QuarkChain

高性能点对点交易网络

0.3.4.版本

更新日期：2018 年 5 月 10 日

本文是根据具有同一版本号的 quarkchain whitepaper（可在 quarkchain.io 上找到）翻译而成，旨在提供中文读者语言上的便利，不可作为投资或者法律以及其他类似场景中的依据，翻译版和英文版有出入之处，以英文版为准。

免责声明

这份白皮书中没有任何内容构成法律、金融、商业或税务方面的建议，在从事任何与此相关的活动之前，你应该咨询你自己的法律、财务、税务或其他专业顾问。无论是QUARKCHAIN 基金会有限公司、项目团队的任何从事 QUARKCHAIN 网络的成员，或项目开发QUARKCHAIN 网络团队,任何经销商/供应商 QKC(经销商)都不对因使用https://www.quarkchain.io（本网站）或任何其他网站访问本白皮书，网站或基金会发布的材料而导致的任何类型直接或间接损失负责。

这份白皮书仅用于一般的信息目的，不构成招股说明书、要约文件、证券要约、投资请求，或任何出售任何产品、项目或资产的要约（无论是数字的还是其他的）。下面的信息可能不是详尽的，也不包含合同关系的任何元素。对于这些信息的准确性或完整性，没有任何保证，也没有任何保证承诺，或声称将提供这些信息的准确性或完整性。该白皮书包含了从第三方来源获得的信息，基金会或 QuarkChain 团队没有独立核实这些信息的准确性或完成。此外，您承认情况可能会改变，因此这份白皮书可能会过时;基金会没有义务更新或纠正与此相关的文档。

该白皮书不构成基金会、分销商或 QuarkChain 团队提供任何 QKC（如本文所定义）的任何要约，也不应将其或其任何部分或其陈述的事实作为与任何合同或投资决定有关的基础，或依赖于任何合同或投资决定。该白皮书中没有包含或可以依赖于对夸克链网络未来性能的承诺、表示或承诺。经销商与贵公司就 QKC 的任何销售和购买达成的协议仅适用于此类协议的单独条款和条件。

通过访问本白皮书其任何部分，代表您向基金会及其附属公司和 QuarkChain 团队声明并保证如下：

a.在任何购买任何 QKC 的决定中，您都没有依赖本白皮书中列出的任何声明;

b.您将并应自费确保遵守适用于您（视情况而定）的所有法律，监管要求和限制;

c.您承认:理解并同意 QKC 可能没有价值，不存在任何对于 QKC 价值的担保,QKC 不适用于投机性投资;

d.任何基金会、其附属机构的成员均不对 QKC 的价值、QKC 的可转让性和/或流动性负

责，或对 QKC 的任何市场通过第三方或其他途径的可用性负责;

e.您承认，理解并同意，如果您是某个地理区域或国家的公民，国家，居民（税务或其他），住所和/或绿卡持有人，您没有资格购买任何 QKC,QKC 的销售将被解释为出售一种证券（不论其名称）或投资产品和适用法律，法令禁止访问或参与 QKC 令牌销售或 QuarkChain 网络，条例或行政法;包括但不限于美利坚合众国，加拿大，新西兰，中华人民共和国和大韩民国）。

基金会、分销商和 QuarkChain 团队不主张作出任何声明、保证或承诺给任何实体或人（包括但不限于保证内容的准确性、完整性、及时性或可靠性）。在法律允许的最大范围内，基金会、分销商、其相关实体和服务提供者对侵权、合同或其他任何种类的间接、特别、附带、后果或其他损失不承担任何责任（包括但不限于任何责任）。因使用该白皮书或任何其他材料所产生的或其内容（包括但不限于任何错误或遗漏）。QKC 的潜在购买者应仔细考虑和评估与 QKC 代币销售、基金会、分销商和 QuarkChain 团队相关的所有风险和不确定性（包括财务和法律风险和不确定性）。

本白皮书中提供的信息仅供社区讨论，并不具有法律约束力。任何人都不得在收购 QKC 方面订立任何合同或具有约束力的法律承诺，并且不会以本白皮书为基础接受虚拟货币或其他形式的付款。买卖合营公司及继续持有合营公司的协议须受一套独立条款及条件或代币购买协议（视情况而定）的约束，并载列购买及继续持有 QKC（条款和条件），应单独提供给您或在网站上提供。如果本条款与条件与本白皮书之间有任何不一致之处，以本条款与条件为准。

所有的贡献将被用于促进区块链技术和网络的研究，设计和开发以及倡导能够处理大规模 TPS 容量，扩展区块链技术的可用性而不牺牲安全性和分散性的核心特性的所有贡献实现一个无堵塞且价格适中的网络，满足所有需要速度和容量的使用场景。基金会，分销商及其各种关联公司将开发，管理和运营 QuarkChain 网络。

这只是一个概念白皮书，描述将要开发的 QuarkChain 网络的未来发展目标。本白皮书可能会不时修改或更换。没有义务更新本白皮书或向收件人提供本白皮书提供的信息之外的任何信息。

本白皮书中包含的所有声明，新闻稿中或公众可访问的声明以及基金会，分销商和QuarkChain团队可能做出的口头声明均可构成前瞻性声明（包括关于意图的声明，对市场状况，经营战略和计划，财务状况，具体规定和风险管理做法的信念或当前预期）。请注意，不要过分依赖这些前瞻性声明，因为这些声明涉及已知和未知的风险，不确定性和其他因素，可能导致未来实际结果与此类前瞻性声明所描述的结果存在重大差异，并且并无独立第三方检讨任何该等陈述或假设的合理性。这些前瞻性陈述仅适用于本白皮书的日期，基金会和QuarkChain团队明确表示不承担任何责任（无论明示或暗示）对这些前瞻性陈述进行修订，以反映该日期之后的事件。

在此使用任何公司和/或平台名称或商标（除了与基金会或其关联公司有关的内容）并不意味着与任何第三方有任何关联或认可。本白皮书中提及的特定公司和平台仅供参考。

本白皮书可能会翻译成英文以外的语言，如果本白皮书的英文版本和翻译版本之间存在冲突或含糊不清之处，应以英文版本为准。您承认您已阅读并理解本白皮书的英文版本。

摘要

QuarkChain 是基于分片技术的区块链底层技术方案，它具有安全、去中心化、高吞吐能力和可扩展的特性，它将实现每秒十万级链以上的交易处理能力（100,000+ TPS）。
QuarkChain 的技术核心包括：

1.可多次分片的双层链结构

QuarkChain 由两层区块链结构组成，第一层为分片层（可以理解为子链层），用于交易记账；第二层为一条根链，用于确认分片中的交易。在不影响根链的情况下，分片层的分片数量可以动态增加，从而来提高系统的整体吞吐量。

2.市场驱动的协作挖矿提供安全保障

为了确保交易的安全性，QuarkChain 基于博弈论框架设计了一个用于激励矿工工作并合理分配算力的机制，其中至少 50%的全网算力将分配到根链上，以防止可能的双花及恶意挖矿等攻击。

3.抗中心化的横向节点扩展

在任何一个具有高的 TPS 处理能力的区块链网络上，一个保存全网账本的超级节点将是非常昂贵的，这会导致中心化。为了避免这一问题，QuarkChain 支持多个廉价的节点组成集群的方式实现一个超级节点的功能，避免了中心化。

4.高效的跨片交易

QuarkChain 网络支持在任何时间任何地点进行跨分片交易，并快速完成交易确认。随着分片的数量增加，交易速度将线性增加。

5.简单的账户管理方式

在 QuarkChain 系统中，每位用户使用整个区块链网络只需要创建一个账户。用户在不同分片上的加密资产将安全的存储在一个智能钱包中，使用体验就如同在单个链上进行交易。

6.图灵完备的智能合约平台

QuarkChain 支持图灵完备的智能合约，并采用了以太坊虚拟机（EVM），以便将以太坊上现有的 EVM DApp 轻松迁移到 QuarkChain 平台上。

目录

1.动机与展望

1.1.区块链技术综述

时间追溯到 20 世纪 90 年代，凯文· 凯利已经预言了一个加密世界的到来“crypto-anarchy: encryption always wins.”前英特尔物理学家蒂姆梅曾说“Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.”（引自《Out of Control》）。正如凯利预言，在 2008 年“区块链”这个词在比特币源代码中被创造出来时，加密时代就已经到来了。

在过去的两年里，许多公司都在积极探索区块链技术。目前世界上几乎所有主要金融机构都在研究区块链。图 1 所示，自 2017 年下半年以来，以太坊系统中的交易请求数量大幅增加，使得交易费用急剧上升。在不久的将来越来越多基于区块链的 DApp 被开发出来，对区块链基础设施的需求持续增长。

