



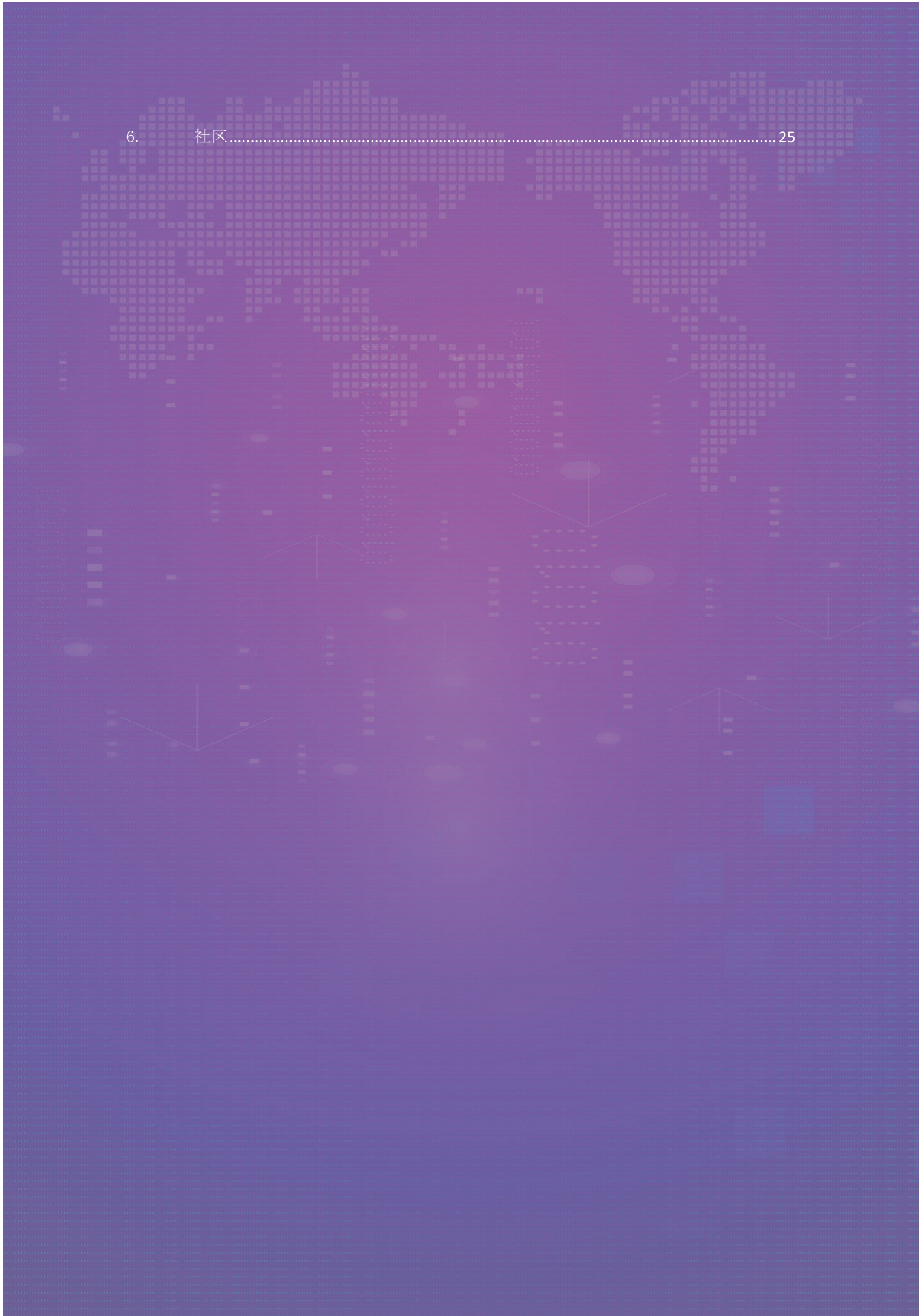
DALICHAIN 白皮书

提供最好用的商业区块链服务

www.dalichain.io

目录

1.	DALICHAIN 的设计理念	1
1.1.	区块链的背景和意义	1
1.2.	区块链的行业趋势	1
1.3.	DALICHAIN 设计思想与价值	2
1.4.	DALI 的产生	3
2.	DALICHAIN 的技术特征	5
2.1.	站在巨人的肩膀上	5
2.2.	融入第 5 代移动通信	6
2.3.	DALICHAIN 的整体网络架构	8
2.4.	DALICHAIN 的基本网络特性	8
2.4.1.	共识机制	8
2.4.2.	安全机制	10
2.4.3.	GAS 的设计理念	12
2.4.4.	区块链浏览器	14
2.4.5.	智能合约&虚拟机	14
2.5.	DALICHAIN 面向商业应用的特性	16
2.5.1.	客户端	16
2.5.2.	跨链网关	17
2.5.3.	对象化描述	18
2.5.4.	零知识证明	20
2.5.5.	可信智能合约商店	20
3.	DALICHAIN 基金会治理架构	21
3.1.	DALICHAIN 基金会的风险评估及决策机制	22
3.2.	DALICHAIN 基金会的信息披露原则	22
4.	DALICHAIN 实施及发展计划	23
4.1.	DALICHAIN 技术发展路标	23
4.2.	DALICHAIN 的生态发展路标	24
5.	创始团队	24



1. DALICHAIN 的设计理念

1.1. 区块链的背景和意义

互联网经过近 30 年的发展，已经实现了信息传递的数字化，无所不在又触手可及的信息已成为了人类生活的一部分。由于过多的信息泛滥，虚假、错误、欺诈信息也无处不在，因此信息互联网并没有解决信用基石的问题。在未来的互联网世界，人类将更为广泛地构筑无所不有、无所不通的数字信任世界，而这个新的数字化世界必须构建在一个信用基石之上，这个信任基石则是区块链技术。

区块链技术作为下一代信用与价值互联网的基础协议，将承载更为智能高效、公平透明的未来社会，成为数字世界的基石。

再过 30 年，当我们再次回望时，我们会真诚地感谢，30 年前的区块链给我们、给这个世界带来的深刻改变。

1.2. 区块链的行业趋势

区块链是一种由多方参与者共同维护的共识系统，并利用密码学来保障安全性、不可篡改性、不可抵赖性，是一种不需要第三方来担保的、高度可靠的信任体系。它作为下一代信用互联网的底层技术，将承载更为智能高效、公平透明的未来社会，成为驱动数字信任世界的引擎。

区块链技术经过多年的发展，已经历了三个重要阶段：

区块链 1.0 是以比特币为代表的数字货币应用，主要解决货币和支付手段的去中心化，其场景包括支付、流通等货币职能。早在比特币创建之初，设计者就考虑让其具有可编程的特征，从而可以支持多种交易类型。

区块链 2.0 是以数字货币与智能合约相结合，为金融领域的业务流程进行优化的应用，可用来注册、确认和转移各种不同类型的资产及合约，如各种金融交易信息、资产登记等。

区块链 3.0 则超越金融领域，为各行各业提供多中心、分布式的解决方案，可实现全球范围内数字化的物理资源和资产分配，能在不同领域之间完成大规模的协作。

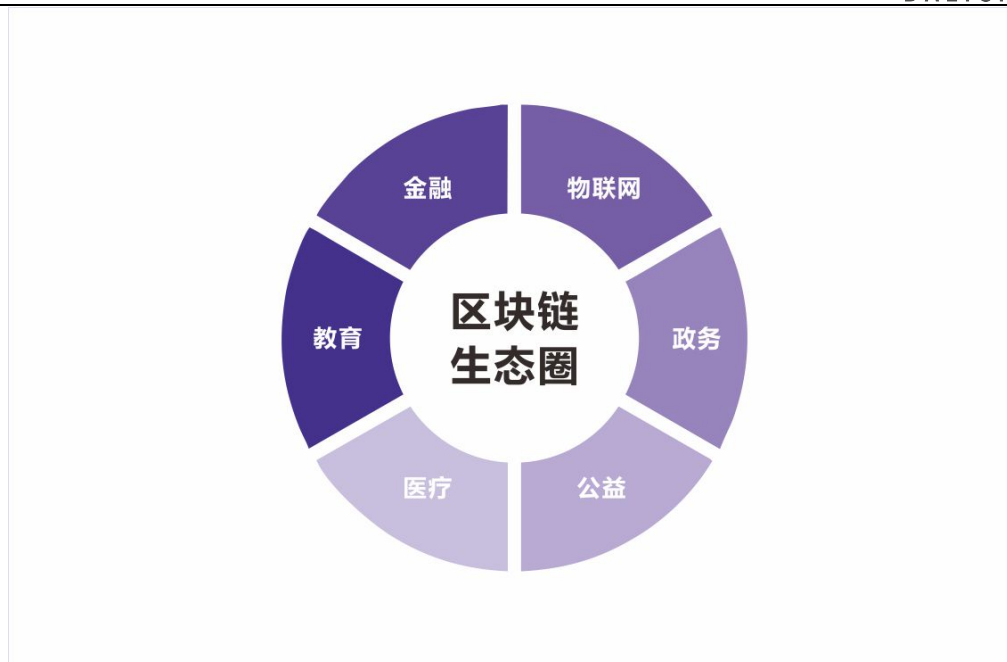


图 1-1：区块链应用生态圈

1.3. DALICHAIN 设计思想与价值

DALICHAIN 作为区块链 3.0 技术，志在打造最好用的、为商业服务的公链。针对物联网、供应链金融、冷链物流、数字 IP、公益慈善等行业进行了长期研究和技术探索，已形成了适用于多种行业的区块链解决方案。区块链注定将对这个世界产生巨大的影响，DALICHAIN 作为这一革命的参与者，有责任去攻克区块链发展道路上的各种难题，让区块链技术更成熟，让行业应用更简单，让世界更美好。

