Naby NBA

安全、隐私、无法追踪

白皮书

V 1.0

说明

此文档是 Naby（NBA）白皮书 V1 版本，主要介绍 Naby（NBA）的背景、定位、技术 特性和应用场景等内容。未来我们会持续升级此文档，使其与技术实现保持一致。

免责声明

技术在不断发展，区块链也在不断进步，Naby（NBA）开发团队未来会根据需要改进、 完善现有技术方案，并持续完善技术白皮书。

目录

摘要

区块链技术被认为是继蒸汽机、电力、信息之后第四个最有潜力引发生产力和生产关系颠覆性革命的核心技术。自 2009 年以比特币为代表的区块链技术诞生以来，该项技术取得了长足的发展和越来越多的关注认可，尤其是近年来区块链技术已经成为全球关注的焦点。区块链行业研究和开发人员在底层核心技术实现到链上应用再到各类场景落地应用等各个层面开展了全方位的探索，但纵观区块链技术的整个发展过程，现阶段区块链技术离大规模实用化还有较大差距，尤其是区块链底层核心技术还未取得较大突破，还存在许多技术难题有待攻克，目前开展的各类区块链场景落地应用很大程度上根基不稳，难以发挥实效，因此当前迫切需要对区块链底层基础设施开展研发，进而为各类区块链应用提供可靠支撑，从而推动区块链技术在各领域各行业真正的落地应用，使区块链这一颠覆性技术更快更好地为人类社会服务。

Naby（NBA）以提供全球价值 Naby 网基础设施为目标，针对现有区块链基础设施普遍存在的实用化程度较低，尤其是交易拥堵、交易费高、交易确认时间长抗量子攻击能力较弱、通信层节点匿名性不高、交易匿名保护、通信和多链融合能力较弱、存储空间较大等问题和需求，优化提升区块链技术在各个层面的协议和机制，实现价值传输网络各层次的支撑协议，作为真正的区块链 4.0 基础设施，为各类价值传输应用提供基础设施，为构建全球价值 Naby 网提供现实可行的技术途径。

Naby 打造攻克了关键技术难题的全领域生态级别的底层基础设施，其主要技术创新包括：1 在底层 P2P 网络节点通信层面，结合现有基于 Tor 的匿名通

信网络、基于区块链的分布式 VPN 的优点实现了独创的匿名 P2P 通信网络，设计实现了节点匿名接入的方法，并实现了私有加密的通信协议，极大地增强了底层通信网络中节点的匿名性，确保节点间通信难以被追踪和破解。2 在底层数据结构层面，采用了新型数据结构，增强式的有向无环图（DAG）——哈希网（HashNet，HN），从而实现异步并行的事件共识验证，提升了系统的可扩展性。3 在分布式共识机制层面，设计了一种安全高效的双层共识机制，基于增强 DAG 的 HashNet 共识和基于随机选择函数的拜占庭协商（BA-VRF）共识，该共识机制具有并发量高、交易确认速度快的特点，可快速构建面向不同应用场景的生态体系。4 在抗量子攻击层面，采用新型抗量子攻击密码算法，通过将 ECDSA 签名算法替换为基于整数格的 NTRUsign 签名算法，同时用 Keccak-512 哈希算法替换现有的 SHA 系列算法，降低了量子计算飞速发展和量子计算机逐步普及带来的威胁。

1

背景

1.1. 区块链发展概况

区块链技术起源于化名为“中本聪”（SatoshiNakamoto）的学者在 2008 年发表的奠基性论文《比特币：一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。凯文·凯利在《失控》一书中描述：生物逻辑的自然、社会、技术的进化规律就是从边缘到中心再到边缘，从失控到控制再到失控。区块链的技术基础是分布式网络架构，正是因为分布式网络技术的成熟，去中心、弱中心、分中心及共享、共识、共担的组织架构和商业架构才有可能有效地建立起来。

数据结构的区块链 3.0 技术兴起，区块链系统较之前更加高效、可扩展强、互通性强、以及具有更良好的用户体验，其应用也进一步延伸到医疗健康、IP 版权、教育、物联网、共享经济、通信、社会管理、慈善公益、文化娱

乐等更为广。

最近两年，部分国家虽然对数字货币的使用和发展持保守态度，但世界各国在区块链底层技术研发以及将区块链与实际应用场景相结合的落地方面一直持积极态度，随着人们对区块链技术的适用范围和可用性的认知程度的提高，人们以极大的热情开展区块链底层核心技术、链上应用和场景落地的研发和实施。人们对区块链技术的研究和探索主要集中于 3 个层面：1 底层技术及基础设施层，主要包括基础协议与区块链相关硬件内容。2 通用应用及技术扩展层：为行业垂直应用层提供服务和接口及相关技术服务，提供的服务包括智能合约、快速计算、挖矿服务、信息安全、数据服务、BaaS、解决方案、防伪溯源等。3 垂直行业应用层：在金融、数字货币、娱乐、供应链、医疗、法律、能源、公益、社交、物联网及农业等垂直领域落地实施。当前，人们投入了极大的热情开展区块链技术的研发和应用，在从事区块链研究和开发的团队中，从事区块链底层技术研究的团队占比约为 20%，将区块链用于各个实际应用场景和垂直行业的团队占比达 80%，相对于应用层而言，底层协议能够创造 Token 市场价值，另外还分散了应用层数据中心化的传统模式。在区块链体系下，应用层的项目本身成为了完全的服务方，不再拥有用户流量与数据。这些

个人数据的价值分散到了用户身上，底层协议相对于应用层会更有价值。

底层数据结构，传统的区块链原本是比特币等加密货币存储数据的一种独特方式，是一种自引用的数据结构，用来存储大量交易信息，由多条交易记录组成区块，区块从后向前有序链接起来，最终实现无法篡改，方便追溯等特点。传统区块链的块链式结构是阻碍区块链提高并发性的瓶颈，技术极客们不断寻找更高效的数据块链接形式，提出有向无环图（DirectedAcyclicGraph，DAG）与区块链相结合的解决方案，以下称为“DAG 链”。DAG 中不存在记账者打包区块这一过程，而是记账过程通过用户相互确认来实现，从而可以大大缩短了交易确认的时间。

