个个交易，新来的 unit 通过 hash 引用之前的 unit，既表明对被引用的 unit 的确认，也创建了它们之间的偏序。DAG 中没有区块的概念，用户发送的合法 unit 能够直接上图，不需要矿工打包才能上链。

有向无环图的特性使得一个 unit 可以同时被多个 child units 引用，同样地，一个 child 也可以引用多个 parent units。前者使得多个用户可以独立并发地发送各自的 unit，而只需要引用自己眼中的 tip unit，有利于网络的高并发；后者使得一个 unit 能够同时引用多个 tip units，网络能够快速收敛。这两种特性是 DAG 的精髓，为高吞吐量的分布式账本设计提供了可能。

3.2.2 Unit

Unit 是 DAG 的基本单元。当用户有相应的需求时，他们创建相应的 unit（如转账或存储数据），广播进入 DAG。没有中央权威节点来判定哪些 unit 能够加入，哪些被拒绝。相反的，每一个全节点能够根据协议规则独立判断是否转发并将相应的 unit 加入 DAG 数据库，只要合法的 unit 都有资格加入 DAG。

用户在创建 unit 时，需要对其进行签名，并支付相应的手续费。手续费的一部分会被“第一个”将其引用的 child unit 所收取，这鼓励新来的 unit 引用最新的 tip unit，促进 DAG 收敛。

新 unit 通过 hash 引用，直接或间接包含了之前的 units。新的 unit 不断被加入，它们引用的 unit 将会获得越来越多的确认。如果要篡改一个 unit，需要篡改其 child unit 的 hash 引用和签名，接着是 child unit 的 child unit 等等，以此类推，雪崩效应。并且这些 units 对应的都是分布式网络中匿名的用户，很难去定位更不用说联合。这种由 hash 引用带来的链式关系给 DAG 一种天然的抗篡改特性。

3.2.3 Key unit

Key unit 是 DAG 中的一种特殊 unit，它由挖矿竞选产生的矿工经 PBFT 共识产生，在上层 DAG 中起到交易确认和定序作用。

3.2.4 共识

分布式账本技术中，共识的核心就是定序。比特币中的定序通过以下原则实现：默认最长链上的交易为合法交易，后续任何与该链上交易冲突的双花交易都被认定为非法而不会被矿工打包进入区块。

DAG 中如果有两笔交易试图花费同一笔 UTXO，分两种情况考虑：

a. 两笔交易之间已经有偏序。此时我们可以很确定地拒绝后一笔交易，因为根据 hash 引用已经能够明确为它们定序。

b. 两笔交易之间没有偏序，也就是它们之间不存在包含（直接或间接引用，下同）关系。此时，由于无法判断哪笔交易合法，两者都会进入 DAG 数据库，等进入稳态之前再判断双花并进行处理。

3.2.5 激励机制

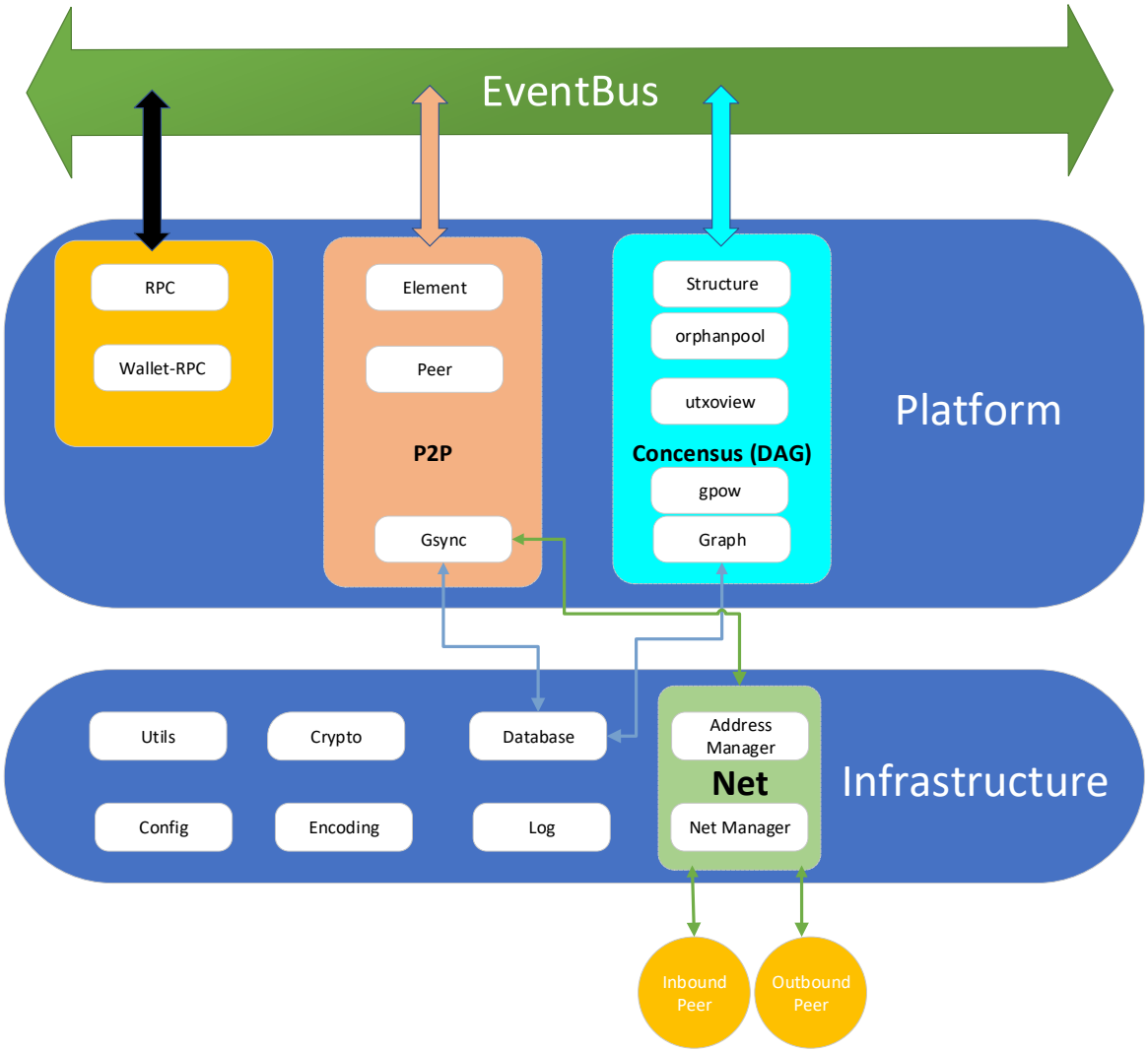
DAGkor 的激励分为两部分：一是对促进 DAG 收敛，引用 tip unit 的 child unit 的奖励；二是对维护系统安全，确认交易的矿工的奖励。