DALICHAIN 将为企业提供一个稳定、方便使用的区块链云服务平台。企业用户可以通过调用不同的技术接口，直接使用区块链技术的各种功能，在业务层面实现应用与区块链网络的分离，整个过程企业用户不需要关心区块链具体的技术实现细节。

- a) 链上应用：区块链系统提供通用服务接口供数据上链，对接难度低，不影响企业现有业务流程；
- b) 链内应用：使用智能合约来部署基于区块链的分布式企业应用，使其具备更高的安全性、健壮性、稳定性；
- c) 离链应用：AI、大数据等核心价值系统采用该方式灵活部署，根据业务需求可动态配置不同的离链应用，实现高扩展性。

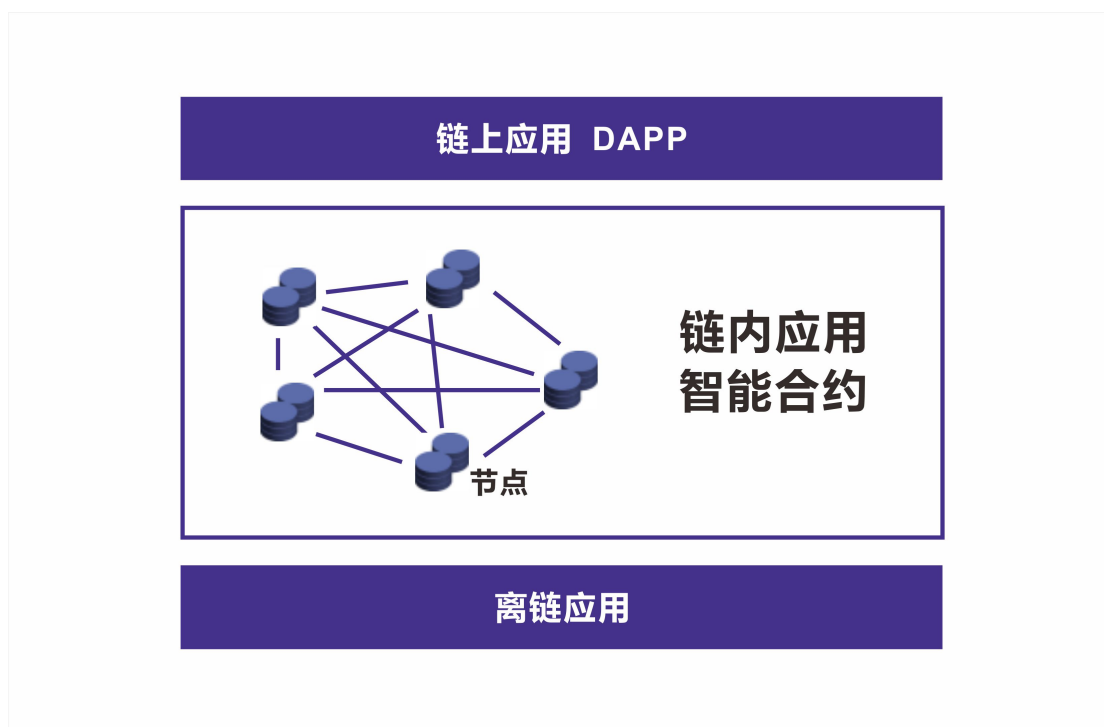


图 1-2：DALICHAIN 的应用分层

1.4. DALI 的产生

DALICHAIN 的原生代币，命名为 DALI，代表 DALICHAIN 的使用权。总共发行 2.1 亿枚，其总量上限已设定，永不增发。DALI 作为数字经济的通证，使得整个区块链平台有了一个内生的、等价的、所有参与方共同维护的交换媒介，将对数字资产的保护与升值产生全球性的影响。

DALICHAIN 团队作为区块链世界中的“科技造梦者”，将利用先进的区块链技术结合实体经济，带领人们进入数字经济新世界。

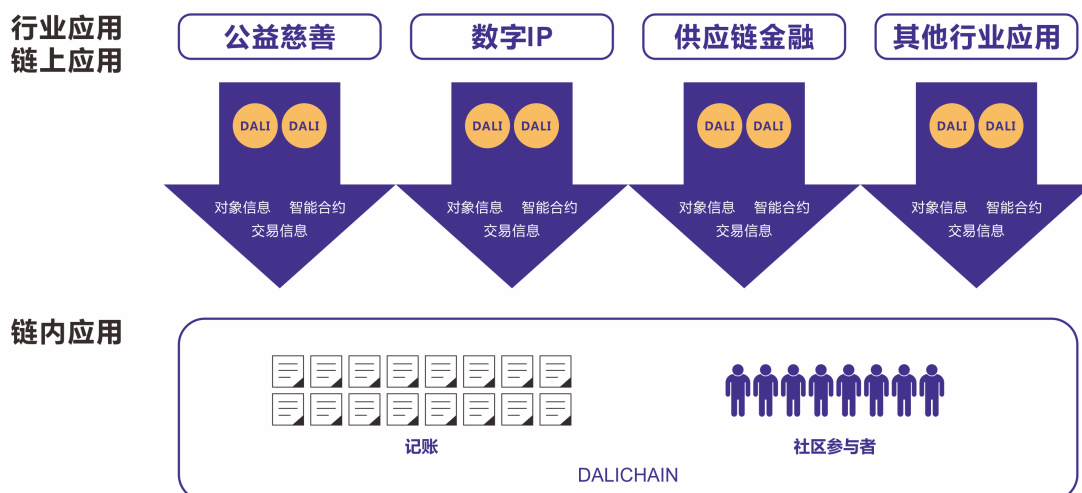


图 1-3：DALI 在 DALICHAIN 中的使用

DALI 作为 DALICHAIN 使用权的载体，随着市场的交易丰富，将不断提升价值和创造价值，增值的动因有如下几点：

a) 支撑的行业繁荣、市场规模持续扩大

DALICHAIN 的市场持续扩大（接入的行业越多，DALI 流通越快速）及用户数量的几何式增长均会带动 DALI 增值。以艺术数字 IP 领域为例，持有 DALI 的用户群、持有艺术品版权的用户群、文创领域合作机构、艺术家等用户会构成 DALICHAIN 用户生态，而 DALI 就是生态内的血液，充当用户间价值传递的介质。

b) 承载的行业应用的资产规模扩大

DALICHAIN 支撑的行业应用的资产规模也将影响 DALI 的价值。以数字 IP 为例，IP 总量增长和单品 IP 升值，都会带来总交易量的上升，促进 DALI 在链上的流通，也会拉动 DALI 的增长。链上应用的资产规模越大，DALI 的增值效应就会越大。

c) 业务种类的增加

以数字 IP 为例，随着 DALICHAIN 的发展，生态内各种业务流程逐渐清晰，在 DALICHAIN 承载的数字版权流通、交易、IP 孵化、指数排行等资产或资金的流转环节，都会产生可观的 DALI 使用需要，而 DALI 持有者无疑是最大的获益者。DALI 的使用场景将越来越广泛，这将会形成大量供需关系，从而推升 DALI 的价值。

d) 信用体系的建立

随着 DALICHAIN 生态发展，其在资产、用户、机构等方面会逐渐建立信用机制，未来伴随着信用体系的运转产生的价值也是非常可观的。

2. DALICHAIN 的技术特征

2.1. 站在巨人的肩膀上

DALICHAIN 的快速发展离不开区块链的演进，区块链演进经历了以比特币为代表的 1.0 时代，以太坊智能合约为代表的 2.0 时代。我们感谢所有在数字世界付出了巨大努力的各界精英们，这条路上我们并不孤单，我们是站在了巨人的肩膀上，并根据自身业务做了独特创新处理。区块链技术演进如下图：



图 2-1：区块链的演进历史

区块链 1.0-比特币：2009 年初，比特币网络正式上线运行。作为一种虚拟货币系统，比特币的总量是由网络共识协议限定的，没有任何个人及机构能够随意修改其中的供应量及交易记录。在比特币网络成功运行多年后，部分金融机构开始意识到，支撑比特币运行的底层技术——区块链实际上是一种极其巧妙的分布式共享账本及点对点价值传输技术，对金融乃至各行各业带来的潜在影响甚至可能不亚于复式记账法的发明。

