PCHAIN 建议书

世界第一个支持 EVM 的原生多链系统

让大规模区块链行业应用成为可能

PCHAIN 基金会
pchain.org
2018-1-18

目 录

1 概要

互联网极大地提升了信息传播的效率，20 余年的发展将人类社会全面带入了自媒体时代。被誉为价值互联网的区块链使得数字资产的传播效率大大提升，让自金融成为可能。未来的各行各业都将被区块链所改造，就像互联网重构传统的各行各业一样。提升各行各业的手段通常有两种，一种是金融，一种是科技。金融和科技的结合称为 Fintech。而 Fintech 的核心就是区块链。为什么？因为区块链技术从诞生之日就自带金融属性。不带金融属性的区块链只能称为 DLT 分布式账本。其他的 Fintech 技术，例如大数据、云计算、人工智能，与金融只是结合。金融并不是这些技术的原生属性。

区块链技术始于中本聪提出的比特币一种点对点的加密电子现金系统[1]。以太坊[2]在比特币现金系统的基础上扩展了基于区块链的智能合约功能，从而开启了区块链重构各行各业的新蓝图。以太坊运行基于 Solidity 语言的智能合约，为编写、部署 DApp（分布式应用/区块链应用）提供平台。

金融是资金与资产的互换。在区块链所构成的新经济蓝图中，它表现为以比特币为代表的数字货币和以智能合约为代表的数字资产。 数字货币，区块链本身作为一个分布式记账系统，记录收入和支出。智能合约，允许用户自定义规则，利用代码来表达自己的逻辑。两者都利用了区块链的去中心化和不可篡改性保证了价值的记录和传递。

支持智能合约的公有区块链，在高速发展的同时，面临如下几大问题 1）缺乏统一有效的 Oracle 方法。由于比特币的自身闭环，比特币系统内的所有数据都是系统生成的，因而不存在数据/知识自身有效性和真实性的问题。而在智能合约环境下，我们需要获取外部系统的数据/知识，而外部数据/知识的有效性和真实性的问题往往成为智能合约的瓶颈和障碍。2）对大规模交易支撑不够、单链竞争对造成资源浪费、浏览和还原交易较为复杂。3）跨链的需求日益增长、智能合约数据兼容问题不方便升级。

PCHAIN 是一种新型的原生多链系统，使得区块链智能合约的大规模行业应用成为可能。PCHAIN 的主要技术方向包括 1）全球第一个支持 EVM 的原生多链结构，基于多层 Sharding 的 POS 共识技术，提升交易性能。2）基于 Knowledge Graph 知识图谱的全新 Oracle 机制，使得智能合约更容易闭环。PCHAIN 内生的符合 W3C 标准的 Smart Data 可有效解决智能合约内生知识不足的问题，并可成为智能合约的功能要素，例如市场汇率等外部数据。3） PCHAIN Smart Data 的目标是产生有价值的数据，过滤数据噪音，成为智能合约 Oracle 的构成元素。这些 Smart Data 可广泛的应用于各种 PCHAIN 的智能合约、以及其他的跨链请求。Smart Data 一方面可以成为区块链与人工智能结合的中间层，另一方面为区块链与外部大数据的结合提供便利。因而具有非常广阔的应用前景，包括去中心化的分布式问答、预测市场、分布式知识图谱构建[11]、社交网络、数字身份等领域。4）中继方式的跨链，使得数字货币与数字资产的交换更为便捷。可使用各种 Token(例如 BCH、ERC20)直接调用 PCHAIN 里的智能合约。

2 智能合约的现状

本质上，比特币是通过从时刻 t 到时刻 t+1 期间所发生的一系列<From, To, Value>的交易 Tx 三元组，完成了从全账本状态 S_t 到 S_{t+1} 的转换。而以太坊则将这段时间内的交易 Tx 扩展成为了可包含智能合约调用的<From, To, Value, SmartContract, Function, Parameter>六元组，从而完成状态 S_t 到 S_{t+1} 的转换。

相对于支持数字货币的区块链，支持智能合约的区块链的主要目的，不仅仅是把数字货币的流转记录清楚，而是要把现实生活中约定好的规则代码化，形成智能合约。

智能合约在区块链上部署以后，各方都不能对现有的规则进行随意更改。而且在条件触发以后，规则会自动执行，各方都不能有额外的操作空间。

随着智能合约的发展，现在已经不仅仅是规则代码化；区块链的各种行业应用，为了保证数据的不可篡改，开始编写更复杂的智能合约，把以往记录在数据库中的数据开始记录在区块链上；从而区块链的数据和操作/交易越来越复杂，支持的应用规模也越来越大。

2.1 支持智能合约的方式

一般情况下，用户使用特定的智能合约语言来编写程序，部署到区块链上，然后区块链内部会调用虚拟机来执行合约方法、返回结果。

目前区块链对于编程语言和虚拟机有两种处理方式：

一种是自己定义新的编程语言，并开发虚拟机以运行该语言编写的应用。例如以太坊，使用 Solidity 语言和 EVM 虚拟机[3][4]。

另一种方式是利用现有的编程语言和虚拟机，例如 HyperLedger[5]，使用 Java 语言和 JVM 虚拟机。（HyperLedger 主要用来组建联盟链和私链；而我们的目的是建设一条公链，所以暂时不是我们讨论的重点。）

2.2 存在的问题

目前支持智能合约的区块链，从实际运行的情况看，存在着如下问题：

- 对大规模交易支撑不够

  以以太坊为例，目前每秒大约可处理 13 笔事务。而对于以 Facebook 为例，每秒钟处理约需要 17.5 万笔事务。就处理的规模而言，目前区块链离最主流的社交应用还有很大一段距离。

  但从现有事务的处理机制而言，对大规模交易的支持也不够有力。当前，所有的 DApp 的事务都会放在一起处理，打包进入同一个区块。当一个 DApp 的交易非常繁忙，发送了大量事务而造成服务阻塞、不能及时形成区块时，其他 DApp 的事务也不能进入区块，从而对其他 DApp 也造成了拥堵。导致其他 DApp 的响应也不及时。例如前一段时间的 status ICO 事件[6]，就是一个 DApp 的拥堵导致系统不能正常运行的例子。

