PENROSE

面向新零售的商用区块链架构系统

V1.0

2018 年 7 月

PENROSE

面向新零售的商用区块链架构系统

V1.0

2018 年 7 月

1、PENROSE 概述

1.1 新零售

随着全人类整体加速了向数字化世界的迁移进程，数据的采集与生产、存储与计算、分发与交换、分析与处理已经普遍存在于跨地域、跨领域、跨主体、跨账户的各种组织与企业之中。

在传统的中心化商业模式陷入“大而不能倒”的窘境并引发金融危机之后，追求多方参与和对等合作的新型商业模式凸显价值。这种全新的模式我们称之为“分布式商业”，其特点在于多方平等参与、智能协同、专业分工、价值分享等。

在分布式商业下，经济活动再也不是处境艰难的买家和卖家之间的对抗性竞争，相反成为了项目与志趣相投的人进行合作的事业，零和博弈被多赢局面所替代。

通过运用区块链、大数据、人工智能等先进技术手段，对商品的生产、流通与销售过程进行升级改造，进而重塑业态结构，并对线上服务、线下体验以及现代物流进行深度融合，是分布式商业时代零售发展的新模式。

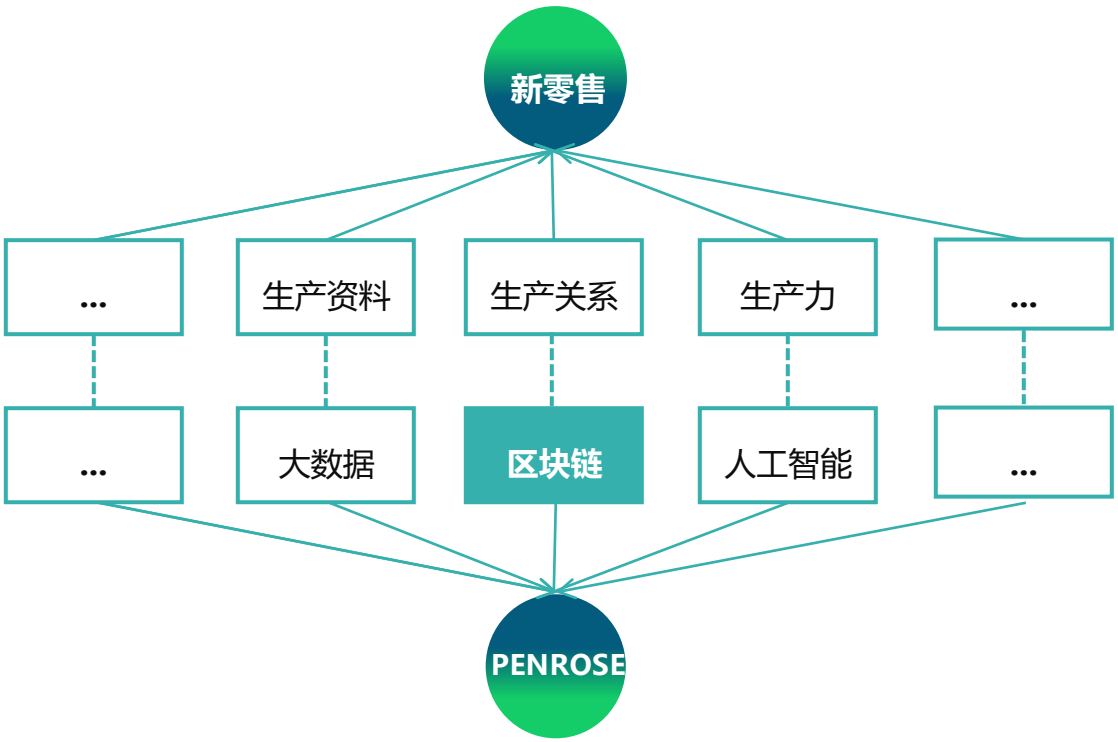


图 1.1 PENROSE 整体构思

1.2 区块链

大数据、人工智能、区块链是推动新零售发展的核心技术，这三种技术分别对应着生产资料、生产力和生产关系，PENROSE 是对这三种技术进行组织架构的一个分布式商业平台。

数据是新一轮技术革命最重要的生产资料，而建立在大数据、云计算之上的数据分析、数据监控，将会让这些生产资料发挥充分的力量，服务于未来商业体系中的商家、用户。人工智能是未来科技革命的重要生产力，它使得机器能够胜任一些通常需要人类智能才能完成的复杂工作。

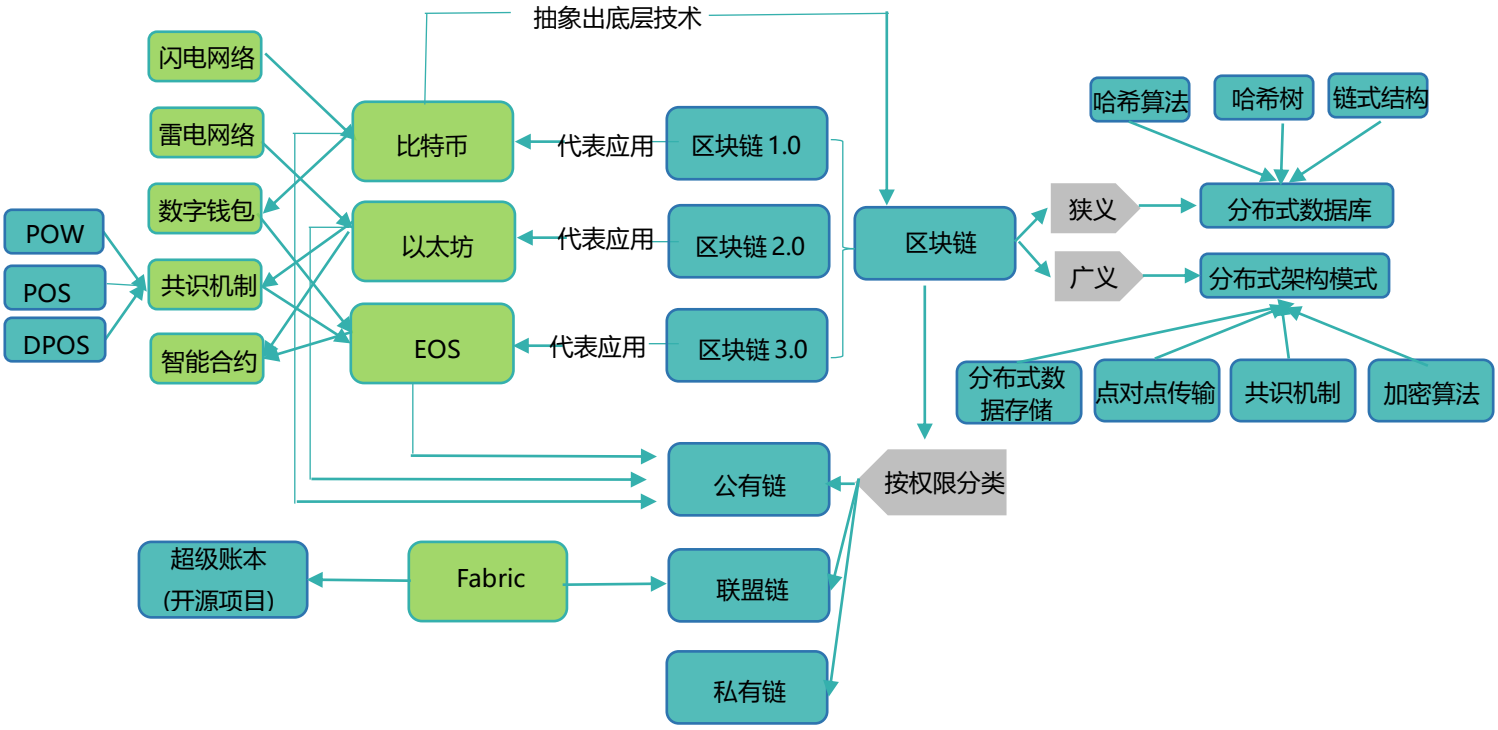


图 1.2.1 区块链

如果把人工智能对应到生产力的话，那么区块链则是很重要的一种生产关系，它是随着密码学、社会经济学、计算机科学、数学发展到一定时间而产生的一种实践理论。而正是因为区块链的逐渐成熟，才使得分布式商业变得可能和切实。区块链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、利用密码学的技术保证数据传输和访问控制的安全、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。

区块链分为两个部分，一是底层技术、二是通证经济生态，两者缺一不可。区块链的底层技术实际是一个基于共识的分布式密码学账本，所记下的数据是相关各方所认可的客观事实，这就确保了区块链上的数据高度一致、不可篡改和彻底透明。

分布式商业实现的基础是区块链经济，分布式的结构是人们可以大规模协作的基础，共识算法促进信任的产生和传递，密码学保证了隐私数据的安全受到保护。

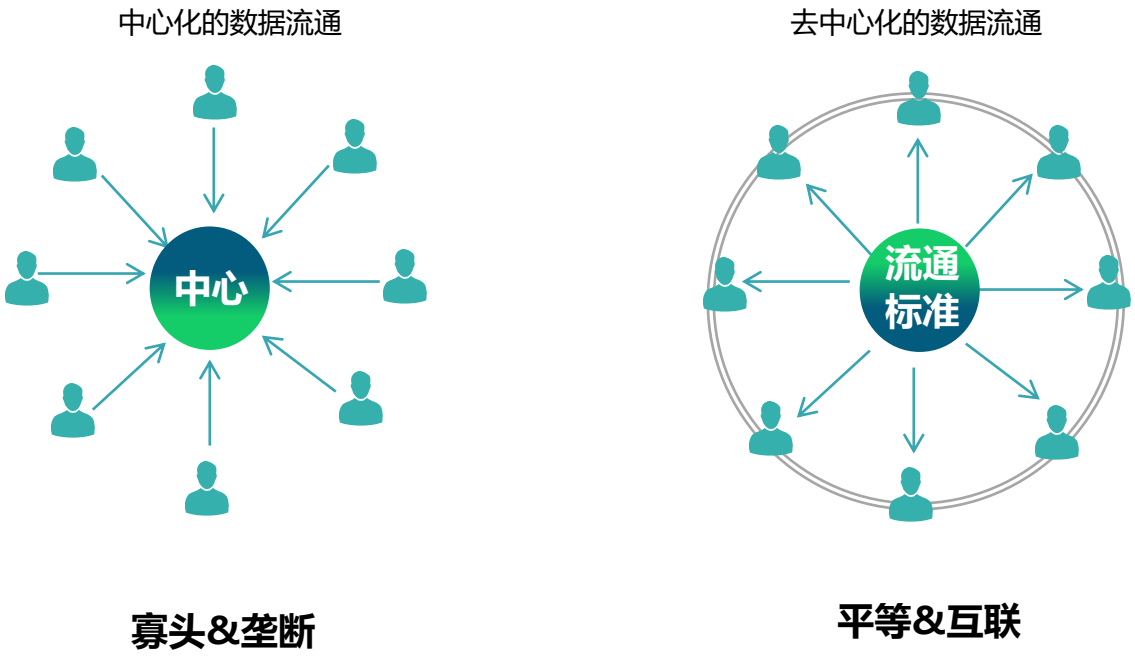


图 1.2.2 区块链数据流通方式

区块链从数据流通的方式上实现了去中心化信任。信任，就是相信他人将自己作为一个目的而不是一种手段来对待——你不会被他人出于私利去利用或操控来实现其应急目的，而是被视为一个有价值的存在。过去，我们需要中介来做商业行为之间的背书，我们才敢相互信任，但这样却增加了时间和费用的成本。区块链使得数据及信任可以直接在组织与组织、个人与个人间流转，创造了生产关系的转变，减少了摩擦，提高了效率，我们彼此的收益都会增加。

另外，区块链还解决了数据确权的问题，所有的数据应该归还给创造数据的人；其次是所有的行为都可以被量化以及货币化，每一个人都是自己数据的 CEO，可以经营自己的数据并赚到钱；最后是智能化合约自动执行，不可篡改、完全透明、安全性高，大大降低了信任的成本，减少交易的摩擦，从而提高效率。