从其实质分析，区块链就是一种无须中介参与，亦能在互不信任或弱信任的参与者之间维系一套不可篡改的账本记录的技术。区块链 1.0 的典型特征如下：

- a) 以区块为单位的链状数据块结构。
- b) 全网共享账本。
- c) 非对称加密。
- d) 源代码开源。

区块链 2.0-智能合约（以太坊）：2014 年前后，业界开始认识到区块链技术的重要价值，并将其用于数字货币外的领域，如分布式身份认证、分布式域名系统、分布式自治组织等。这些应用称为分布式应用（Dapp）。用区块链技术架构从零开始构建 Dapp 非常困难，但不同的 Dapp 共享了很多相同的组件。区块链 2.0 试图创建可共用的技术平台并向开发者提供 BaaS（Blockchain as a service）服务，极大提高了交易速度，大大降低资源消耗，并支持 PoW、PoS 和 DPoS 等多种共识算法，使 Dapp 的开发变得更容易。区块链 2.0 的典型特征如下：

- a) 智能合约：区块链系统中的应用，是已编码的、可自动运行的业务逻辑，通常有自己的代币和专用开发语言。
- b) Dapp：包含用户界面的应用，包括但不限于各种加密代币，如以太坊钱包。
- c) 虚拟机：用于执行智能合约编译后的代码。虚拟机是图灵完备的。

DALICHAIN 致力于提供针对企业应用整体需求的区块链技术。确保交易速度、交易安全性、分布式应用能力、便捷性、低碳环保等，并形成支持不同分布式应用（Dapp）的能力。优化比特币与以太坊在业态应用方面存在的交易速度、共识机制、灵活性、大数据处理、能耗浪费等值得提升的方面。

2.2. 融入第 5 代移动通信

二十年来从 2G（第二代移动通信）到 5G（第五代移动通信），移动通信网络不断更新换代。在 4G 时代以前，移动通信网络都是为连接“人”而生，但随着万物互联时代的到来，移动通信网络将面向连接“物”而演进；从而在未来移动数字世界形成人人互联，万物互联的超级移动通信网络。

为满足人人互联、万物互联的特点与需求，基于蜂窝的窄带物联网（Narrow Band Internet of Things, NB-IoT）成为万物互联的一个重要支撑。NB-IoT 构建于蜂窝网络，只消耗大约 180KHz 的带宽，可直接部署于 GSM 网络、UMTS 网络或 LTE 网络，以降低部署成本、实现平滑升级。

NB-IoT 在物联网应用中的优势显著，为传统蜂窝网技术及蓝牙、Wi-Fi 等短距离传输技术所无法比拟。首先其覆盖更广，在同样的频段下，NB-IoT 比现有网络增益 20dB，覆盖面积扩大 100 倍。其次是对海量连接的支撑能力，NB-IoT 一个扇区能够支持 10 万个连接。目前全球有约 500 万个物理站点，假设全部部署 NB-IoT、每个站点三个扇区，那么可以接入的物联网终端数将高达 4500 亿个。同时 NB-IoT 的功耗更低，仅为 2G 的 1/10，终端模块的待机时间可长达 10 年。在成本上也将更低，模块成本有望降至 5 美元之内。未来随着市场发展带来的规模效应和技术演进，功耗和成本还有望进一步降低。此外，NB-IoT 连接所收集的数据可以直接上传云端，可以支持更广泛的大数据分析与应用。

整体上 5G 移动通信的发展必然也是 P2P 为核心的分布式架构，原来的中心化架构必然要进行演进；而区块链是天生在 P2P 的理念之上的系统；将区块链与 5G 通信深度结合可更好的支撑 DALICHAIN 的技术发展和应用：

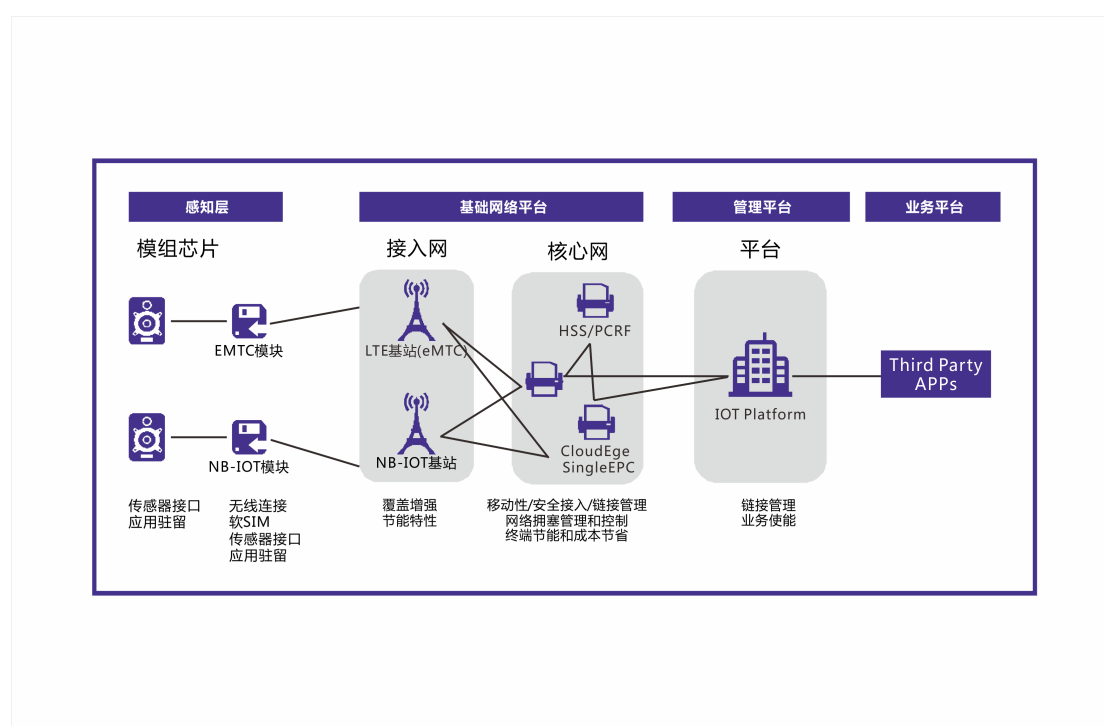


图 2-2：NB-IoT 网络拓扑图

- 终端接入的可信身份验证（可以广泛的应用在物理 IP 的存证方面）；
- 每个接入者（物）的隐私保护（移动通信密码学与区块链密码学结合）；
- 网络数据的真实性保护（相得益彰）；
- 提供便捷快速的 P2P 传输（得益于 5G 的发展）；
- 智能方便的费用结算（基于智能合约分布式结算，不依赖于中心，也不依赖于全共

识);

f) 可以创建新的商业模式。

2.3. DALICHAIN 的整体网络架构

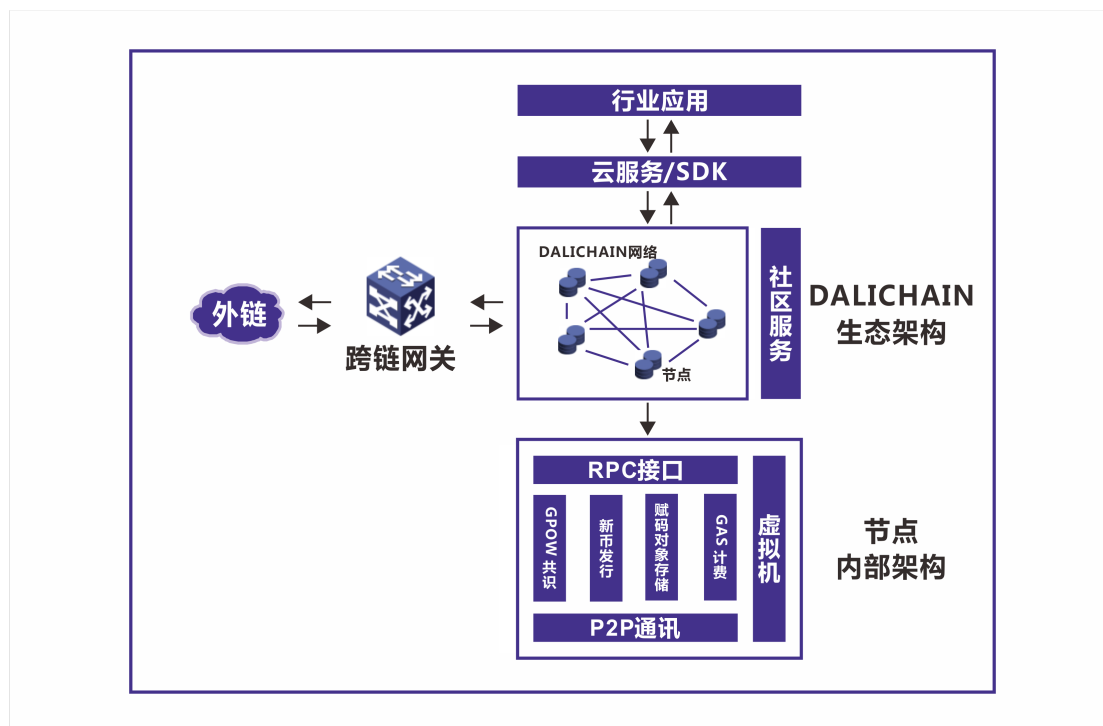


图 2-3：DALICHAIN 系统架构图

2.4. DALICHAIN 的基本网络特性

2.4.1. 共识机制

共识机制作为区块链的一项核心技术，在区块链生态发展中有着相当重要的作用，简单来说是指所有节点通过记账并共享账本来完成数据同步的自动化过程，形成共识后的每个节点将拥有相同的账本数据。区块链技术发展至今，被广泛使用的共识机制主要有两种，分别是：POW（Proof of Work，工作量证明）和 POS（Proof of Stake，权益证明），两种共识算法各有特点，适用于不同的生态场景。

