BLOCKCHAIN

SimpleChain 联盟链白皮书

Consortium Blockchain Whitepaper

浙江数秦科技有限公司

2020.11.25

目 录

1 设计背景

区块链诞生于移动互联网时代，联盟链则在数字经济时代迎来了历史发展机遇。国家最高决策层已将区块链提升到国家战略高度，推动联盟链技术与实体产业的结合，而跨链技术及隐私保护则成为联盟链发展的精神内核。

1.1 联盟链发展现状

相比于公链的发展，联盟链的起步时间较晚，其概念大约产生于2015年，2016年由Linux基金会发起的开源HyperLedger项目最早公开联盟链代码。随着Hyperledger、R3等知名项目的发展，国内的探索者开始注意到这项技术，各大型企业也逐步针对不同场景进行小范围实践，与此同时，独立型的区块链创业公司也逐渐浮出水面，争先挖掘联盟链应用的潜在前景。目前，联盟链已经在知识产权、供应链金融、分布式身份认证和公益等多个领域落地，解决了具体业务上的痛点。以联盟链为基础构建生态可根据行业需求和内在规律优化系统，帮助企业在解决现有系统存在问题的同时拓展其业务的丰富性。

联盟链的快速发展对监管也提出了更高的要求，国际及国内标准化组织和相关机构均在积极推动区块链标准体系的制定和完善，监管机构通过区块链的标准化、规范化来甄别纷繁复杂的各种区块链应用，去伪存真，助力市场形成健康、公平的发展环境。

从联盟链领域发展来看，其准入门槛较高，除需建立标准化的区

块链底层技术，还需要根据应用的具体需求和行业特性实现智能化监管，引导区块链应用的快速落地，推动区块链产业规范有序地发展。

1.2 国家战略技术推动联盟链的进化与落地

紧随着全球推进布局区块链技术发展的步伐，国务院于 2016 年正式将区块链技术列为战略性前沿技术，并在 2019 年将区块链正式上升为国家战略。高屋建瓴的战略判断揭开了区块链发展的新篇章，而联盟链关键技术的研究也成为了热点所在，是新一轮科技和产业革命的主要驱动力。

中央银行数字货币就是基于联盟链体系，利用区块链的分布式记账、不可篡改和实时记录的特性完善银行间的结算系统，但结算效率问题仍然是难点所在。从技术层面看，区块链技术的局限问题滞缓了区块链应用落地，分布式记账效率无法达到中心化交易系统相应的水准，因此技术的进步是联盟链发展的关键。从监管层面看，联盟链将全过程记录上链的方式让整个金融体系更加透明化，更利于央行的监管，让金融意义上的洗钱、偷税和漏税等行为彻底成为过去式。在不远的将来，随着区块链技术的成熟，联盟链将与更多的实体经济深度融合，不断完善国家区块链建设的总体布局。

1.3 跨链技术和隐私保护成为重要方向

目前，大部分的联盟链应用都停留在内部闭环阶段，数据只能在单个联盟链生态中流通，与生态外的其他联盟链难以协作互动。而随

着行业需求的增多和互通需求的增加，隐私保护问题又接踵而至。针对行业应用的落地和商业场景互通问题，跨链协作和隐私保护已经成为联盟链发展的主要方向，除此之外，还需要考虑性能、成本等多方面的建设因素。

当前已成型的的跨链解决方案主要有三种类型：公证人跨链、主动兼容跨链平台、被动兼容跨链平台。其中，公证人跨链最为简洁，只需要各联盟链出具“中间人”参与交易确认和验证即可。跨链协作主要是为了实现数据共享的目标，其中最大的障碍就是数据隐私问题。目前项目中采用比较多的方式就是多重签名，实现由多方控制的更高级别的隐私保护，也有不少项目积极研究安全多方计算技术及可信执行环境技术等加密计算技术，通过绕过信息读取的方式直接进行加密计算。未来，随着跨链技术的不断完善和升级以及隐私保护问题的解决，使得更多的联盟链生态实现互通，通过合作和信任创造超出想象的价值体系，促进分布式的数据交换和合规框架下的价值交换。