哈希算法，哈希运算能够实现数据从一个维度向另一个维度的映射，通常使用哈希函数实现信息摘要，hash 函数碰撞概率极低，并且能够隐藏原始信息。区块链中哈希函数特性包括：函数参数为 string 类型，固定大小输出以及计算高效。常用的 hash 算法包括 MD5 和 SHA 系列算法。但量子计算机下 SHOR 算法可以将攻击哈希算法的复杂度从(2)降为(2/)，传统的哈希算法受到量子攻击的威胁。签名算法，签名算法通过用私钥对信息进行加密变换以保证信息的不可否认性。当前区块链主要使用基于椭圆曲线的 ECDSA 数字签名算法，该签名算法首先需要生成个人的公私钥对：(sk,pk):=generateKeys(keysize)，sk 私钥用户自己保留，pk 公钥可以分发给其他人；其次，可以通过 sk 对一个具体的 message 进行签名：sig:=sign(sk,message)这样就得到了具体的签名 sig；最后，拥有该签名公钥的一方能够进行签名的验证：isValid:=verify(pk,message,sig)。但量子计算机下 SHOR 算法可以将攻击 ECDSA 签名算法的复杂度从，ECDSA 签名算法无法抵抗量子攻击。

匿名交易保护，在公有区块链中，每一个参与者都能够获得完整的数据备份，所有交易数据都是公开和透明的，但对于很多区块链应用来说，这是致命的。不仅用户希望他的帐户隐私和交易信息被保护，就商业机构来说，包含重要资产和商业机密的帐户和交易信息更应当受到保护。比特币的隐私保护思路是，通过隔断交易地址和地址持有人真实身份的关联，来达到匿名的效果。但这样的保护是很弱的，通过观察和跟踪区块链的信息，通过地址 ID、IP 信息等还是可以追查到帐户和交易的关联性。为了解决区块链的隐私保护问题，目前有一次密钥、环签名、同态加密、零知识证明等几种方式。

网络层 P2P 通信，P2P 网络技术是区块链系统连接各对等节点的组网技术，学术界将其翻译为对等网络，在多数媒体上则被称为“点对点”或“端对端”网络，是一种建构于传输层的覆盖网络（overlaynetwork）。不同于中心化网络模式，P2P 网络中各节点的计算机地位平等，每个节点有相同的网络权力，不存在中心化的服务器。但节点的信息容易被泄漏。

共识层共识机制，目前主要有几大类共识机制：PoW、PoS、DPoS、PBFT。PoW 工作量证明，就是人们熟悉的比特币挖矿，通过计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储。可实现完全去中心化，节点自由进出，但挖矿造成大量的资源浪费，共识达成的周期较长，不适合商业应用。PoS 权益证明，PoW 的一种升级共识机制，根据每个节点所占代币的数量和时间，等比例的降低挖矿难度，从而加快找随机数的速度。PoS 还是需要挖矿，本质上没有解决商业应用的痛点。DPoS 股份授权证明机制，类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账，其整个共识机制还是依赖于代币，很多商业应

用是不需要代币存在的。PBFT：PracticalByzantineFaultTolerance，实用拜占庭容错算法，是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制，每个状态机的副本都保存了服务的状态，同时也实现了服务的操作，尽管可以存在多于 3+1 个副本，但是额外的副本除了降低性能之外不能提高可靠性。

激励层激励机制，为了保证区块链分布式系统的正常运行，需要大量的诚实节点保持在线，激励机制则是用来奖励这些对系统有贡献的用户，从博弈论的角度来说，激励机制应该要使得用户诚实行为的收益远远大于恶意行为。

智能合约，基于区块链的智能合约包括事务处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约。比特币只支持简单的脚本语言，以太坊拥有图灵完备的智能合约语言，但是智能合约的拟定和部署十分繁琐，且容易受到攻击。Byteball 的智能合约简单易部署，但却是非图灵完备的，不利于合约应用的扩展。

1.2 当前区块链基础设施存在的问题

现阶段，各类底层协议项目如 EOS、NEO、ArcBlock 等项目层出不穷，但大部分底层协议项目是在以太坊基础之上进行迭代，与区块链 3.0 的标准有一定的差距，更谈不上区块链 4.0。而大部分开展区块链落地业务的团队，受限于底层协议的性能、适用范围和稳定性，目前也都处于早期探索阶段，虽预计在 2017 年可以看到一大批行业应用出现，但在底层协议不断更迭的同时，超过 98%的项目都将会被时代淘汰。概括起来，目前区块链技术主要存在以下问题。

性能低。性能过低是当前区块链技术面临的主要挑战之一。比特币使用的区块链理论上每秒最多只能处理七笔交易，以太坊稍有提高，但也远远不能满足应

用需求。截至 2018 年 12 月，一个简单的 DApp 应用程序就会减慢以太坊交易吞吐并大幅增加交易费用。今天的消费者应用程序必须能够每天处理数千万活跃用户。另外，有些应用只有在满足一定的交易吞吐量时才有意义，因此平台本身必须能够处理大量的用户并发。长时间的交易延迟会阻碍用户的使用，使得建立在区块链上的应用程序与现有非区块链备选方案的竞争力大大降低。使用门槛高。今天的区块链应用程序仅仅是为知道如何使用区块链的少数技术人员而建立的，而不是主流消费者。几乎所有的区块链应用都要求用户运行区块链全节点或轻节点。较高的学习成本严重阻碍了区块链走向大众的进程。例如，基于以太坊的游戏 CryptoKitties 可能是有史以来最易于使用的 DApp，但它仍然需要用户安装 Metamasklightwallet 浏览器扩展程序，并且用户还需要知道如何安全购买 Ethers，并将其与 Metamask 一起使用，这大大影响了用户体验。为了吸引普罗大众的广泛使用，区块链应用程序应该像今天的 Naby 和移动应用程序一样简单。使用成本高。区块链技术的高使用成本是阻碍其成为主流应用的另一个主要障碍，同时也限制了需要灵活构建免费服务的开发人员。与 Naby 对比，区块链技术应该能够支持免费应用程序。让区块链免费使用是其被广泛采用的关键。一个免费的平台也将使开发商和企业能够创造出有价值的新服务。平台锁定。与任何计算机技术的初期一样，区块链存在严重的“平台锁定”问题。开发人员必须首先决定采用哪个区块链，然后编写该特定平台的代码，这样导致将应用程序切换到其他区块链会非常困难。开发人员不希望被锁定在某一种区块链技术，而是需要这些应用程序能在多个平台上运行，以提高开发复用的效率。应用范围较窄。当前人们对区块链抱有很高的期望，特别是随着加密数字货币价格日益上涨，各大新闻媒体为区块链绘制了非常美好的蓝