图 1

由于大量的交易请求，每天以太币的交易费急剧上升（2018 年初，是六个月前的 47 倍）。

（来源：etherscan.io）

1.2.区块链的发展背景

比特币是区块链 1.0，它启动了金融领域的数字货币技术革命。区块链 2.0 是以太坊。以太坊开发的“智能合约”，使得区块链不仅能实现现金的功能，还能实现诸如贷款或债券等多种金融工具。以太坊智能合约平台现在市值约 840 亿元（来源：https：//coinmarketcap.com/）。

区块链的另一个前沿创新被称为“权益证明（POS）”。目前多数区块链使用“工作量证明（POW）”，这需要大量的电力进行哈希运算来争夺记账权，而且效率不高。相比之下，POS 共识机制，就是根据用户持有代币数量，以及用户占有这些代币的时间来决定记账权和分配区块奖励。这大大减少了争夺记账权而消耗的电力，同时提升了效率。

区块链的关注者认为，这项技术将激发每个行业的创新，并推动我们的通信和交易的大规模变革，但这在目前的状态下是不可能的。正如图 1 所示，随着需求的增加，区块链面临的另一个问题是可扩展性。我们目前现有的区块链无法安全地处理 Visa 等中心化支付系统发生的交易量，Visa 可处理 56000TPS 的交易。比特币和以太坊 10-20TP 的吞吐量与之相比还相差很多数量级，甚至离 IoT 微型支付所需的 TPS 也差很远。然而具有这种能力的区块链系统通常会牺牲安全性和去中心化特性，这是区块链技术必须提供的关键特性。目前基于区块链网络的可扩展性问题为其广泛的应用带来了重大限制，所以我们必须首先开发一个能够处理大量交易而不影响安全性和去中心化特性的底层区块链。

1.3.QuarkChain 的设想

QuarkChain 引入了全新的基于分片技术的区块链架构，旨在用区块链技术满足全球范围商业活动的需要。我们的核心成员从开发十亿 TPS 的集中式大型系统的经验中受到启发，将这些技术和思路应用于区块链，创建了针对区块链可扩展性问题的独特解决方案。该解决方案旨在大幅扩大区块链的可用范围而不损害其安全性和去中心化的特点。

我们的设计将推动区块链进入下一代，将当前的 TPS 提高数千倍，达到预计的 100,000+ TPS，同时保持安全性和去中心化。我们正在建设的网络大幅减少拥堵，因此每个人都能负担得起使用这个网络的费用。我们相信这种网络适用于每个需要更高 TPS 的行业，并鼓励这些

行业在不久的将来采用我们的区块链网络作为底层进行开发。最终，QuarkChain 的目标是建立一个高吞吐量的平台类支持分布式社交媒体、高频交易、物联网（IoT）、游戏和金融支付等应用。

2.区块链的挑战

区块链目前面临三大挑战：安全、去中心化和扩展性。

2.1.安全问题

作为点对点交易网络，首要任务始终是安全。区块链，顾名思义，是一连串的数据连接成的“块”，这使得它具有一些提供安全手段的固有特性。尽管区块链具有以上的安全属性，但还是存在漏洞、以及一些新的恶意攻击，因此在开发应用时需要选择一个安全的底层区块链平台。

实际上区块链分布在一个不断更新的并保持在一个特定的共识（如 POW 或 POS）同步的点对点网络中。基于 POW 的区块链需要至少控制 51%的全网算力来执行双花攻击。这种攻击很大程度上取决于网络的分散化程度，即区块链网络越分散，攻击就越难进行。如果区块链节点充分的分散，对于单个实体（单个矿工或单个矿池的所有者）来说，获得超过 51%的全网算力的代价是极其昂贵。

2.2.去中心化问题

自 2013 年以来，许多区块链项目已经初具雏形。 与中心化情况不同，去中心化存储和交易可以大幅降低成本，所以任何公司，不仅仅是大公司，甚至是个人，都可以利用这项技术。 正如我们前面提到的，去中心化也可以提供区块链安全性，然而权力下放也带来了挑战。 例如，POW 机制下全网算力的增加导致少量算力的矿工只有非常低的概率能获得区块奖励，但是矿池的出现让少量算力的矿工可以通过加入矿池来参与挖矿活动，无论单个矿工是否成功获得记账权，都可由对矿池的贡献来获得相应比例的奖励，而不是等待很长时间去争夺记账权。矿池鼓励了集中化，这成为以 POW 为共识机制的区块链的风险。 例如，截至

2013 年，前六大矿池拥有比特币全网 75%的算力。

2.3.可扩展性问题

下面我们回顾一下现有的解决可扩展性问题的方法。

2.3.1.多区块链

解决可扩展性问题的一种方法是独立运行多个区块链（例如，比特币，比特币现金，莱特币，以太坊），尽管这会降低每个区块链上的交易需求，但这样做有几个限制。如果两个区块链使用相同的共识算法，则算力可能不平衡，在算力较少的链中，容易被获得足够的算力来进行双花攻击。拥有多个区块链也将限制跨链交易，在交易所进行数字资产交换是跨链交易的常用方式，然而它已成为加密数字资产最不安全的地方，因为已有很多交易所被攻击。此外，交易所的交易还会带来额外的交易费用和更长的处理时间。用户还需要为跨链交易维护多个账户或地址，这引入了私钥管理问题和进一步的安全问题。

2.3.2.闪电网络

闪电网络是另一种缓解区块链可扩展性问题的方法。基本思想是固定的一组当事人之间的频繁交易，直到所有各方都完成交易然后，其中一方将只发布最终结果，而无需在链上生成多个交易记录。一个闪电网络一般需要两个交易体来创建或销毁一个接受链下交易的支付通道。链外 TPS 在理论上是无限的。然而，闪电网络只适用于固定的一组当事人之间频繁的交易，而如果用户的交易目标是随机的并且交易行为偶尔发生的话，那么就会导致低效率。透明度是另一个问题，因为交易是通过闪电通道而不是主区块链来追踪的。一些链外解决方案依赖于受信任的第三方，如具有区块链的特点的支付宝。这意味着我们将建立另一种中心化支付方式，而世界上已经有很多类似的支付方式。

2.3.3.分片

最初分片技术是将大型数据库中的数据分成较小的部分，这是集中式系统解决可扩展性问题的最常用方法之一。例如，BigTable 系统和 Cassandra 数据库是在非区块链世界中解决

大吞吐量问题两个例子。

值得注意的是，以太坊采用分片技术来扩大规模，其一期开发工作即将完成。然而，在现有区块链上采用分片技术是很复杂的，据估计需要 3 至 5 年的时间才能在以太坊上能够完全支持其它基本分片特性（例如跨分片交易）。主要挑战包括跨分片交易，单个分片管理等安全问题，以及进一步的可扩展性问题也没有得到解决。也有如 omniledger 号称引入复杂的共识协议达到 100000 TPS 的不同方案。在其他一些情况下，用户的帐户也被分片，结果用户可能要操作多个账户才能与他人进行交易。

2.4. “不可能三角”的权衡

虽然“不可能三角”（安全性、去中心化、可扩展性）对区块链都很重要，但它们之间也存在可以有一些相关性和权衡取舍问题。 如图 2 所示，如果想增加安全性或者隐私性，每次交易都需要大量的数据，这意味着更低的交易速度和更大的存储量。