POW 是比特币使用的共识机制，优点是去中心化程度高，节点参与门槛低，节点数量越多系统越稳定；缺点也是显而易见的：随着节点数量越来越多，网络会变得越来越拥堵，造

成交易确认时间延迟越来越长；另外，日渐成熟的挖矿产业链逐渐形成了算力集中的趋势，会造成的资源浪费和“51%攻击”的问题。

POS 的出现正是为了解决以上 POW 的问题，但 POS 完全摒弃了去中心化的思想，将记账权交给了持有 Token 的节点，这种方式虽然避免了资源浪费，但又形成了新的中心化问题，甚至可能造成世袭的局面（尤其是 DPOS，股权权益证明），使整个生态变得中心化，因此 POS 并不适用于公链。

DALICHAIN 作为一条公链，经过研究和慎重考量，最终选择采用 POW 作为基础，在其系统架构上针对未来商业应用的需求进行优化，形成了 DALICHAIN 独有的共识机制——GPOW（Green Proof of Work，绿色工作量证明）。GPOW 继承了比特币网络的主要特性，在主要参数上做了优化：区块大小为 10M，平均出块时间为 1 分钟，这使得交易确认时间被缩短到 6 分钟（比特币为 60 分钟）。除了性能提升之外，DALICHAIN 还引入了全新的算力规则，杜绝因算力集中引发的一系列问题，从而保障 DALICHAIN 在长期的发展过程中，节点始终能保持稳定、随机，在避免资源浪费的情况下同时又能保障系统的稳定性。

GPOW 的技术特性如下：

a) 提供节点记账服务费

比特币网络为了提升网络稳定性，需要激励更多的节点参与进来，激励机制的算法会拿出一定量的比特币奖励参与记账的节点，节点通过 POW 机制争夺记账权，这个过程被称为“挖矿”，而参与争夺的节点被称为“矿工”。随着比特币网络的发展，形成了巨大的挖矿产业，也同时造成了巨大的能源损耗，因此这不是一个可持续发展的技术。

因此，DALICHAIN 移除了挖矿增发奖励的机制，突出了记账服务收费模式。随着更多的行业应用引入，更多的高价值信息记录，记账服务收费将成为对参与记账节点的巨大奖励。所有节点都可以参与记账，通过记账成功获得相应的记账服务费。

b) 节点标识

基于对 DALICHAIN 发展的充分考量，为保证整个网络的可持续高效性，DALICHAIN 在保障节点质量方面进行了诸多创新，节点标识就是其中一项。节点标识是指通过技术手段鉴别出诚实节点和非诚实节点（非诚实节点：定义为进行非法交易、不合规打包的节点），并用过奖惩机制尽可能多的保障诚实节点数量，减少非诚实节点的数量，将 DALICHAIN 网络保持高质量、高效的运行；实现可持续的生命力。

c) 分片（Sharding）

分片源于通信领域的网络优化技术，DALICHAIN 将其核心思想应用到了 GPOW 中，用于解决节点数量过多造成的网络拥塞问题。使用分片技术后，整个网络的性能不会随着网络规模的扩大而明显降低，维持整个网络高效运行；同时，分片服务可具备无限的可延展性，支撑不同行业的持续发展。

d) 算力均衡算法

DALICHAIN 坚持节点公平竞争的原则，通过算力均衡算法拒绝超高算力的节点接入（例如矿场、专业工作站等），避免出现区块链网络的中心化倾向（算力中心化是比特币发展的重大风险之一），造成不公平的竞争以及价值分配。算力管理作为一项节点准入条件，将通过硬件对超出标准的节点进行限制，使所有节点的算力保持在一个相对均衡分布的水平，这个将通过随机算法，根据网络整体算力的发展而实现持续的网络自优化，无需人工干预。

2.4.2. 安全机制

比特币区块链试验网络经过长期运行，已经证明了区块链在交易及历史记录存储上的安全性，DALICHAIN 的安全机制则建立在比特币之上，通过增加去中心化算力均衡算法等增强特性，就拥有了更强大的区块链安全性。

除了保留比特币核心安全技术之外，DALICHAIN 还针对行业应用专门设计了安全加密接口，为不同需求的行业提供 SDK，企业可将自己的加密算法对接到 DALICHAIN 中，无需按照公链固定的加密算法重新设计系统，大大节约了开发成本，同时降低了企业应用系统与 DALICHAIN 对接的适配门槛。

为接入服务提供此等能力，是目前世界上最独特的服务能力。

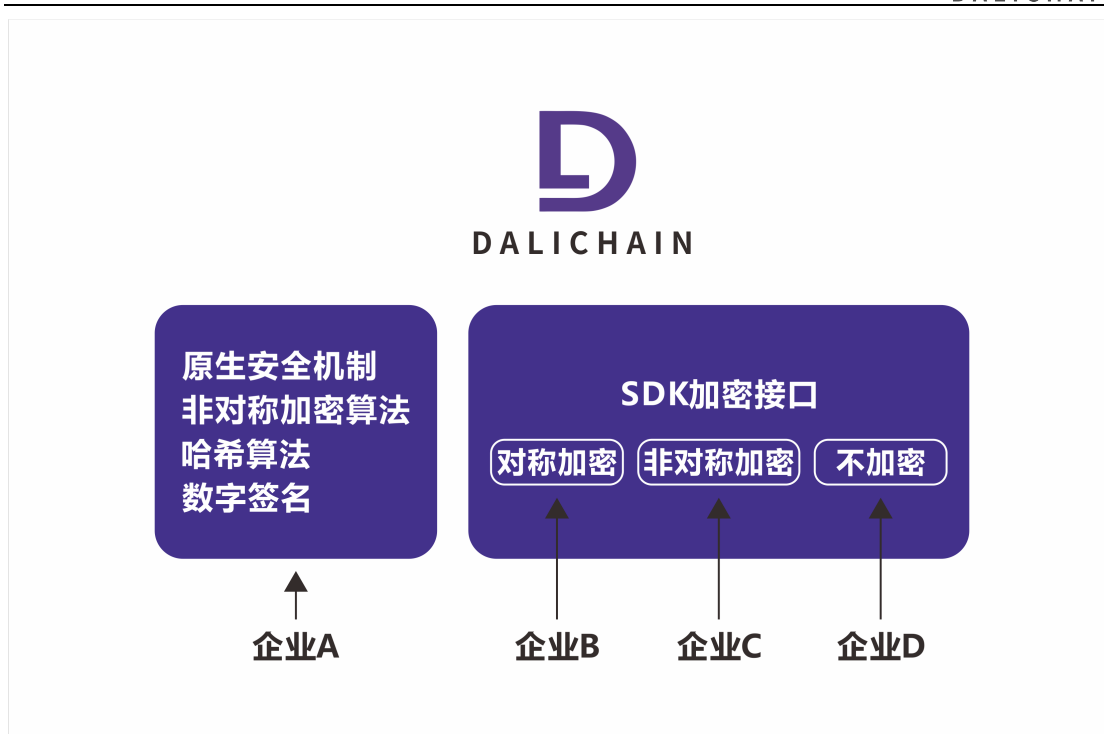


图 2-4：DALICHAIN 的安全机制

由于区块链的透明性，原则上所有节点可以保存和查看链上信息。但是考虑到 DALICHAIN 将支撑不同行业的应用，个别行业会有一些需要上链但不愿意完全公开的信息，我们除了 SDK 外，还将特别集成“洛克密法”智能合约，为上链信息提供不同私密性保护：

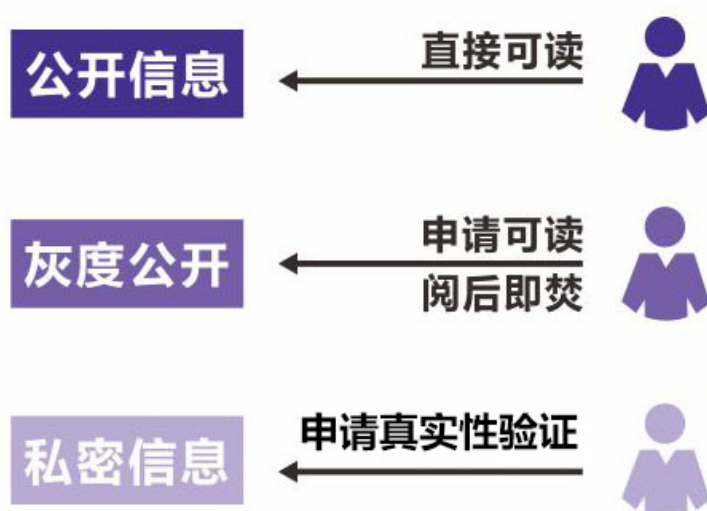


图 2-5：洛克密法智能合约功能

- a) 基础信息公开，标的赋码及规格描述信息，可在平台层面强制公开。例如在公益领域，资金的来源和用途必须做到实时全公开，且不可篡改，在此所有的链上信息必须强制全公开，这样才能真正展现公益的本质。
- b) 灰度公开信息，将使用对称加密算法对信息进行加密；密钥使用商家公钥加密，确保仅商家可以发放对称密钥。基于 DALICHAIN 独有的“洛克密法”智能合约临时解密发送给阅读需求人（事前指定/临时申请），且提供阅后即焚选项。例如在酒店行业的智能锁应用，用户在办理入住时可临时获取一个开锁密钥，在入住期间用于对应房间智能锁的解锁，当入住时间到期后自动失效。
- c) 私密信息，由商家使用自己公钥加密（只有商家能使用私钥解密），信息验证人提交需要验证的特定商家的敏感信息，洛克密法智能合约将对信息进行是否匹配的验证，并返回验证结果给信息验证人。例如在金融行业，客户的隐私信息上链存证后不能公开，而只有特定客户或商家才能查看，这时候就需要特定的验证方式来解决数据私密性的问题。