3.3 高可靠性的底层区块链

DAGkor 采用基于 PBFT 共识机制确保上层 DAG 账本的安全，参与共识的成员将记录在底层区块链中。矿工通过 POW 参与竞选共识成员，共识成员在其工作期间通过 PBFT 共识产生 key unit，并在全网广播，以此推进 DAG 的稳定，及时确认新加入的 unit。

4.工程化的模块设计

4.1 上层 DAG 架构



1) EventBus

EventBus 是系统中不同的组件之间进行相互通信的机制。组件可以向 EventBus 中发送事件而无需知晓谁会接收该事件或者有多少人会接收该事件。组件可以注册以侦听某个事件，但并不关心谁会发送该事件。松耦合使组件的修改和替换变得容易，只需要新的组件接收和发送事件的方式一致即可。事件引擎控制系统的并行性，是影响系统处理吞吐率的核心部件。

2) RPC 和 Wallet RPC

RPC 主要是为 DAGkor-cli 客户端提供远程调用服务。

Wallet RPC 主要是为 g-wallet 提供远程调用服务。

3) P2P

P2P 模块主要是提供 inbound 和 outbound 的网络连接，新建立一个网络连接，则为每个连接的节点建立一个 peer，节点之间通过 Gsync 模块实现 unit 等信息的同步。

4) Consensus（DAG）

共识模块，是 DAGkor 的重要设计核心。涉及到孤 unit 的处理、UTXO 的处理、unit 上图和图稳态的推进，等等。

5) Net

网络模块，涉及地址管理和网络连接管理。地址管理是为本节点挑选可以建立连接的节点的 IP 地址，网络连接主要是建立 inbound 和 outbound 两种连接。