2 设计目标

SimpleChain 联盟链以简单高效的共识机制、高可用性和可扩展性、全方位的安全机制、简洁的合约设计、多角度的性能优化为设计目标，构建功能完善、技术成熟的联盟链底层架构，为上层业务应用提供标准化服务和技术组件。

2.1 简单高效的共识服务

SimpleChain 联盟链设计了可插拔共识，以适应用户在应对不同应用场景需求,目前支持 PoA(Proof-of-Authority)共识算法与 Raft（Reliable, Replicated, Redundant, and Fault-Tolerant）共识算法。PoA 共识中，所有交易的验证均由授权节点进行，而授权节点的产生则通过相对去中心化的方式,这在一定程度上保障了网络的安全性。相比起来，Raft 共识则更为简便，通过触发选举领袖的方式来选择出块者，负责打包和同步交易信息。上述两种共识均不要求节点像 PoW（Proof-of-Work）那样花费计算资源来解决复杂的数学逻辑，授权节点能按指定的时间间隔生成区块，在时间可控制的同时提高交易验证的速度。综上所述，PoA 共识算法和 Raft 共识算法可以使得联盟链更好地适用于各类应用场景，以低成本、高可控的优势最大程度地提高交易效率。

2.2 更高的可应用和可扩展性

SimpleChain 联盟链支持多语言、多开发环境适配的 SDK，并提供完整的节点部署教程与安装文档，提供最大限度的区块链自主部署便利性。此外，SimpleChain 联盟链在其服务平台上提供基于混合云的云节点部署接口，能够实现基于多级安全技术要求的远程云服务器节点部署，降低用户硬件门槛。联盟链管理平台更提供了区块链浏览器、节点管理、合约管理三大功能，保证了联盟链的易用性。

2.3 全方位的安全机制

SimpleChain 联盟链在通信安全、节点权限管理、密码算法以及密钥管理上均做了全面有效的配置，从而保障系统的安全性。节点之间、节点与客户端之间通信采用 TLS 安全协议，支持国密算法和国密通信协议，采用 CA 服务管理节点密钥，同时设定了网络准入机制和共识准入机制，用于限制授权节点的加入、退出联盟链。目前，大部分区块链通常会采用多重签名机制来避免单个授权节点作恶，或者让验证人来自不同的区域和利益集体避免集体作恶。SimpleChain 联盟链则设置了特定的节点控制规则，可以有效控制恶意节点的攻击范围，并在一定的有效期内将其踢出，确保网络可靠正常地运行。

2.4 简洁的合约设计

SimpleChain 联盟链提供了图灵完备的编程语言和相应的运行环境。区别于比特币的 UTXO 模型和脚本只能运行部分计算，

SimpleChain 联盟链的脚本编程语言能运行所有可能的计算，也就是所谓的图灵完备。任何用户均可以在 SimpleChain 联盟链上开发智能合约，并进行合约生命周期管理，实现合约的升级、冻结等功能。为规范合约的应用，需要事先确认业务范围、业务流程、数据权限、是否合规、是否侵害互相利益和用户利益等细节问题，待达成共识后才可在链上组建联盟链，并通过部署智能合约去实现具体的业务逻辑。

2.5 多角度的性能优化

SimpleChain 联盟链从提升交易执行效率和并发两个方面优化了交易执行，使得交易处理性能达到万级以上，让系统性能得到有效提升。一方面，基于 DAG 算法根据交易间互斥关系构建区块内交易执行流，最大化并行执行区块内的交易，以达到交易并行执行的效果。另一方面，通过共识、同步等各个环节的异步化以及并行处理实现交易生命周期的异步并行处理。目前，SimpleChain 联盟链已获得赛迪测评证书，TPS 达到 80000+。

3 联盟链架构

SimpleChain 联盟链的整体架构包括四层——底层服务层、核心层、接口层和应用层，数据存储上采用分布式存储，数据同步上做到交易的同步和状态的同步，并通过引入虚拟机模块支持合约的执行与调用。

3.1 整体架构

整体架构上，SimpleChain 联盟链划分为底层服务层、核心层、接口层和应用层，整体架构如下图所示：

图 1　SimpleChain 联盟链整体架构

底层服务层主要提供联盟链的基础数据结构、算法库和分布式存储。核心层主要实现联盟链的核心逻辑，其中包括链核心层和管理层。链核心层用来实现联盟链的链式数据结构、交易执行引擎和存储驱