2.4.3. GAS 的设计理念

为更好的面向企业提供区块链服务产品，DALICHAIN 引入了燃料币 GAS 的概念，GAS 币值相对稳定，无限量发行；DALICHAIN 通过严格遵守准备金保证制度来确保 GAS 发行的稳定性和真实性，例如，每发行 100 个 GAS，都将有等量的资金保障（资金来源于企业充值）。GAS 与保证金的具体定价取决于提供企业服务所在国的法律法规的要求。

GAS、DALI 与日元（JPY 举例）的三者关系如下（举例）：

GAS单价恒定为0.2日元

$$\text{GAS 单价} = 0.2 \text{ 日元}$$

DALI兑换GAS数量的公式

$$1 \text{ DALI} = \text{DALI 市场价格} \times 5 \text{ GAS}$$

例：DALI实时市场价格为1000.00日元，则1 DALI = 1000 * 5 GAS = 5000 GAS

图 2-6：GAS、DALI 与日元的关系图示意

GAS 作为虚拟机内的“燃料货币”，用于支付每行代码的运行，简单来说运行虚拟机内的代码需要消耗一定数量的 GAS，当 GAS 消耗完后，代码将终止运行并滚回到初始状态，有效防止了死循环情况的发生。

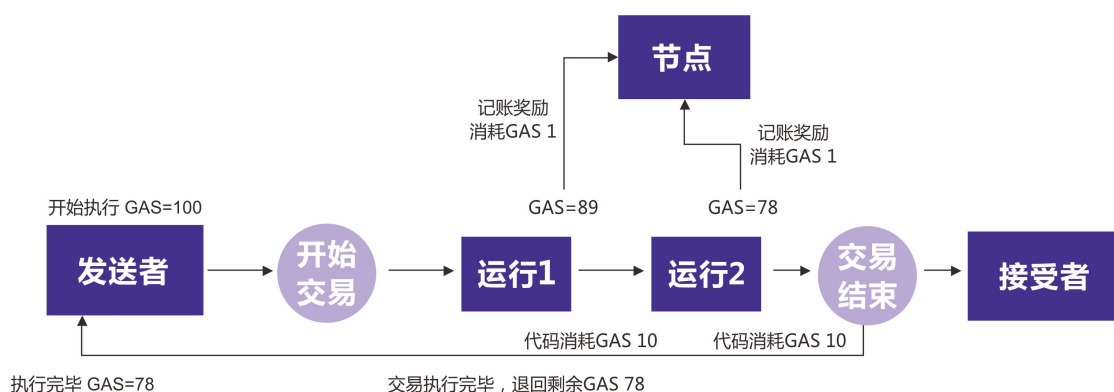


图 2-7 GAS 的运行机制

2.4.4. 区块链浏览器

区块链浏览器是区块链网络的查询窗口，所有上链登记的数据资产和交易信息都可以在区块链浏览器中查询到，一般用户会使用区块链浏览器来查询区块中的交易信息。

DALICHAIN 的区块链浏览器是经过精心设计的可视化交互界面，用户能轻而易举地获取到各种关于 DALICHAIN 的信息（企业加密信息除外），例如可查询区块 ID、区块高度、交易 ID 等关键信息，让一切上链数据将有迹可循。

2.4.5. 智能合约&虚拟机

智能合约（Smart Contract）是一种可编程的程序化规则，参与方触发条件后将按程序执行结果，全程无需人工干预。由美国一位学者尼克萨博（Nick Szabo）于 1995 年提出。

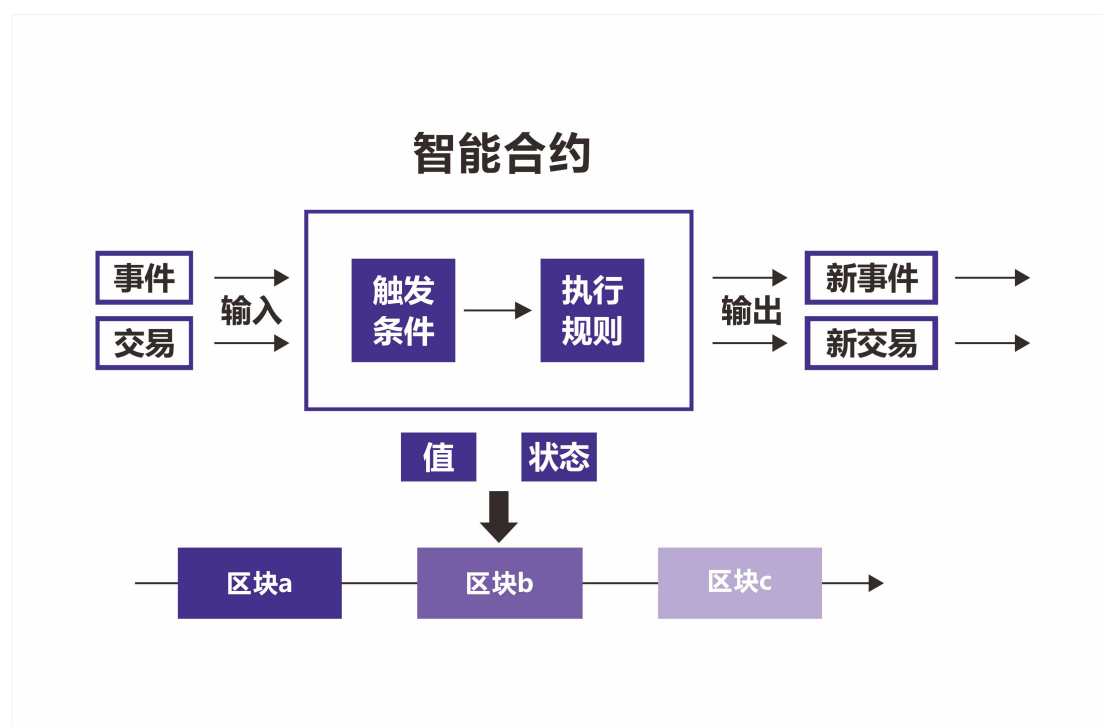


图 2-8：DALICHAIN 智能合约模型

智能合约是可以运行在区块链网络上的计算机程序，它的核心在于交易事件在经过智能合约的处理后，事件的值和状态也将随着区块链传递，基于区块链的智能合约的构建及执行分为如下步骤：

- a) 创建智能合约：由区块链内的多个节点共同参与制定；
- b) 存储智能合约：通过区块链网络扩散到每个节点；

c) 执行智能合约：触发条件，执行规则。

虚拟机是运行在区块链上的一个智能合约代码运行环境，和区块一样会存储在每个节点里，当触发虚拟机程序条件时（有智能合约交易），每个参与共识的节点会执行相同的计算（执行该智能合约代码），确保智能合约运行结果的一致性。现在行业内主流的图灵完备虚拟机，理论上能进行任何类型的运算，但也普遍存几点不足：

1) 同步调用机制

智能合约执行完毕后才能继续打包后续的数据，如果该智能合约执行时间较长，这样对整个网络打包共识会造成延迟；甚至还有可能遇到恶意代码，长时间占用资源，让后续的数据迟迟不能被打包，导致网络拥塞（也是一种拒绝服务攻击）。虽然现在的主流虚拟机采用 GAS 上限机制来限制代码时间，但没有从根本上解决问题。同时，这种同步调用限制了网络执行复杂合约业务的能力，导致复杂业务无法使用基于区块链的智能合约。因此，我们认为同步调用机制并不适合于所有的合约场景，应该采用不同机制来满足不同的业务场景。

2) 智能合约代码漏洞

当前，智能合约由于缺乏有效的代码检测机制和友好的辅助测试手段，导致众多智能合约应用都爆出致命/严重的安全漏洞，给合约所有者带来了极大的财产损失，造成了用户对区块链网络信任的严重不良影响。