图。但实际上，区块链技术目前仍处于起步阶段，大多数区块链服务缺乏丰富的功能，应用范围较窄。在区块链开发社区中也缺乏相应的激励机制。因此，当前迫切需要开展区块链底层协议研究，攻克区块链底层核心技术，对区块链技术层面各个维度进行重新设计或加以改进，解决和满足交易拥堵、交易费高、交易确认时间长、抗量子攻击能力较弱、节点通信匿名性不高、缺乏交易匿名保护功能、通信和多链融合能力较弱、存储空间较大等问题，优化提升区块链技术在各个层面的协议和机制，实现真正实用化的价值传输网络各层次的支撑协议，为各类价值传输应用提供基础设施，为各类 DApp 开发提供底层开发平台，为构建全球价值 Naby 提供现实可行的技术途径。

2

Naby 定位

2.1 愿景

Naby 简称 NBA。Naby 底层技术作为的合约层技术支撑，汇款合约是构建 Naby 的 C 端服务的底层智能合约，遵循原子交易（AtomicCross-ChainTransactions，ACCT）和交易及服务（ExchangeasaService，Eaas）原则，其中 ACCT 底层采用用 Naby 核心代码，借助 NabyZone 和 NabyHub 构建链到原子的交易通路，如 BTCChain—BTCzone—Hub—ETHzone—ETHChain。可实现大额主流数字货币之间的去中心化撮合交易。憧憬一下 Naby 广泛应用后的世界，人们的任何行为和活动均可实现自动支付、自动评价、自动保存、自动判断合法性，人们可以自行选择一生的行为和活动是否保存。随着人工智能的逐步演进，可以诞生具备个体完整意识、完全自主智能的虚拟人，人们将现实生活中的各种资产完全转移到链上后，代表一个个人类社会个体的虚拟人将和个体资产一起，永远在链上保存和演化下去，实现了人类社会的虚拟永生，这就是 Naby 网和区块链完整结合后，现实世界和虚拟世界之间的信息映射和价值映射完全实现后的世界。

2.2 目标

Naby 的目标是构建一个通用、支撑功能完善、性能高、易于使用、用户体验好、可扩展的基于增强有向无环图的区块链 4.0 基础设施，打造支撑各类链

上应用的区块链 4.0 生态系统。Naby 聚焦区块链基础设施和平台层核心技术。P2P 网络通信协议、新型抗量子攻击密码哈希算法和签名算法、独创双层共识和挖矿机制、支持交易匿名保护、图灵完备智能合约等特性，采取公平分发机制，支持第三方资产发行、通信、多链融合等功能，能以公有链、联盟链、私有链等形式落地到实际应用场景。Naby 的愿景是实现价值传输网络各类关键技术，构建全球价值 Naby 区块链生态，为各类价值传输应用提供基础网络。

2.3 生态体系

Naby 充分吸收现有区块链 1.0、区块链 2.0 和区块链 3.0 项目的优点，解决它们的突出问题和技术缺陷，构建更加繁荣的应用生态。Naby 创新设计了链上链下数据映射机制，基于有向无环图(DAG)和哈希网(HashNet)的新型增强数据结构、基于 HashNet 共识和 BA-VRF 共识双层共识机制、引入外部触发条件的高级图灵完备智能合约、基于抗量子攻击的 Keccak512 哈希算法和 NTRUSign 签名算法、基于环签名和零知识证明交易匿名保护机制，具有交易快速确认、抗量子攻击、节点匿名通信、交易匿名保护、高级智能合约、数据上链等区块链 4.0 的功能特性，并通过采取公平分发机制，支持第三方资产发行、通信、多链融合等功能。Naby 的愿景是构建全球价值 Naby 区块链生态，为各类价值传输应用提供基础区块链网络，支持各类实际应用以公有链、联盟链、私有链等形式落地。在特定应用中，Naby 将特定应用场景数据进行 Hash 运算，Hash 值存储在 Naby 上，面向的应用场景已经不限于区块链 1.0 背景下以比特币为代表的数字货币应用，不限于区块链 2.0 背景下数字货币与智能合约相结合的金融领域，以及不限于区块链 3.0 在政府、健康、文化和艺术等领域上的应用尝试；基于 Naby 的区块链 4.0 主链将成为多个行业的基础设施，形成基于区块链

的完善行业生态体系，将广泛而深刻地改变人们的生活方式。

3

基于 P2P 的匿名通信技术

Naby 底层通信网络采用 P2P 架构，然后在其上加入了节点间匿名访问机制来确保信息服务的隐私保护性。P2P 是英文 Peer-to-Peer 的缩写，称为“对等网”或“点对点”技术。IBM 将 P2P 定义为：“P2P 系统由若干 Naby 协作的计算机构成，且至少具有如下特征之一：系统依存于边缘化（非中央式服务器）设备的主动协作，每个成员直接从其他成员而不是从服务器的参与中受益；系统中成员同时扮演服务器与客户端的角色；系统应用的用户能够意识到彼此的存在，构成一个虚拟或实际的群体。”

在 P2P 系统中，每一个节点（Peer）都是平等的参与者，承担服务使用者和服务提供者两个角色。资源的所有权和控制权被分散到网络的每一个节点中。P2P 技术使得网络上的沟通变得很容易、很直接，并且把对中间服务器的依赖减少到最小。P2P 技术改变了“内容”所在的位置，使其从“中心”走向“边缘”。也就是说它改变了 Naby 区块链生态现在以集中式的网站为中心的状态，资源不保存在服务器上，而保存在所有用户的 PC 机上。P2P 技术使得终端不再是被动的客户端，而成为具有服务器和客户端双重特征的设备。因此 Naby 具有去中心化的特性。

Naby 的 P2P 网络匿名通信主要通过以下方式实现：（1）在本机运行一个代理服务器，这个代理服务器周期性地与其他 Naby 交流，维持一个 TLS 链

接，从而在 Naby 网络中构成虚拟链路。具体为，每个用户运行自己的代理程序：获取目录，建立路径，处理连接。这些代理接受 TCP 数据流，并且在同一条线路上复用它们。Naby 在应用层进行加密，在每个中继节点间的传输都通过点对点密钥来加密，形成有层次的结构。它中间所经过的各节点，都把客户端包在里面。证密钥和短期的会话密钥，验证密钥来签署 TLS 的证书，签署中继节点的描述符，还被目录服务器用来签署目录。会话密钥则用来解码用户发送来的请求，以便建立一条通路同时协商临时的密钥。TLS 协议还在通讯的中继节点之间使用了短期的连接密钥，周期性独立变化，来减少密钥泄漏的影响。