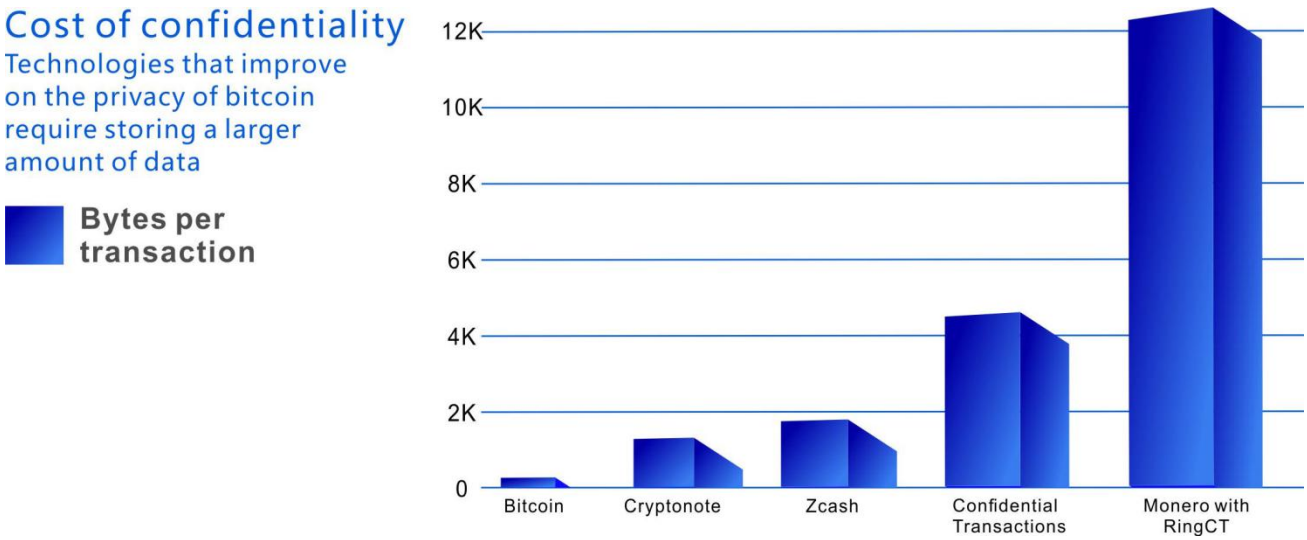


图 2 安全性和可扩展性（TPS）之间的权衡说明

（来源：Danny Yang, Jack Gavigan, Zooko Wilcox, “Survey of Confidentiality and Privacy Preserving Technologies for Blockchains,” R3, Nov. 2016）

随着需求的不断增加，区块链的终极目标是在保持安全性和去中心化程度在一个适当的水平，尽可能的提高可扩展性。

3.QuarkChain 技术

3.1.设计原则

QuarkChain 的设计主要基于以下原则：

●在保证安全性和去中心化的同时提高可扩展性
● 为用户体验质量（QoE）实现无缝跨链交易
●为客户提供简单的账户管理
● 开放标准以支持各种 Dapp
●建立一个激励驱动的生态系统

3.2.系统架构

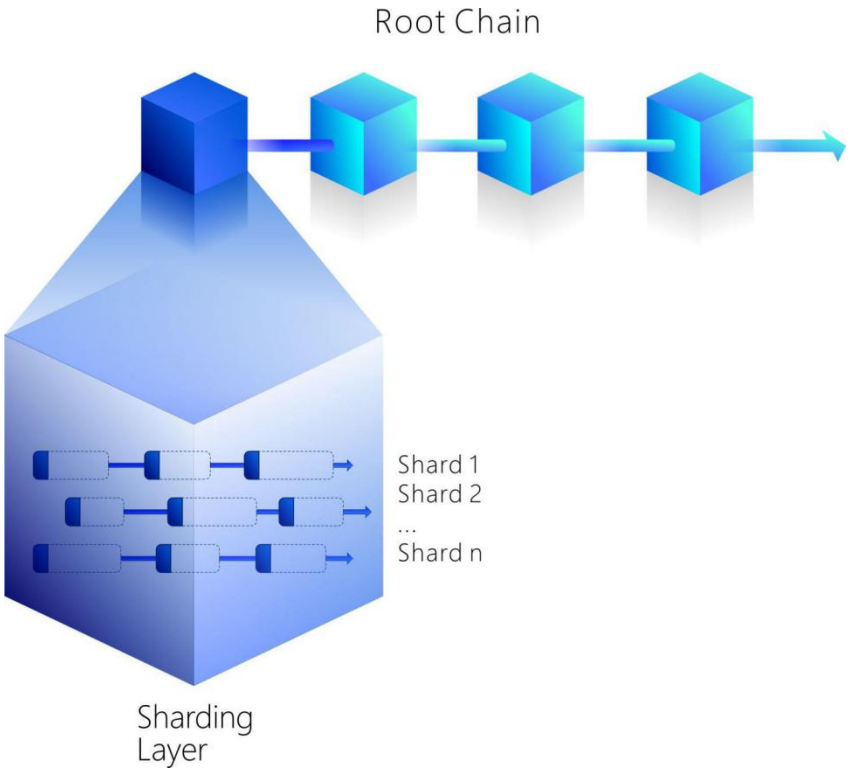


图 3 QuarkChain 的两层区块链的示意图

其中每条分片处理一个事务的子集合，而根链则通过在根链中包含分区的区块头来确认分区。

对于当前的区块链技术，链中每个区块都有两个基本功能：

●记账，包括记录目前的区块状态，进行交易并记录结果。数据密集型是分类账的关键属性——既要维护当前分类账，又要详细描述交易细节，包括来源、目的地、金额、执行代码等。数据可以被包装成一个块，区块大小和尺寸限制是当前区块链发展的瓶颈。

●确认，确认交易结果，通过计算达到预期的难度（POW）获得区块打包权。这样可以确保攻击者通过挖掘另一个分叉来改写交易在经济上是低效的。确认本身是一项计算密集型任务。

基于此，QuarkChain 采用分而治之的思想，将两个主要功能分别在两层实现，从而在提高可扩展性的同时保证安全性。详细设计如下：

●QuarkChain 包含一个有弹性的分片层，其中包含一系列分片。每个分片独立是处理所有事务的子集。因此，随着分片数量的增加，分片层可以同时处理更多的事务。其结果是系统容量随着分片数量的增加而增加。

●QuarkChain 还有一条根链（也叫主链），用于确认来自分片层的所有区块。根链不处理任何交易（因为它不是经济高效的），根链具有足够的算力支持来保证安全。

●QuarkChain 区块网络也被设计为支持能够动态增加分片。添加更多的分片很容易，而且很快，而用户几乎感觉不到这一点（如果在网络堵塞之前添加了分片，用户可能会感觉到交易的速度更快）。

	链名称	块名称	间隔区间	主要功能
上层	根链	根块	几分钟内	确认
下层	分片	小块	几秒内	记账

表 1 QuarkChain 链的结构

3.3.协同挖矿

协同挖矿的目标是通过设计激励机制和难度算法使得算力能均匀的分配到网络上。

●算力在分片之间均匀分配。这确保所有分片被均匀开采，因此系统吞吐量（即 TPS）随着分片数量的增加而增加。

●根链在全网算力中占有很大的比例（超过 50%）。这可以防止双花攻击，而恶意矿工需要至少 50%* 50%= 25%以上的算力来执行攻击。

值得注意的是，QuarkChain 网络有多个分片和一条根链。每条区块链提供不同的奖励和困难。矿工们可以选择任何区块链以最优的算力价格获得回报。这创造了一个开放的市场经济模型，区块链是一个卖方，货物是区块奖励（代币），而矿工是一个以算力为货币的买方。我们希望设计一种销售模式，即使市场上的每一方都追求自己的利益，但各方的集体行为都可以造福于所有人。

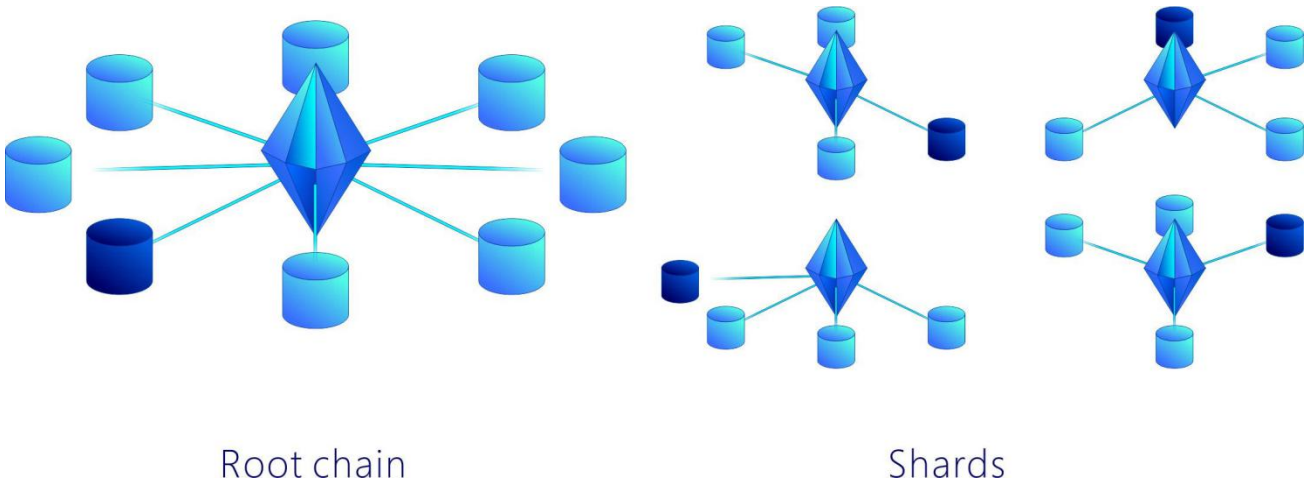


图 4 协同挖矿的例子

其中根链中的块具有足够大的奖励和难度来保护所有分片中的块（以及其中的交易）。

3.4.共识算法

为保护所有交易，QuarkChain 系统中的根链和分片运行以下共识算法：

●与比特币和以太坊相同，根链运行 POW 算法。这意味着当分叉发生在根链上时，长度（或总难度）最长的分叉将存活下来。

●每个分片运行一个称为根链优先 POW 共识算法。给定一个分片上的两个分叉，为了确定哪个分叉能够存活，一个节点在比较分叉之前会比较它们对应的根链。如果分叉的根链较长，那么无论叉子多长时间，叉子都能存活。通过这种共识算法，双花攻击者必须创建：