- 多个 DApp 混合在一条链上，浏览和还原交易较为复杂

  当有很多 DApp 部署在主链上之后，每个 DApp 的数据，包括交易数据，散布在区块链的各个区块里。在需要在区块链上对某个特定的 DApp 的操作进行追溯和还原时，会需要对全链进行遍历，效率相对较低。

- 缺乏统一有效的 Oracle 方法

  比特币系统自身从数字货币的产生、分配和转移是一个完整的闭环。当我们扩展到智能合约时，整个系统往往是一个开环状态，从而需要一种中介节点将所有的区块链外部信息以 Oracle 先知的形式告知区块链。

- 目前单条链的 POW 容易对算力造成浪费[7]

  目前支持智能合约的公链基本都采用 POW 方式达成共识，在矿工竞争生成区块时，每一个区块要消耗所有矿工的算力，这种方式对全网的算力造成了巨大的浪费。

而且 POW 容易带来分叉，这样会对交易生效的实时性带来一定的障碍。POS 虽然避免了算力浪费，但目前公开发布的系统并没有有效解决女巫攻击的经典问题。

- 智能合约数据兼容问题，不方便升级

  由于进入区块链的数据（包括智能合约的代码）不可篡改，理论上来说，对已经部署的智能合约是不可改动的。这样在现有的智能合约出现了 bug 的情况下，进行修复就非常的困难。虽然有各种方案可以解决这个问题，但都不太容易。例如方案之一：把原有智能合约的数据全部导出，在升级的智能合约中写入。在这种方案下，如果数据量巨大的话，会消耗大量的时间，而且原有智能合约的交易相关的数据很可能就丢失了。

  由于软件的开发（包括智能合约的开发）不可避免的会出现 bug，如何保证智能合约能够以一种保证数据不被篡改的方式升级，已经是一种较为急迫的需求。

2.3 相关工作

多链通过结构化重构的方式对原有单链结构进行有效 sharding 的方式。其直接的作用就是使得整个区块链结构不再表现为一台计算机的处理能力。随着多链个数的增加，其计算和存储能力呈线性增长。有不少相关工作都进行过这方面的尝试，例如 LISK[18]、Asch[19]和 Ardor[20]。然而，这些多链结构都没有对 EVM 进行直接和有效的支持。因而或者是非图灵完备，或者是由于没有 gas 的考虑，当智能合约出现问题时，容易陷入无限循环中。或者其改进的 BFT 算法有较强的中心化倾向。PCHAIN 是首个在多链结构上对 EVM 进行支持的区块链项目。

跨链考虑的是多条链或原生多链内部之间的交易.早期的工作通常基于 BTC，例如 BTC Relay[21]，BlockStream[22]和 RootStock[15]。RootStock 是一个依附于比特币区块链的 Secondary 链，它通过 BTC 与其内生的 SBTC 进行等比例兑换从而提供智能合约能力。然而，它的 secondary 链依然是单链结构，因此，它与以太坊一样，同样面临严重的性能瓶颈问题。。Polkadot[13]将跨链进一步定义为 Parachain, Relaychain 和 Bridge。与 Polkadot 希望 One Size fits All 的通用跨链定位不同，PCHAIN 是要支持非原生 Token 的智能合约调用。Cosmos[16]提出了一种 ABCI 的结构用于连接不同的异构链。然而，Cosmos 目前的改进的 BFT 共识算法通讯代价过高，且不支持 Validate 的动态加入和退出。

不少提升性能的工作都在从考虑提升 Transaction Processing 和随机共识的角度进行设计，例如 Dfinity[17]、Zilliqa[12]和 Aelf[14]。与这些工作的不同之处在于，PCHAIN 通过多链结构可更好的从 Data Processing 和 Sharding 角度提升区块链的整体性能，并且根据多链结构设计出了新的共识方法。

3 PCHAIN 的主要技术及其结构

针对上面的支持智能合约的单链的缺陷，这里提出了一种多链的方式来改进对 DApp 的支持。新的多链为 主链 + 多条侧链 结构（如下图），该链相邻的两条侧链加上主链，像希腊字母π，所以我们命名它为 PCHAIN。

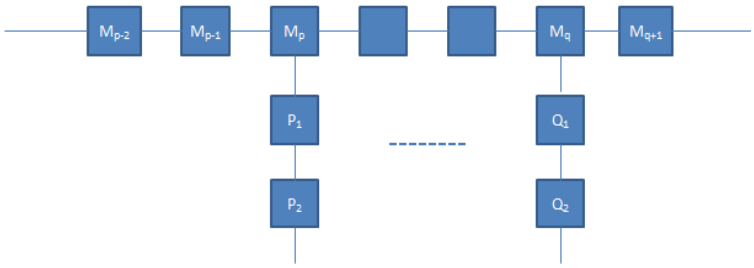

图 1 主链 + 侧链示意图

下面对该链的特点进行介绍。

1）PCHAIN 的生长

如图 1 所示，上面水平方向的区块链为主链，垂直方向的链为侧链。

主链上处理创建用户、用户转账、创建智能合约等各种交易，当这些交易发生时，主链会生成区块。

当创建一个新的 DApp（即新的智能合约）时，会创建一条侧链。以图 1 为例，在主链当前区块为 M_{p-1} 时收到创建智能合约的请求。主链执行该请求并生成区块 M_p，同时生成一条新的侧链 P，P 的第一个节点 P_1 指向执行请求的主链上的区块 M_p。P_1 中包含智能合约的二进制码。在有请求调用 P 链上的智能合约时，由 P 链来处理该请求并生成新的区块 P_2；侧链 P 以处理智能合约方法的方式进行增长。

另外，侧链上还有一种增长方式，就是升级智能合约。当升级该链上的智能合约时，最新智能合约的二进制码会放在最新生成的区块中。

2）主链和侧链的职责

如上 3.1 节主侧链生长方式所述，主链主要存储各种账户信息，以及账户之间的数字货币的转移等。主链还负责和其他现有外部公链或者联盟链的交互，并提供接口为侧链提供相应的服务。

侧链主要记录和特定智能合约相关的数据。

3.1 PCHAIN 技术要点

3.1.1 非原生 Token 的智能合约调用

PCHAIN 支持跨链调用。通过 PCHAIN 提供的工具集，利用其他链上的、非 PCHAIN 原生的 Token 就可以调用 PCHAIN 上的智能合约。工具集目前支持 BCH，以及遵循 ERC20 协议的 Token。