3) 无法访问互联网

目前，主流的虚拟机均没有访问互联网的功能，也就是说虚拟机只在本地运行，无法取得互联网外部数据，与互联网应用形成互动，在商业应用上给智能合约带来了极大的局限性。

4) 开发语言受限

智能合约的开发语言各家各不相同，但无一例外都没有采用目前最为流行的编程语言，阻碍了区块链智能合约应用的发展。

DALICHAIN 作为一条专为行业应用打造的公链，针对各种商业场景有充分的考虑。因此，在具备图灵完备虚拟机完整功能的基础上，还针对以上问题进行了优化，使虚拟机更适合商用：

a) 同时支持同步调用和异步调用

为了支撑各种行业应用，DALICHAIN 将同时支持同步调用和异步调用，由用户在部

署智能合约时进行选择，以便支持用户的不同的合约应用场景。

b) 提供形式化验证接口/服务。

形式化验证是一种利用数学推理来验证软硬件设计意图的技术手段，它具备比仿真验证更高的效率，比普通测试手段更完备的结果，从而能快速验证代码的安全性。也就是说，利用形式化验证能更快更准确地发现智能合约代码的安全漏洞。DALICHAIN 计划集成提供形式化验证的接口/服务，在智能合约发布前可利用业界成熟的形式化验证工具对代码进行检测，帮助开发者更高效地发现安全漏洞，大大降低智能合约的安全风险

c) 虚拟机将开放互联网访问功能

该功能为一项可选项，开发者可按需应用到不同的行业。开放互联网访问的虚拟机可将外部数据源引入到虚拟机内，为未来商业应用场景带来更多的可能性；

d) 支持多编程语言

基于对区块链行业发展的考虑，DALICHAIN 的智能合约脚本语言将逐渐支持主流编程语言(例如 C++、JS、Python、Go 等)，这一举措将大大降低开发者进入门槛，将有效支持行业的快速发展。

2.5. DALICHAIN 面向商业应用的特性

2.5.1. 客户端

DALICHAIN 提供轻节点客户端（移动端）和全节点客户端（Windows/Linux）。

轻节点客户端即面向普通用户的移动客户端，将提供转账、币币互换、第三方密钥存管等基础功能；全节点客户端则面向专业技术人员，除了能实现转账、币币互换的基础功能外，还具备以下特性：

a) 记账费

类似比特币的挖矿，节点可参与网络的竞争记账，DALICHAIN 坚持低耗的原则，鼓励节点将算力贡献到行业应用上，因此所有节点在成功打包区块后都将获得记账费，该费用可理解为行业需求方支付给节点的记账服务费。

b) 发币功能

任何开发者都可以基于 DALICHAIN 发行 Token，整个过程都在全节点客户端上操作完成，用户在发币界面设置好相关参数后，即可进行一键发币。

默认情况下，新发行 Token 的规则与 DALICHAIN 网络主币相同，即设定好总量后将一次/多次发行，没有挖矿的过程，只有记账节点能获得记账费（在后续版本中，我们将探讨基于挖矿激励发币的可能性。）

值得注意的是，发行者必须设置 Token 是否有发行上限总量，并且该信息将随着发币交易一起记录到区块上，对所有人公开。也就是说，任何参与者都能轻松看到该 Token 是否有发行上限总量，该数据不能修改，在一定程度上避免了被暗箱操作的可能。这种灵活的设计将帮助个人用户和企业用户实现不同场景的业务应用。发币功能也是 DALICHAIN 为用户提供的一种金融赋能工具，用户可将加密数字货币与自身的商业模式做结合，创造出一种流通于业务内部的加密数字货币，对业务附加新的金融属性，从而实现新的商业模式，创造更多的价值。

c) 发布智能合约

全节点客户端将提供面向普通用户和开发者的智能合约发布功能，DALICHAIN 坚持简单易用的原则，将打造全新的用户体验，让没有编程基础的普通用户也能发布简单合约，让专业开发者选用自己擅长的主流语言进行高级智能合约发布。

2.5.2. 跨链网关

区块链技术经过多年的发展，现在全球已形成了大量的公链、私链、联盟链，由于各种链的背后属于不同运营方，使每条链几乎都成为了信息孤岛。DALICHAIN 认为未来的区块链将会与今天互联网的格局相同：互联网是由千千万万个局域网汇集而成，而区块链网络也会由无数个公链、私链、联盟链汇聚而成，形成一个巨大的“互联链”，用户的资产可能会存在不同的区块链上。

如何实现同一用户在不同链上的资产统一？如何实现不同用户在不同链上资产的转移和交易？如何实现智能合约的跨链调用？即“如何跨链”将成为区块链行业必须要解决的热点问题之一。DALICHAIN 基于自己对区块链的深入认知和对行业趋势的精准把握，提出区块链跨链网关的理念，跨链网关是不同的链之间的节点对接器、请求转换器、数据同步器，将实现不同区块链节点对接，智能合约跨链调用转换，数据和资产在不同链之间的同步和转移。

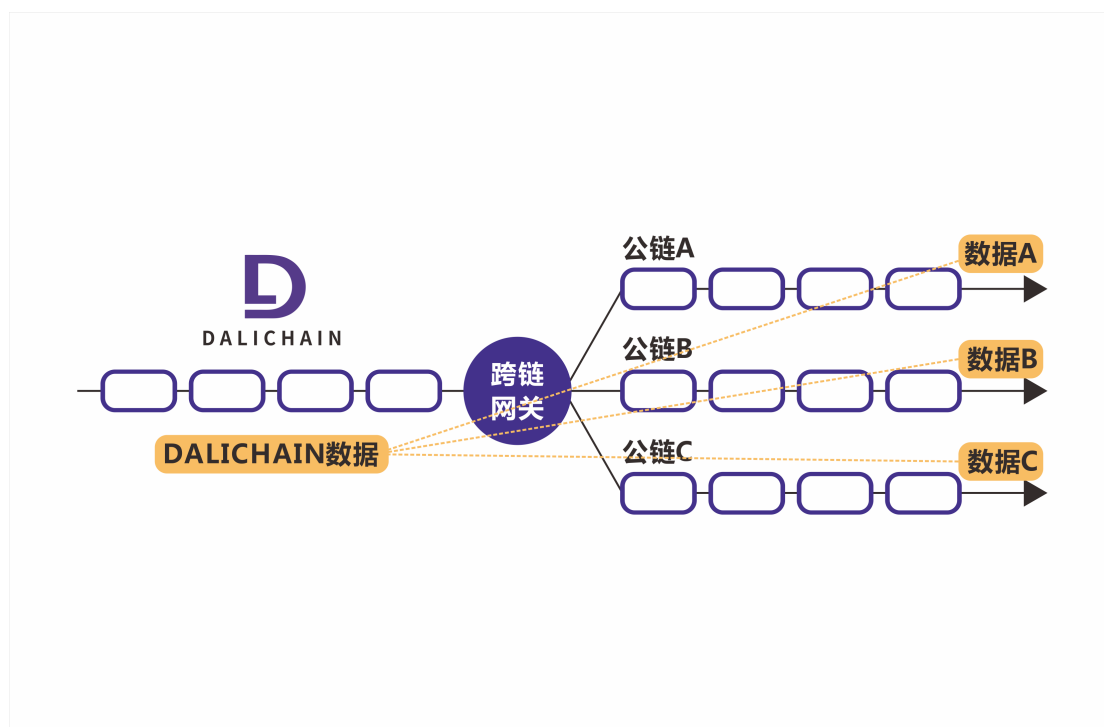


图 2-9：跨链网关示意图

跨链网关是区块链技术发展的必然趋势，使用跨链网关能打通不同链之间的壁垒，带来行业的价值增量。DALICHAIN 将会不断完善跨链网关技术，让跨链网关进入全球的区块链生态，让可信的数据、可信的资产，构建一个可信任的世界，进一步开拓人类的商业新边疆。

2.5.3. 对象化描述

2008 年的美国次贷危机，由于在贷款业务及以其为基础的证券层层打包封装，同时因缺乏相应的监管措施，导致次级贷款和债券混杂其中，造成了上下游信息不对称，最终爆发了危机。表面上原因是金融监管的缺失，而实际上是因为监管机构缺乏一个有效的监管工具，导致整个过程没有被提前预警，如果在初级环节发现了隐患并进行节制，就不会出现这样的情况。

现在，监管机构需要利用一个更高效的科技手段来避免类似悲剧再次发生，这个工具就是基于区块链的对象化描述。

无论是实物或虚拟，万物皆可归纳为对象。对象化描述简单来说是指将万物之间的状态和关系进行标记上链，达到资产跟踪的目的。这些看似零散的数据在未来的数据分析中至关重要，区块链数据即价值的体现，是企业未来的核心竞争力。