动、基础 P2P 网络通信、共识机制和区块同步机制。管理层主要实现联盟链的管理功能，包括参数配置、账本管理和 AMOP。接口层则面向联盟链用户，提供多种协议的 RPC 接口、SDK 和交互式控制台。应用层主要实现基于图灵完备编程语言的智能合约、权限管理、角色管理、合约生命周期管理、DApp 应用等。

3.2 数据存储

SimpleChain 联盟链在继承 SimpleChain 公链原生存储的同时，还引入了高扩展性、高吞吐量、高可用、高性能的分布式存储。存储模块主要包括世界状态存储和数据存储两部分。

世界状态存储可进一步划分成 MPTState 和 StorageState。MPTState 使用 MPT 树存储账户的状态，与 SimpleChain 公链一致，StorageState 则使用分布式存储的表结构存储账户状态，不存历史信息，去除对 MPT 树的依赖，性能更高。

数据存储支持 LevelDB 数据库。SimpleChain 联盟链共有 BlockDB、StateDB 和 ExtrasDB 等三个 LevelDB 数据库，BlockDB 保存块的主体内容，包括块头和交易，StateDB 保存账户的状态数据，ExtrasDB 保存收据信息和其他辅助信息。

3.3 数据同步

数据同步是 SimpleChain 联盟链节点重要功能之一，作为共识的辅助，它给共识提供必需的运行条件。数据同步分为交易同步和状态

同步。交易同步确保每笔交易能正确到达每个节点，状态同步确保区块落后的节点能正确的回到最新的状态，因为只有持有最新区块状态的节点才能参与联盟链共识。

3.3.1 交易同步

交易同步使得 SimpleChain 联盟链网络的交易尽可能到达所有节点，为共识中将交易打包成区块提供基础。一笔交易从联盟链客户端发往某个节点，节点在接收到交易后，会将交易放入自身的交易池中供共识去打包。与此同时，节点会将交易广播给其它的节点，其它节点收到交易后同样将交易放到自身的交易池中。

交易在发送的过程中会存在丢失的情况，为了能让交易尽可能到达所有的节点，收到广播过来交易的节点会根据相应的策略，选择其它的节点再进行一次广播。然而，如果每个节点都没有限制的转发/广播收到的交易，网络带宽将被占满，导致出现交易广播雪崩的问题。为了避免交易广播的雪崩，SimpleChain 联盟链采用较为精巧的交易广播策略，在尽可能保证交易可达性的前提下减少重复的交易广播。SimpleChain 联盟链主要遵循以下规则：对于 SDK 传输的交易广播给所有的节点，一条交易在一个节点上只广播一次，当收到了重复的交易不会进行二次广播。

SimpleChain 联盟链通过上述策略能够尽量让交易到达所有的节点，但在极小的概率下还是会出现交易无法到达全部节点的情况。交易尽可能到达更多节点的目的是为了让此交易快速被打包、共识、确

认，使得交易能够更快地得到执行结果。若交易未到达全部节点，只会使得该交易的执行时间变长，不会影响交易的正确性。

3.3.2 状态同步

状态同步使得 SimpleChain 联盟链节点的状态保持在最新。联盟链状态的新旧是指联盟链节点当前持有数据的新旧，即节点持有的当前区块块高的高低。若一个节点的块高是联盟链的最高块高，则此节点就拥有联盟链的最新状态。只有拥有最新状态的节点才能参与共识，进行下一个新区块的共识。

若一个全新的节点加入区块链网络，或一个断网的节点恢复网络时，此节点的区块落后于其它节点，状态并非最新，需要进行状态同步。需要状态同步的节点会主动向其它节点请求下载区块，整个下载的过程会将下载的负载分散到多个节点上。区块的下载通过请求的方式完成，整个流程说明如下：