数据是未来以互联和机器学习为主的经济中最重要的成分，AI 算法分析数据会产生许多改变世界的发现。而对于数据收集能力有限的企业，数据交易将是一个互惠互利的工作，可以促进公司的创新，创造新的收入来源。然而由于目前数据交易市场上存在数据非法倒卖，信息透明度低，易被篡改等问题，导致数据交易的规模受限。

区块链的去中心化、安全性和不可篡改可追溯性，可以让参与主体之间建立信任，推进数据交易的可持续大幅增长：数据所有权、交易和授权范围记录在区块链上，数据所有权可以得到确认，精细化的授权范围可以规范数据的使用。同时，数据从采集到分发的每一步都可以记录在区块链上，使得数据源可追溯，进而对数据源进行约束，加强数据质量。基于区块链的去中心化数据交易平台，可以形成更大规模的全球化数据交易场景。

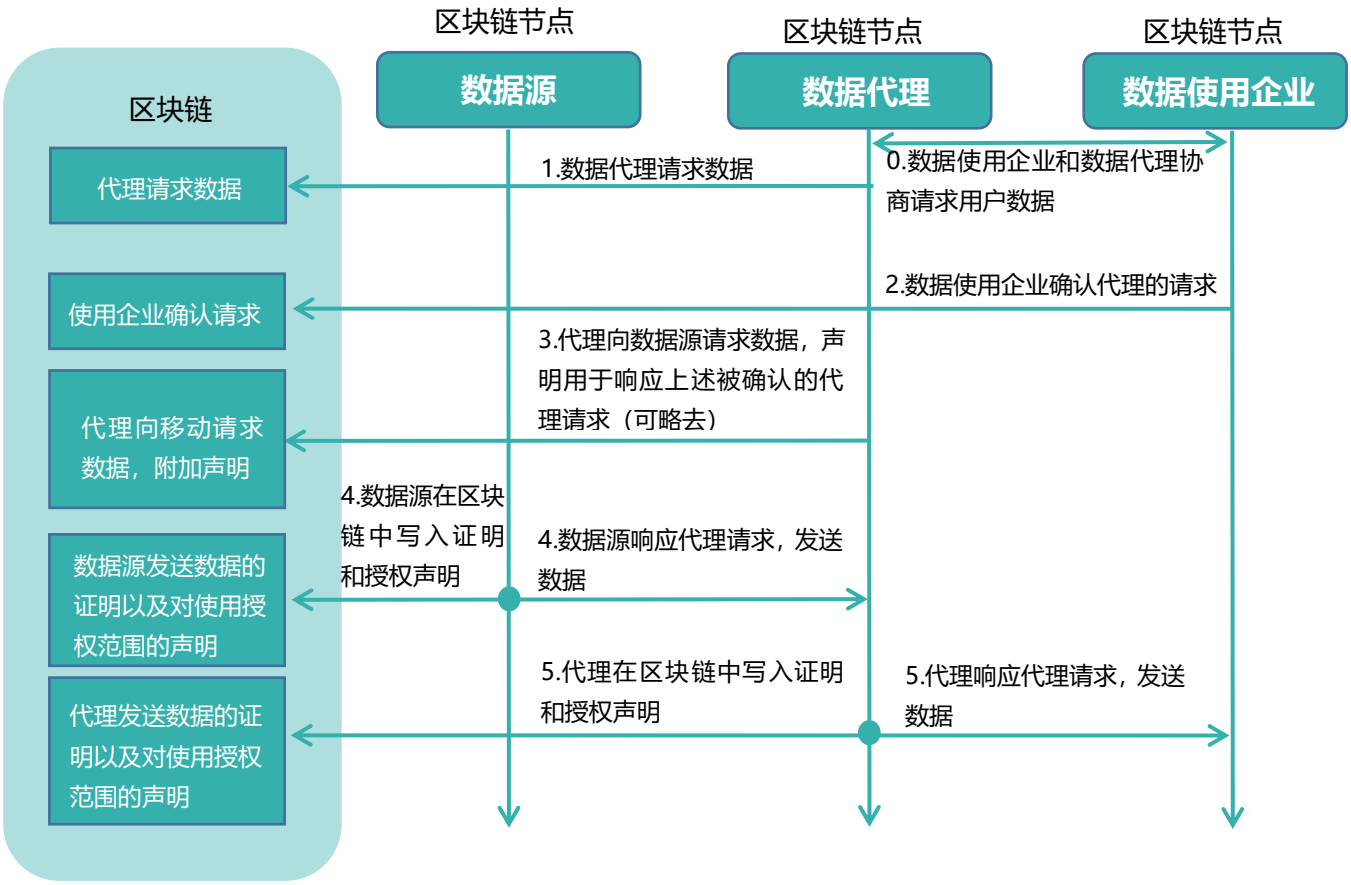


图 1.2.3 基于区块链的去中心化数据交易

特别是在物联网领域，分布广泛的物联网设备、传感器等会收集大量的数据。去中心化数据交易网络能很好的支持分布、实时和精细化的数据交易，可以成为物联网领域数据交易的媒介；同时它也能引入信任度，持续保持透明度，很好的支持物联网领域数据交易生态系统的参与主体，包括数据采集，存储，交易、分发和数据服务各个流程的参与者；最后，去中心化数据交易网络也需要在可扩展性，交易成本和交易速度方面有突破，才能加速推动物联网领域数据市场的商用化。

1.3 生态

PENROSE 致力于打造全球第一个面向新零售的分布式商业平台，希望未来能够承载以下商业应用场景：商业合同签订、品牌维权保护、微商铺建立、供应链金融、商品周期管理等等。在 PENROSE 运营稳定之后，比如像美的的供应链平台、微商平台，都可以建立在 PENROSE 之上。

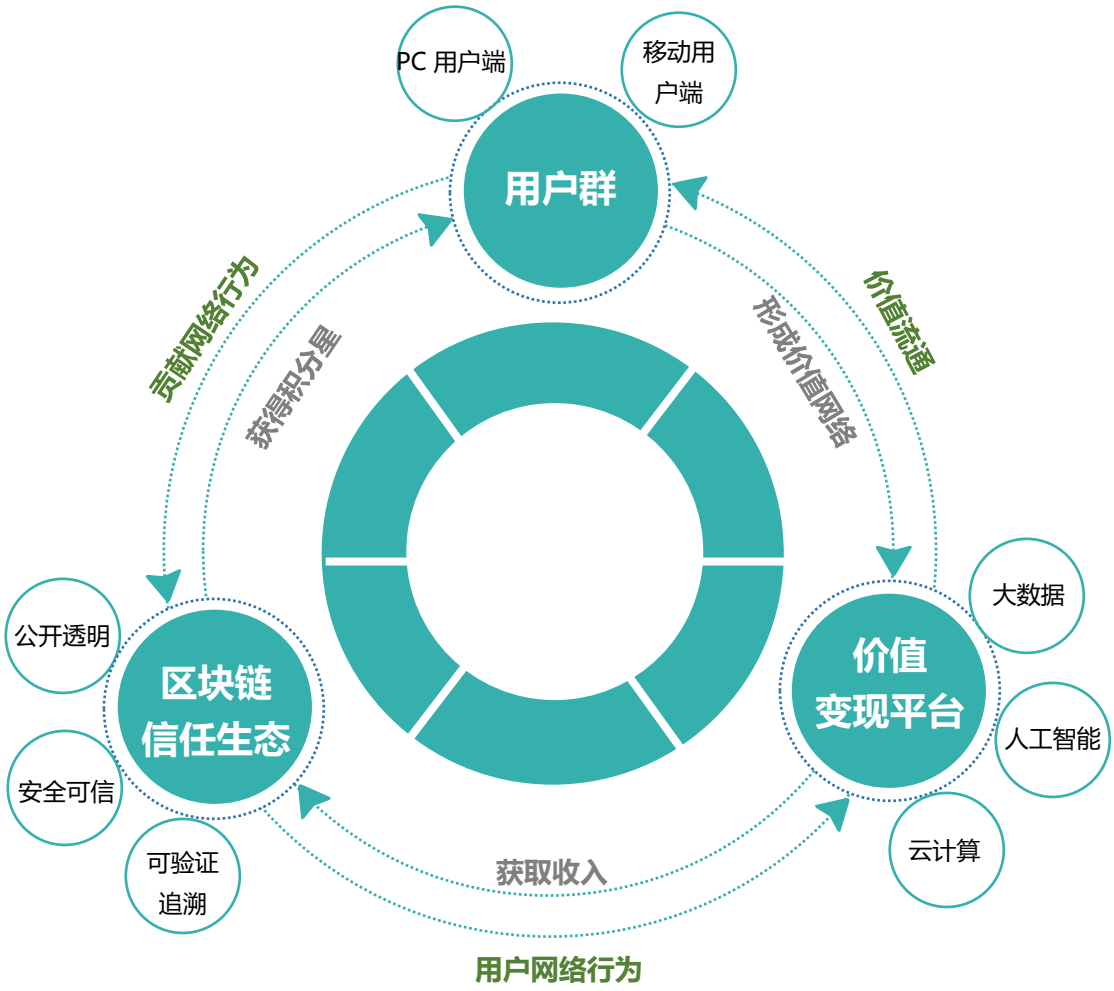


图 1.3.1 PENROSE 生态

（1）生态权益的分享和共赢

现代商业场景中，我们看到，消费者的参与推动了某些大的平台或者公司的发展，而这些大的平台或者公司壮大之后，公司的市值上涨、股票升值却没有直接分享给消费者。而在 PENROSE 之上建立的商业生态，消费者可以从整个生态的壮大中分享到收益。在 PENROSE 之上的各种应用中，用户创造了价值，必然会获得相应的代币奖励。

比特币作为区块链的创始级应用得益于它搭建了一套非常完善的公有链模型和基于这个模型的工作和激励机制。如何通过商业模式建立较好的区块链应用场景的激励机制，让各区块链应用真正产生商业价值，是区块链规模化应用的核心挑战之一。

（2）可验证追溯

品牌侵权、假货横行，一直是困扰消费者、商家的头痛问题，通过区块链的不可篡改性，解决商品源头数据的可信问题，是 PENROSE 生态的一大特色。每年的 315 打假仅是打假过程中的冰山一角，产品溯源防伪仍是目前社会和企业的主要难题。以食品为例，虽然有绿色食品标识，但因为人为因素在整个供应链中参与过多，导致对中间环节的数据可信度存在较大疑问，这会对社会和企业的公信力产生很大的影响。食品是否是绿色无污染的，高端艺

术品/奢侈品是否为赝品等一系列问题仍然摆在社会面前。

区块链技术依托其具有的数据不可篡改、交易可追溯以及时间戳的存在性证明机制，可以很好地解决供应链体系内各参与方在数据被篡改时产生的纠纷，实现有效的追责和产品防伪。

以牛奶溯源为例：目前牛奶溯源主要有奶牛业主，奶牛饲料提供商，奶牛灌装厂商，物流方，监管方，售卖方（商场超市）。首先奶牛业主通过第三方传感器，获得奶牛日常的喂养过程以及牛奶的检测数据并记录在账本中，针对这些数据，监管部门或防疫部门会根据其数据给予奶牛业务提供相应的支撑，并补充到分布式账本中。奶牛饲料提供商给奶牛业主提供的饲料情况的数据上链后，可有效对非法饲料跟踪和定责。再通过灌装厂商的灌装流程数据，以及物流方的数据，从而获知牛奶的运输中的保鲜度。通过售卖方，可以方便普通用户通过终端应用获取想要购买奶粉的整个生产和售卖流程，从而杜绝非法产品，有效构建政府公信力，同时基于数据的共享，各方可以知道相互的需求，实现更为有效的合作互赢。当然在牛奶生产过程中，发现数据不达标则会马上预警进行调整，并且不达标的数据无法生成平台认证的质量签名，对应牛奶将被拒绝销售，且数据超标的，将及时进行销毁，从而保障牛奶品质。同时监管部门对不能认真保障牛奶质量的业主，给予相应的惩罚，取消其奶牛饲养资格，并将业主加入非诚信人员名单，对其后续的经营资质产生很大影响形成督促作用，目标是形成自治的良性循环，避免人为弄虚作假。

（3）供应链金融

PENROSE 之上的供应链金融服务平台，可以优化应收账款融资流程。对供应商来说，可以有效缩短账期，降低融资成本，并保护购销过程敏感信息不被泄漏；对金融机构来说，平台将有效杜绝虚假贸易，提高运营和风控效率。