a. 恢复交易的小块

b. 包含小块的较长根链分叉。

这种攻击难以执行，因为攻击者必须获得整个网络至少 50%（根链上的全网算力）* 51%= 25%全网算力（如图 5 所示）。

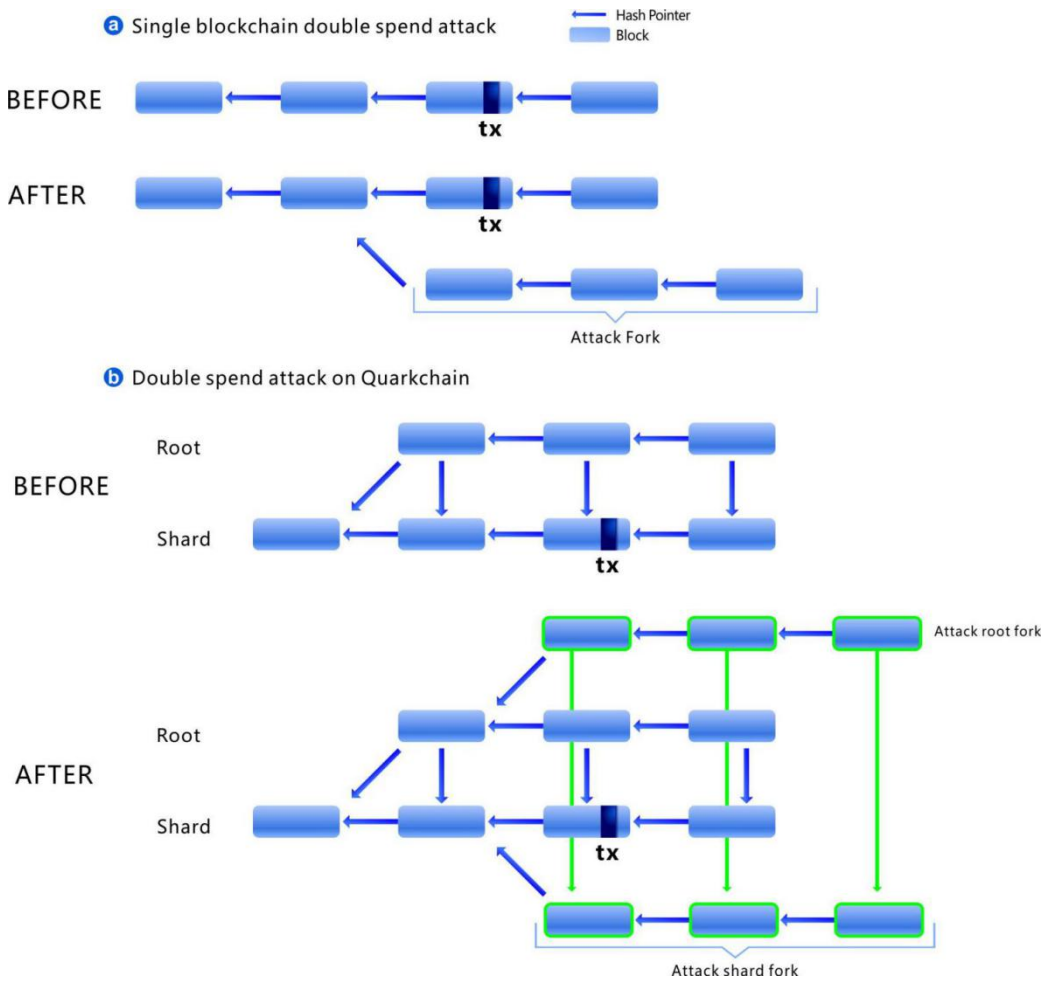


图 5 双花攻击图解

3.5. QuarkChain 网络的早期验证

由于 QuarkChain 网络非常复杂且高度动态，因此几乎无法提供分析方案。 为了验证我们的设计，我们采用网络模拟来模拟一个包含 18 个节点和 8 个分片的网络，这使我们能够在早期验证我们的激励机制和难度算法。

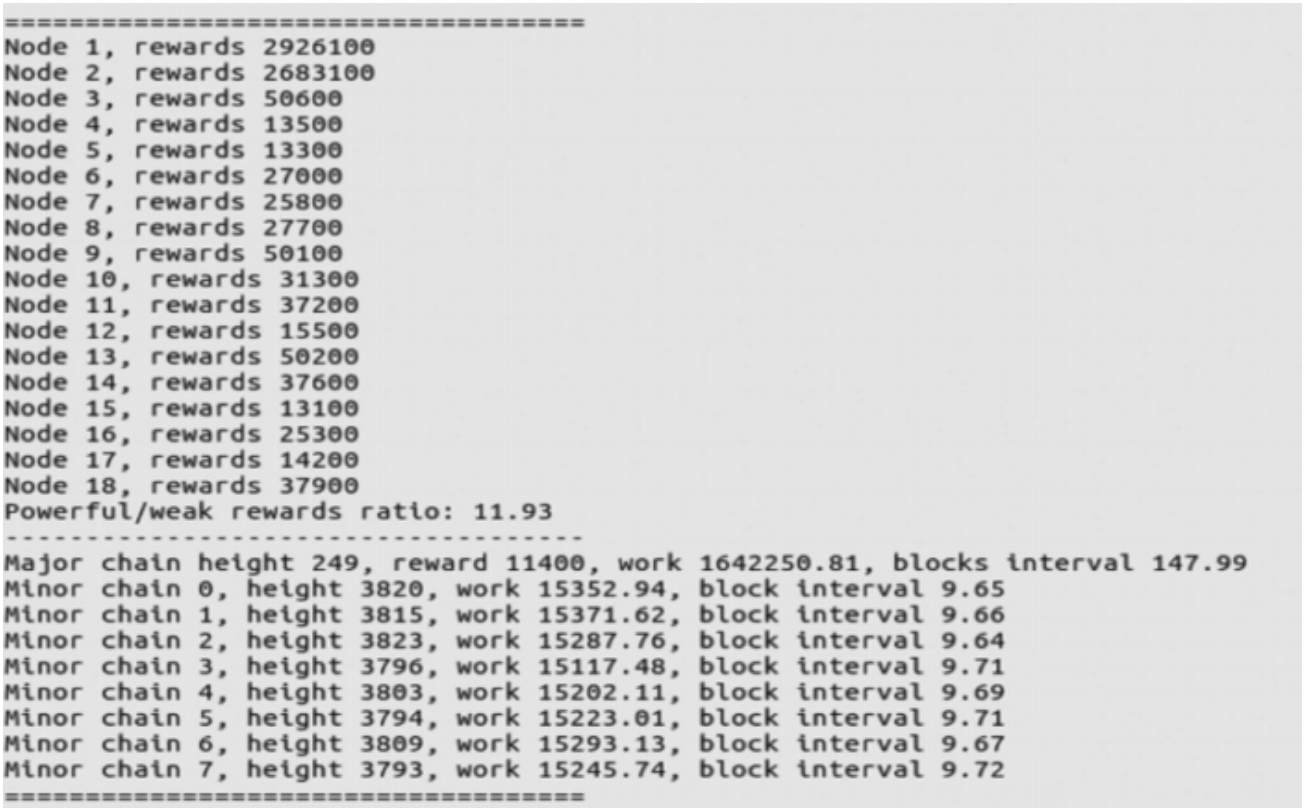


图 5 显示了协作挖矿的模拟结果的快照

模拟中有 18 名矿工，其中两名矿工的算力是其余 16 名矿工的 100 倍。

QuarkChain 系统有 8 个目标出块时间为 10 秒的分片和一个目标出块时间为 150 秒的根链。通过分析，我们得到了一些有趣的结论：

●所有分片的高度约为 3800，并且彼此非常接近。另外，它们都具有类似的工作量（即预期哈希生成一个块的量），块间隔非常接近 10 秒。这意味着所有分片被均匀开采，使得吞吐量约为单一链情况的 8 倍。