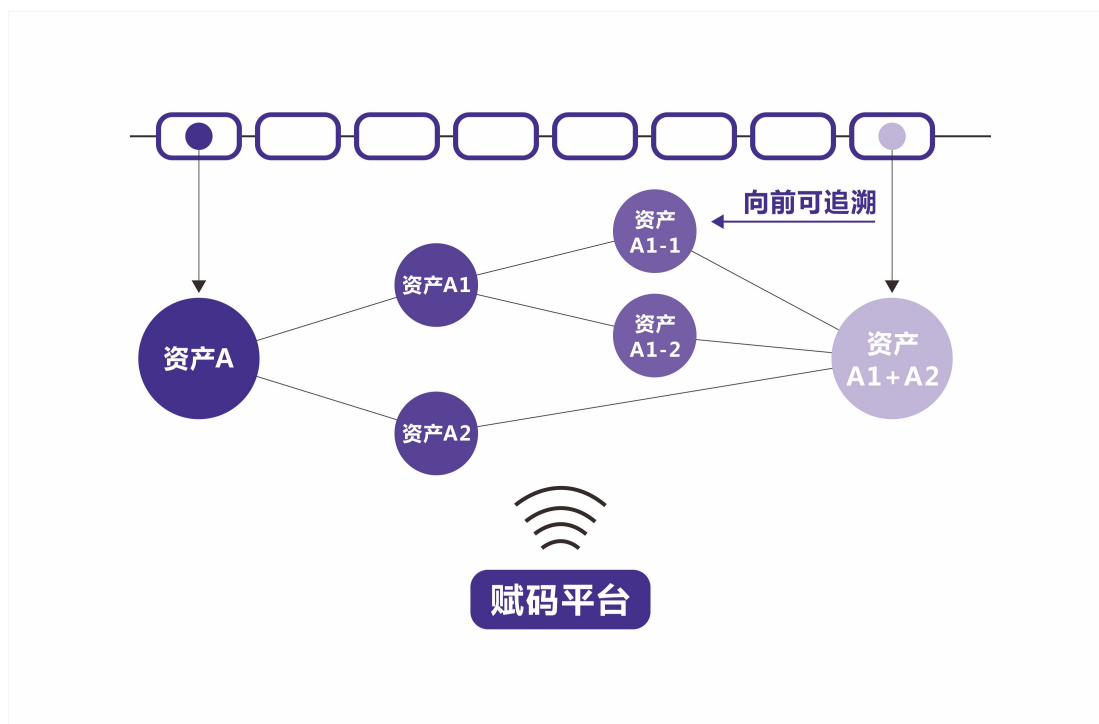


图 2-10：对象化描述功能示意图

利用 DALICHAIN 对象化描述 SDK, 可将所有对象量化成原生、聚合、拆分等若干种状态, 并上链永久存证。在以上美国次贷危机的例子中, 如果使用了对象化描述工具, 从第一笔贷款即可开始跟踪状态, 借款人的收入状态、抵押贷款情况、利率的变动等因素都可以逐一量化成数据, 记载到区块链上并通过前端程序进行数据分析, 并且所有数据没有被篡改和丢失的风险, 这样可在第一时间发现异常, 从而避免悲剧的发生。

同样, 在其他行业应用中, 利用该技术可将业务数据进行标记, 使数据在传输过程中的每一种状态都有迹可循。这与传统的物联网标记技术不同, 对象化描述不仅能记录资产的状态, 还能通过区块链不可篡改的特性实现对数据的原子化追踪, 有效避免了因数据缺失、数据关系紊乱造成的损失。

DALICHAIN 通过集中赋码/智能合约赋码的方式可将任何资产映射到区块链网络中, 经过时间的累积, 数字资产将具备生物有机体的特征, 每一条数据都会随着时间和事件的变化而演化。当数据量足够大时, 整个系统将形成一个分布式、去中心的高智能机体, 这对行业意义重大, 是构成未来区块链 AI 不可或缺的一部分。

2.5.4. 零知识证明

零知识证明 (zero-knowledge proof) 指的是证明者能够在不向验证者提供任何数据信息的情况下,使验证者相信数据是正确的,整个过程不需要对数据进行公开验证和解密。简单的说,零知识证明通过间接证明的方式做到了既保护了数据隐私,又保障了数据安全。在 DALICHAIN 中, DALICHAIN 为此提供一个可选项,企业根据自己的行业需求可选用零知识证明进行数据验证,这样能有效解决上述隐私性问题。

2.5.5. 可信智能合约商店

DALICHAIN 提供智能合约商店功能,就是一个集中展示和销售智能合约的网上平台。平台上的开发者可以通过销售自己编写的智能合约来获取更多的利益。而链上的用户则可以选择各类符合要求的智能合约来完成交易,用户还可以通过购买智能合约模板来定制化符合自身需求的智能合约。

智能合约商店中的智能合约模板都是经过形式化验证的可信智能合约,通过形式化验证将大大降低由于代码漏洞带来的安全风险。形式化验证是一种利用数学推理来验证代码设计意图的科学技术手段,利用该技术能更快更准确地发现代码的安全漏洞。因此,使用经过形式化验证的智能合约模板,可大大降低各方面的安全风险,能让用户安全放心地使用。

DALICHAIN 提供的可信智能合约商店的独特价值如下:

- a) 用户可以通过一个平台集中的找寻自己所需的智能合约,无需花费大量时间成本去网上找寻;
- b) 智能合约商店中,行业通用的智能合约模板能大大降低用户的成本,无需请专业人员进行智能合约的开发,用户可以购买后根据自身的需求进行简单开发就能得到满足需求的智能合约;
- c) 所有智能合约模板都是经过专业的测试验证,没有测试验证能力的用户也无需担心智能合约模板的质量,可以放心的使用,提高使用效率,降低用户的使用成本;
- d) DALICHAIN 还能提供形式验证的功能接口,代码检查工具为其他开发者编写的智能合约进行形式验证,代码检查以及律师审核,这样能大大保障智能合约商店里的每一个合约都是安全可信的;

- e) 独立智能合约开发者可以向智能合约商店提供自己编写的智能合约,经过安全和质量审核后就可以在商店内进行销售,可以让开发者获得更多的收益。

3. DALICHAIN 基金会治理架构

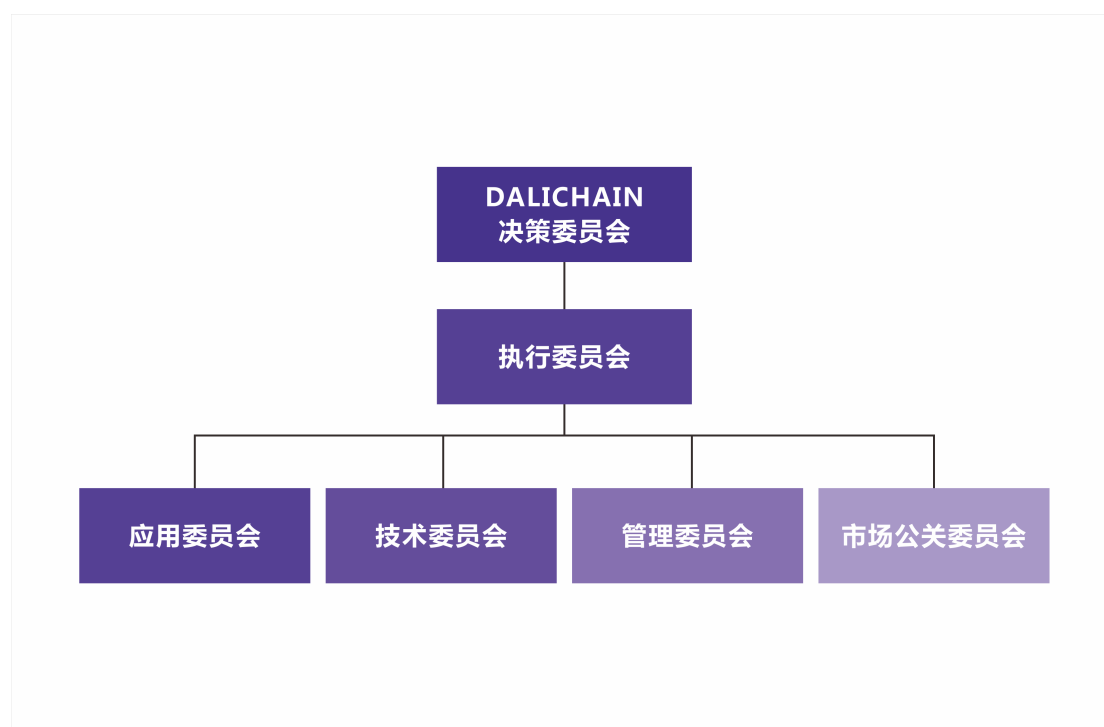


图 3-1: 基金会组织架构图

DALICHAIN 基金会(以下简称“基金会”)是非营利性组织。基金会致力于 DALICHAIN 的开发建设和 DALICHAIN 生态的公开透明化,促进 DALICHAIN 生态安全、健康、和谐的发展。

基金会治理结构的设计宗旨是保障项目的可持续性发展,以及构建管理架构和提升管理效率。基金会由 DALICHAIN 的开发人员和职能委员会组成,组织架构主要由决策委员会、应用委员会、技术委员会、管理委员会和市场及公共关系委员会组成。基金会成立初期,决策委员会由基金会主席、DALICHAIN 核心开发人员和管理成员组成,每期任期为二年。