供应链金融业务非常适合采用区块链与分布式账本技术。平台针对信用评级高、融资成本低的核心企业，运用区块链技术将供应链交易信息进行链接，将信用从中心企业向末端供应商传递，以提高金融资源在供应链属企业间的配置效率。

具体来说，PENROSE 可以为供应链金融在以下方面提供强有力的支持：首先，通过区块链的不可篡改性，记录供应链金融上下游企业和周边企业的资金流、物流、商流过程，降低供应链金融过程中，可信数据采集、传递的难度；为金融机构获取第一手的供应链信息提供便利。如果企业广泛部署物联网终端，结合企业信息化系统的进销存信息，可以真实的勾勒出企业的运营情况与资产情况；企业透过企业网银、银企直联等渠道与上下游企业产生资金往来，提供真实的财务资金信息；这些信息将帮助金融机构在进行贸易融资、仓单贷款、应收账款贷款过程中极大简化信用评估流程与成本，以此降低企业融资的成本，提供融资的效率；

其次，通过“智能合约”等技术手段，为企业间“合同信任”关系之外，添加新的保障措施，简化企业间互担保、风险分摊、回购、履约等经营行为的流程，降低违约纠纷处理的时间成本和资金成本。以合同融资为例，合同的买方与卖方建立起中长期的供应关系，采购方的销售数据衍生出对原材料的采购需求的评估数据，市场的真实供需关系是融资回收的第一保障；若采购方企业提供风险缓释措施，在风险条件触发后，采购方是否按指令进行回购、退款等风险补偿履约措施，直接影响融资贷款是否产生不良资产。现行的操作中，上述履约约束主要来源于“合同信任”，但履约过程中可能存在法律争议，后期将增加法律纠纷的处理时间及成本。引入区块链“智能合约”，将上述合同约定事项上链，使其变为自动触发与操作，从技术的角度弥补履约中的意外过程和主观违约可能，保障融资安全。

2、PENROSE 架构

PENROSE 的架构采用 EOS+QTUM+CMT 的架构。

EOS 是一个免费的、开源的区块链软件协议，提供给开发者和企业家一个平台，来建设、部署和运行高性能的去中心和应用（DAPPs）。EOS 软件引入一种新的区块链架构设计，它使得去中心化的应用可以横向和纵向的扩展。这通过构建一个仿操作系统的方式来实现，在它之上可以构建应用程序。 该软件提供帐户、身份验证、数据库、异步通信和跨越数百个 CPU 内核或集群的应用程序调度。 由此产生的技术是一种区块链架构，它可以扩展至每秒处理百万级交易，消除用户的手续费，并且允许快速和轻松的部署去中心化的应用。

QTUM 是首个基于 UTXO 模型的，采用权益证明（PoS）共识机制的智能合约平台。Qtum 量子链同时具有货币属性和平台属性，同时兼容比特币和以太坊两种生态。Qtum 的账户抽象层 AAL 允许 EVM 在 UTXO 模型上运行，兼容多种虚拟机，底层具有比特币的安全性。Qtum 的互惠权益证明机制 Mutualized Proof-of-Stake（MPoS）通过于其他节点分享收益，增加攻击成本，并且改进了现有 PoS 项目不支持图灵完备的智能合约虚拟机的缺点。量子链采用分布式自治协议（Decentralized Governance Protocol, DGP），基本实现了对参数类的分布式自治。量子链的目标是实现策略类参数治理，无需更改软件版本实现区块链网络的自动升级和快速迭代。另外，Qtum x86 虚拟机将能够有更加优化的 Gas 模型，有解锁 AAL 的强大功能，并且有丰富的标准库。

CMT 草莓糖是下一代的商业交易区块链协议，CMT 主要从两方面着手解决问题，低效率和低开发产出。CMT 提出区块链技术有三个方向是会随着社区共识的推进渐渐成熟落地的：新的共识机制，网络分片，离链计算。CMT 提出在区块链技术的基础扩展性问题解决之后，如何让第三方的企业应用能够在一个系统性解决方案上更有效更容易地开发成为关键。CMT 的实施路径主要是从以太坊 EVM 的缺点入手，首先智能合约的触发通常需要链外的条件，而以太坊的 oracle 是一个残缺的解决方案，因为它的不标准化，其次由于复杂的编程规则，多数智能合约只能是中间件简单的拷贝，另外 DApp 中间件不能被封装和重用，还有 DApp 中间件没有与区块链的货币激励系统进行集成，使得 DApp 大多数是采用中心化的方式在运行。

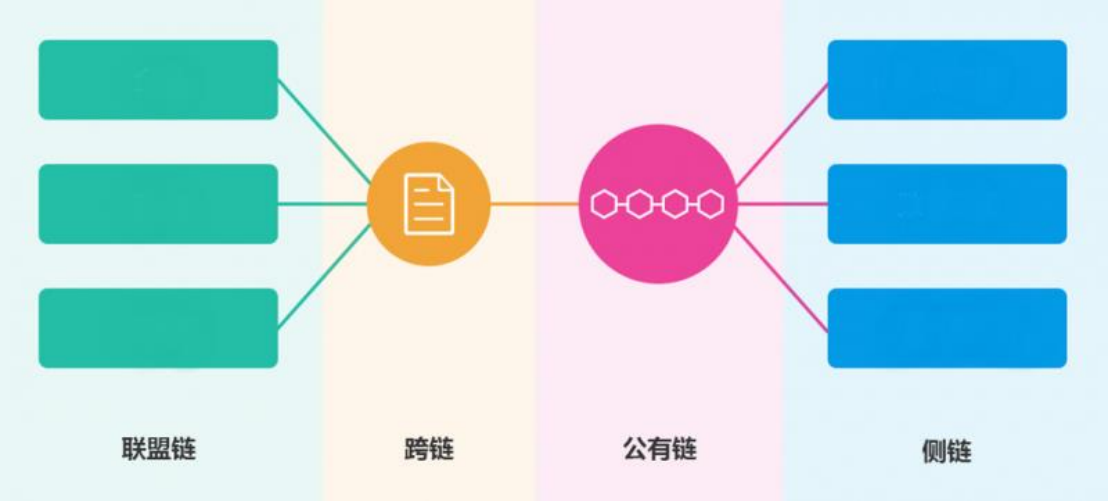
PENROSE 在 EOS 和 Qtum 的基础上，提出了比 CMT 更加落地的目标和解决方案，EOS 是大而全的系统性框架，给出了 DPOS 共识算法、账户权限机制、应用程序的确定性并行执行、Token 模型与资源使用、治理、脚本和虚拟机以及跨链通信等等的解决方案，再加上量子 Qtum 的移动端友好虚拟机，可以很好地实现 PENROSE 的首个面向新零售的商用区块链架构系统的目标。

2.1 跨链通信

公有链是一种面向大众，完全开放的区块链，全世界的人都可以参与系统维护工作，匿名和开源是公有链的两个特性。匿名体现在公有链的节点之间无需彼此信任，无需公开身份；而开源体现在整个系统运作公开透明。基于匿名和开源两个主要特性，公有链现阶段稳定支撑着数字资产的流转，这也极大地促进了区块链概念和技术的普及，比如比特币、以太坊等。

联盟链考虑到实际商业应用，增加了权限控制、安全机制、可监管审计等商业特性，目前已处于应用探索阶段，部分应用场景如：金融、医疗、供应链等正在尝试用联盟链解决信息协作问题。具有代表性的联盟链技术框架有超级账本的 Fabric 项目。

针对企业级应用，现有的公链由于缺乏对成员准入的控制且在性能等方面存在缺陷，难以满足商业应用的需求；而联盟链虽然定位于企业级应用，目前仅实现了信息的安全共享，但缺乏对价值流转的支撑，难以大规模应用。



PENROSE 在 EOS 的基础上，被设计为跨区块链友好， 通过生成消息存在证明与消息时序证明变的简单而实现。这些证明与应用架构设计相结合，即围绕消息细节的跨链传输和有效性验证时隐藏应用程序开发者的架构设计。

另外，用于轻客户端的 Merkle 证明也为跨链提供了必要的基础，相比于比特币的支持通过全节点的完整记录获取每年 4MB 大小的区块头信息来验证交易。每秒 10 个交易，一个有效的证明需要 512 字节。PENROSE 在 EOS 的基础上，使用特殊的哈希链结构，可以使用少于 1024 字节的大小来完成任意交易的存在性证明。如果假设校验节点在过去几天内所有的区块头一直增长（2MB 的数据），那么验证这些交易将只需 200 字节就够了。

当需要验证其他链时，有譬如时间/空间/带宽的多样性优化可以做。追踪全部区块头（420MB/年）将保持证明体积的轻巧。只追踪最近的头可以提供最小长期存储和证明大小来获得。另外，一个区块链可以使用懒惰的评估方法，即它记住过去证明的中间值哈希。新证明只需要包含指向已知稀疏树的链接。确切的方法将取决于那些包含对 Merkle 证明引用的交易所在的外部区块的比例。

一定密度的联系后，将变得更为高效，一个链包含另一个链整个区块的历史和消除证据一起，这样就不需要通信便可以验证了，处于性能原因，应最小化跨链证明的频率。

当于外部区块链进行通信时，区块生产者必须等待到 100%确信一个交易已经被另一个区块链确认为不可逆后才会接收它成为一个有效的输入。

2.2 共识机制

PENROSE 采用 DPoS 共识算法，理论上可达 10000+TPS。

PENROSE 网络选取的超级节点有 23 个，候选人节点有 254 个，超级节点的硬件配置只需要普通的笔记本电脑，大大降低准入门槛，但是每一个超级节点的账户 staking 挖矿的数量会有要求。

EOS 默认的 0.5s 的出块速度在全球性的分布式网络中尚未得到有效验证，网络延迟很可能会造成区块链分叉和停止。PENROSE 采用 6s 的出块时间，每个节点每次只出一个块，每个区块奖励为 9 个 PRT。待链稳定运行后，PENROSE 有可能恢复 0.5s 的出块时间，在稳定的基础上进一步提升链的性能。

EOS 需要用户抵押币来获取资源，从而竞争性地使用区块链，继而达到 “免交易手续费” 的目的。然而，超级节点可获得 1% 的年化奖励，这实质上将交易手续费转嫁为了用户必须承担的 1% 年化通胀。为了链的安全性，防止被 DDOS 攻击，PENROSE 恢复了交易手续费，以交易执行的种类计费，用户无需指定手续费金额，系统将会自动从交易发起方的余额中扣除，如果余额不足，交易失败。

如果不给投票用户分红，普通用户的投票意愿就会降低，这会导致全网的投票比例降低，那么几个大户联合就可能操纵投票影响选举，从而进行分叉攻击。所以，我们鼓励超级节点给投票的用户进行分红，充分活跃普通用户的投票参与度。

PENROSE 每年大约有 9000 万 PRT 奖励，超级节点可以自行设置自己的佣金比例，比如 1%。那么节点当选并出块后，可以拿走每个块奖励的 1%，剩余 99% 会进入每个节点的奖励池。节点根据每个用户的投票金额和时间得出用户 “票龄”，再根据节点所有用户的 “总票龄”，计算出每个用户在奖励池中的分红占比，给节点投票的用户随时可以从奖励池中提取分红。

如果 PENROSE 全网只有 3 亿的 PRT 参与投票，那么所有这些投票用户将平分 9000 万 PRT 的奖励，年化利率约为 0.9 亿/3 亿，也就是 30%。用户的年化利率随着投票参与率的升高而降低。随着币总量的上升，每年的奖励比例也会逐年下降。

为了减少自动分发消耗大量运算资源，PENROSE 的投票分红需要用户手动领取，领取快慢并不影响分红数量，所提取分红会立即变成可用余额。

用户每次提取分红后，在节点中的 “票龄” 会归零重新累计。

PENROSE 实行一票一投的用户投票机制，1 个 PRT 只能投给某一个节点，但是一个用户可以给多个节点分别投不同数量的币。

假设一个用户有 1000 个 PRT，节点 A 的佣金比例是 1%，用户投给 A 300 个 PRT，节点 B 的佣金比例是 1.5%，用户投给 B 100 个 PRT，那么该用户的可用余额还剩 600 个 PRT，用户最终可以从这两个节点分别获得相应的投票分红。