（2）Naby 网络中的数据包使用了随机的路径来掩盖足迹，这样在某个点的观察者并不知道数据真正从哪里来，真正的目的地是哪里。客户端在 Naby 网络中增量地建立一条加密线路。这条线路每次只扩展一跳，而且每次扩展的中继节点只知道数据来自哪个中继节点，数据将要被发送到哪个中继节点去。没有任何一个中继节点知道整条线路。客户端与每一跳都协商了一组独立的密钥来保证每一跳不能追踪走过的中继点。一旦一条线路建立了，就可以用来进行数据交互了。

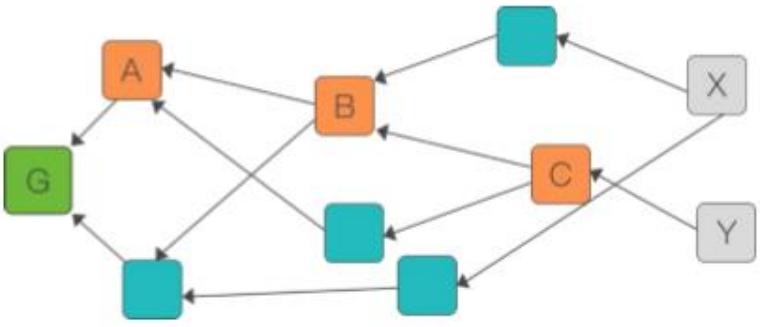
目录服务器是其网络的核心，负责收集 Naby 网络中的中继节点信息并以节点快照及节点描述的形式发布给 Naby 代理；中继节点是 Naby 网络的基础，在网络中的匿名通信流量都是通过由多个中继节点所组成的匿名通信链路来转发的；代理运行于 Naby 用户端，它负责建立匿名链路并在用户的网络应用程序与 Naby 匿名链路之间中转网络流量。在图 3-1 中，由 3 个中继节点构成了一条 Naby 匿名通信链路，这 3 个节点依据其位置依次为入口位置、中间位置与出口位置。

4

数据结构

4.1 基础 DAG 数据结构

Naby 在第一阶段采用基础 DAG 结构存储交易数据。当前已经有 Naby 和 Byteball 等多个项目利用 DAG 成功构建了能够长期稳定运行的公有链，证明了 DAG 链的技术先进性和性能。在 Naby 中，交易信息被封装成一个个单元（Unit），单元与单元之间相互链接组合成一个 DAG 图。由于单元可以链接到任意一个或多个之前的单元，不需要为共识问题付出更多的计算成本和时间成本，也不必等待节点之间数据强同步，甚至没有多个数据单元拼装区块的概念，因此可以极大提高交易的并发量，并把确认时间降低到最小。Naby 的 DAG 数据结构如图所示，单元之间的有向边表示两个单元之间具有引用关系，图中有一条由 B 指向 A 的有向边，表示 B 引用 A，A 是 B 的父单元，B 是 A 的子单元，同时，我们称单元 C 间接引用 A，A 是 C 的祖先单元；单元 G 不具有任何父单元，称之为创世单元，创世单元是唯一的；单元 X，Y 不具有任何子单元，这类单元被称为顶端单元。



单元由单元头部和单元消息两部分组成。其中单元头部主要包含以下字段：

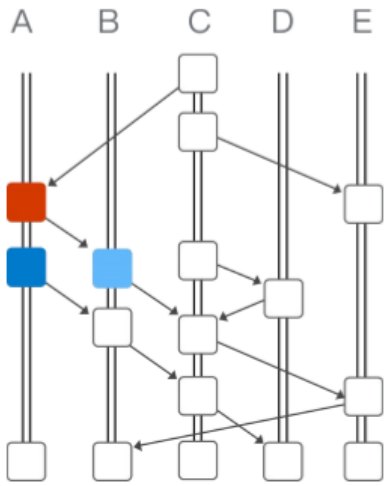
- 单元版本；
- 代币标志符；
- 单元创建者签名：单个签名或多个创建者共同签名；
- 父单元 hash：所引用的单个或多个父单元的 hash；
- 见证人列表：具有相同见证人的其他单元（通常是父单元或祖先单元）的 hash。

单元消息部分用于存储交易的信息，Naby 具有多种类型的交易，包括支付，数据存储，投票等等。

类似于区块链中每个新块需要确认先前的所有块，DAG 中的每个新子单元需要确认其父单元，父单元的所有父单元。如果尝试修改 Naby 中过去的记录需要与大量且越来越多的其他用户协调，其中大多数是匿名的陌生人。因此，不可更改性是基于与如此大量的陌生人协调的复杂性，这些人难以达成一致，对合作没有兴趣，并且每一个人都可以否决修订。单元发布之后，立即开始确认，并且确认可以来自任何时候由任何人发布的一个新单元，用户互相帮助：通过添加一个新单元，发布者也确认了所有以前的单元。

4.2 基于增强 DAG 的 HashNet 数据结构

HashNet 是一种有向无环图（DAG），是由无数个顶点和连接顶点的有向边组成。下图记录了全网所有节点在什么时间以什么样的顺序给其他节点发送了什么样的数据，每个节点都在内存里有这样一个 HashNet 的拷贝。



上图中有 5 个计算机节点 A,B,C,D,E，每个节点拥有一个放置顶点 vertex(也叫 event)的柱子。最新发生的事件，会被放置的在图顶部，HashNet 是随时间向上增长。HashNet 的特征

1.顶点。就是一个事件，包括：创建的时间戳，0 个或者多个交易，创建者的签名，以及 self-parent 和 other-parent 的 hash 值。

2.HashNet 有两种边，垂直边和斜边。

5

共识机制

在 Naby1.0 版中，Naby 所使用的共识机制为基础 DAG 共识和 BAVRF 共识相结合的双层共识机制。自 Naby2.0 版开始，基础 DAG 共识将替换为基于 HashNet 的 DAG 共识，Naby 的共识机制为 HashNet 的 DAG 共识和 BA-VRF 共识机制相结合的双层共识机制。

5.1.1 基础 DAG 共识

主链是在指定单元所见的 DAG 图中沿着子-父链接找到一个单链，可以把所有单元都关联在一起。我们从任意一个顶点开始，都可以构建一条主链。如果以相同的规则在两个不同的顶点选择主链，这两条主链在回溯过程中一旦相交，它们会在交点之后完全重合。重合部分称为稳定主链，最坏的情况，两条主链在创世单元相交。所有的单元要么直接在这条稳定主链之上，要么从稳定主链上的单元沿着 DAG 的边缘通过少量的跳跃可以到达。因此稳定主链可以在两个冲突的无序单元之间建立总序。首先，给直接位于稳定主链上的单元做个索引，创世单元索引为 0，创世单元的子单元索引为 1，以此类推，沿着稳定主链给主链上的所有单元分配索引。对于不在稳定主链上的单元，我们找到第一个直接或间接引用此单元的主链单元。这样，就给每一个单元分配了一个主链索引（MCI）。然后，给定两个单元，拥有较小 MCI 的单元被认为是更早生成的。