应用委员会负责项目执行和应用推广,技术委员会负责代码审核和技术顾问,管理委员会负责人事和财务管理工作,市场公关委员会负责宣传和社区服务。

3.1. DALICHAIN 基金会的风险评估及决策机制

为了制定和完善风险管理体系和制度，基金会要求每年就 DALICHAIN 可持续性进行安全评估，评估内容包括项目质量、项目进度、项目应用，例如智能合约和简单合约应用、威胁识别分析，管控措施评估分析，风险界定、处置等阶段。

a) 事务安排

基金会将根据事件特性，例如事件影响程度、影响范围、影响代币量和发生的概率进行分级，按照优先级进行决策，对于优先级高的事件，尽快组织基金会相关委员会进行决策。日常事件类型主要分为管理类事务和代码类事务。

b) 管理类事务

对于基金会普通管理类事务，由基金会成员进行会议商讨，最终由财务及人事管理委员会和基金会主席共同决定。

c) 代码类事务

对于开源社区的代码问题和筹集资金的使用问题，决策通常采取成员投票机制。社区中每个成员根据所持达利的数量和币龄决定投票权重，通过基金会投票系统进行投票，投票结果将有导向性作用。决策委员将依据社区投票结果作最后裁定。对于需紧急处理的技术类事件(例如影响整个社区的事件、软件安全，系统升级等)的决策，由技术委员会审核后提交至决策委员会，决策委员会通过投票表决，采取特权机制落实到社区中。基金会将通过投票机制避免分歧的产生，若产生分歧，由决策层人员的达利数量和币龄决定投票权重。

3.2. DALICHAIN 基金会的信息披露原则

DALICHAIN 基金会将定期披露报告，对财务管理信息、项目进程、市场信息和版本信息进行披露。此外，基金会也将对突发事件进行即时披露。

发布报告	披露内容
月报	按月发布月报，披露每月项目进展及版本升级预告；项目资金使用事宜，截至月末的市场持币情况；

中报	年中发布中报，披露半年的项目进程及版本升级总结及预告；项目资金使用事宜；下半年的项目规划及预算；截至年中的市场持币情况
年报	年末发布年报，披露本年的项目整体进程及版本更新；项目资金使用情况 & 未来一年计划；来年的项目整体规划及预算；截至本年末的市场持币情况，管理团队变动情况；

4. DALICHAIN 实施及发展计划

4.1. DALICHAIN 技术发展路标

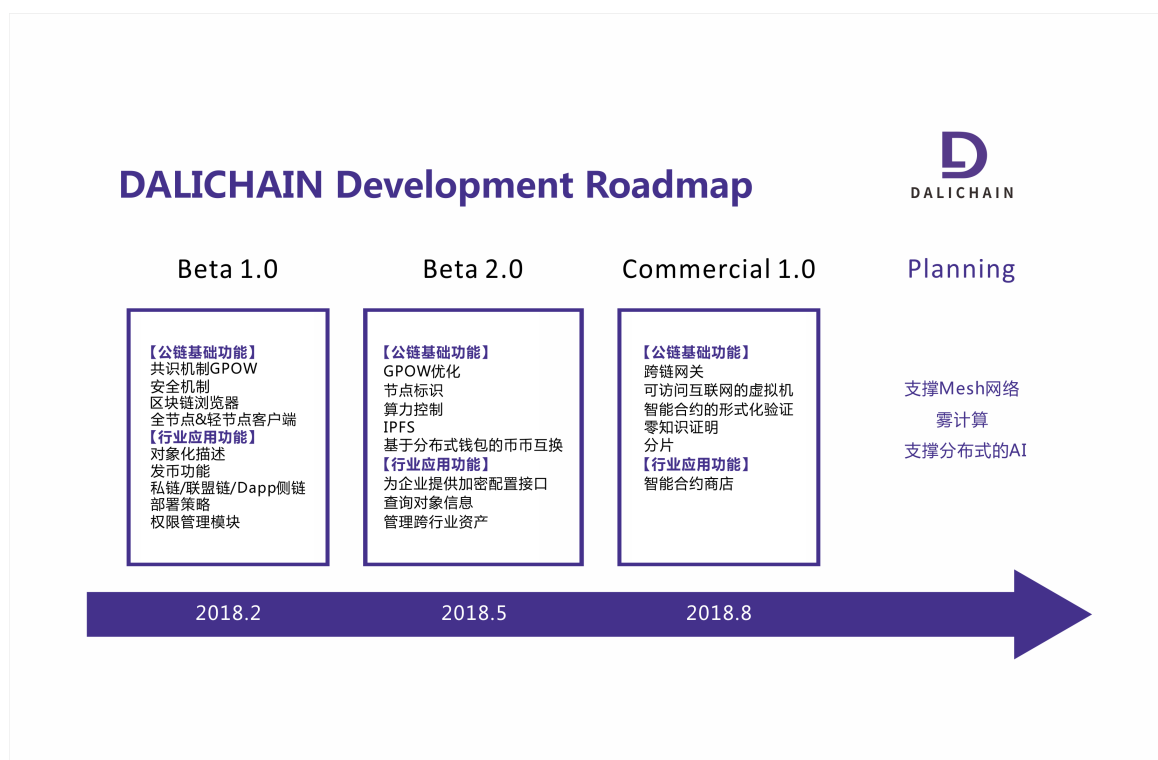


图 4-1：DALICHAIN 技术发展路标

4.2. DALICHAIN 的生态发展路标

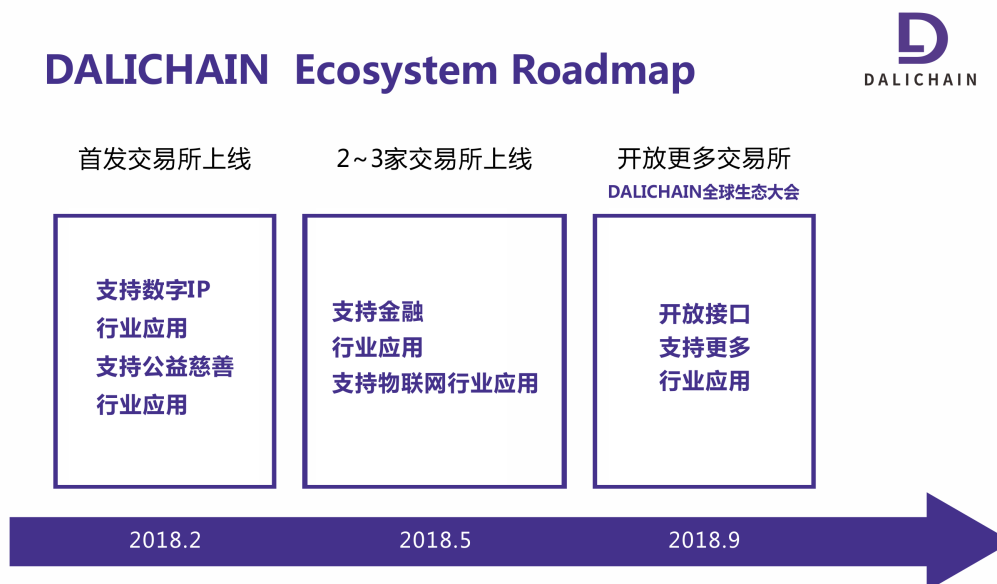


图 4-2：DALICHAIN 生态发展路标

5. 创始团队

要在未来已来的数字世界占有一席之地，真正引领数字时代的发展，就必须组建一个强大的团队。一批经验丰富而又风华正茂的 80 后前华为人走到了一起，组成了核心技术团队，技术能力与商业实操能力兼备，具有全球化运营的历史经验。

彭钊：曾负责华为 WCDMA 产品的全球营销，足迹遍布 5 大洲，具有全球化的前瞻视野。与 150 多个国家运营商建立合作，拜访并交流超过 30 个运营商的 CEO/CTO。与中国领先的公益组织阿拉善 SEE 建立了合作关系，于 2017 年 6 月发布了阡陌区块链绿色商城。

程文彬：曾负责华为 OSS 解决方案，产品在全球多个领先运营商得到商用，支撑全球超过 3.5 亿终端用户。华为 10 年的工作经历，除了擅长网络架构设计外，还积累了网络安全设计及计算机密码学应用方面的丰富经验。多种网络技术的积累和对网络架构的深度理解，都成为了快速理解和融入区块链世界的保障。2017 年初，主持并构建了全球第一个公益区块链行业应用。

吕伟康：从华为跨界到百度爱奇艺，从最底层技术一直到应用层技术的实践者，有丰富

的研发团队管理经验。多年网络架构经验，设计的高并发服务器集群已全面投入使用，对网络安全有比较深的研究与实施，曾帮助爱奇艺成功抵挡多次 DDOS 攻击。对区块链技术有深入的研究，致力于区块链技术的应用落地，精通 P2P 分布式存储与计算。

胡大鹏：资深信息化运营领域专家，具有丰富的行业应用及市场推广经验，曾与华为密切合作。连续创业者，移动互联网、新媒体运营、社交网络运营、内容运营和 IP 孵化专家。深入研究和实践价值互联网的构建，致力于探知区块链应用领域的商业延展。

6. 社区

官网：www.dalichain.io

K 站：<http://x.btckan.com/tshare/zh/ksite/188>

Telegram：<https://t.me/DalichainGlobal>

Facebook：<https://www.facebook.com/Dalichain-624923874521001>

Twitter：<https://twitter.com/dalichain>

Medium：<https://medium.com/@dalichain>

Email：service@dalichain.io



THE END