PENROSE 支持用户调整投票数量，即增加或减少投票。如果增加投票，则自动进行一次分红领取，并扣除可用余额。如果减少投票，也会自动进行一次分红领取，同时减少的币量会有 3 天的冻结时间，3 天后，用户需要手动进行 “解除冻结” 操作，才能把投票金额变为可用余额。

2.3 智能合约

（1）智能合约生命周期管理

a. 允许开发者设计和创建包含商业逻辑的智能合约，业务服务系统通过接口等交互机制与区块链系统交互。

b. 提供智能合约的生命周期管理功能，如创建、调用、升级、销毁。

C. 提供对智能合约的升级与数据迁移能，但是要满足原智能合约设定的升级规则。

（2）智能合约组合服务

a. 通过组合已有的一个或多个智能合约来创建新的服务功能

b. 为服务使用者设计集成的接口使其能访问多个区块链系统服务功能。

（3）智能合约测试服务

a. 对区块链系统中实现的组件功能进行测试，以确保这些组件完整并正确地实现了服务功能。

b. 对区块链系统中实现地组件功能进行测试，以检测这些组件地系统安全性与健壮性。

c. 确保服务功能接口地互操作性。

d. 测试宜覆盖区块链系统中地服务部署节点。

（4）智能合约模板服务

a. 提供智能合约地模板

b. 对于通用类型地合约可以设置简单地参数，生成合约 template，经过简单地改动就可以部署。

c. 提供界面化的操作流程，只需拖动即可完成商业智能合约的构建。

（5）区块链 API

计划提供 restful, rpc, websocket 等 API，可以调用区块链各种服务。

2.4 虚拟机

PENROSE 的虚拟机有以下特点：

支持多种主流编程语言：C/C++/Go/Rust 等；

丰富的标准库，提高开发效率；

更加优化的 Gas 模型：为标准库函数设定合理的 gas，便于估计

冯·诺伊曼结构，加强版的智能合约，代码即数据，多任务协作，终端和恢复

第一类 Oracles，无需运行合约即可获得某些合约数据

区块链动态分析，更全面地分析区块链状态

选择性数据存储，节省宝贵地区块链上资源

清晰地依赖关系树，有可能并行运行智能合约，降低 gas 费用

2.5 分布式存储

PENROSE 采用星际文件系统（IPFS）作为底层存储方案。IPFS 是分布式文件系统的超媒体协议，它可以让用户的数据分布存储于网络的各个节点，节点在下载信息的同时会向其它节点扩散，这意味着信息被越多的人浏览，数据会越多的分布于整个网络。这样做的好处有很多，数据分布于网络中成千上万的节点上，攻击者想要阻止其他人访问是不可能的。参与者不必全天候的运行自己的节点（虽然这么做有助于网络安全），数据拥有者在关闭客户端的时候，他的数据在网络中依然可以访问。类似于 BitTorrent，访问和下载的人越多，速度会越快，体验越好。

2.6 可信信息管理

“预言机”解决方案让区块链的智能合约获取现实世界的不确定数据信息成为了一种可能，例如资产价格、货币汇率、股票指数等等。通过经济激励与博弈机制来让不确定的外部信息进入区块链智能合约，让智能合约的执行能够依赖现实世界的数据执行相关业务过程。

PENROSE 中，采用特定的共识机制对提交信息的确定性做出判断，让信息知晓者在经济利益驱动下基于区块链数字身份提交现实世界的数据信息，一定的惩罚机制也确保了信息会向着数据的确定性和正确性方向进行收敛。

PENROSE 中，联盟参与方添加到 PENROSE 网络需要交一定的保证金，同时设置奖惩机制。如果事后发现造假，PENROSE 网络会扣除保证金。虽然联盟链是弱共识，但是它能保证一定的数据信任以及资产信任。这个交易完成以后再往主链上走，把各个联盟链的数据和资产在主链上进行交换流通。

2.7 用户统一识别 ID

所有参与主体，包括一切人、物、组织、系统等在 PENROSE 网络中使用统一的身份标识，PENROSE 网络根据身份标识权益管理与业务处理，PENROSE 网络支持主体的多身份标识管理。

身份标识使用去中心化的方式进行管理，包括身份标识产生、使用、验证、存储，以实现隐私保护与安全交易。

产生：每个身份标识采用非对称加密 PKI 加密机制生成，产生对外公开的地址信息。身份标识的所有者保管地址与私钥信息。此外支持部分参与主体选择数字认证中心颁发的证书进行标识。

使用：身份标识的主体通过私钥信息，操作其在 PENROSE 网络所有权益或数字资产进行交易，并向 PENROSE 网络发起申请。

验证：PENROSE 网络进行所有权益检查与交易验证，通过后形成网络共识。

存储：产生的身份标识相应的公开信息，将被作为公开信息存储在 PENROSE 网络的分布式账本中。

此外身份标识支持只能合约拓展，以实现更丰富的身份标识管理，满足不同业务领域的身份管理要求。如在供应链金融场景，需要满足业务主管地区的 KYC 需求，采用扩展的智能合约进行 KYC 内容的设置与存储。

3、PENROSE 模块

3.1BAAS 模块

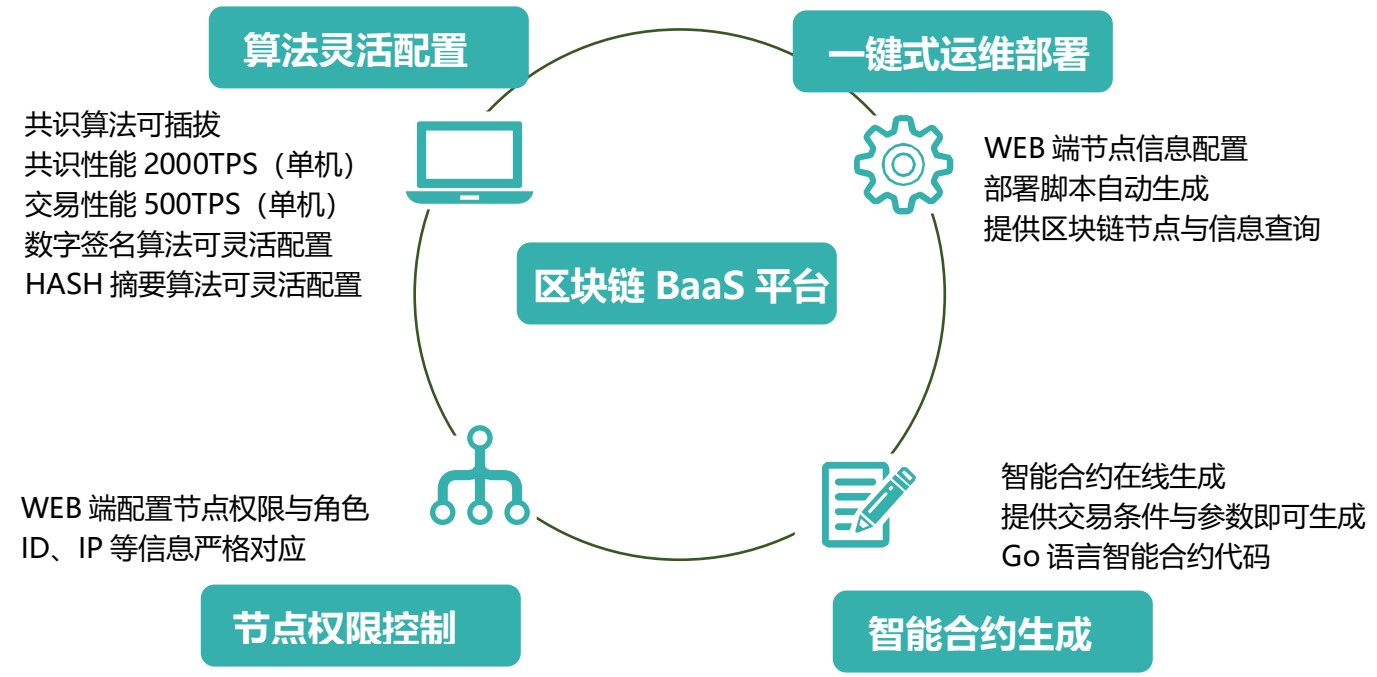


图 3.1 BAAS 模块服务

为了更好地支持上层业务对区块链模块的集成应用，PENROSE 以 BaaS 为建设目标，通过丰富的 API 接口为上层业务及产品提供灵活方便的功能集成、运维部署服务。提供的 BaaS 服务接口包括：

（1）节点权限认证控制

基于联盟链地应用场景，各个节点地链上权限及角色配置都可以通过运维软件的 WEB 界面进行配置。每个节点的模块 ID、IP 地址、角色信息（Order 节点、Peer 节点、Endorse 节点等）、组织信息及链通道信息都严格对应，防止越权访问。

（2）共识算法可插拔

默认情况下支持“PBFT+”共识算法，同时支持通过 API 接口调用包括 PBFT、PAXOS 等其他共识算法，实现共识算法的灵活配置。

（3）加密算法自定义配置

可以通过 API 接口配置选择不同的数字签名算法（ECDSA\SM2\后量子签名算法）、HASH 摘要算法（SHA256\SHA384\SM3）。

（4）一键式运维部署

PENROSE 提供基于 WEB 界面的运维软件实现区块链部署的节点配置，包括节点 IP、节点 ID、节点数据库配置、共识算法及加密配置，运维软件根据配置信息自动生成部署脚本，然后执行脚本即可启动区块链服务；此外，运维软件还提供区块链节点信息查询、区块信息查询等功能。

（5）智能合约动态生成

基于已开展的应用场景，PENROSE 提供在线生成智能合约功能。通过运维软件的 WEB 界面输入交易条件和参数（例如交易价格、交易对象、生效时间、例外条件）后，即可自动生成基于 Go 语言的智能合约代码。

3.2 应用模型

以应用开发者的视角，假设要开发一个商品贸易系统，业务的参与者包括贸易买卖双方和物流企业，这个系统要帮助买卖双方建立交易合同、跟踪货物运输过程、交付结算。在 PENROSE 中:

（1）定义参与业务的各个主体的身份账户

为参与者注册登记一个由公钥私钥对（证书）表示的身份账户。由符合国家标准的证书所表示的身份账户时能够代表一个特定的法人，由该账户签发的数据可以在法律上被人为是该法人做出的确认。

（2）编写智能合约对业务过程做出定义

把参与者之间达成的商业协议以智能合约代码的形式进行定义，以数字化形式约定贸易的商品属性、数量、交付价格、交付期限、交付条件、运输方式、交割检验标准、贷款计算方式、贷款支付时限等。