●根链的工作量大约为 1.6M，接近我们预期的 1.8M（占全网算力的一半，因为所有分片每 10 秒工作量为 15K，根区块链出块速度比分片长 15 倍）。

4.QuarkChain 在区块链中的定位

QuarkChain 揭示了区块链设计的全新路径。在本节中，我们讨论它与其他现有技术的关系及定位。

4.1.单链和多链 QuarkChain 的关系

QuarkChain 在根链上的 50%的算力分配是可重新配置的（例如，25%或 75%）。通过调节算力，QuarkChain 可以与现有的区块链系统类似。

●如果根链的算力为全网算力 100％，那么 QuarkChain 网络就变成了单一区块链系统，因为在分片上没有矿工，所有的矿工只会挖掘根链，弱矿工可能会加入矿池。此外，根链区块可以包括多个小块，从而使得根块基本上是一个不限区块大小，最终组成单链区块链系统。

● 如果根链的算力为 0%，那么 QuarkChain 网络就成为一个多重独立的区块链系统。QuarkChain 的每个分片都可以视为独立区块链。它当然更具可扩展性，而且由于弱矿工不需要加入采矿池，因此它也更加分散。然而，这是非常不安全，由于算力分散，恶意攻击者可以容易地对 100 条分片中的一个区块链执行双花攻击，只需要全算算力的 1/200。

4.2.QuarkChain 的安全性、去中心化和可扩展性

QuarkChain 在根链上至少拥有 50%算力分配增强了网络的安全性。另外，QuarkChain 比单链区块链系统更分散，因此 QuarkChain 也是安全和去中心化的。

●大幅度提高网络的吞吐量

我们采用先进的分片技术（子链层）来提高系统容量，并可以根据需要动态提升系统处理能力，以便每秒处理更多交易。

● 比单链区块链系统更分散

随着单链区块链系统的算力增加，弱矿工的预期回报时间显着增加，他们必须加入采矿池以及时得到回报。这极大地鼓励了集权，并且伤害了区块链的核心价值。 QuarkChain 旨在更加分散化，因为较弱的矿工不需要加入采矿池来收集奖励。

●安全

QuarkChain 网络中的所有交易都受到全网 50%算力的保护，而双花攻击需要至少 25%的全网算力。这虽然比单区块链的 50%小，但由于 QuarkChain 更加分散，恶意矿工在 QuarkChain 网络中得到 25%的全网算力是很困难的。

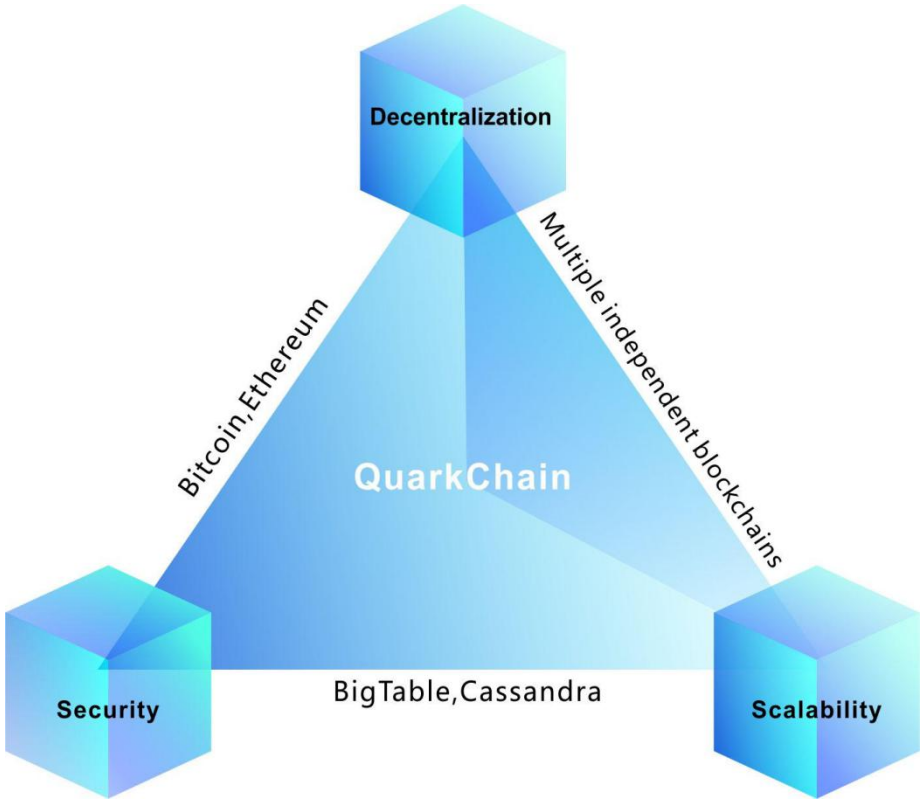


图 6 QuarkChain 兼顾安全，可扩展和去中心三大重要特征。

5.QuarkChain 的核心特征

不同于许多通过提高现有系统可扩展性的解决方法，QuarkChain 从一开始就为了高性能来设计的--类似于集中化高性能系统的方案。 QuarkChain 具有以下重要的价值观：可用性（快速，简单），去中心化（公众可参与），安全（可靠）。下面列出了 QuarkChain 的核心特征。

5.1.抗中心化横向扩展性

为了构建一个不受恶意攻击影响的点对点网络，传统的区块链技术要求每个节点完全验证所有区块并拒绝任何无效的区块。同样，验证所有小块和根链块的 QuarkChain 中的节点称为超级节点。如果 QuarkChain 中的每个节点都作为超级节点运行，则 QuarkChain 可以具有与传统区块链相同的安全级别。

但是，在高吞吐量区块链系统中运行超级节点是非常昂贵。例如，一个 250 字节 1M TPS 的事务需要 2 Gbps 的网络带宽，这对许多用户来说成为一个巨大的障碍。另外，流量每天会产生大约 20 TB 的数据或者每年产生 7PB 的数据。超级节点对 CPU，存储，内存和网络带宽提出了高要求，而且这些要求可能只能由商业机构提供（例如，公司在其数据中心使用强大的工作站）。这极大地阻碍了去中心化，损害了区块链的核心价值。