原理如下：当在其他公链上通过 PCHAIN 提供的工具集，使用该公链一定数量的 Token 调用 PCHAIN 中的智能合约时，工具集会先通过 Knowkedge Graph 中的 Smart Data 获取该 Token 和 PCH（PCHAIN 的 Token）的汇率，当能够兑换的 PCH 足够运行需要调用的智能合约时，就会将该数量的 Token 转移给 PCHAIN，并在 PCHAIN 中燃烧对应数量的 PCH 来调用智能合约。

以 BCH 为例，调用过程如下：在调用之前，调用者通过工具集告知 PCHAIN 他需要调用的智能合约的名称、函数、参数；PCHAIN 会根据该调用计算需要消耗的 PCH，再通过 Smart Data 中的 BCH 和 PCH 的汇率，计算出相应的 BCH 数量，并返回给调用者。随后，调用者在工具集中填入上一步骤中返回的 BCH 数量，以及再次填入智能合约的名称、函数和参数，

进行签名后发送请求。PCHAIN 接收到该请求后，会燃烧掉相应的 PCH，为调用者调用相应的智能合约，并返回结果。

为 BCH 提供的工具集中，需要调用的智能合约的信息会通过 OP_RETURN 来携带。鉴于该指令携带的信息量的限制，将来会考虑提出 BUIP 来添加新的指令，以携带更多信息。

对于遵循 ERC20 协议的 Token，在得到该 Token 一定数量的授权之后，PCHAIN 可以使用 ERC20 的接口进行 Token 的支取，并根据汇率，在内部燃烧相应的 PCH，为之调用智能合约。

另外，由于 PCHAIN 本身支持 EVM，当然也支持发行遵循 ERC20 协议的 Token。PCHAIN 可接入多种外部公有或联盟链，如图 2 所示。

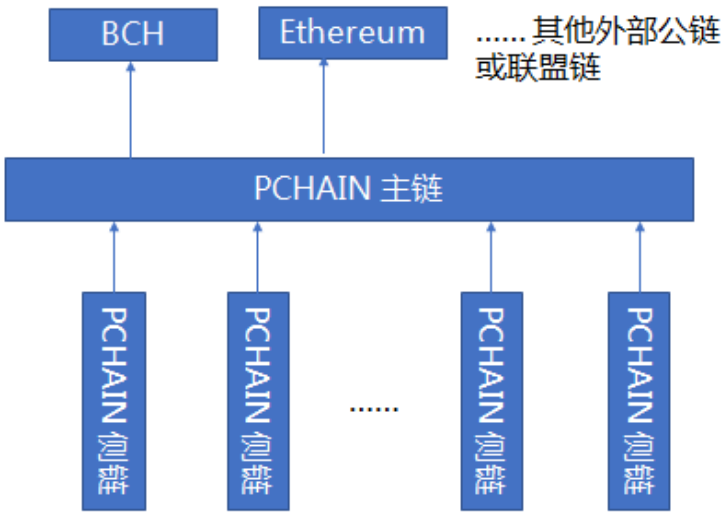

图 2 PCHAIN 总体结构图

3.1.2 Sharding 共识机制

PCHAIN 支持不同层面的 Sharding，并提供 POS 共识机制选择，从而提高运行和存储效率，支持链条的扩展。

就目前的共识机制而言，无论是 POS 还是 POW 共识机制下，所有的交易最终都只能串行执行和验证。而对于目前流行的基于 POW 公链，无论是 Bitcoin 网络还是 Ethereum 网络，挖矿的时间消耗甚至远远超过了交易本身执行和验证所带来的时间消耗。最终的结果就是全网只能用到一个节点的算力，性能难以提高，结构难以扩展。

PCHAIN 通过引入不同层面的 Sharding 机制，并支持 POS 共识机制，从而支持链条的扩展并提高运行效率。

PCHAIN 从两个方面来进行 Sharding：

- 主侧链分层结构

  对于主链，为侧链提供注册，查找，存储，存证等功能；并支持跨链交易。而具体的业务逻辑，可以创建一条侧链去单独完成。

  这样就避免了所有的业务交易都在一条链上完成的情况，从而大大减少了主链的运行和存储压力，而侧链也能消除原来单链模型下的其他业务的干扰。

- 对于节点较多的特定链条，采用交易级别的 Sharding

  当某一链条的节点较多，并且交易过多时，PCHAIN 会自动在该链内部启用此 Sharding

机制。具体实施如下：

- ✧ 对当前时间点做标记，作为一个新纪元(epoch)的开始。
- ✧ PCHAIN 首先通过可验证的随机函数，区隔链条中的所有节点，依次将它们分成不同的小组，这些分组叫做执行组。并通过同样的过程，选取部分‘有资格’的节点另外形成一个小组，这个小组叫做治理组。
  注：‘有资格’是指有足够的 PCH 并申请成为治理组的一员。
- ✧ 将进入的交易进行分类，例如根据发起请求的用户的不同，将交易发到特定的执行分组，该组内部对该交易进行执行和验证，在交易级别达成共识。、
- ✧ 在一个特定的时间间隔之后，所有的执行分组会将执行验证后的交易列表打包提交给治理组，治理组对来自于不同执行分组的这些交易列表汇总后在区块级别达成共识，形成区块，并广播到全网。
- ✧ 在每一个纪元的时间结束时，确保所有节点都同步到最新的区块，状态一致；随后进入新的纪元。