（1）进入下载流程的节点：随机挑选满足要求的节点，发送需要下载的区块区间；

（2）收到下载请求的节点：根据请求的内容，回复相应的区块；

（3）收到回复区块的节点：在本地维护一个下载队列，用来对下载下来的区块进行缓冲和排序，其中下载队列是一个以块高为顺序的优先队列。下载下来的区块会不断的插入到下载队列中，当队列中的区块能连接上节点当前本地的联盟链，则将区块从下载队列中取出，并连接到节点当前本地的联盟链上。

3.4 虚拟机

SimpleChain 联盟链虚拟机是智能合约代码的执行器，当智能合约被编译成二进制文件后被部署到 SimpleChain 上，用户通过调用智能合约的接口来触发智能合约的执行操作。虚拟机执行智能合约的代码，修改当前区块链上的状态。被修改的数据会被共识，确保一致性。执行器在这个过程中类似于黑盒，输入是智能合约代码，输出是状态的改变。

传统的虚拟机是耦合在节点代码中，为了智能合约在应用上能有更快的执行速度，满足大规模交易的需求，SimpleChain 联盟链将执行器的接口抽象出来，形成接口标准，兼容各种虚拟机的实现。通过接口标准，SimpleChain 联盟链节点可以对接多种虚拟机，支持多类型语言进行开发，例如 Solidity、C#、C++、Python 等。

4 联盟链功能模块

SimpleChain 联盟链通过特有的技术架构，实现了系统吞吐能力的横向扩展，大幅提升性能，可插拔共识机制、节点安全机制、高效智能合约等功能模块的设计使得联盟链在安全性、易用性、可运维性、可扩展性等方面具备行业领先优势。

4.1 可插拔共识

SimpleChain 联盟链基于多群组架构设计了插件化的共识算法，不同群组可运行不同的共识算法，组与组之间的共识过程互不影响。SimpleChain 联盟链目前支持 PoA 和 Raft 等多种共识算法。

4.1.1 PoA 共识算法

PoA 共识算法由选定的权威节点轮流负责出块，可通过投票的方式增加或删除出块节点，一方面确保出块的稳定性，另一方面减少为达成共识而造成的资源浪费。PoA 共识具备以下特点：

（1）依靠预设好的授权节点（signers）产生区块；

（2）可以由已授权的授权节点选举（投票超过 50%）加入新的授权节点；

（3）即使存在恶意授权节点，它最多只能攻击连续块{数量=（SIGNER_COUNT/2）+1}中的 1 个，期间可以由其他授权节点投票踢出该恶意授权节点；

（4）可指定产生区块的时间。

PoA 的工作流程如下：

（1）在创世块中指定一组初始的授权节点，所有地址保存在创世块 Extra 字段中；

（2）启动挖矿后，该组授权节点开始对生成的区块进行签名并广播；

（3）签名结果保存在区块头的 Extra 字段中，Extra 中更新当前高度已授权的所有授权节点的地址，由于会有新加入或踢出的授权节点；

（4）每一高度都有一个授权节点处于 IN-TURN 状态，其他授权节点处于 OUT-OF-TURN 状态，IN-TURN 的授权节点签名的区块会立即广播，OUT-OF-TURN 的授权节点签名的区块会延时一点随机时间后再广播，保证 IN-TURN 的签名区块有更高的优先级上链；

（5）如果需要加入一个新的授权节点，授权节点通过 API 接口发起一个 proposal，该 proposal 通过复用区块头 Coinbase（新授权节点地址）和 Nonce（“0xffffffffffffffff”）字段广播给其他节点。所有已授权的授权节点对该新的授权节点进行“加入”投票，如果赞成票超过授权节点总数的 50%，表示同意加入；

（6）如果要踢出一个旧的授权节点，所有已授权的授权节点对该旧的授权节点进行“踢出”投票，如果赞成票超过授权节点总数的 50%，表示同意踢出。

4.1.2 Raft 共识算法

Raft 属于 CFT（Crash Fault Tolerance，即故障容错）类算法，是一个允许网络分区（Partition Tolerant）的一致性协议。当系统出现网络和磁盘故障、服务器宕机等普通故障时，仍能针对某个提议达成共识，Raft 算法性能较好、处理速度较快，可以容忍不超过一半的故障节点,即 Raft 保证在一个由 N 个节点构成的系统中有(N+1)/2（向上取整）个节点正常工作的情况下系统的一致性。