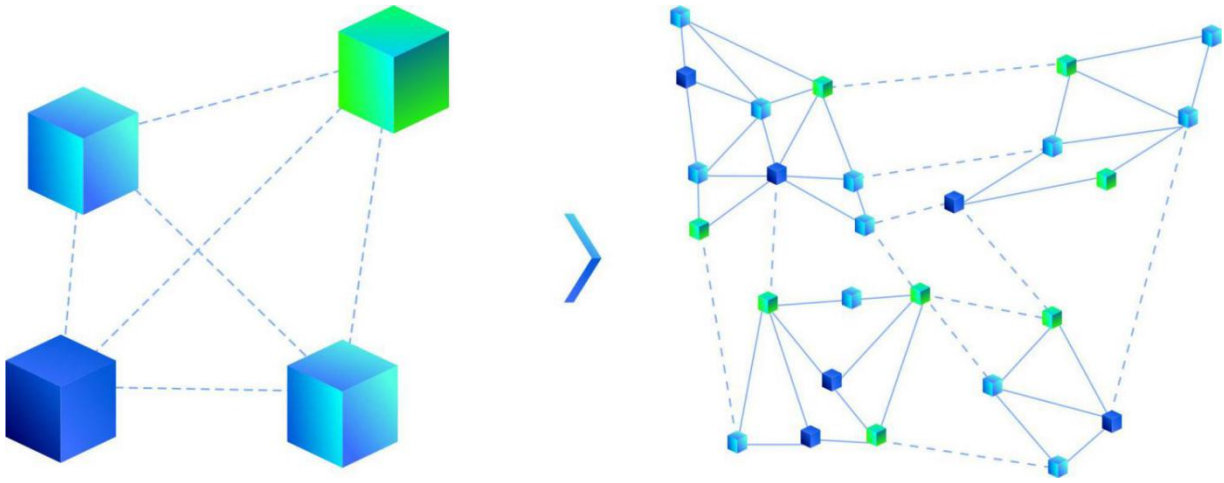


图 7（a）

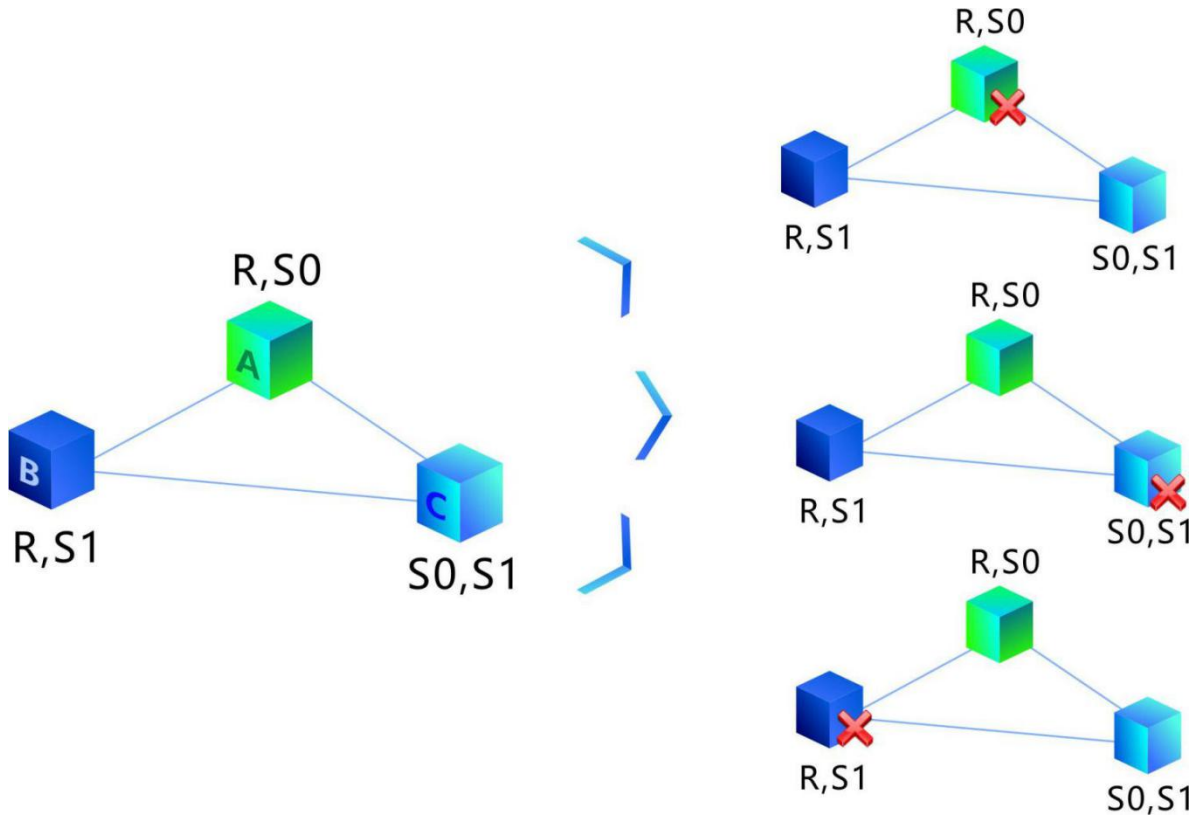


图 7（b）

图 7（a） 说明 QuarkChain 网络的横向扩展性，其中四个超全节点（左）被四个节点集群（右）取代，其中每个集群中的节点彼此诚实。 （实线表示诚实的连接，虚线表示不可靠的连接）

图 7（b）显示了有 2 个分片的 QuarkChain 集群的高可用性，甚至一个节点崩溃（右），集群仍然可以充分验证网络。例如，假设有 2 分片的系统，A 验证分片 S1 和 S0，B 验证分片 S1 和根链，C 验证分片 S0 和根链，其中 A，B，C 都是互相可信的，那么，B，C 可以形成集群，能够充分验证任何交易。

QuarkChain 通过允许集群中的多个诚实节点作为完整节点运行来解决这个问题。群集中的每个节点只验证一个子集。只要它们的子集的联合覆盖根链和分片，我们就可以证明它们能够完全验证整个区块链而不需要建立昂贵的超级节点。另外，如果其中一个节点在群集中崩溃，其余节点仍然能够完全验证任何块，因为它们中的任何两个形成另一个群集，从而实现这样的集群的高可用性。

此外，为了鼓励在网络中形成这样的集群，QuarkChain 将激励节点回答关于随机块的信息（例如，随机选择的分片或根区块链上的随机块的哈希信息作为问题）。这样的问题将鼓

励节点存储全网的账本，短时间从网络上按需下载随机块来回答将是低效的。

5.2.高效、安全的分片交易

在 QuarkChain 系统中，我们将交易分为两类：

●分片内交易，其中交易的输入和输出地址位于同一分片中。
●跨分片交易，其中交易输入和输出地址位于不同的分片中。

分片内交易很简单，因为分片已经包含分片的完整账本信息。由于两个分片之间的同步问题，跨分片交易很困难。 QuarkChain 完全支持跨分片交易，在某种意义上说：

●任何用户都可以随时发出跨分片交易。
●跨分片交易可以很快被确认。
●随着分片数量的增加，跨分片交易的吞吐量可以线性提升。

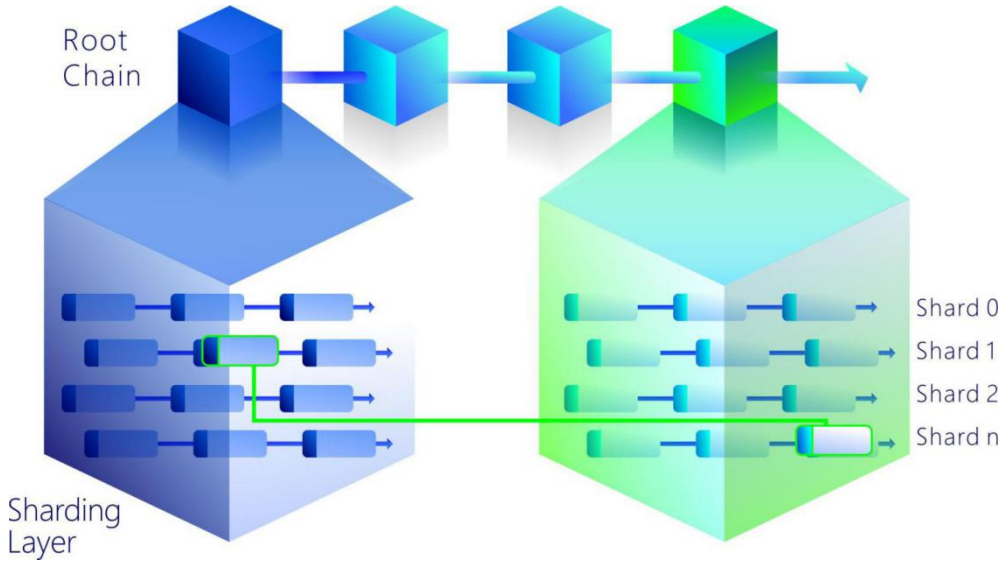


图 8 跨分片交易的图示

只要跨分片交易被根链确认，交易就可以输出。

QuarkChain 的这些关键功能创造了高性能传输网络，任何人都可以以经济高效的方式轻松执行任何交易。

5.3.简易的账户管理

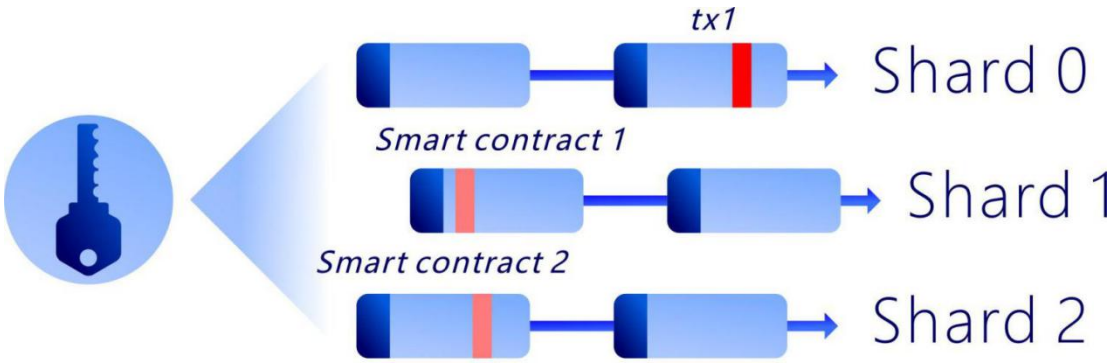


图 9 简易账户管理的示意图

其中一个拥有私钥的帐户可以在任何分片上执行交易。

与用户可能需要在不同分片中创建多个帐户，以便与网络中的所有用户或者智能合约交互的其他解决方案不同，QuarkChain 系统极大地简化了帐户管理，用户只需要一个帐户即可管理所有分片上的地址以及能与所有用户无缝的互动。另外，我们将创建一个智能钱包应用程序，该应用程序将自动为用户执行跨分片或分片内交易（包括智能合约），并且用户不需要知道交易在哪个分片中进行。 一些用户可能会选择高级的方法来管理他们的地址，例如：允许支付总是通过分片内交易，从而使交易被快速确认。