在这种方式下，交易真正有了并行的执行验证，在单一链条内摆脱了单节点算力的魔咒。图 3 和图 4 分别显示了交易进入不同的执行组，以及治理组汇集打包的过程：

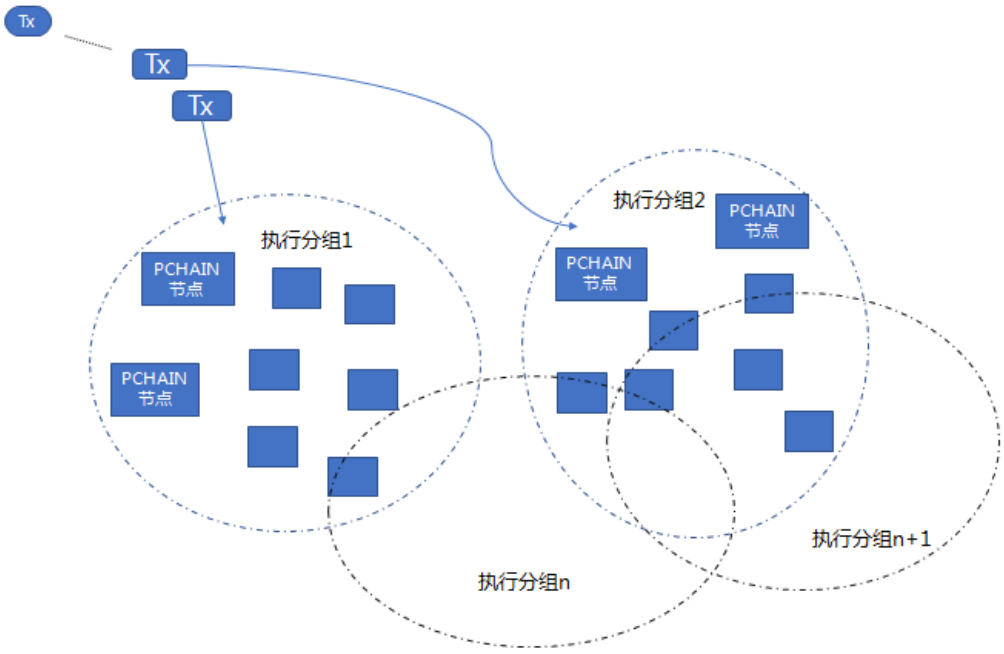

图 3 PCHAIN 交易分组处理 Sharding – 交易分发

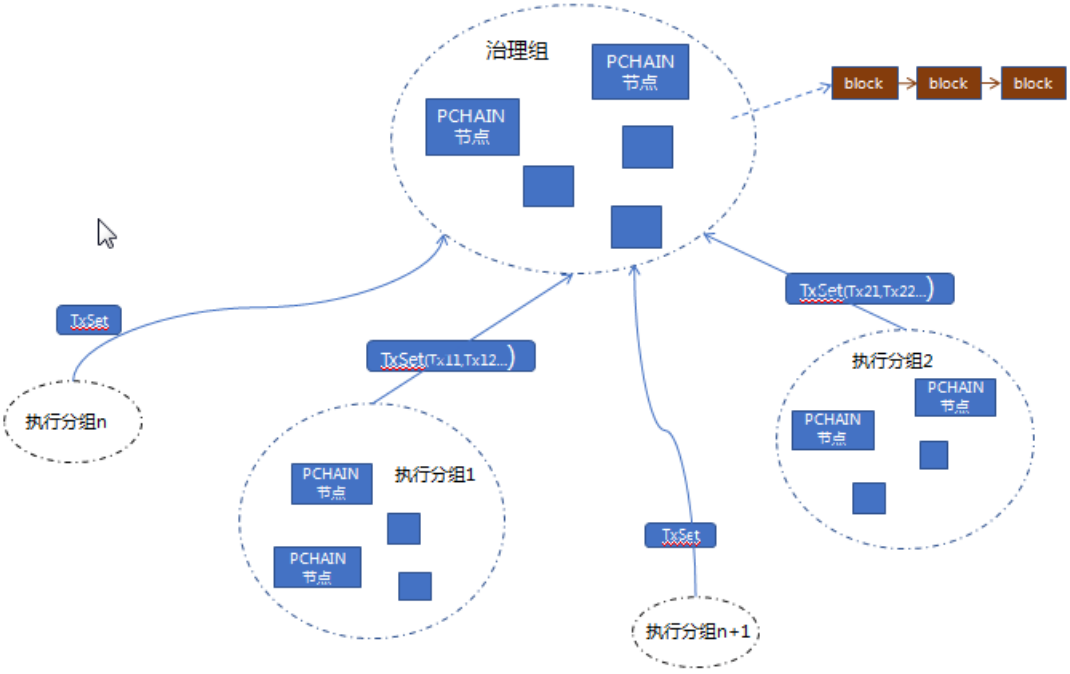

图 4 PCHAIN 交易分组处理 Sharding – 汇集打包

PCHAIN 为每条链提供 POS 机制的选择：

PCHAIN 目前每条链在初始化时默认采用 POS 作为共识机制。在 POS 作为共识机制时，可以大大减少达成共识需要的时间，非常快速地打包交易形成区块。从而避免挖矿的时间消耗，提高运行效率。

3.1.3 Knowledge Graph 知识图谱与 Smart Data

当前智能合约的发展受制于有效的外部数据获取。很多的信息，例如天气预报，交通出行信息，股票价格，汇率等等，需要从区块链外部获取。在以太坊中，有类似 Oracle（预言机）这样的解决方案；链内部署的智能合约可以从 Oracle 中获取相应的外部信息。然而目前的 Oracle 机制都还未形成标准，难以实现不同链间的协同与交换。

Knowledge Graph 知识图谱在 2007 年前后叫 Ontology 本体。在互联网之父 Tim Berners-Lee 的推动下，不断演进发展。资源描述框架 RDF（Resource Description Framework），是一种用于描述 Web 资源的标记语言。RDF 是一个处理元数据的 XML（标准通用标记语言的子集）应用，使用 XML 语法和 RDF Schema（RDFS）来将元数据描述成为数据模型。一个 RDF 文件包含多个资源描述，而一个资源描述是由多个语句构成，一个语句是由资源、属性类型、属性值构成的三元组，表示资源具有的一个属性。资源描述中的语句可以对应于自然语言的语句，资源对应于自然语言中的主语，属性类型对应于谓语，属性值对应于宾语，在 RDF 术语中称其分别为主语 Subject、谓词 Predicate、宾语 Object，即 SPO。SPO 包括实体-属性-值，实体-关系-实体，两种形式。这些三元组在一起就组合成一张有关联的有向图，称为 Knowledge Graph 知识图谱。

PCHAIN 将标准的 RDF 三元组写入内置的区块链知识库，从而形成 Smart Data。PCHAIN Smart Data 的目标是产生有价值的数据，过滤数据噪音，成为智能合约 Oracle 的构成元素。