网络健康发展的组织。虽然期望他们诚实行事，但完全信任任何一个证人

是不合理的，因此会同时选择多个不同的见证人。

5.1.2 双重支付问题

双重支付交易：相同地址发出的任何无序的交易都视为双重支付交易，即使它们没有使用相同的输出，也可称为冲突交易或者矛盾交易。在用户地址发出新单元时，要求相同地址发布的所有单元应当直接或间接包含该地址之前所有的单元，即相同地址的所有单元连通（有序或连续）。因此，在相同地址的所有单元都连通的情况下，在路径上出现较早的交易为有效交易。如果有攻击者特意制造出双重支付交易，那么可以通过主链序号来解决，主链序号较小的交易为有效交易。假设攻击者制造出一条影子链，并在上面发布双重支付交易。当影子链接入到真实的 DAG 中时，根据最优父单元选择策略，影子链上的见证人个数少，因此它不会成为主链的一部分，从而解决了这种场景下的双重支付问题。值得注意的是，如果大多数见证人与攻击者合谋，并在其影子链上发布单元，则攻击者有可能攻击成功。

5.1.3 交易确认

当获得新的单元时，每一个节点会持续追踪自身的当前 MC，好像他们将要基于当前的所有无子单元构建新单元。不同节点各自的当前 MC 也许不同，因为它们有可能看到不同的非稳定单元集合。而当新单元到达时，当前 MC 会不断变化。然而，当前 MC 的足够老的那部分会保持不变。未来所有的 MC 在回溯时将会汇集某个 MC 单元，这个 MC 单元以及之前的所有 MC 单元都是稳定的，不会因为新单元的到来而改变。事实上，创世单元是一个天然的初始稳定节点。假设我们已经基于当前的非稳定单元集合构造了一条当前 MC，并且这条链上已经有一些之前认定稳定的节点，也就是说未来的当前 MC 都被相信

会在这个点或早于这个点汇集，然后就沿同一条路径回溯。如果我们能找到一个方法，把这个稳定点向远离创世单元的方向推进，就可以根据数学归纳法证明这个稳定点存在。而被这个稳定点所引用的单元将获得确定的 MCI，包含在这些单元中的所有消息也将被确认。

5.2.1 HashNet 基本思想

已有的 Hashgraph 共识算法通过 gossip 网络和虚拟投票策略达成交易顺序的共识，该共识的前提是要求网络节点超过 2/3 的投票能力具有 famouswitness 事件的一致投票结果，其中投票是全网的当前投票能力总和，该投票能力通常为节点的持股数量。由于采用了本地投票策略，Hashgraph 可以实现较快的交易确认速度。然而该方法存在以下问题：

1)在广域网环境中，节点波动性较强，全网的投票能力 n 的波动也随之增强，这可能导致系统长时间无法找到满足 2n/3 投票一致的事件，从而无法达成共识。

2)受节点稳定性、处理能力、带宽等因素影响，不同节点处理事件的能力差别较大。若系统中存在大量能力较弱的节点参与投票，同样会造成系统长时间无法达成共识。

3)广域网环境下，节点频繁波动可能导致节点被分割成多个子网。根据 gossip 邻居交换协议，节点会周期性剔除长时间未更新的邻居。当邻居稳定后，节点可在子网内达成共识。此时若子网规模较小，很容易使恶意节点在同一轮产生两个 famouswitness 事件，从而产生双花交易。

4)随着系统规模增大，节点收到的同步信息越来越多，可以预见系统的吞吐率会随节点数目的增加而降低。

基于以上挑战性问题，我们提出 HashNet 共识机制。HashNet 采用基于双层 gossip 拓扑框架，通过“片内自治，片间协作”的方式形成一个分而治之的分布式账本系统。在 HashNet 中，顶层 gossip 网络中的节点称为全节点（fullnode），负责节点拓扑和分片的维护；下层 gossip 网络的节点称为局部全节点（localfullnode），负责交易共识、交易验证、交易存储以及账本一致性。HashNet 共识机制的主要优势在于：

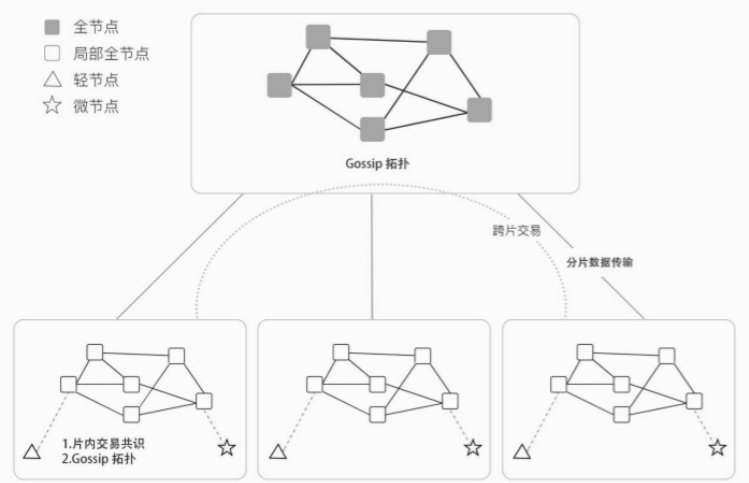
1)全节点和局部全节点具有较强的稳定性和处理能力，能够有效避免 Hashgraph长时间无法达成共识的问题，也能够避免因网络被分割造成的恶意节点攻击问题。

2)采用双层 gossip 拓扑对节点分片，顶层节点不参与交易共识和交易验证过程，分片可并行工作，保证了系统具有较好的可扩展性。

5.2.2 节点类型

HashNet 中节点共分为四类：全节点、局部全节点、轻节点和微节点。

- 全节点：(1) 负责维护节点拓扑，包括全节点的周期性加入退出过程、局部全节点的周期性加入退出过程；(2) 负责更新分片，包括确定每个周期的分片数量、将哪些局部全节点划分到同一个分片。



- 局部全节点：（1）作为代理节点，向轻节点和微节点提供交易代理服务；（2）在分片内，局部全节点作为交易共识的主体，实现交易在片内的验证、共识和记账；（3）在分片间，局部全节点采用 gossip 协议传播各自片内账本信息至其他分片，从而实现账本数据一致性。