（3）联合签署智能合约并触发业务初始条件

智能合约最后需要经过参与者以各自的身份账户做出签署，之后每一方参与者只需要根据自己业务范围内的业务进程做出相应的操作，便触发了智能合约的执行。

在这个过程中，PENROSE 提供以下几个方面的保证：

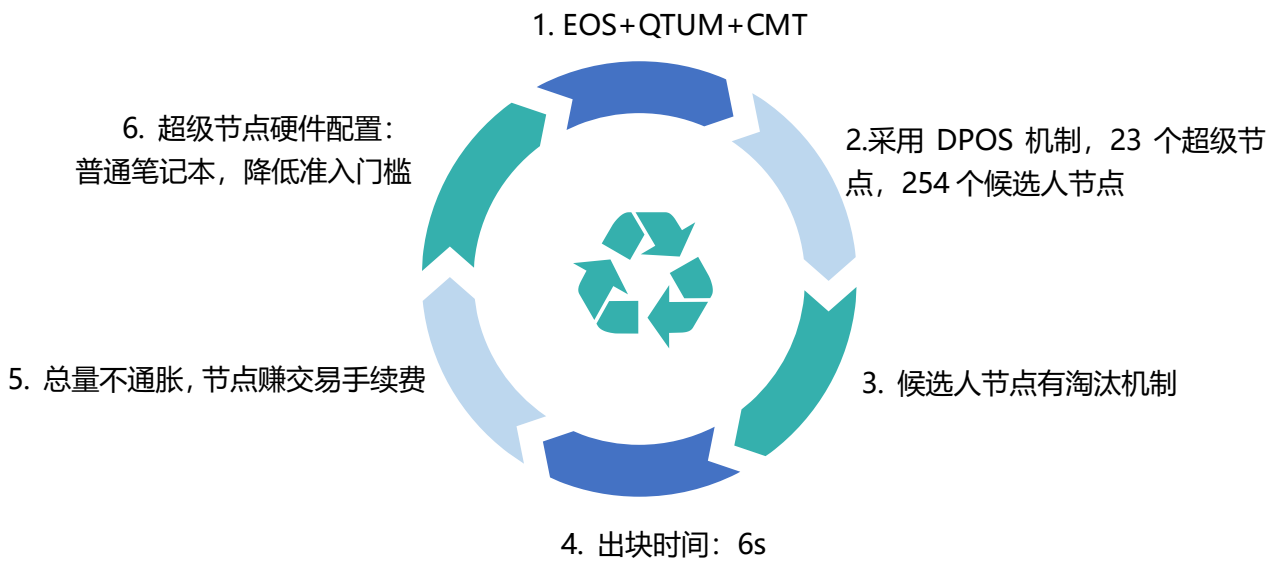
a. 确保合约在每一个参与业务主体的节点上被一致地执行，并得到一致地结果；

确保合约执行过程地每一个步骤都被准确地记录下来；

b. 确保合约执行过程地记录以及最终结果都无法被篡改；

c. 确保参与地主体对合约执行过程地记录以及结果进行签名，确保合约被执行地事实在今后都不可抵赖。

4、技术特性



PENROSE 融合 EOS+QTUM+CMT 技术优势，采用 DPOS 机制，DPOS 相较于 POW 和 POS 的最大亮点在于速度和效率。PENROSE 由 23 个超级节点轮流出块，备有 254 个候选人节点，出块时间 6s。在 BFT 算法中，节点数天然不适合是 3 的整数倍。如果是 21 个节点，且恰好形成了 14 票同意，7 票反对的局面，则既无法达成大于 2/3 的通过，也无法达成大于 1/3 的否决，治理陷入僵局。如果是 23 个节点，不是 3 的整数倍，那么最终会形成 15 票同意，8 票反对的否决决定，或者 16 票同意，7 票反对的通过决定，不会形成僵局。在此基础上，为保证整体网络的安全性，候选人节点具有淘汰机制，23 个节点是由公平公正的方式投票产生，其中还有 254 个候选节点，一旦 23 个主节点没有履行义务，就会被候选节点替换掉，这就是淘汰机制，同时，超级节点硬件配置为普通笔记本，降低准入门槛，并且 PENROSE 总量不通胀，节点赚交易手续费，超级节点可获得 1% 的年化奖励。

5、产品特性

5.1 账户体系

PENROSE 生态中用户的账户体系在确保用户数据安全及隐私有效保护的情况下，又能实现商业活动等场景的行为真实有效。生态内所有参与主体，包括一切人、物、组织、系统等使用统一的身份标识，身份标识使用去中心化的方式进行管理，包括身份标识产生、使用、验证、存储，以实现隐私保护与安全交易。

（1）真实性

a. 在需要实名匹配的情况下，确保用户身份有效性，如签约 DAPP 的支持；

b. 通过可靠节点的引入及节点投票机制，保证实名的可靠性。

（2）安全性

a. 用户自持私钥保证用户链上数据的安全、可靠；

b. 链上数据加密传输机制，确保数据传输过程中的安全；

c. 节点共识机制，确保整个公链的数据安全性和可靠性。

（3）隐私保护

a. 不同场景对不同级别的隐私数据进行加密，确保只有必要数据在必要场景下可以使用；

b. 数据分层授权，公链支持用户将数据根据自身需要分层授权给使用方。

5.2 智能合约

PENROSE 生态中拥有大量适用于商业场景中的智能合约，用户可以自行选择甚至可以便捷地进行智能合约的修改，实现合约、签约、履约端到端全流程在线服务，使业务开展能够更加便捷、安全。同时，penrose 致力于生态的不断发展，通过提供技术规范和开发奖励，鼓励更多有能力的开发者参与到智能合约的开发中来。

（1）丰富的智能合约模板库

PENROSE 智能合约模板库涵盖行业各大类商业往来合作合约书、调查报告、计划书等国际标准合约，同时通过标签化结构梳理，实现智能合约管理（即可按标签选取合约模板），用户可以根据商业应用场景自行选择合适的智能合约。

（2）便捷的智能合约模板编辑系统

参与者可以通过可视化页面进行智能合约编辑操作，在操作过程中，系统可自动填入合同模板（也可手动添加）生成可签约的完整合同，一旦出现有交易要素的变更，亦可实现信息全文关联内容自动检索替换，大幅度减少人为操作修改时间。

（3）智能合约代码开源

通过代码开源，确保合约有效性公开可查，从而开放给所有参与者审验和理解来达到共识，提升应用的可靠性和安全性。

（4）提供智能合约开发规范文档

有能力的技术开发者可以为社区贡献更多可用的智能合约。当然，系统也将就此条发布包括智能合约的安全开发理念、bug 赏金计划指南、文档例程以及工具。

（5）智能合约生态奖励

生态社区为高质量的智能合约开发者提供生态奖励，提供让生态建设者通力合作的环境，并创造忠诚和奖励机制，以此刺激生态的活跃与创新。

5.3 开放的 DAPP 生态

（1）官方社区在初始阶段提供基础 DAPP，供生态用户使用

在基础设置搭建到生态系统扩展的新阶段，由官方社区提供 DAPP，同时在生态运营步入正轨后也支持外部 DAPP 的开发与接入。

（2）开放的 DAPP 生态，为生态技术开发者提供易用的接口，便于接入

DAPP 的开发支持兼容编程语言，以熟悉的语言进行编程的能力为开发人员创造了一个更有利的环境。

（3）外部个人开发者或企业可以根据自己的擅长方向，开发不同的 DAPP 进行接入

DAPP 的开放生态决定了 PENROSE 不对生态引入 DAPP 的种类进行限制，一切依据于外部开发的性质与要求决定，多品类的 DAPP 能够丰富生态的发展与进步。

（4）生态社区为高质量的 DAPP 提供生态奖励

为解决复杂网络部署的后顾之忧，降低开发过程中的时间和资源成本，在生态内部凡是提供贡献的用户都应该获得生态奖励，同时高质量的 DAPP 又为生态用户提供更加良好的用户体验。

（5）开发者可以通过 DAPP 在符合标准的范围内进行盈利

PENROSE 生态为开发者提供全新的盈利模式，允许开发者或团队开发符合平台技术规范和经济模型的应用或算法以及其他方式进行盈利。

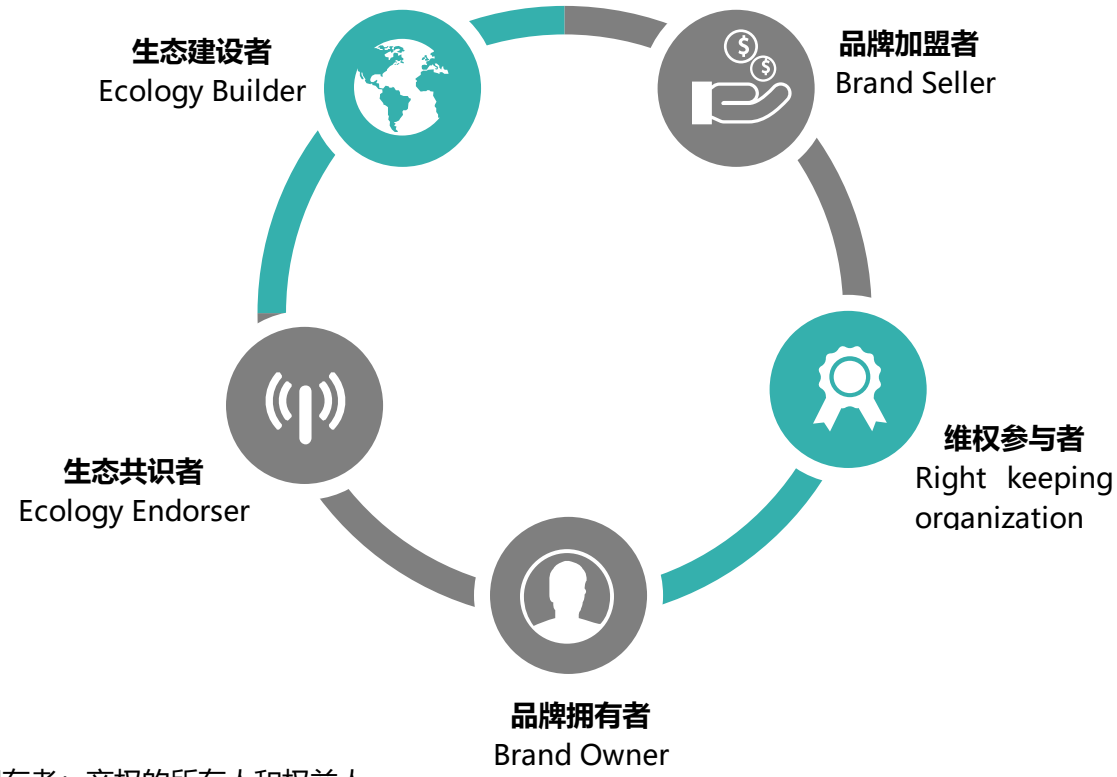
（6）DAPP 开发者可以使用 PRT 作为通用结算单位

为了方便不同 DAPP 上相互结算,我们使用统一的货币单位-PRT 代币用以支付酬劳或者进行交易行为往来。

6、应用场景

6.1 品牌宝

品牌宝是建立在 PENROSE 之上，为品牌商家提供面向电子商务领域监控保护的平台。

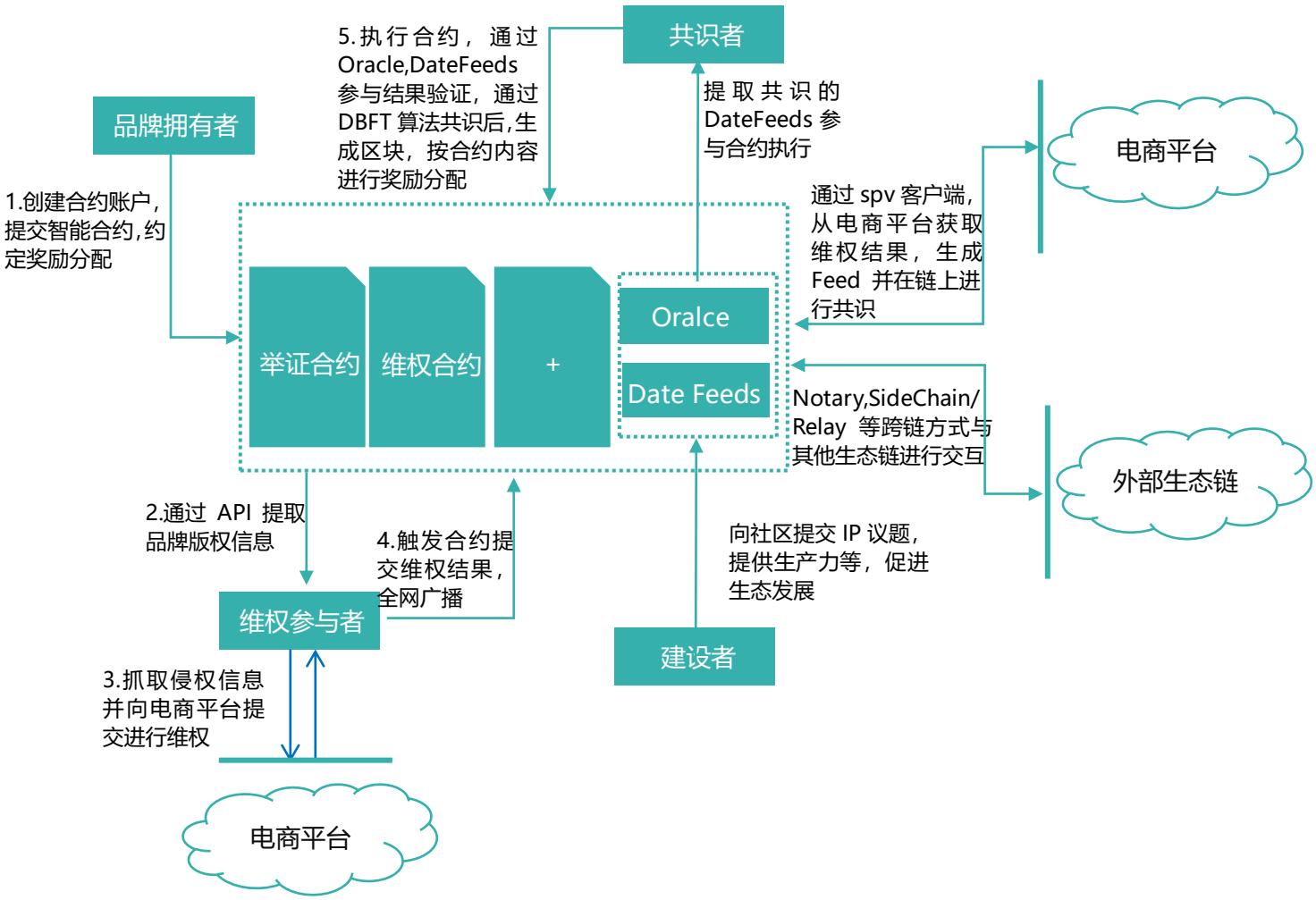


角色:

品牌拥有者：产权的所有人和权益人

品牌加盟者：品牌拥有者的下游群体，该群体在生态中进一步增强了品牌的公信力。

维权参与者：生态中的维权群体，这类群体用自身维权能力，帮助品牌拥有者维护权益；并通过抓取和采集等方式，将侵权信息提交至电商平台的知识产权保护系统，并对侵权信息进行举报。



品牌宝核心工作机制如上图所示，主要涉及以下几个环节：

a. 品牌拥有者创建合约账户提交智能合约约定奖励分配

b. 维权参与者提取品牌版权信息

c. 维权参与者抓取侵权信息并向电商平台提交进行维权

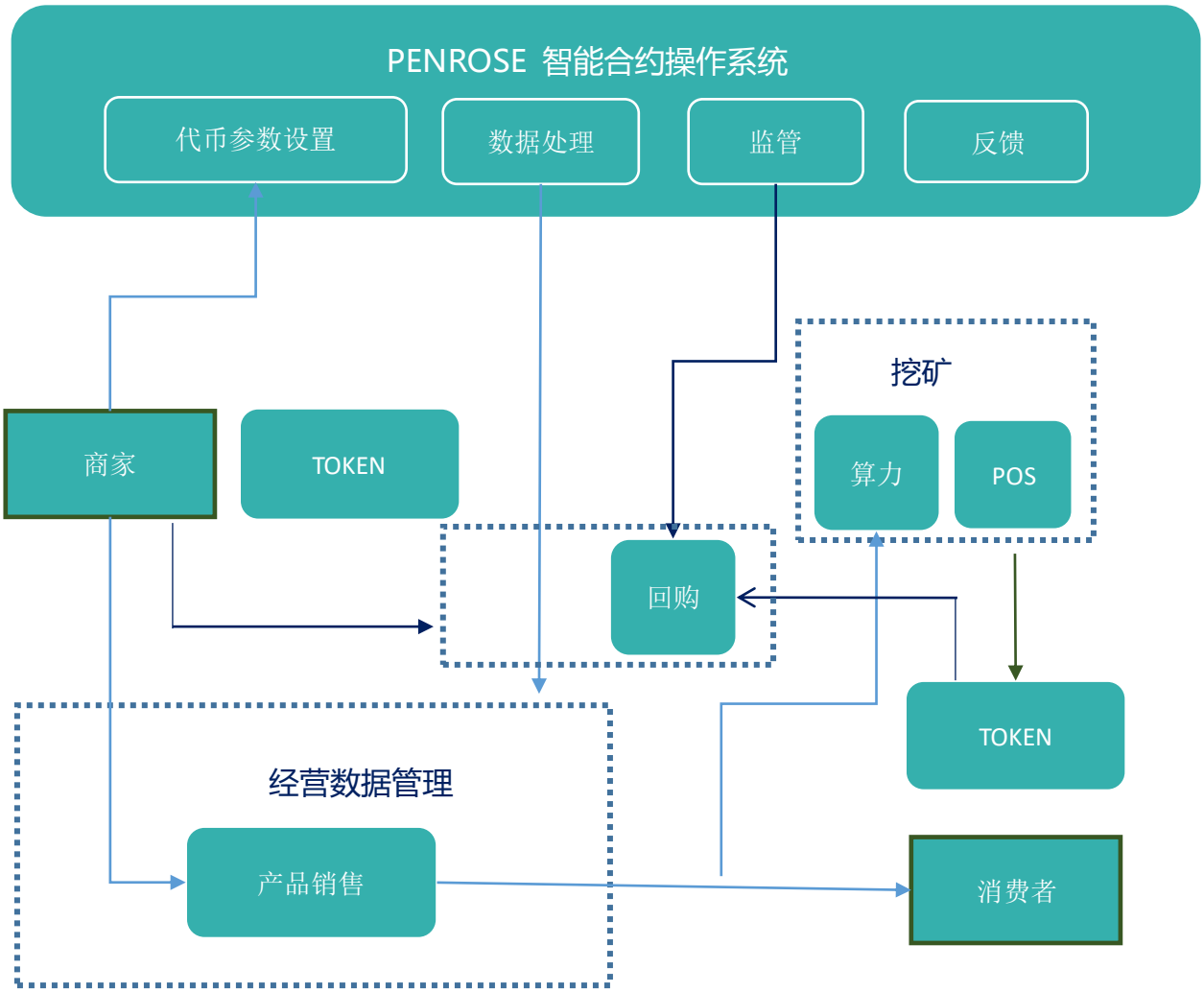
d. 触发合约提交维权结果

e. 合约执行，通过 Oracle, DataFeeds 校验结果，通过则发放奖励

品牌宝就是一个任务型打赏应用。它可以表述为品牌持有者对品牌打假、维权、推广等应用的悬赏。品牌宝就是作为这个行业的 DAO，使品牌商和用户直接建立关系。这样做的好处有：使打假覆盖面广，可以做到人人打假；没有了中间环节，使打假的成本更低。

6.2 品利宝

商家通过品利宝，在 PENROSE 上发行自己的 TOKEN。商家可以通过智能合约模板操作界面，选择要发的 TOKEN 名称、数量。用户通过消费和持仓进行挖矿产出该代币。



参数设置

数量、代币名称、挖矿产出

数据处理

商家的销量、盈利数据、TOKEN 回购金额计算

监管和反馈

回购监管、投诉反馈

6.3 品溯宝

PENROSE 之上的品溯宝，由以下几个部分组成：

IOT 数据采集体系：IOT 体系核心价值在于它在产品生产过程中，对过程数据进行自动采集并上传至分布式数据库，中间无需人工干预，实现数据唯一、可信性。

共识数据处理、存储体系：以 Qtum、Ink 为底层进行自主开发的区块链平台，实现对 IOT 设备采集的数据进行分类存储，其中共识数据存储在区块链中；图片、产品数据存储在 IPFS 分布式存储中，引入以太坊中梅克尔树存储方案。