在 Raft 算法中，每个网络节点只能以下三种身份之一：Leader、Follower 和 Candidate，各身份的作用说明如下：

（1）Leader 由 Follower 节点选举而来，在每一次共识过程中有且仅有一个 Leader，Leader 负责从交易池中取出交易、打包交易成区块并将区块上链；

（2）Follower 以 Leader 节点为准进行区块同步，并在 Leader 节点失效时举行选举以选出新的 Leader 节点；

（3）Candidate 指的是 Follower 节点在竞选 Leader 时拥有的临时身份。

4.2 安全控制

为了保障联盟链节点间通信的安全性及联盟链节点数据访问的安全性，SimpleChain 联盟链引入了节点管理、CA 黑名单和权限控制等三种机制，在网络和存储层面上做了严格的安全控制。

4.2.1 节点分类

SimpleChain 联盟链具有三种节点类型：管理员节点、游离节点、普通节点，三种节点可通过合约接口以及共识算法进行转换。

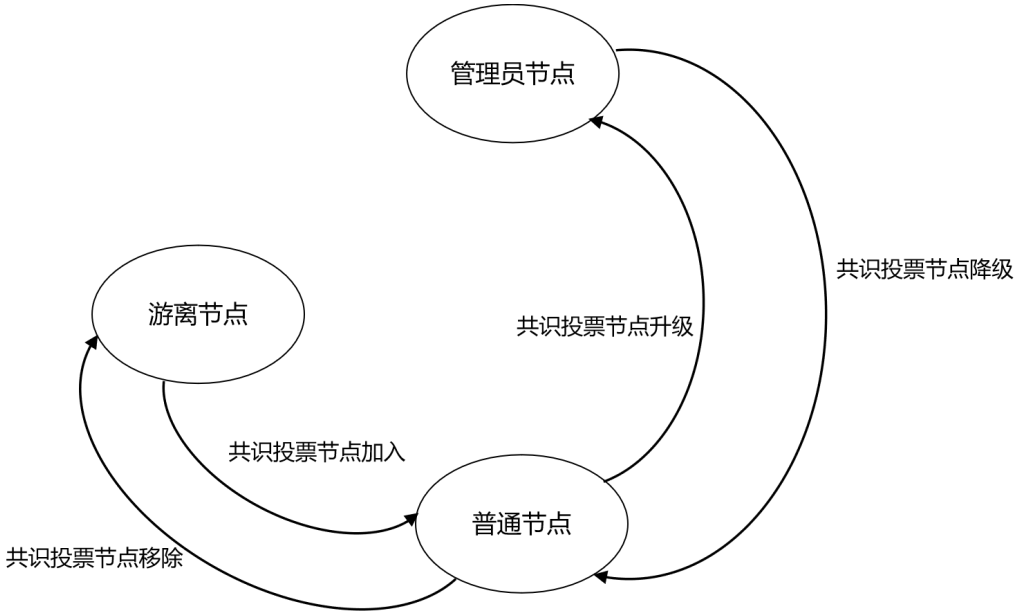

图 2　节点转换流程

节点启动时根据创世区块（节点初始表）来判断节点类型，系统表的黑名单内的节点即游离节点，不具备共识或者同步功能。若需要更改游离节点为普通节点，可通过合约/共识算法进行操作，达到共识后才可成为普通节点。同样，更改普通节点为游离节点也是通过合约/共识算法完成。

4.2.2 节点准入

节点管理机制可分为网络准入机制和共识准入机制，准入机制的规则记录在配置中，节点启动后读取配置信息实现网络及群组的准入判断。

4.2.2.1 节点准入所需的配置项

节点准入管理相关的配置项有：节点证书，CA 黑名单、节点初始列表和节点系统表,其中节点证书表示节点的证书、私钥和根证书，CA 黑名单即 CA 证书吊销列表，配置项具体说明如下表所示。