- 轻节点：通常为轻量级客户端钱包，该节点可通过局部全节点做代理完成数据请求和发送。

- 微节点：通常为智能物联网设备，该节点可通过局部全节点做代理完成数据请求和发送。

5.3.基于可验证随机函数的拜占庭协商共识

基于可验证随机函数的拜占庭协商共识（BA-VRF）共识主要用于选举责任全节点，他是一种基于可验证随机函数（VerifiableRandomFunction，VRF）和 BA 算法构建的共识机制，该共识机制能够随机选出少量全节点作为公证节点，并确定公证节点的优先级。BA-VRF 每一分钟执行一次，每次达成共识将随机选出若干全节点作为公证节点，公证节点有权发送公证单元，公证单元须满足 DAG 共识中的父子引用规则。公证节点发送的公证单元成为稳定主链的单元后，该公证节点可以获得公证奖励。当交易活跃时，新单元不断产生，则公证节点会及时获得公证奖励；当交易不活跃时，极端情况下一分钟内没有新单元产生，已经发送公证单元的节点在发送的公证单元成为稳定主链单元时获得公证奖励，没有发送公证单元的节点不获得公证奖励。

5.3.1.共识状态

BA-VRF 有最终共识和临时共识两种状态。如果一个全节点达到最终共识，意味着任何其它全节点也达到了最终共识或者在同一轮中的临时共识必须

同意这一共识结果，而无论强同步假设是否成立。而临时共识意味着其它全节点可能在其它公证单元上达到了临时共识，没有全节点已经达到了最终共识。所有公证单元都必须直接或间接引用之前生成的公证单元，这可以确保 BA-VRF 的安全性。BA-VRF 产生临时共识有两种情况。首先，如果网络是强同步的，一个攻击者可以以一个很小的概率让 BA-VRF 达到临时共识。此情况下，BA-VRF 不会达成最终共识，也不能确认网络是强同步的。但经过几轮后，很大概率上会达到最终共识。第二种情况是，网络是弱同步的，整个网络都被攻击者控制。此情况下，BA-VRF 将达到临时共识，选举出不同的公证节点集合，形成多分叉共识。这能够避免 BA-VRF 达到最终共识，因为全节点被分成了不同的组，各组之间并不同意对方。为了恢复活性，BA-VRF 将被周期性地执行，直到消除意见分歧。一旦网络恢复到强同步状态，将会在短时间内达成共识。

5.3.2.全节点选择

抽签算法是基于可验证随机函数（VRF）构造而成的，可根据每个参与 BA-VRF 共识的全节点的权重选出这些节点的随机子集。某全节点被选中的概率约等于自身权重与总权重的比值。抽签的随机性源于 VRF 函数和一个可公开验证的随机种子，每个全节点可根据随机种子验证自己是否被选中。

VRF 函数定义：给定任意字符串，VRF 函数输出哈希值和证明结果。

$$(hash,)\leftarrow VRFS(seed||role)$$

哈希值 hash 由私钥和给定的字符串(seed||role)唯一确定，在不知道私钥的情况下，输出的哈希值 hash 与随机数之间不可区分。证明结果 π 使得，知道私钥所对应公钥的节点可以验证哈希值 hash 和字符串 seed 之间是否关联。种

子 seed 是随机选择并且可以被公开获得的，每一轮运算的 seed 由前一轮运算的 seed 生成。抽签算法支持角色指定，如选出协商过程中某一步骤的参与者。所有全节点执行抽签算法来确定自己是否被赋予公证权，被选中的全节点通过 P2P 网络向其它全节点广播自己的抽签结果。需要说明的是，抽签选择全节点的概率与全节点自身权重成正比，以抵御 Sybil 攻击。权重大的全节点可能会被选中多次，为此抽签算法会输出全节点被选中的次数。如果一个全节点被多次选中，那么它就被当成多个不同的全节点。

5.3.3.拜占庭协商

拜占庭协商（BA）能为每一个被选中的全节点确定公证优先级并提供公证优先级的证明。达成拜占庭共识需要执行多个步骤，BA 算法会被执行多次。每次协商都从抽签开始，所有全节点都去查看它们是否被选中成为当前 BA 的参与者。参与者广播一个包含选择公证优先级的消息。每一个全节点用它们收到的公证优先级消息去初始化 BA 算法。上述过程将被不断重复执行，直到某轮协商有足够多的全节点达成共识。在不同全节点之间，BA 算法并不是同步的，每个全节点发现之前的步骤结束后应立即查看新的参与者选举结果。只有全节点在某轮协商中投票并最终达成共识，它才可以参与下一轮协商。BA 算法的一个重要特征是，参与者不需要维护私有状态，仅存私钥，所以参与者每个步骤之后都可以被更换，以减少对参与者的攻击。当网络是强同步的，BA 算法保证如果所有的诚实全节点以相同内容进行初始化，那么可以在很少的交互步骤之内达到最终共识。此情况下，即使存在少量攻击者，所有的诚实全节点也将在有限交互步骤步下在达到最终共识。

6

交易匿名保护

匿名交易与隐私保护是电子货币的重要属性。目前大部分区块链对隐私保护的解决思路是，通过隔断交易地址和地址持有人真实身份的关联，来达到匿名的效果。所以虽然能够看到每一笔转账记录的发送方和接受方的地址，但无法对应到现实世界中的具体某个人。但这样的保护是很弱的，通过观察和跟踪区块链的信息，通过地址 ID、IP 信息并运用 Naby 分析总能得出跟用户相关的某些信息等。Naby 从交易的无关联性和不可追踪性两个方面确保对交易信息匿名保护，并不断迭代改进匿名保护能力。Naby 对交易无关联性 unlinkability 和不可追踪性 untraceablility 进行了规范化的定义，无关联性是指对于任何两个外部交易，不能证明将其发送给同一个人，不可追踪性是指对于每个内部交易，所有可能的发件人从概率上是相等的。无关联性和不可追踪性是强隐私保护的区块链必须满足的属性，Naby 通过采用一次密钥 onetimesecretkey 和环签名 ringsignature 技术来实现对无关联性和不可追踪性的支持。同时，Naby 设计并实现严格的零知识证明 zero-knowledgeproof 模型作为可选择功能，可进一步增强交易匿名性。