5.4.跨链交易

凭借我们的设计架构，跨链交易变得便捷。 由于我们只维护一个根链，所以来自另一个区块链的交易可以通过适配器转换代币来实现，然后像 QuarkChain 一边执行跨分片交易那样执行交易。 另一种方法是将另一个链作为分片容纳进来，使得跨链交易变成跨片交易。

6.QuarkChain 的操作系统

6.1.链上和链下交易

QuarkChain 不仅支持高扩展性的链上交易，它还可以同时采纳链下交易。一些应用程序需要链上和链下不同的处理方式。例如，一些交易需要访问外部数据（不在区块链上）。QuarkChain 双层结构使得这种链上和链下处理非常灵活，这将使我们的系统支持更多机遇和应用。

6.2.智能合约

QuarkChain 将通过以太坊虚拟机（EVM）支持智能合约。 EVM 是智能合约中使用最广泛的执行引擎。大多数基于 EVM 构建的现有 DApp 可以直接部署在 QuarkChain 平台上。此外，利用 QuarkChain 高扩展性的特点，我们将提供额外的可扩展接口，如正在执行的联系人分区，通过不同的链传送智能合约的具体数据。

6.3.帐户管理

由于用户可以通过私钥管理分片和根链所有地址，因此用户理论上上将拥有与分片数量相同的地址数量。如果分片的数量很大（例如，数千或数万），则用户可能在多个分片中具有多个余额，因此管理所有分片中的所有余额可能是不方便的。我们通过定义以下两种类型的账户进一步简化账户管理：

●主帐户：主帐户是默认分片中用户的地址和余额。
●次帐户：次帐户管理剩余分片中用户的其他地址。

为了简化管理，如果交易需要（例如，访问不同分片中的智能合约），并且如果在交易之后在次账户中存在余额，则用户的大多数交易将从主账户发起，暂时转移到次账户中的地址进行交易，交易结束后余额将被移回主账户。这可以确保用户的余额大部分时间都在主账

户中，因此用户不需要管理次账户地址中的余额。此功能由智能钱包执行，由 QuarkChain 团队提供，并作为开源项目。

6.4.智能钱包

QuarkChain 中有两种典型的交易：

●将与地址相关的一些代币转移到另一个可能在同一分片中的地址
●在特定的分片中执行智能合约

使用这些交易时，智能钱包将简化帐户管理，以便用户不需要知道底层详细的分片/跨分片操作：

●对于转账交易，智能钱包将自动检测用户的主账户（用户在默认链中的地址），并相应地执行链/跨分片交易
●对于智能合约交易，如果智能合约不存在于用户主账户的同一分支中，则智能钱包将自动将代币转移到智能合约所属的分部中的用户次账户。智能钱包将在分片中执行智能合约交易。如果次帐户中有余额，智能钱包自动将余额从次帐户转移到用户的主帐户（可选）。

7.QuarkChain 生态系统

7.1.代币经济

QKC 作为原生加密数字货币是 QuarkChain 网络生态系统的主要组成部分，其设计目的是仅用做 QuarkChain 网络上的数字代币。QKC 最初将由团队在以太坊上发布符合 ERC-20 标准的数字代币，并在最终在 QuarkChain 主网启动时将这些数字货币迁移到 QuarkChain 主网上。如上所述，QuarkChain 网络的主要目标是解决当前区块链系统的可扩展性问题。

QKC 是一个不可退还的功能实用程序令牌，将作为 QuarkChain 网络参与者之间的交换单位。引入 QKC 的目标是在 QuarkChain 网络生态系统内互动的参与者之间提供便利安全的支付和结算模式。QKC 不以任何方式代表基金会，其分支机构或任何其他公司，企业或企业的任何股份，参与，权利，所有权或利益，QKC 也不会授权代币持有人承担任何费用，股息，收入，利润或投资回报，并非旨在构成新加坡或任何相关司法权区的证券。 QKC 只能在 QuarkChain 网络上使用，并且 QKC 的所有权除了有权使用 QKC 作为启用 QuarkChain 网络的使用和交互的手段之外，不具有任何明示或暗示的权利。

QuarkChain 关键应用场景将集中在金融科技领域和游戏产业。QuarkChain 的代币将扮演非常重要的角色，它体现 QuarkChain 的价值，如下所述：

●价值载体

加密货币的本质是价值的载体，这是 QKC 最重要的属性。

●交易货币

在 QuarkChain 网络上使用某些设计功能时 QKC 被作为必需的“燃料”，QKC 能提供经济激励措施，鼓励参与者在 QuarkChain 网络上贡献和维护生态系统。需要计算资源来运行 QuarkChain 网络上的各种应用程序和执行交易，以及区块链上附加块/信息的验证和验证，因此这些服务和资源的提供者将需要为这些资源的消耗（即在 QuarkChain 网络上进行“挖掘”）以保持网络完整性，QKC 将用作交换单位来量化和支付所消耗的计算资源的成本。

与以太坊类似，QuarkChain 网络上的每笔交易都需要支付交易费用。由于 QuarkChain 具有强大的事务处理能力，交易费用将非常低。交易费用只能由代币支付。 QuarkChain 网络支持智能合约，QuarkChain 网络的智能合约交易通过向合同地址发送消息来完成。

●贡献奖励

作为一个点对点系统，利用经济手段产生积极的反馈可以促进系统的不断发展。QKC 将作为奖励来分发，激励社区为该系统作出持续贡献。 QuarkChain 网络的用户和 QKC 的持有人在没有积极参与的情况下将不会收到任何 QKC 奖励。

QKC 是 QuarkChain 网络不可或缺的一部分，因为没有 QKC，就无法激励用户消耗资源提供服务为 QuarkChain 网络的整个生态系统带来益处。

7.2.业务发展

7.2.1.去中心化移动应用（DApps2go）

我们相信基于移动设备的 DApp 将更常见，更具生态价值。2014 年全球有 44.7 亿人使用手机和 68%的移动互联网用户。由于移动网络处理区块链能力低，基于移动的分布式应用程序目前非常有限。

QuarkChain 具有强大的吞吐能力来完全支持移动 DApps（DApps2go 计划），其基础设施设计以移动应用为导向。此外，我们将提供链上开发工具来创建一个友好的 Android 环境，使 DApps2go 的开发尽可能简单。我们还将分配大量的代币来激励在 QuarkChain 上构建 DApp 的开发者。我们轻松的横向扩展区块链技术使得区块链上的社交网络，在线存储，游戏和共享经济成为可能。例如，开发人员可以在 QuarkChain 上构建一个完全分散的点对点共享 DApp。它可以轻松处理每年 74 亿次的出行，这个数字是世界上最大的共享出租车公司在 2017 年完成的。QuarkChain 同时还将取消拼车服务费用，以降低为客户使用出行服务的成本。QuarkChain 是建立共享经济业务的理想平台。

7.2.2.MVP（最小可用产品）原则下的快速链上迭代

QuarkChain 旨在通过采用精益创业方法学来构建 - 测量 - 学习这反馈循环，以此缩短

产品开发周期。因此，我们允许开发人员在分片上运行最小可行产品。凭借 QuarkChain 强大的处理能力，开发人员可以在测试网上部署和测试其产品，并收集快速反馈。 QuarkChain 测试网上的 Onchain Demo Show 区将提供超级平滑和快速的测试体验，帮助 DApps 的产品经理和开发人员快速验证他们的想法。

7.2.3.面向需求的业务场景

QuarkChain 会为世界带来真正的区块链商业方案。这类企业必须对高吞吐量区块链拥有强大的需求，并能够真正解决现有的客户或业务需求。验证将是一个很好的区块链应用领域，它充满了挑战性和成本低效的问题。诸如国家身份证明文件背后的高防伪技术等现有手段对于中小型企业而言可能过于昂贵。然而，借助分布式账本和先进的加密保护私钥，我们相信可以通过提供价格合理且易于使用的防伪解决方案来支持小企业主的商业需要。该解决方案还可用于教育系统验证文凭和确认实验室原始数据。 QuarkChain 将始终与这些企业保持开放和协作，并帮助他们扩大业务。