表 1　节点转入管理相关配置项表

配置项	作用	影响范围	是否可改	存放位置
节点证书	证明自己是由可信第三方许可的节点	网络配置	可改配置	本地存储
CA 黑名单	记录本节点禁止与哪些节点建立网络通信	网络配置	可改配置	本地存储
节点初始列表	记录创世块阶段参与共识/同步的节点列表(管理员节点白名单、节点白名单、节点黑名单)	共识配置	固定配置	本地存储
节点系统表	记录当前参与共识/同步的节点列表（管理员节点白名单、节点白名单、节点黑名单）	共识配置	可改配置	链上存储

4.2.2.2 节点准入的流程设计

SimpleChain 联盟链节点的准入机制将结合智能合约加以控制，在合约中设立节点表、节点黑名单、管理员节点表，其中，管理员节点是对节点加入网络、节点进入黑名单等操作进行审核的角色。普通节点与管理员节点之间可相互切换,申请操作的节点必须为管理员节点。

账户将使用证书私钥方式进行管理，网络中只使用一个 CA，因此需要在调用交易之前的账户解锁操作中进行验证操作，以确保无其他 CA 签发的证书私钥对应的账号伪装发送交易。节点准入有以下具体流程：

1、节点申请加入网络

网络外的节点 A 申请加入网络，需提前与网络中存在的节点 B 进行线下交互，由 B 节点提交权限准入申请交易，管理员节点对申请进行审核，半数以上同意即可加入网络。

2、普通节点移入黑名单

若普通节点 A 被移入黑名单，A 将断开与联盟链网络的连接，无法同步区块数据。该操作由管理员节点发起，所有管理员进行审核，半数以上管理员同意即可移除。

3、普通节点升级为管理员节点

普通节点 A 可以升级为管理员节点，由管理员节点发起，所有管理员节点进行人工审核，半数以上节点同意即可通过。

4、管理员节点降级为普通节点

管理员节点 A 经审核后可降级为普通节点，由管理员节点 B 发起，管理员节点进行人工审核，半数以上管理员同意后即可通过。

4.3 合约设计

SimpleChain联盟链基于智能合约的定义设计了完整的智能合约平台，支持智能合约的拓展，能够基于智能合约编写逻辑复杂的业务操作来实现丰富的场景应用。

SimpleChain联盟链的智能合约程序在SimpleChain联盟链虚拟机上运行，智能合约代码是存在于SimpleChain联盟链执行环境中的“自治代理”。用户可在SimpleChain联盟链上开发智能合约，开发的智能合约代码将存在于SimpleChain联盟链账户中，这类存有合约代码的账户叫合约账户。相应地，由密钥控制的账户为外部账户。合约账户不能自己启动运行自己的智能合约。若要运行一个智能合约，需由外部账户对合约账户发起交易，从而启动其中代码的执行。

SimpleChain联盟链提供图灵完备的编程语言和相应的运行环境，SimpleChain联盟链智能合约具有以下特征：

（1）合约生命周期：SimpleChain联盟链中智能合约的典型的生命周期覆盖合约编写、编译、部署、调用、升级、冻结等六个环节。

（2）合约类型：SimpleChain联盟链提供图灵完备的智能合约能力，具有更好的性能及对开发者友好的特性。

（3）合约扩展：SimpleChain联盟链智能合约提供多种形式的合约扩展能力，包括RSA验签、Base64编解码、上下文获取、JSON &XML解析等。

5 应用场景

作为安全可控的企业级联盟链底层架构，SimpleChain 联盟链可以应用于各类业务场景，联盟链节点加入网络的机制由已在网络中的所有管理节点进行投票做出判断，增加明显的可控性和安全性。机构和企业能够根据需求通过 SimpleChain 联盟链构建自己的行业生态，促进行业发展和价值流通。

SimpleChain 联盟链适用于多类型业务场景，目前已在政务、金融、知识产权保护、司法存证等多行业领域有落地应用。通过行业联盟链的建设来优化不同生态系统的协同流程，实现科学决策、高效指挥，有效提升服务管理水平，同时推动多部门资源共享。对于政务服务而言，通过区块链实现精细化管理，有效缩短流转办事时间，促进多部门协同，提高业务审批效率；对金融服务而言，可依托市场和监管“双轮驱动”，全面整合数据资源，实现智能化数据管控，提升行业风险管理水平；对商品溯源服务而言，可实现多方共同记录溯源信息，使产业链数据可视化，让数据得以高效管理。