这些 Smart Data 可广泛的应用于各种 PCHAIN 的智能合约、以及其他的跨链请求。Smart Data 一方面可以成为区块链与人工智能结合的中间层，另一方面为区块链与外部大数据的结合提供便利。因而具有非常广阔的应用前景，包括去中心化的分布式问答、预测市场、分布式知识图谱构建[11]、社交网络、数字身份等领域。

如图 5 所示，PCHAIN 节点内置 Knowledge Graph 知识图谱的相应模块。PCHAIN 的知识图谱模块由一系列内生 API 组成。PCHAIN 主链主动对外接入各种具有公信力的结构，获取相关领域的知识，以特定的形式记录下来填入知识图谱模块。并对内提供 API，其他智能合约可以调用知识图谱模块的服务，从而得到相关信息。同时知识图谱模块将会对外开放并保持审核制度，欢迎知识提供商接入，PCHAIN 会对接入服务进行一定的审核。随着知识提供商的增多，获取外部信息就会越来越方便。Smart Data 可支持多种知识谱图应用，例如基于区块链的众包社区激励机制 [11] 。

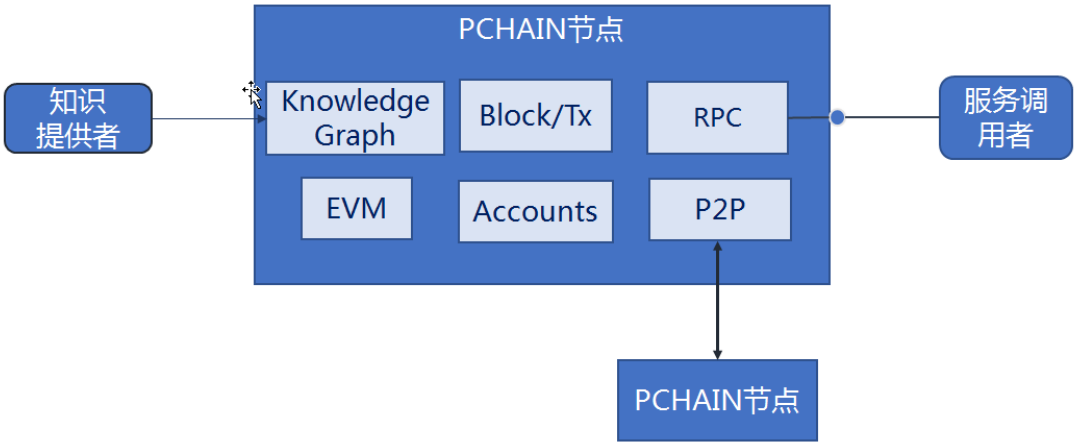

图 5　PCHAIN 节点组件及通讯图

3.1.4　支持 EVM

现在流行的区块链基本都支持智能合约，从解释执行图灵不完备的脚本语言，到采用虚拟机的方式运行流行的 Java，Go，Nodejs；方式比较多，也都能很好的完成各自领域的需求。EVM 则另起炉灶，支持了一门新的语言 Solidity。通过执行图灵完备的 Solidity，EVM 一方面能够很好的完成业务逻辑，另一方面，由于对所有的指令都能够进行掌控，从而对恶意的代码逻辑（例如无限消耗 Gas）能够进行一定的抵御，同时对调用智能合约产生的费用（通过对指令的执行和消耗的内存计费）能够进行得合理而透明的计算。

另外，EVM+Solidity 已经建立了完整的 RPC 机制，可以通过 http 访问的形式来调用。并且得到了 Nodejs Truffle 框架相当完善的支持，可以用 js 来接入；这为页面应用的编写提供了很大的便利。这些都是 EVM 在目前非常受欢迎以及得到很多支持的原因。

考虑到这些因素，PCHAIN 目前在主链以及侧链上，都采用 Solidity+EVM 来进行智能合约的编写和运行，从而能够让 EVM 现有的用户可以快速在 PCHAIN 上搭建新的或者移植已有的 DApp 应用。

3.2 其他技术要点

帐号机制

目前的区块链账号(Account)机制分为两种，UTXO 和余额。比特币采用的 UTXO（Unspent Transaction Output，未花费交易输出），主要利用地址来标识相关的账目。如果需要统计某个地址可用的余额，需要把相关的 UTXO 汇总进行统计。以太坊基于余额。余额成为账号的一个属性，而造成金额改动的交易另行记录。

PCHAIN 的主要目的是部署执行 DApp，所以采用账户系统，在发生花费或者收益时，可以从余额直接扣除或增加。

多链联合共识

基于特有的多链结构，同时会有多个链的交易请求进入系统。对于所有链的请求处理，都基于一个客户端进行，即一个客户端参与所有链的共识达成和交易存储。这里的达成共识的过程主要分为 3 个阶段。

1）选择参与达成共识的链

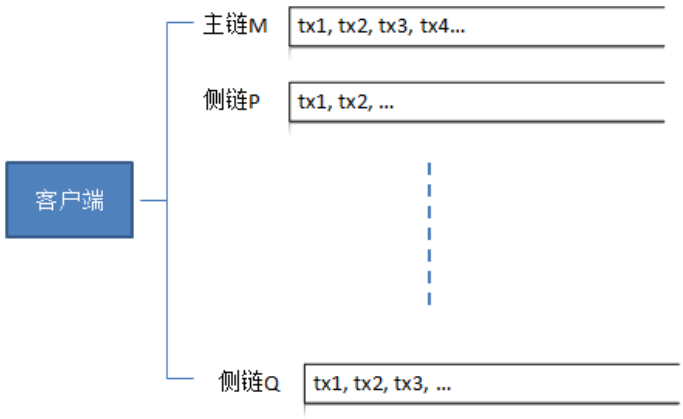

图 6 链事务集合示意图

如上图所示，在一个客户端会接收来自各条链的请求，并为每条链准备一个相应的事务集合。主链 M 中有事务 txm1，txm2...，侧链 P 中有 txp1，txp2...，侧链 Q 中有 txq1，txq2，txq3...准备参与共识。

考虑最简单的情况，客户端在某一时刻，参与其中一条链的共识。客户端知道每一条链前一段时间生成的区块的速度，以及当前每一条链的待处理事务的个数。在生成区块的激励和处理事务的激励已经确定的情况下，客户端可以判断为哪一条链生成区块最有利。当前目前有一条链生成区块速度较慢时，意味着参与者条链会有更高的成功率；而后续描述的激励机制也会促使客户端参与当前待处理事务较多的链。这样就达到了各条链根据事务多少而得到适时处理的要求。