7.2.4.QuarkChain 物联网

区块链应用于物联网（IoT）有着巨大潜力。使用 QuarkChain 可以降低成本，并且有助于快速实现物联网转移的价值。IoT 通常包含大量设备，并且可能会同时发生大量事务。QuarkChain 将作为一个平台，为物联网应用提供大量低成本的设备以及在高速交易中扮演重要角色。利用智能合约还可以实现数据的自动采集和处理，从而建立更多的数据维度。

7.2.5.用于 AI 和大数据的 QuarkChain

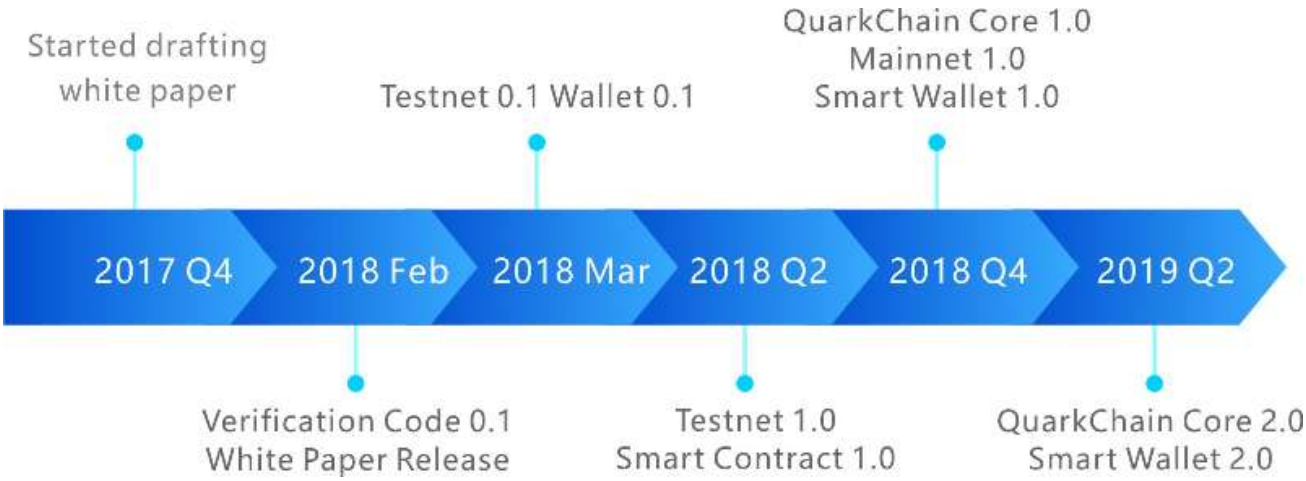
区块链为经济交易提供了一个数字平台，因此它与人工智能（AI）密切相关。区块链可以很多方面使用 AI 技术，例如，通过强化学习，智能钱包可以更高效，以便可以将普通交易的双方分配到同一条分片或至少更近的分片中，以降低交易成本。然而，这要求区块链开发具有可重新设计的能力，而 QuarkChain 恰恰提供了这一功能。

区块链将真正涉及到大数据，它会生成时间和空间数据。随着区块链增长，数据量快速增长。无论是私有链还是公有链，这些数据都会为公司或整个世界经济带来巨大的价值。基

于 QuarkChain 平台，可以开发许多数据挖掘算法和经济模型。 QuarkChain 愿意与数据分析师和经济学家合作开发新的经济模型，而且为这些模型将带来有价值的反馈，以进一步提高 QuarkChain 设计。

考虑到开发理念，我们谨慎地选择 2-5 个不同行业的业务合作伙伴，在这些行业中，高吞吐量的区块链可以最大限度地发挥起来。

8.路线图和时间线



●2017 年第四季度：完成白皮书初稿。

●2018 年 2 月：我们发布了一个白皮书版本，并开发了 verification code0.1，主要用作我们系统的概念验证;。

●2018 年 3 月：我们发布了 Wallet 0.1 和 Testnet 0.1。 Testnet 0.1 支持包括分片和跨分片交易在内的基本交易。

●2018 年第二季度：我们将发布 Testnet 1.0，并提供智能合约支持。

●2018 年第四季度：我们将发布 QuarkChain Core 1.0，Mainnet 1.0 以及 Smart Wallet 1.0。 QuarkChain Core 1.0 将提供 QuarkChain 的基本功能和基本优化。我们计划同时启动我们的主网。

●2019 年第一季度：我们将发布 QuarkChain Core 2.0，Mainnet 2.0 以及 Smart Wallet 2.0。 QuarkChain Core 2.0 将进一步优化 QuarkChain Core 1.0 并启用集群功能，从而使群体廉价节点可以形成群集并作为完整节点运行。

9.风险

您承认并同意购买 QKC，持有 QKC 以及使用 QKC 参与 QuarkChain 网络存在很多风险。在最坏的情况下，这可能会导致购买的全部或部分 QKC 的损失。

9.1.不确定的法规和执法行为

许多司法管辖区的 QKC 和分布式账本技术的监管状况尚不清楚或未得到解决。虚拟货币的监管已成为世界所有主要国家监管的主要目标。无法预测监管机构如何，何时或是否应用现有法规或制定有关此类技术及其应用（包括 QKC 和 QuarkChain 网络）的新规定。监管行为可能会以各种方式对 QKC 和 QuarkChain 网络产生负面影响。如果监管行为或法律法规的变化使其在此类司法管辖区内运营非法，或在商业上不希望获得运营所需的监管批准，基金会（或其附属机构）可能会停止在某一辖区的运营。在这样的管辖权。在咨询了广泛的法律顾问并持续分析虚拟货币的发展和法律结构之后，基金会将对销售 QKC 采取谨慎的态度。因此，为了销售令牌，基金会可以不断调整销售策略，尽可能避免相关的法律风险。对于代币销售，基金会正与新加坡精品公司律师事务所 Tzedek Law LLC 合作，在区块链领域享有盛誉。

9.2.信息披露不充分

截至目前，QuarkChain 网络仍处于开发阶段，其设计理念，共识机制，算法，代码及其他技术细节和参数可能会不断更新并经常更新和更改。虽然本白皮书包含了与 QuarkChain 网络有关的最新信息，但它并不完全完整，可能仍会由 QuarkChain 团队不时调整和更新。QuarkChain 团队没有能力也没有义务向 QKC 的持有人通报关于开发 QuarkChain 网络项目的每个细节（包括开发进度和预期里程碑），因此信息披露不足是不可避免的和合理的。

9.3.竞争对手

各种分散应用程序迅速崛起，行业竞争日益激烈。有可能建立替代网络，利用 QKC 和/或 QuarkChain 网络的相同或相似的代码和协议，并尝试重新创建类似的设施。 QuarkChain 网络可能需要与这些替代网络竞争，这可能对 QKC 和/或 QuarkChain 网络产生负面影响。

9.4.人才流失

QuarkChain 网络的发展取决于现有技术团队和专家顾问的持续合作，他们在各自的领域都非常有知识和经验。任何成员的损失都可能对 QuarkChain 网络或其未来发展产生不利影响。此外，团队内部的稳定性和凝聚力对 QuarkChain 网络的整体发展至关重要。团队内部的冲突和/或核心人员的离开可能会发生，从而对未来的项目产生负面影响。

9.5.未能发展

QuarkChain 网络的开发将不会执行或实施按计划出于各种原因，包括但不限于任何数字资产，虚拟货币或 QKC 价格下跌，不可预见的技术困难以及活动开发资金短缺。

9.6.安全漏洞

黑客或其他恶意团体或组织可能会尝试以各种方式干扰 QKC 和/或 QuarkChain 网络，包括但不限于恶意软件攻击，拒绝服务攻击，基于共识的攻击，Sybil 攻击，smurfing 和欺骗。此外，第三方或基金会会员或其分支机构有可能有意或无意地将弱点引入 QKC 或 QuarkChain 网络的核心基础设施，这可能会对 QKC 或 QuarkChain 网络产生负面影响。此外，密码学和安全创新的未来是高度不可预测的，密码学或技术进步（包括但不限于量子计算的发展）的进步可能会给 QKC 和 QuarkChain 网络带来无效的密码共识机制，支撑该区块链协议。

9.7.其他风险

上面简要提及的潜在风险并非详尽无遗，并且与您购买，持有和使用 QKC 相关的其他风险（如条款和条件中更加具体的规定），包括那些基金会无法预料。这些风险可能会进一步实现为意料之外的变化或上述风险的组合。您应该对基金会，其分支机构和 QuarkChain 团队

进行全面的尽职调查，并在购买 QKC 之前了解 QuarkChain 网络的总体框架，使命和愿景。

www.quarkchain.io
contact@quarkchain.io