6) Database

DAGkor 采用 badger DB 作为数据库基础组件。Database 提供了创建 bucket、读写数据等基础功能。

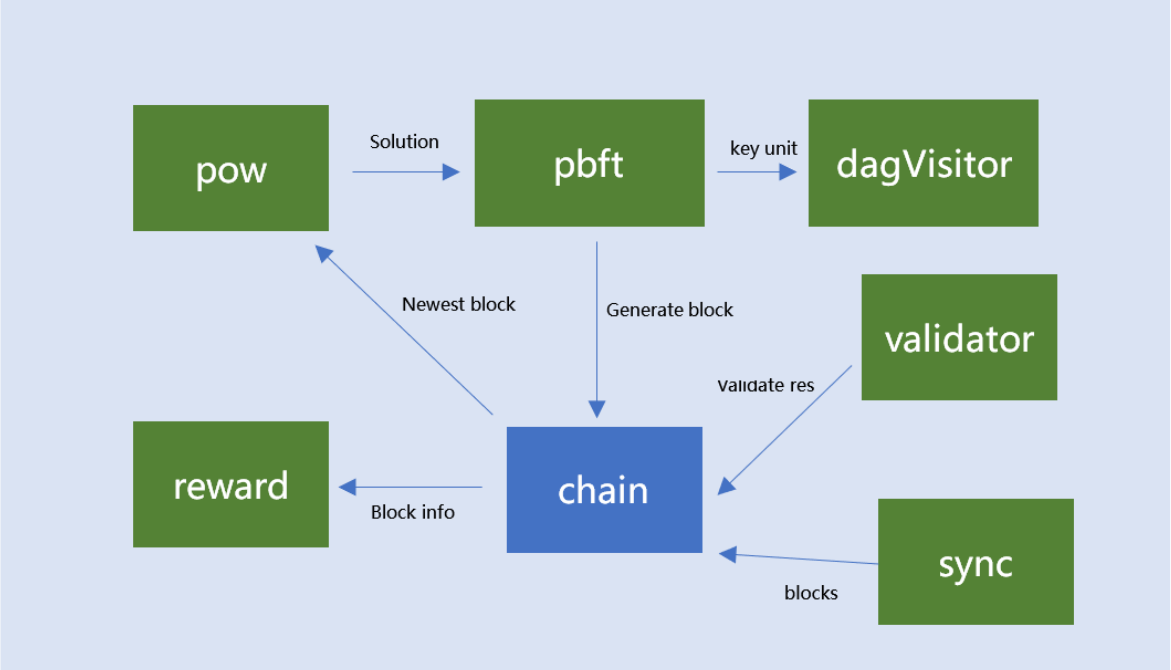
7) Crypto

Crypto 库提供了椭圆曲线和 hash 算法。该模块支持 ecdsa、ed25519、secp256k1 等椭圆曲线算法；支持 Sha3 hash 算法。

8) Log

日志模块提供了 6 中不同级别的输出，同时也实现了文件分割的功能。

4.2 底层区块链架构



1) Chain

维护区块链的数据和整个链的状态。提供连接新区块及查找链上区块数据等功能。

2) POW

提供挖矿的启动与停止功能，并提供工作量证明验证等功能。

3) PBFT

共识成员的交互协议，通过 PBFT 共识产生 key unit 以及新区块。

4) Validator

负责验证一个区块是否合法，提供对区块验证的接口。

5) Sync

负责通过底层区块链的同步协议。

6) DAGVisitor

底层区块链访问上层 DAG 的中间模块，提供上层 DAG 到底层链的连接功能。

7) Reward

负责计算和发起一个区块奖励金的 UTXO，提供发起奖励金 UTXO 的机制，并提供验证一个奖励金 UTXO 是否合法的接口。

5.公链比较

5.1 比特币

作为区块链的先驱，目前最成功的区块链项目之一，比特币是衡量一个竞争币的基石。然而比特币存在的问题也同样非常明显，落后的比特币脚本无法实现完整的智能合约，不能胜任资产发行、供应链管理等市场需求。缺乏管理核心的比特币团队很难提供软件更新，TPS 提升、智能合约等新功能的支持更是遥遥无期。

DAGkor 具有的双引擎智能合约，既支持高效的轻量级智能合约引擎 go-lisp，又支持功能强大的智能合约引擎 EVM，能够应对目前市场的需求。

5.2 以太坊

为了完善比特币的不足，以太坊建立了图灵完备的虚拟机，用户可以在以太坊中建立各式各样的智能合约来扩展应用领域的需求。然而，以太坊基于区块链的存储也存在其局限性。虽然相比比特币而言，以太坊在每秒处理交易量(TPS)有了很大的提升（每秒 15 笔左右），这还远远不能满足当今市场对于交易量的需求。

DAGkor 采用了独特的双层链设计，在保证安全性的前提下，提供了理论上无限的交易吞吐量，与此同时 DAGkor 基于 DAG 的账本结构几乎可以实现交易的即时确认。

5.3 ByteBall

为了提升区块链的交易吞吐量(TPS)，ByteBall 率先采用了基于 DAG 的账本结构，能够实现理论无上限的交易吞吐量。在高吞吐量的前提下，依然保持交易的快速确认的良好特性，得到业界的普遍肯定。然而 ByteBall 使用 Witness 作为共识算法的核心，交易的确认需要依赖 Witeness 不断地发布交易来推动，一直被人诟病其不具备去中心化特性。

DAGkor 采用独创的双层链技术，普通节点可以通过挖矿竞争来参与交易的共识，并获得一定的奖励。这样可以在保证高吞吐量、交易几乎即时确认的同时，实现真正的去中心化。

5.4 EOS

EOS 作为 2018 年最受瞩目的加密货币，具有高吞吐量、交易即时到账、完备的智能合约引擎等特点，然而高门槛的超级节点机制也使得 EOS 的去中心化受到质疑。DAGkor 采用的双层链技术使得高吞吐率与去中心化特性并存，与此同时 DAGkor 还具备抗量子特性可以抵御量子计算机的攻击。高安全性、高吞吐率、去中心化以及抗量子特性使得 DAGkor 成为一个真正的面向未来的区块链系统。

6.研发线路图

7.结论

DAGkor 是一种集中目前区块链大部分优势于一身，并在此基础上进行创新，具有其独有特性的分布式账本系统。

DAGkor 致力于通过创新性的区块链解决方案来推动去中心化应用的落地，也在为推动区块链技术的发展贡献出自己的力量。然而我们的努力不会止步于此，我们会继续进行技术创新，打造社区等方式来不断完善我们的产品，通过不断地进化来适应未来发展变化的需求。