6.1. 一次密钥

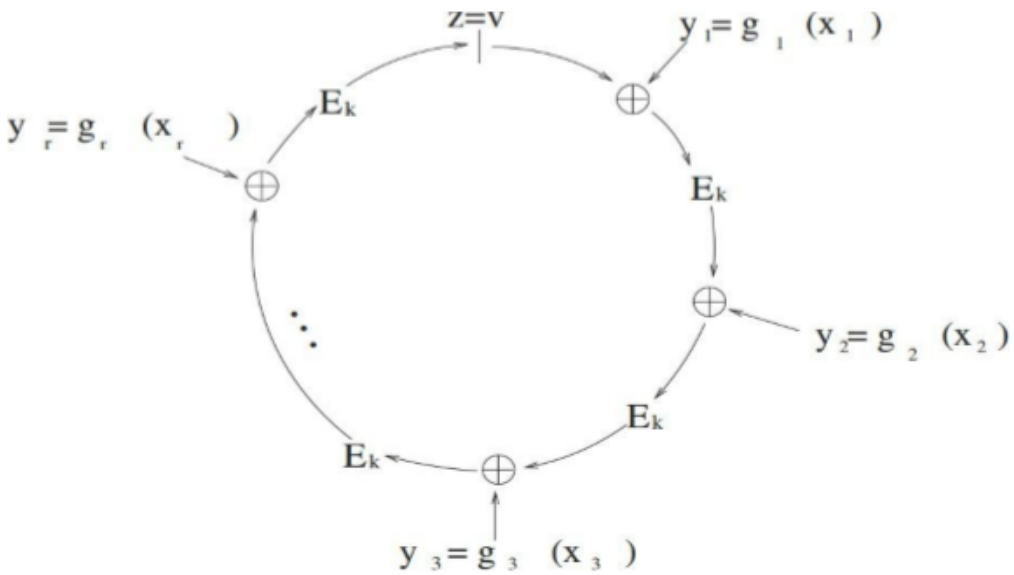
Naby 采用一次密钥技术来实现交易的无关联性。一次密钥是指发送方对每个交易使用单独的密钥进行签名。与通常的区块链交易中接收方只用到一对公

私钥不同，在一次密钥方案中，每次交易中接收方需要用到两对公私钥，交易发起时，交易发送方使用交易接受方的两个公钥和随机数生成临时公钥，发送方将该临时密钥作为地址进行交易，接收方执行 Die-Hellman 交换并结合他的一个私钥信息可以获取临时私钥。由于一次密钥只可以有接受方验证，保证了交易的正确性。同时，每次交易使用

不同的随机数，即使与同一个接收方进行多次交易，因其一次密钥不同，也不能将其进行关联，保证了交易的无关联性。

6.2.环签名

一次密钥主要是保证了交易接收方的隐私，为了同时保证交易发送方的隐私，InterValue 采用了环签名技术。环签名是一种群签名(GroupSignature)技术衍生而来的多用户签名技术，该签名摆脱了群签名的诸多弊端，如不再需要群管理员、具有不可追踪性等。



在环签名技术中，消息由一组签名者进行签名，验证者无法得知谁是具体的签名者。因此，环签名能够很好的解决签名者身份隐私保护的问题，实现交

易的不可追踪性。另一方面，由于一般的环签名技术将签名者隐藏在一组用户之中，会带来双重支付（double spending）的问题，可采用可链接环签名技术 linkable ring signature 解决这一问题。

6.3. 零知识证明

零知识证明技术是 1985 年由 S.Goldwasser、S.Micali 和 C.Racko 提出的，最初设计用于达成证明者能够在不向验证者提供任何有用信息的情况下，让验证者正确认证证明者的目的。零知识证明本质上是在传统的数学证明中引入随机性和交互的要素，用问答方式进行证明的交互证明系统，后来发展出非交互性方式，在计算机科学和密码学领域具有深远影响。在实际应用中，零知识证明要求验证者不能在验证过程中获取新的知识，即恶意验证者，使验证存在误差，同时防止技术性导致的验证误差。

加密数字货币 Zcash 第一次使用零知识证明实现其交易的隐私性，不同于将发送者的交易区块删除的方式，Zcash 使用作废列表标识交易者发送后的区块，旷工仅仅验证交易区块的哈希值，实现了交易的完全匿名。

6.4. 匿名交易与隐私保护

作为区块链 4.0 技术，Naby 通过保密交易（confidential transaction）实现匿名交易与隐私保护，Naby1.0 版至 3.0 版借鉴加密货币 Monero 的隐私保护方法，采用一次密钥和环签名技术实现保密交易。Naby4.0 版借鉴当前 Zcash 的匿名保护方法，在前期版本的基础上增加严格设计的非交互零知识证明，把非交互零知识证明作为可选择功能，支持实现交易的完全匿名，有效抵抗恶意验证者，满足不同应用场景隐私保护需求。

7

团队发展及规划

7.1 基金

NBA 由颠覆式技术创新基金 Byzantine Partners 和专业数字资产投资和咨询服务资本 Orichal Partners 战略支持。

Byzantine Partners 凭借在投资管理、交易、研究及创业孵化等超过数十年的综合经验，专注于支持和投资改变行业游戏规则的颠覆式技术创新，以及有前途的数字资产。在旧金山、首尔、新加坡设有办事处。

Orichal Partners 相信加密货币的发明象征着社会价值在记录，转移和分配方式的重大改变，并为新一代金融创新和社会发展建设铺路。

Byzantine Partners 和 Orichal Partners 投入资金用于 Naby 的研发，对 Naby 的开源、社区建设、特性建议的审议等进行管理；同时致力于项目本身的财务、团队建设、对外关系等，使得项目更好的运行。

7.2 团队

Gino Caleb

CTO，博士，主要研究方向为分布式计算技术，共发表高水平论文 30 余篇，撰写专著 4 部，主持和参与高级别科研项目 10 余项。一直从事 P2P 系统架构设计，对双层结构对等计算拓扑有深度的认识。

Roger Angus

首席架构师，博士，主要研究方向为分布式计算、云计算、机器学习。在分布式系统的可扩展性、可靠性以及弹性优化处理方面有深刻认识，对区块链底层技术和工作原理有深刻理解和实际操作经验。

Jason Frank

Naby 安全事业部负责人，计算机科学与技术博士，长期致力于区块链、机器学习、网络安全的研究，在智能合约、主动学习、深度学习等方面有多年的研究基础。

Gary Bobby

Naby 生态建设负责人，博士，研究方向为机器学习，智能信息处理，信息系统等，发表论文 20 余篇，长期从事大型信息系统与分布式应用实践，具有丰富的产品研发和系统设计经验，较早开始区块链的研究，对区块链的应用与生态构建具有深刻认识。

Storm Dennis

工学硕士，高级程序员，区块链技术专家，在 IBM 的系统科技部工作多年，具有丰富的 Hadoop 及 MapReduce 开发经验。2012 年接触比特币，熟悉加密货币原理，交易所钱包的存储对接方案，目前专注于智能合约和区块链应用方。