终端消费体系：作为品溯宝面向用户的环节，这个体系包含了查证功能，实现消费者对所购买产品的溯源信息查询、代币兑换等功能。

品溯宝的核心工作机制和流程：

a. 产品生产过程中的数据采集

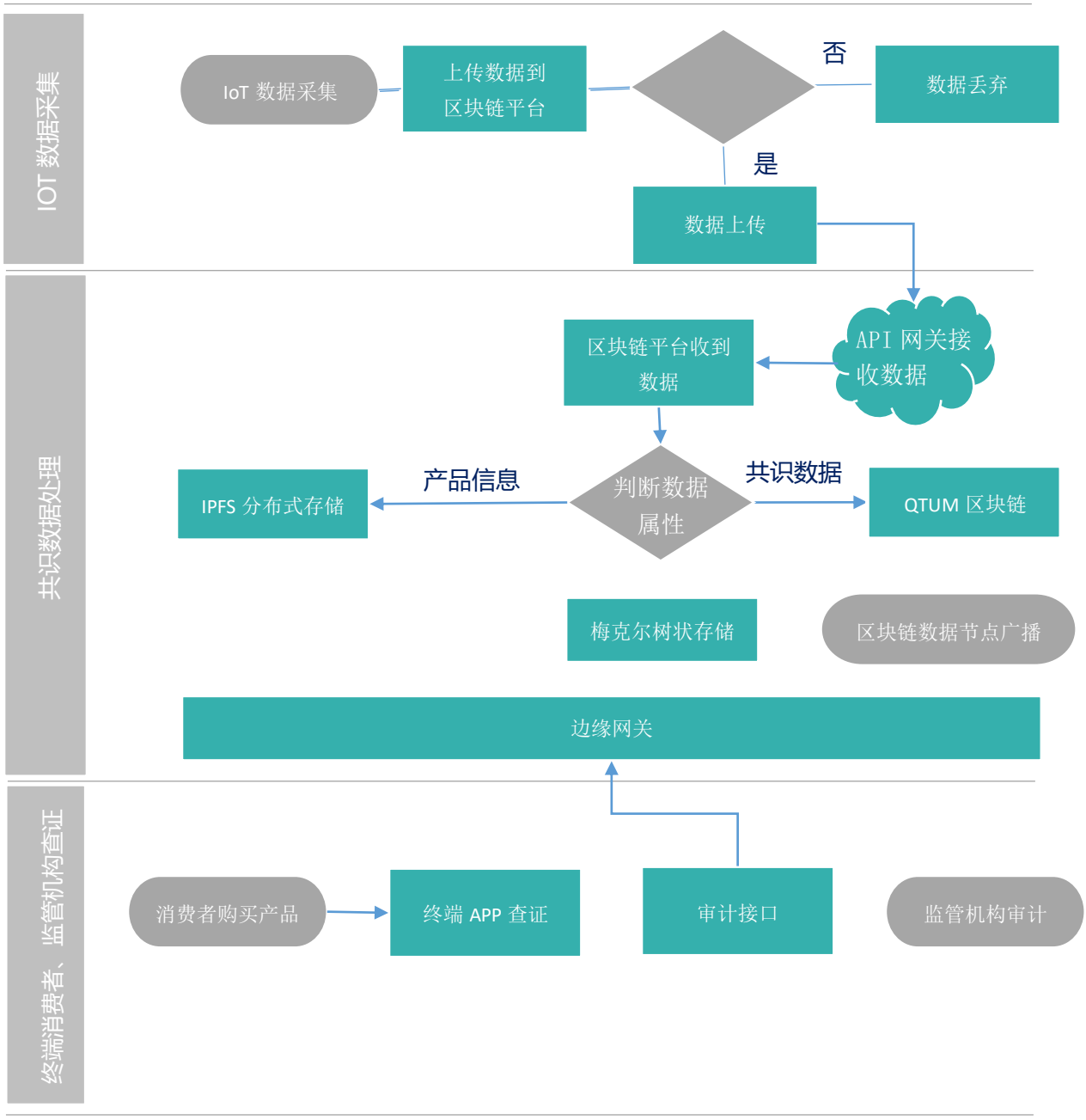
b. IOT 采集的数据通过 API 边缘网关上传至品溯宝

c. 品溯宝对边缘网关传输的数据源进行身份认证，以确保数据时由经认证的节点上传

d. 品溯宝对认证后的数据进行分类存储，并广播到联盟链中的所有节点

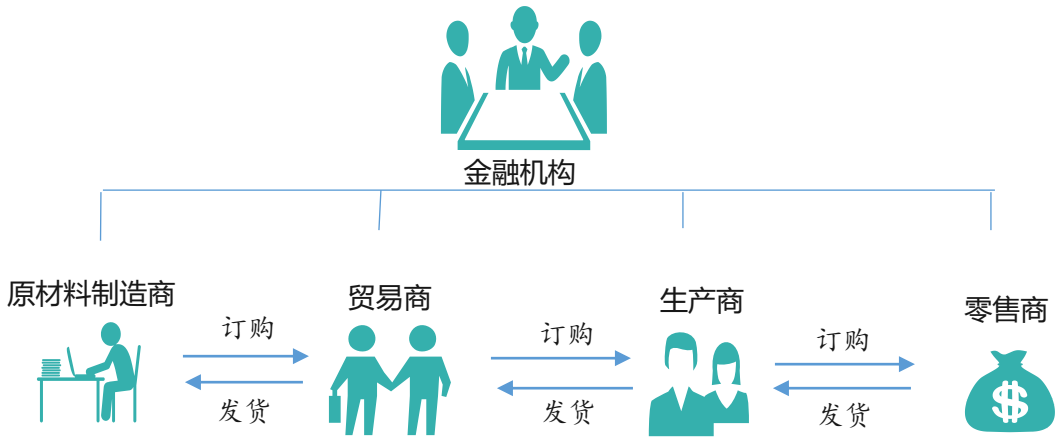
e. 终端用户使用 APP 进行产品真伪查证

f. 监管层对平台中所有的产品进行审计

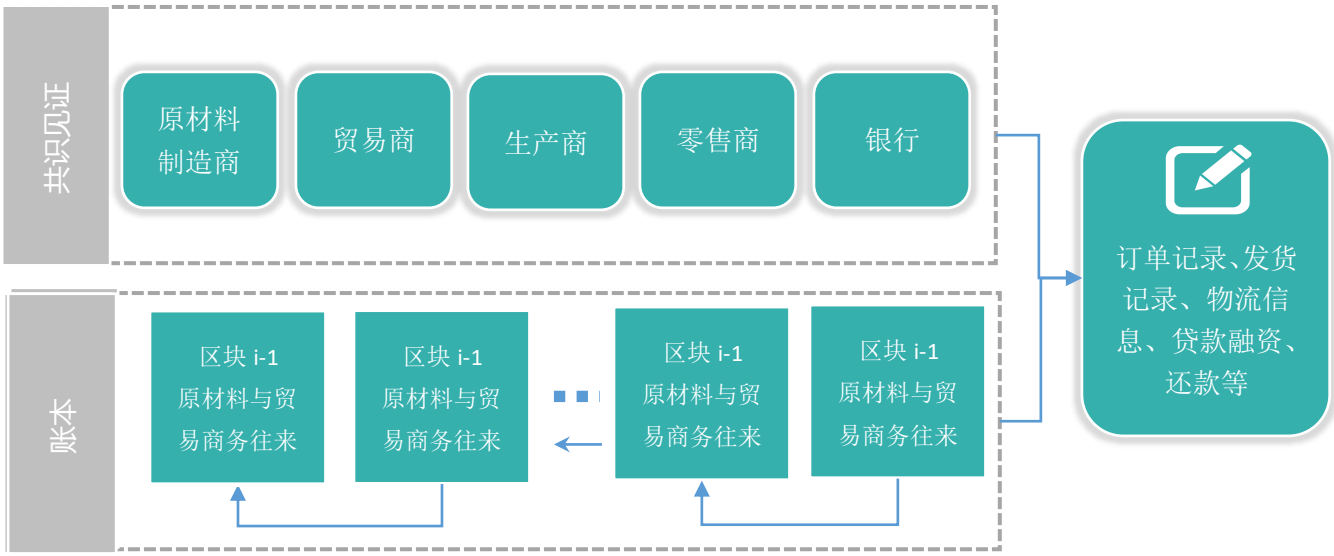


通过品溯宝，可以实现品牌溯源。它的实现步骤首先对商品的生产、流通数据采集，然后上次该数据到区块链平台。这些数据采用分布式存储，存储到各个节点上。在查证环节，只要把数据调出来即可，查证环节通过 APP 进行查证数据。

6.4 品融宝



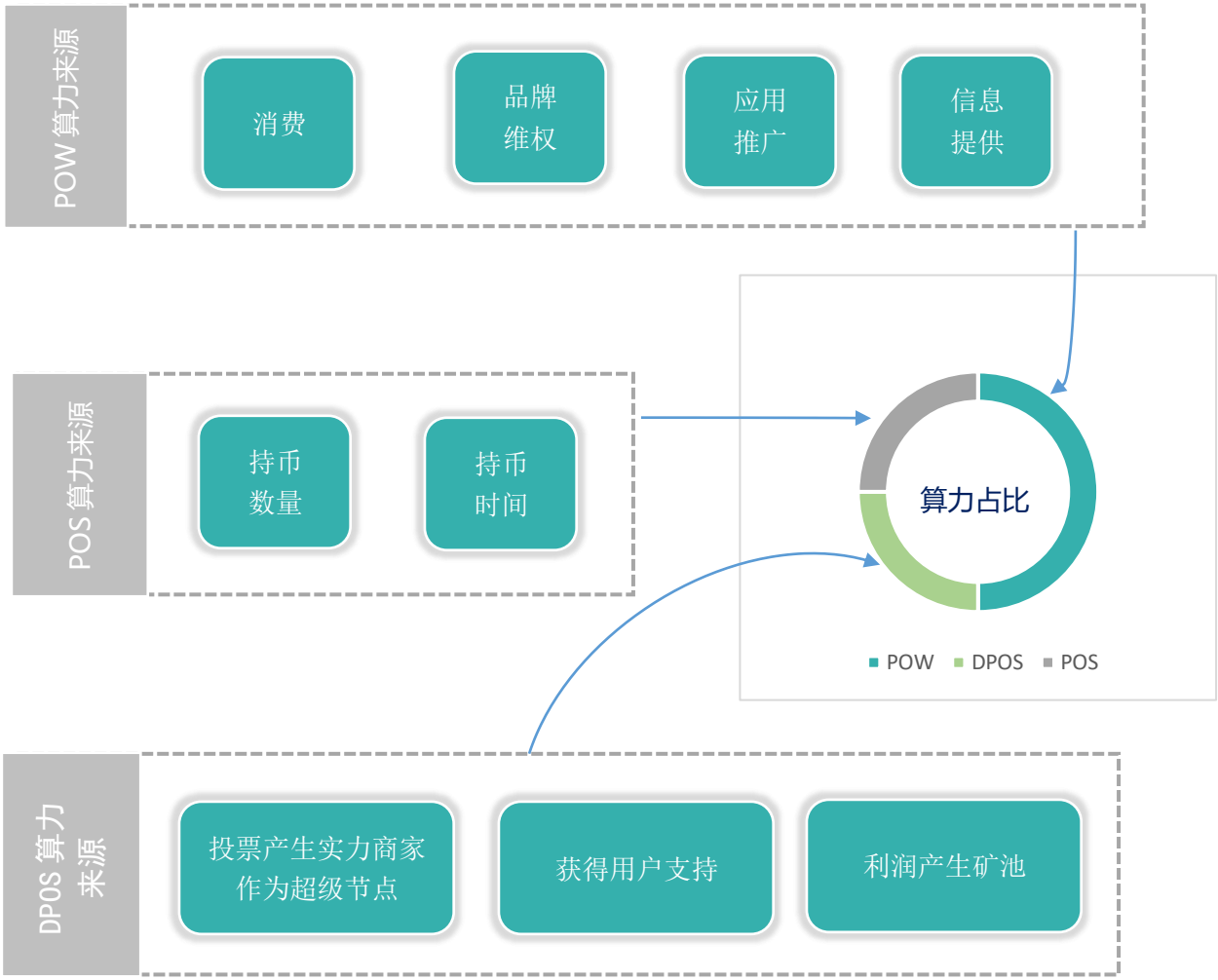
品融宝的用户角色：原材料制造商、贸易商、生产商、零售商。通过 PENROSE 对各个角色行为进行数据存储，从而获得经营信息，给金融机构对用户进行信用评估提供依据。



PENROSE 利用分布式账本记录和跟踪交易信息，可以获得贸易交易量、交易时间、物流信息、应收款或应付款。从这些信息中，可以判定各个环节的商家运营情况，给贷款融资提供依据。

另一方面，贷款负债信息、还款信息、违约信息也有效记录在分布式存储系统中，区块记录信息不可篡改和永久保存，给金融机构有价值的信息。

6.5 挖矿生态



POW

通过分布式零售环节，用户进行消费挖矿。品牌宝、品溯宝、品利宝的应用之中，用户的行为记录作为算力，进行挖矿。为了更快的把 PENROSE 的应用推广开来，把推广作为算力来源；用户也可以通过信息提供获得算力，提供信息包括对商家的监督信息、技术反馈。

POS

用户通过持有 PENROSE 代币获得算力。持有的数量越多，时间越长，所奖励的代币就越多。

DPOS

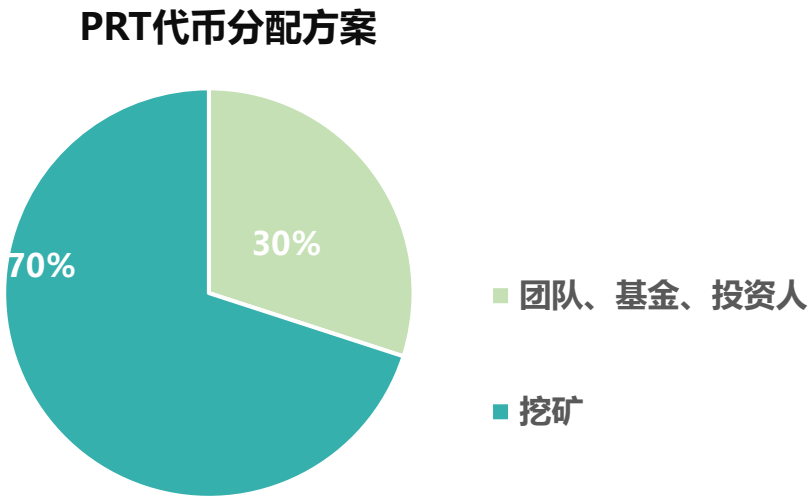
以商家作为超级节点，进行组团挖矿。矿池的产量和参与商业用户量、经营利润、运营客户好评有关。

7、TOKEN 模型

7.1 分配方案

PRT 用途：未来在 PENROSE 生态中，PRT 将会是整个生态的血液。举例：PENROSE 之上的应用用户使用应用时都会需要消耗一定量的 PRT，而在应用中贡献价值的用户将会获得一定量的 PRT。

PRT 的总量为 10 亿，基于 Qtum 的 QRC-20 标准发行的 Token，属性使用币，其中 30%为团队、基金、投资人，70%为挖矿奖励。



7.2 治理机制

PENROSE 基金会治理结构的设计目标主要考虑开源社区项目的可持续性、管理有效性及数字资产的安全性。PENROSE 基金会的治理采用 PENROSE 决策委员会、PENROSE 执行委员会和职能委员会三层治理结构，同时会引入外部的董事，包括投资人、研究院校的学者作为独立董事。

PENROSE 将构建汇聚技术爱好者、垂直行业资源、投资者和第三方开发者形成一个以区块链技术为核心且具有全球影响力的开源社区。通过垂直行业资源将区块链技术落地到新零售的各个场景种，形成多个场景应用，然后把各个场景应用融合到 PENROSE 网络中，打造高效、稳定的价值流转体系。

8、团队成员

8.1 发起人团队

怒 发

互联网领域资深专家，高级运营专家，曾就职于阿里巴巴集团 5 年，是阿里巴巴广告业务部 TOP 记录保持者，连续创业者，经营的公司规模达 200 多人，具有丰富的企业管理经验，具备敏锐的市场分析能力和洞察能力。

赵 冲

区块链领域的技术专家，南京大学硕士，中国首届区块链大赛优秀奖得主，浙江数秦科技有限公司首席技术官，保全网(baoquan.com)联合创始人，云挖矿平台汇比特(sumbtc.com)创始人，杭州晓冲科技有限公司 CEO。

初 旭

区块链行业技术工程师，蚂蚁金服技术专家，基金产品线技术负责人，恒生电子资深技术专家、兼产品线负责人。13 年进入区块链领域，一直从事比特币、以太坊、Hyper ledger 等区块链技术的研发和探索。

白惠源

16 年互联网从业经验，阿里巴巴集团 10 年，历经从数百人到 2 万人，先后管理多块核心业务，有着极为丰富的运营管理经验和沉淀。平安集团互联网金融创新业务副总裁、兼陆金所副总经理。知名独角兽公司合伙人、首席运营官，在其率领下 2 年间创造估值近百亿，新经济领袖人物。

胡耀宗

在阿里巴巴集团任职 10 年期间，担任阿里巴巴渠道总监；世纪佳缘副总裁，慧聪网副总裁；杭州梦想小镇孵化器纵贯会创始人，拥有丰富的电商资源，精通团队管理，擅长运营搭建，互联网行业的领军人物。

明 锋

曾在阿里巴巴集团任职 5 年，担任阿里巴巴品牌业务部负责人、兼诚信通续签团队负责人。连续创业者，担任多家公司的总经理，中小企业品牌导师，拥有百人以上规模团队的管理经验，善于产品定位，互联网行业资深专家。

李 浩

区块链技术专家，前蚂蚁金服区块链平台部高级研发工程师，前保全网 CTO，数字货币交易所币易联合创始人，对区块链分布式系统，共识算法，智能合约以及矿池技术等都有深入的研究。

研究生学历,2016 年毕业于 University of Laverne，有丰富的海外市场及投资经验。

Ryan Ren

Adrian Niculae

General Manager at Anemona Com，Studied at ThinkBuzan，From Ploiesti，Romania，He is a foreign promoter in the block chain of New World.