如果客户端要同时参与多条链的共识达成，和单条链类似，只是要起多个线程来进行分别处理；客户端能参与共识的链条数取决于客户端的软硬件性能。

2）随机产生主节点

在有足够多的客户端表达需要对某条链（假设为 P）进行共识时，会把这些节点形成一个集合。接下来的动作都在这个集合内进行。

在这个集合内的客户端中，先随机挑选一个节点来充当主节点。

3）利用 BFT 来生成区块并广播给全网

在产生了主节点之后，接下来就进入 BFT 协议，和其他节点开始协商需要处理的区块链 P 的事务，进行验证投票，最终形成区块。

生成区块以后，广播到全网，就完成了此次关于 P 链的一次共识。此处的共识机制其他的多块生成机制都能同时生成多个区块，但是对链的生长机制有区别[8][9]。

PCH 的发行和激励机制

在 PCHAIN 中，将使用数字 Token PCH 来对生成区块的劳动进行衡量。

PCH 会在生成区块时，对参与共识的所有节点的账户进行发放，这是 PCH 的发行方式。在用户调用智能合约时，会针对调用的指令所需的资源进行统计，从而计算出用户需要支付的 PCH；这一部分 PCH，也会被分发给参与共识的账户。

存贮机制

在区块链中，将会有账号余额，公钥；账号之间的交易；合约的地址、二进制码；合约的存储和调用记录等。这些交易都会采用 Merkle Tree 进行 hash 验证，并且存到底层数据库中（例如 levelDB）。

智能合约升级

当前以太坊的 EVM 以及 Solidity 语言已经相对比较成熟，而且经过了长时间的考验。所以本项目选择在 EVM 的基础上进行改造，支持智能合约，并实现智能合约的升级。支持智能合约升级的方案如下：

1）原有智能合约 C，其发布者为 A，其原有的存储为 S，所有的调用/交易为 T，都记录在侧链 P 中

2）在有了新的智能合约 C1 时，必须有 A 来发布，而且新的智能合约 C1 也会部署在侧链 P 中；新的智能合约 C1 可以增加存储字段，但不能减少字段，可以增加新的方法，不能减少方法。

3）在新的合约部署 C1 时，可选择原有合约 C 是否仍然可以调用；如果允许，则 C 和 C1 都提供对外服务，如不允许，对 C 的所有调用都会返回“版本已作废，请使用新版本”的提示。推而广之，后续新的合约 C2 可以对 C 和 C1 做是否作废的决定。一个版本在作废以后，就不能再重新开放提供服务。

底层机制会对不同版本的智能合约进行管理。在智能合约调用时，根据智能合约对应版本的地址进行匹配，选择相应的代码在虚拟机上执行。

对外接口

PCHAIN 会提供类似于以太坊的 RPC 服务[10]，对外暴露各种管理和查询功能。例如账号查询，转账，区块和交易查询，合约存储查询等。目前支持基于 HTTP 的 REST API。

4 PCHAIN 的优势

首次提出 PCHAIN Smart Data 方式，并在此基础上形成 Knowledge Graph 知识图谱，帮助智能合约形成闭环。

每个 DApp 都有各自的链，浏览和还原交易非常简单

对于关注的 DApp，只需要对该 DApp 对应的侧链，从原始区块开始，到最新区块结束进行遍历，就可以获得该 DApp 相关的所有数据；从而对交易进行还原，提供浏览。 不再需要像单链上一样，所有不相关的区块也要进行扫描；大大提升了效率。

对大规模交易提供支撑

在多个 DApp 的交易累加而造成整体规模较大时，对应到每个侧链，规模会相对较小；现在每个侧链都会自己生长，从而对主链和其他侧链不会产生影响。

在单个 DApp 的交易规模较大时，全网算力会因为激励机制像该链集中，从而保证区块能够及时生成，交易能够获得尽快执行。

对于同时有多个 DApp，每个 DApp 都有很多交易时，则系统会处于相对繁忙的状态，对于拥堵有可能难以避免。但是这种情况发生的几率较小。

新的共识方式使得计算并行化

公链原有的 POW 机制下，每个节点都在挖矿，从而同时产生新块的几率较大，分叉的几率也比较大。在新的共识机制下，需要形成一个群体在进行共识，从而分叉的几率大大减少。同时，采用新的机制，每个群体达成共识时，不在需要进行密集的 CPU 运算，能够节省不少电力。全体节点可以分成多个小的群体，每个群体对一条链进行共识。形成了并发共识的行为。每个群体之间可以有交集，即每个节点可能会同时参与多个链条的共识，进一步加大了并发的力度。这样，网络的算力得到了极大的利用，从而使 PCHAIN 的生长更为顺利。

支持智能合约升级

通过前述的方式，新的 PCHAIN 支持智能合约的升级。

容错性高

在 PCHAIN 的结构下，主链只做记录，理论上不会出现大的故障。而当一条侧链出现了状况时，收到影响的只有该条侧链，而不会影响到主链和其他侧链的生长。当出现状况需要纠正时，对单链进行处理就可以。