8

Token 经济模型

8.1 Token 经济模型

Naby 在基于 4.0 区块链技术“自主创新、安全高效、开放共享”设计原则的指导下，Naby 未来将携手行业合作伙伴及其技术供应商，共同探索行业区块链发展方向，共同推动区块链应用场景落地。

自主创新：Naby 区块链注重自主创新，目前在关键领域已经拥有多项自主知识产权的独特核心技术，在共识算法、海量数据并发处理、账户安全管理、风险控制等方面具有技术积累。

安全高效：Naby 可信区块链，能够有效实现信息共享，保护信息安全，提升系统效率。开放分享：Naby 将搭建区块链基础设施，开放内部服务能力，与行业伙伴共享，共同推动可信互联网的发展，打造区块链的共赢生态。

为了有效激励社区建设者与参与者，实现平台生态的自发式增长，Naby 平台发行平台通行的原生 Token—NBA，NBA 是平台的唯一权益证明，是基于 ERC-20 标准发行的一种权证，待项目主网完成将映射到 Naby 主链。

8.2 Token 基本信息:

代币简称: NBA

总发行量: 1700 万枚永不增发

分配方案：

基金持有：50% （Byzantine Partners 持有 30% Orichal Partners 持有 20%）

公募：10% （用于公开募集）

节点市场：40% （用于激励节点市场）

9

项 目 发 展 路 线

1、团队为未来制订详细的发展规划，团队将构建有据可查的 API 和库，实现用户与 Naby 区块链之间的互动。

2、Naby 团队将使用开源方法为 Naby 区块链背后的协同技术开发创建框架。我们将建立适当的程序，用于讨论和审核针对区块链底层协议和软件的更改。

3、团队将对区块链执行广泛的测试，从对协议的测试到联合各家实体(如钱包服务和交易平台)对网络进行整体测试，从而确保系统在发布前运转正常。

4、团队将努力促进社群的发展，并且在 Naby 生态系统发布之后，将为第三方创建智能合约确立相应路径。

5、团队将与社群一起，在通往非许可型生态系统的道路上攻克技术难题，力争实现我们在发布后 3 年内的目标。

10

法 律

在过去一年中，美国，新加坡，瑞士和德国等国家的金融当局收紧了对加密代币众售的政策或发出警告，因为通证越来越多地被归类为证券。Naby 通证销售承认并将遵守几个主要司法管辖区的安全法规，并遵守 KYC 和 AML 法规。详细地说，这意味着如下几点：

10.1 证券法规

请仔细阅读本部分。如果您对您应采取的行动有任何疑问，我们建议您咨询您的法律，财务，税务或其他专业顾问。本文档中列出的信息可能并不全面，并不代表合同关系的任何要素。本文档不代表投资，税务，法律，法规，财务，会计或其他建议，也不能作为可能参与 Naby 生态系统支持和开发的唯一理由。在做出决定之前，潜在买方必须咨询其法律，投资，税务会计和其他顾问，以确定此类交易的潜在利益，限制和其他后果。本文件的任何部分均不是发行招股说明书或要约，其目标不是作为证券要约或在任何类型的司法管辖区内以证券形式进行投资的要求。本文档未按照任何司法管辖区的法律或法规编制，该法律或法规禁止或以任何方式限制与数字代币或其使用的任何形式有关的交易。

10.2 KYC 和 AML

了解用户的客户（KYC）和反洗钱（AML）法规在技术细节方面因国家/地

区而异，但它们都需要根据恐怖主义，禁运和政治暴露人士（PEP）的各种清单对客户的身份进行核实和核对。Naby 正在与专业服务提供商实施此流程。在向人群进行投融资的流程中，身份验证和 AML 检查之后将检查投资者类别。如果仍有疑问，则会进行人工调查。从加密到法定货币的交换将由受监管的经纪人/交易所进行，银行将获得 KYC 和 AML 报告。

10.3 治理

Naby 准备聘请一家国际会计师事务所来评估 Naby 通证经济模型及流程，审计其会计，并提供有关其如何遵循其指导方针的报告。

11

风险提示

11.1 监管风险

由于区块链的发展尚处早期，全球暂无明确的有关募集过程中的前置要求、交易要求、资讯披露要求、锁定要求等相关的法规。目前全球各国政府政策会如何制定和实施尚不明朗。这些因素均可能对专案的发展与流动性产生不确定影响。而区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则 Naby 应用或 Naby 本身可能受到影响。例如法令限制使用、Naby 有可能受到限制、阻碍甚至直接终止 Naby 应用和 Naby 的发展。

尤其需要指出的是，本专案禁止向美国、中国大陆等法律禁止的国家和地区推介。凡这些国家或地区居民通过其他管道获取 Naby 资讯，与专案方无关，自行承担法律风险。

11.2 竞争风险

当前区块链领域专案众多，竞争十分激烈，存在较强的市场竞争和专案运营压力。Naby 专案是否能在诸多优秀专案中突围，受到广泛认可，既与自身团队能力、愿景规划等方面有关，也受到市场上诸多竞争者乃至寡头的影响，其间存在面临恶性竞争的可能。

11.3 人才流失风险

Naby 是一支活力与实力兼备的人才队伍，团队由区块链领域的资深从业者组成，技术开发人员具有多年区块链开发经验。但在今后的发展中，不排除有核心人员离开、团队内部发生冲突而导致 Naby 整体受到负面影响的可能性。

11.4 专案技术风险

密码学的加速发展或者科技的发展诸如量子电脑的发展，或将密码破解的风险带给平台，这可能导致 NBA 的丢失。专案更新过程中，可能会出现漏洞，漏洞发现后会及时修复，但不能保证不造成任何影响。类似影响造成的损失，专案方不会承担。

11.5 应用缺少关注风险

产品存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用。这样一种缺少兴趣的现象可能会对应用造成负面影响。

11.6 骇客攻击风险

骇客或其他组织供攻击风险，包括但不限于拒绝服务攻击、Sybil 攻击、恶意软体攻击或一致性攻击等。

11.7 未保险损失风险

不同于银行帐户或其他金融机构的帐户，存储在帐户或相关区块链网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为其损失担保。

11.8 目前未可知的其他风险

除了本白皮书内提及的风险外，还可能存在着一些创始团队尚未提及或尚未预料到的风险。此外，其他风险也有可能突然出现，或者以多种已经提及的

风险的组合的方式出现。

请参与者在做出参与决策之前，充分了解团队背景，知晓专案整体框架与思路，理性参与。