From the United States，Studied International business at University of Phoenix，He is the American promoter of the New World on the block chain.

Jerry Hoyler

郭金辉

互联网营销总监，阿里巴巴集团 5 年从业经验，网销宝部门核心骨干。担任多家公司的销售总监，善于销售团队的组建和管理，带领的团队屡次荣获销售团队冠军，在团队管理上面有着独特的见解，且取得卓越的成绩。

财务专家，曾就职于博库网络传媒集团，有着丰富的财务管理经验，精通各类财务制度流程的建立和优化。多年的企业财务实战经验，善于成本控制、数据分析、财务预算等方面。

叶海燕

丁 欢

阿里巴巴商家成长中心资深产品专家，有着 5 年丰富的产品运营经验，曾服务上千家国内外知名品牌。百博维权创始人兼总经理，善于团队搭建和管理经验，互联网运营行业资深专家。

Lives in Mumbai, Maharashtra，Studied at University of Mumbai.

Sanjay Pawar

其 他

新界项目工作人员，目前超过 100 人，每天都在正常进行开发和推进工作。

8.2 投资人及顾问团队

张瑞东

美国内布拉斯加大学林肯分校信息管理学博士，美国威斯康辛大学终身教授，浙大 AIF 区块链工作室主任，曾任美国华人国际信息系统协会会长（ICISA）。研究领域包括云计算的架构及优化、区块链及数字货币技术的应用及开发、电子商务、开源技术以及下一代互联网的发展及应用。

郑 刚

复旦大学经济学博士学位，2014 年入选上海市委组织部评定的“上海市领军人才”，现任东吴（苏州）金融科技有限公司董事长。历任上证所技术中心副主任、技术规划与服务部总监、上海证券通信有限责任公司副董事长兼总经理。获得证券期货行业科技进步一等奖、上海市金融创新奖。沃顿商学院的访问学者。

帅 初

Qtum 发起人，毕业于 Draper University(英雄学院)和中国科学院，之前就职于阿里巴巴集团，博士期间就致力于区块链技术的开发和研究，具备丰富的区块链行业的开发经验。

唐 凌

纸贵科技创始人&CEO；Ink labs 基金会主席；Jenga Block-chain Capital 管理合伙人；西安交通大学区块链技术研究实验室发起人、APEC 未来学院顾问委员会委员、丝绸之路创新设计联盟专家组成员

Daniel

英国克兰菲尔德大学金融硕士-曾任英国顶级区块链企业 Credits 商业总监,及 Fintech-Labs 商业经理，具备丰富的区块链项目管理和运营经验。

赵 敏

复朴投资创始人，德同资本(浙江)总经理，同时是众多上市公司，聚光科技，泰瑞机器的投资人。

任杰锋

四季大通集团董事局主席，江苏省南京市政协委员，《中国食品安全报》副理事长兼副总编辑，CCTV2008 年度“三农先锋”人物中国健康营养工作委员会会长。

David K. Waldman

President & CEO，David has a B.S. in Communications and Political Science from Northwestern University. He has a long and successful track record working with publicly traded companies of all sizes and across a wide range of industries, and has served as vice president at a leading New York City based investor relations firm, as well as two other premier investor relations firms. He is a leading export on communications counsel.

Rodd Leeds

Rodd consults for microcap companies across the country now. He worked in Wall Street and was a member of the American Stock Exchange. He served as Vice President of Marketing and Sales for this company.He purchased a private ambulance service, and later sold to an entity that became the largest private ambulance company in the U.S. in a deal backed by Morgan Stanley.

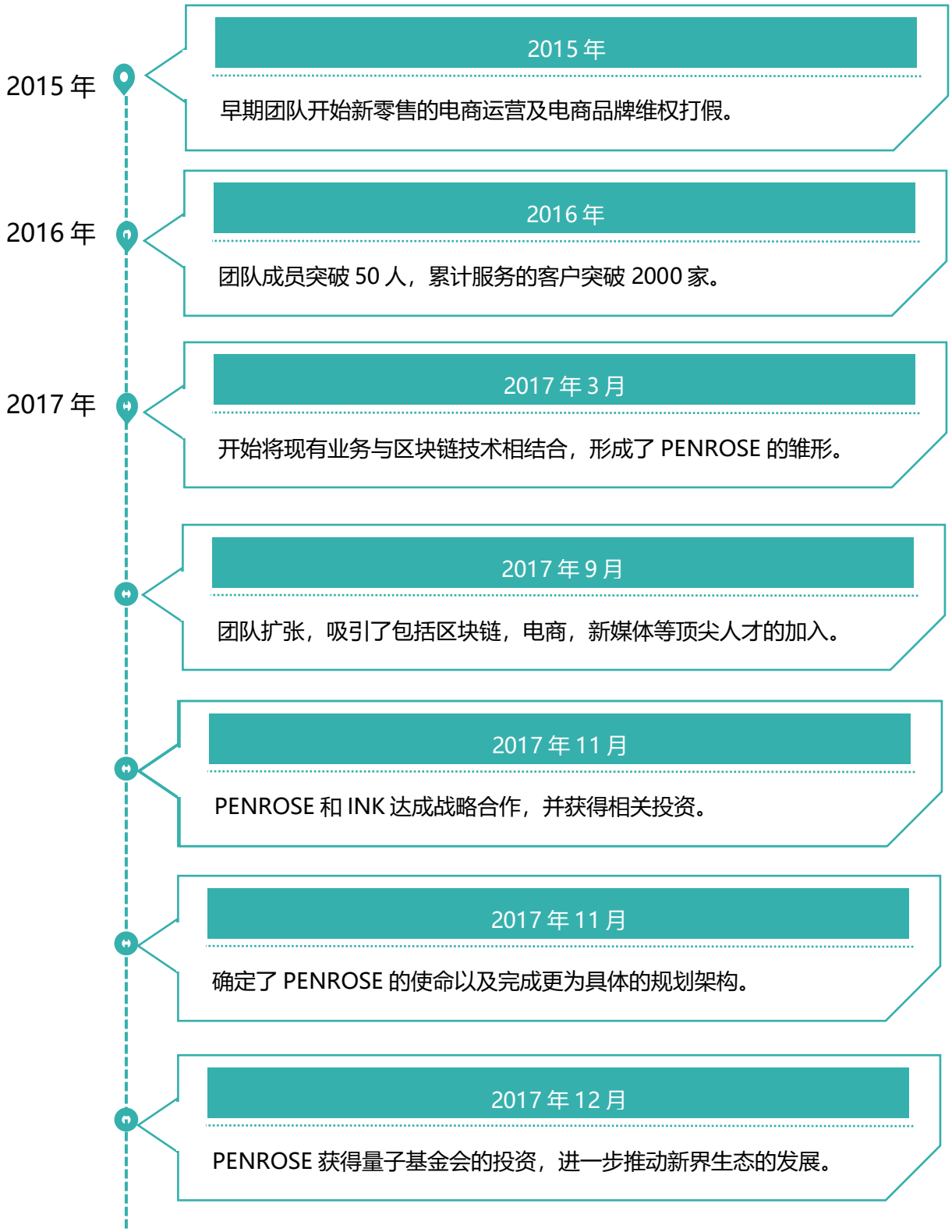
俪博士

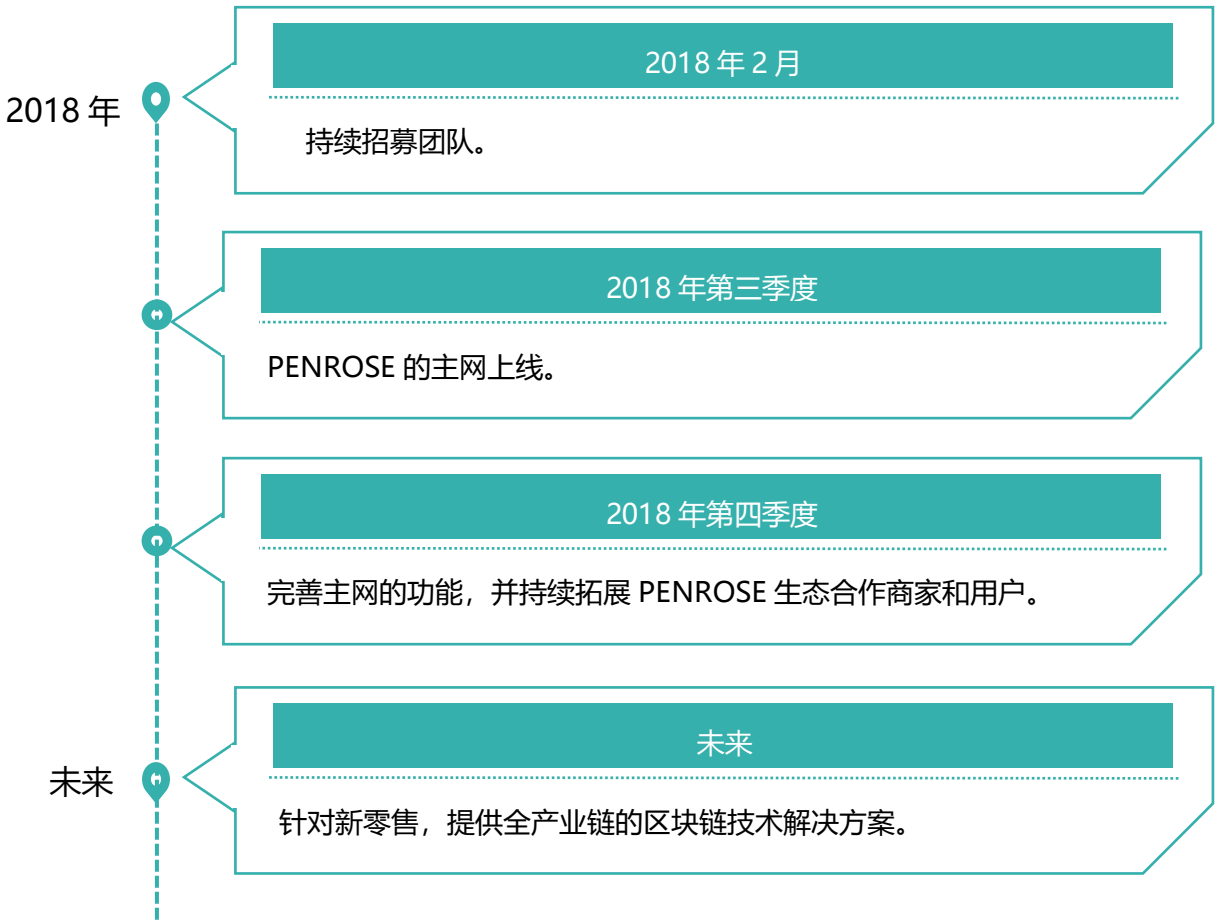
汇钰资本创始人。

徐小龙

现 Qtum 首席开发工程师（中国），硕士毕业于中科院研究生院，曾供职于微软，后加入过腾讯天美工作室，拥有着非常丰富的软件开发经验。

9、PENROSE 发展路线





PENROSE 主体机构拥有丰富的商业零售、品牌维权方面经验。早在两年前，服务商家就超过 2000 家，拥有很扎实的客户基础。PENROSE 不同于多数区块链项目，在于我们已经自有商业盈利模式并产生巨大利润。通过开发 PENROSE 区块链应用，可以解决机构主体以及整个行业所面临的问题。这也是 PENROSE 开发设计的初衷。

PENROSE 的市场覆盖面广，价值潜力巨大。PENROSE 团队，通过三年多的实践，已经对自己的区块链技术解决方案充满信心！