可扩展性好

当有新的 DApp 要部署时，扩展一条侧链即可。对于新链的生长，在现有的共识机制下，并不会造成太多的负担。

5 PCHAIN 的愿景与适用场景

5.1 PCHAIN 的愿景

PCHAIN 是世界上第一条支持 EVM 的原生多链系统，使得大规模区块链应用成为可能。

5.2 适用场景

PCHAIN 能够适用众多基于智能合约的场景：

- 分布式人工智能、分布式问答、大数据交易
- 数字资产交易 - 为数字资产的交易提供可靠的记录。数字资产包括资产数字化后的凭证、或者本身就是数字化的网络虚拟资产（各种游戏道具、代币等）。智能合约可以对数字资产在进行登录、转让、售卖等各个操作环节进行记录，这些操作记录到区块链以后，对所有的参与方都公开透明，从而为审查带来极大的方便。
- 游戏 - 为游戏定下不可作弊的规则。这里的游戏主要指博弈类的游戏，在规则制定之后，游戏过程和结果都会严格按照规则进行，从而避免人工对结果的影响。例如彩票发行和结果的抽取，例如掷骰子决定胜负，等等。
- 公证系统 - 为承诺提供不可篡改的依据。在公证系统中，很重要的一环就是凭证的真实性。如果在区块链中记录了该凭证，则在后续公证的实施过程中，就不会出现因为对凭证有所质疑的纠纷。
- 痕迹社交 - 记下所有说过的话。现有的社交记录，基本都会时间久远而清掉；另外，也有些社交场景支持阅后即焚。这样，社交的记录最终都会消失掉。但是对于“认真”的对话，我们可能希望能够进行永久地保存，并且都能查看。智能合约+区块链 能够满足这样的场景。
- 全周期协作系统 - 从播种到收获，到市场流通，全周期协作
  绿色生态链，从农畜的养殖活动，到屠宰，到运输，到销售，全过程都进行跟踪记录。在物流供应链领域，从产品的生产，到运输，到上架，再到消费者手上，整个过程也都会进行跟踪记录。这些全周期的协作系统，能够让各个环节的参与者能够共享数据，增加协作和信任。

6 发展规划

6.1 资金兑换和管理

6.1.1 兑换方式

本项目将采用现在定向+公开方式来兑换 Token，以支撑项目的进行。

1) PCHAIN 的 Token 的名称为 PCH，总共会产生 210,000,000（2.1 亿）PCH。
2) 兑换及分配比例

其中，15%第一轮定向兑换，10%作为第二轮定向兑换。20%作为公开兑换。25%分配给团队和早期贡献者。另外的 30%则作为社区建设。

比重	数量	用途	说明
25%	5250 万	定向兑换	开发和运营项目；人员工资，开发软硬件采购，办公开销，法律/税务等各种开销
20%	4200 万	公开兑换	开发和运营项目；人员工资，开

			发软硬件采购，办公开销，法律/税务等各种开销
25%	5250 万	团队和早期贡献者	团队成员和早期贡献者激励
30%	6300 万	社区建设	PCHAIN基金会及PCHAIN社区建设

兑换分为两轮。第一轮分为两个阶段：定向兑换和公开兑换阶段。公开兑换仅面向法律、法规允许的国家和地区公民。第二轮定向兑换将在第一轮结束后一段时期，视开发和运营情况择时进行。

第一轮定向兑换 15% 即 3150 万 PCH 折扣 20%	**公开兑换 20% 即 4200 万 PCH**	
	早鸟周（一周）基准	**结束周（一周）110%**

6.1.2 资金使用

对于兑换到的资金，将按如下比例进行使用：

65% - 进行 PCHAIN 系统研发，包括人员工资，软硬件采购等

20% - 进行市场宣传，包括人员工资，推广费用等

10% - 进行运营，包括举办各类活动等

5% - 进行法律合规，包括支付律师咨询费用等

6.1.3 PCHAIN 基金会

PCHAIN基金会（以下简称“基金会”）是非营利性组织。基金会通过设立相关部门，致力于PCHAIN的研发,对PCHAIN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。

基金会拟设立以下部门：

- 总体执行部
  基金会设立总体执行部，其职能为全面负责基金会的正常运行。包括部门设立和职能调整，人员招聘，对外交流等各种事务。
- DApp 管理部
  DApp管理部负责对所有加入到PCHAIN中的DApp进行跟踪和管理，与DApp开发者保持沟通，以保证PCHAIN的发展能为DApp的开发和部署提供最好的服务。
- 代码审核部
  由于黑客的攻击，目前即使是非常大的区块链项目，也都存在大量资产丢失的事例发生。这里借鉴其他社区的做法，成立一个代码审核委员会，以审查所有提交到开源社区的代码，特别是牵涉到PCH流转的部分。
- 行政及对外公关部
  负责财务及人事管理，对项目的支出，以及人员变动进行掌握和协调。在项目有重大发布，或者出现有影响力的事件时，负责出面进行宣传和应对。

6.1.4 系统用途

PCHAIN 的系统用途主要有两方面：

- 促进智能合约上链

  在 PCHAIN 建成以后，在智能合约上链，以及调用智能合约时，都需要支付一定的费用，该费用使用 PCH 结算。除了挖矿可以获得 PCH 外，还可以在交易市场上获取 PCH。在 PCHAIN 建成规模以后，会有越来越多的应用上链，在链上进行的交易也会越来越多，对 PCH 的需求也会增加，PCH 本身就会增值。从而 PCHAIN 项目会因此得到增值。

- 提供基于 PCHAIN 的服务

  作为 PCHAIN 平台的提供方，对 PCHAIN 的核心技术以及应用开发接口具有主导权。我们可以基于 PCHAIN 提供便捷的产品，例如查询平台等。也可以为 DApp 的需求方提供技术方案，从而使 DApp 的开发更为顺利，例如智能合约的升级等。

目前有 3 个国际知名大型区块链应用项目已确立将基于 PCHAIN 系统搭建，例如，由国际著名音乐制作人打造的区块链文化项目，已获得日本金融厅区块链协会的认可，并由日本大富电视台、凤凰网、人民网、新浪、搜狐、腾讯、网易等多家媒体报道； 与清华大学国家重点实验室合作的抗量子区块链研究项目，获得多位院士认可。另有，多家区块链应用项目沟通进行中。

6.1.5 法律与项目风险

基金会将遵循各国相应的法律法规，为全球 PCHAIN 社区和爱好者提供技术和资金支持，以促进 PCHAIN 项目的顺利进行。虽然本项目经过充分的市场调研，做了完善的技术储备，但是在市场及技术不断变化的当今，并不能确保项目一定会取得预期效果，不能排除 PCH 的归零风险。敬请投资人进行风险控制。

6.2 团队成员

PCHAIN拥有一个国际化资深技术开发、研究与管理团队，具有多年区块链行业经验。

曹锋 CEO

复旦大学计算机博士，中国第一个区块链国际专利发明人，国内影响力最大的区块链联盟ChinaLedger共同发起人，中国区块链研究联盟高级研究员，中物联区块链协会首席科学家，完成全球第一笔区块链收益权转让暨中国第一笔区块链金融真实交易。他是中国区块链发展的实践者与推动者，成功创立多家区块链企业，获顶级风投投资及多项区块链金融创新大奖。曾担任IBM中国研究院互联网金融首席科学家，3次获IBM全球杰出奖，IBM下一代人机大战项目中国区负责人，专利评审委员会联合主席，W3C RDF标准委员会成员；他的创新成果已成功应用于中、美等150多个国家，发表22篇国际顶级论文，30余项美国专利，并担任多个ACM IEEE顶级国际会议论坛主席。

吕浩进 CTO

清华大学计算机硕士，国内早期的区块链技术专家，带领团队负责完成多项国际领先的区块链项目，具有深厚的区块链理论与实践经验。曾在SAP上海实验室等著名外企任职，擅长产品优化与创新，系统级软件的设计实现，分布式服务器集群的搭建，大数

据存储、挖掘与展现，大型软件开发流程与质量控制。

徐若淞 市场负责人

原公信宝首席市场营销官， 复旦大学物理学学士， 曾供职于华为技术，中国移动及同盾科技，在大数据，信贷风控，通信及物联网领域有丰富的行业经验。

马占峰 区块链存储与优化

西安交通大学计算机硕士，底层区块链技术专家， 资深软件工程师，拥有10多年世界500公司工作经历，一直专注于数据库系统和分布式系统，获得多项数据库领域的美国专利，具有丰富的系统开发和性能优化经验。

郑凯 内存数据库算法

电子科技大学计算机科学与工程学院教授，博士生导师，中组部“青年千人计划”专家。2012年博士毕业于澳大利亚昆士兰大学，2012-2016年在昆士兰大学信息与电子工程系担任研究员、讲师。主要研究领域包括大数据管理，社交媒体数据分析，时空数据库，不确定数据库， 内存数据库，区块链技术等。在数据库、数据挖掘领域顶级会议(CCF A类)和期刊(SCI 检索)，如SIGMOD，ICDE， EDBT，ACM TODS， The VLDB Journal，IEEE TKDE等发表论文100余篇，著有《区块链技术详解与实战》（待出版），谷歌学术引用超过1400次，H-index=21。2013年获澳大利亚优秀青年基金(Australia Research Council Discovery Early Career Research Award)；2015年获数据库顶级会议ICDE最佳论文奖。担任重要数据库国际会议的程序主席(APWeb 2016)和大会主席(DASFAA 2017)，担任国际SCI期刊WWW Journal、Geoinformatica、Frontier of Computer Science的客座编委，担任IEEE TKDE， VLDB Journal，ACM TODS等多个顶级数据库期刊的特邀评审和多个国际顶级会议的程序委员，如ACM SIGMOD (2015年，2016年)，CIKM (2014年，2015年)， ICDE (2018年)，WWW(2018年)

崇志宏 知识图谱算法

东南大学计算机科学与工程学院、软件学院副教授、博士、硕士生导师。曾在澳大利亚新南威尔士大学和新加坡University of Illinois Research Center in Singapore从事学术访问和研究。主要从事区块链、大数据、知识图谱、深度学习的理论研究与工程应用研发。先后主持和参与国家自然基金、863、国家重点和国防总装重点项目九项，主持华为、中国电子集团、焦点科技等企业的校企合作项目十多项。在数据库和人工智能领域主要会议和期刊上发表论文十多篇。

张振杰 分布式数据库与索引算法

新加坡国立大学计算机科学博士，美国伊利诺伊大学高等数字科学中心的高级研究科学家，研究领域包括了数据库查询和索引、高维数据挖掘和因果关系分析、数据挖掘和机器学习中的隐私保护、高速数据流处理，以及弹性云计算技术。他在数据库、数据挖掘和机器学习领域内发表了超过50篇高水平论文，其中包括SIGMOD、VLDB、ICML、VLDB Journal和IEEE TKDE等多个顶级会议和期刊。这些论文目前有超过1800次引用，平均引用率大于30。他是2013年国际数据隐私研讨会和2015年亚太网络会议的共同程序主席，十多个国际顶级会议的程序委员会委员，以及多个国际一流学术期刊的审稿人。他于2015年获得IEEE数据工程技术委员会（TCDE）的青年学术奖。他也是2008年新加坡国立大学总统奖获得者，以及2013年IEEE国际云计算工程会议最佳论文奖得主。

6.3 路线图：

- PCHAIN Position Paper 完成 T
- Dewdrop 阶段 – T+7 个月
  完成 PCHAIN 核心系统的开发，支持账户系统、智能合约的部署等，发布技术白皮书，
  测试网上线。
- River 阶段 – T+12 个月
  主网上线， 同时完成对外 API 的文档编写和 wiki 的搭建。
- Sea 阶段 – T +15 个月
  扩展知识图谱与 Smart Data 区块链能力，支持外部开发接口。
- Ocean 阶段 – T +18 个月
  引入多项区块链应用项目，形成 Knowledger Graph 区块链联盟

在对 18 个月的里程碑的结果进行检查以后，后续再针对具体的发展状况，制订新的计划。力争 PCHAIN 保持正确的研发和服务方向，保持技术和市场的领先地位。

7 参考文献

[1] Bitcoin. https://bitcoin.org
[2] Ethereum. https://ethereum.org
[3] Solidity. solidity.readthedocs.org
[4] Ethdocs.org . "What is Ethereum? — Ethereum Homestead 0.1 documentation"
[5] HyperLedger. www.hyperledger.org
[6]https://news.bitcoin.com/status-ico-generates-over-60-million-but-fails-to-deliver-meanwhile-ethereum-flounders/
[7] https://en.wikipedia.org/wiki/Blockchain#cite_note-te20151031-1
[8] Bitcoin Wiki. https://en.bitcoin.it/wiki/Merged_mining_specification
[9] Plasma. https://www.plasma.io/plasma.pdf
[10] https://github.com/ethereum/wiki/wiki/JSON-RPC
[11]白硕|基于区块链的众包社区激励机制
[12]Zilliqa. https://www.zilliqa.com/
[13]Polkadot. https://polkadot.io/
[14]Aelf. http://aelf.io/
[15]Rootstock. https://www.rsk.co/
[16]Cosmos. https://cosmos.network/
[17]Dfinity. https://dfinity.org/
[18]LISK. https://lisk.io/
[19]Asch. https://www.asch.io/
[20]Ardor. www.ardorplatform.org/
[21]BTC Relay. btcrelay.org/
[22]BlockStream. https://www.blockstream.com/