技术白皮书

可信自动化@移动网络边缘

摘要

SnapScale 是针对 5G 网络边缘分布式 MEC 基础设施打造的联盟区块链平台。借助移动网络运营商的 5G 及 MEC（多接入边缘计算）基础设施，SnapScale 致力于建立领先的联盟区块链技术平台及 MEC 资源管理平台，有效解决困扰物联网的数据安全、流通、共享等问题，最终实现任意规模、任意类型的物联网设备的互联互通。

SnapScale 专注于使用分布式账本技术（DLT），将与移动网络运营商、Hyperscale 云厂商等企业合作伙伴在 5G 网络边缘建立一个智能、分布式的物联网生态系统。

1 行业背景

1.1 面临的问题

近几年，物联网行业呈现出蓬勃发展的态势，但依然面临设备安全、个人隐私、架构束缚和多主体协同等亟待解决的问题。

设备安全：不同行业、不同类型的物联网设备和数据量都在快速增长，且缺乏统一的互联网标准，物联网面临的安全挑战日趋严峻。

个人隐私：近些年层出不穷的个人隐私数据的泄露，让物联网从业者重新思考数据的归属问题、数据变现的边界以及智能安防产品的良性生长模式问题。

云计算架构束缚：云计算依然是物联网的基础，随着物联网设备数量呈几何式增长，基础设施的运营和维护成本居高不下；传统的云计算网络已经无法满足车联网、工业物联网、虚拟现实等应用场景的低延时需求。

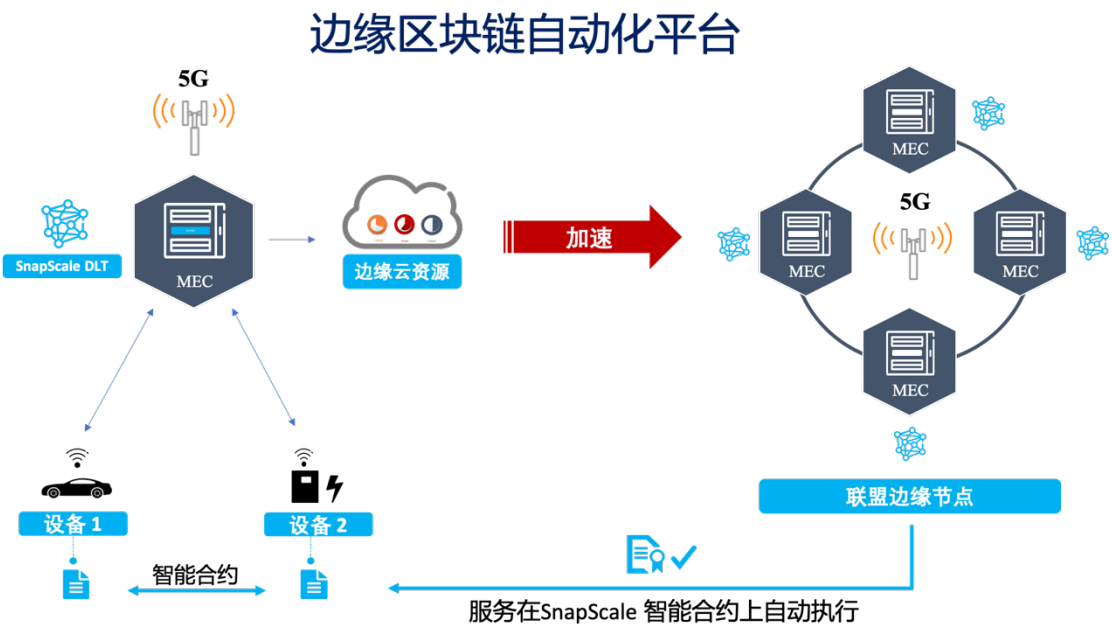
多主体协同：越来越多的物联网应用场景需要跨主体进行协作，信任成本和沟通成本高昂降低了各主体间的沟通效率。

1.2 基于区块链和边缘计算的物联网解决方案

5G（The 5th Generation of Networks）技术即第五代移动通信网络，跟 4G 相比，5G 在接入速率、时延、连接密度这几个关键指标有 10 倍量级的提升。5G 三大应用场景为：增强移动宽带（eMBB），海量机器连接(mMTC)和高可靠、低时延高可靠通信（uRLLC）。借助 5G 技术，车联网、虚拟现实（VR）、增强现实（AR）、工业自动化、智慧医疗等对时延要求比较高的应用将迎来大规模爆发。

SnapScale 使用边缘计算降低时延，提升终端的用户体验。传统云计算网络结构中，在设备边缘端获得的信息需要传输到核心网中心数据机房，待数据处理完毕之后再进行回传，边缘计算则将用户常用到的数据，放在离用户比较近的边缘云中，从而降低用户存取网络信息和服务的延迟，这对与 5G 应用来说尤为重要。

如下图所示：SnapScale 分布式账本搭建在移动网络边缘的 MEC 服务器上，物联网设备通过智能合约进行身份验证、可信数据管理，M2M 支付等自动化操作，并通过联盟边缘节点与其他的 MEC 服务器进行沟通，实现 MEC 服务器之间的信息交互。未来，移动网络运营商和第三方认证机构可作为边缘节点加入联盟，提供身份认证、跨运营商通信等服务。



区块链诞生于 2008 年，最大的特性是分布式和不可篡改。SnapScale 使用分布式账本技术（DLT）让物联网设备进行点对点的数据交易，避免中心化机构进行数据造假或篡改，同时降低信任成本，使得物联网设备之间进行自动化的数据交易和共享，从而打破信任壁垒，实现真正的价值互通。

物联网是一个天然的分布式系统，区块链和边缘计算的架构也是分布式的，SnapScale 的解决方案实现了物联网、区块链和边缘计算的完美契合。区块链平台作为基础服务部署在边缘 MEC 服务器上，可以和各类边缘行业应用有机结合，发挥区块链技术在数据安全、CA（Certificate Authority）认证和隐私保护方面的独特优势。同时边缘计算服务器通过提供低时延、可靠的计算和存储资源服务，改善区块链性能。SnapScale 新型的物联网解决方案，具备以下特性：

分布式账号系统

据 GSMA 预测，2025 年全球物联网设备（包括蜂窝及非蜂窝）联网设备将达到 252 亿个。任何一个传统的账号系统都不能满足如此海量设备的数据交易需要，SnapScale 将建立一个分布式的、去中心化的账号系统。

设备之间进行可信自动化交易

智能合约可通过 SDK 调用实现轻松部署，海量的物联网设备通过分布式应用（DApps）智能合约进行可信、自动化交易，极大降低信任成本。

安全性

中心化的数据收集和服务方式，无法从根本上向用户保证数据的合法使用。区块链支持点对点的数据交易，可以避免中心化数据库的数据造假和篡改。

数据可审计、易追踪

区块链通过时间戳、哈希加密算法、共识机制等技术保证上链数据不可篡改，且可追溯，从而增加造假难度，减轻审计工作压力，提高审计效率。

高性能、可扩展

SnapScale 采用混合双链治理结构和 FPGA 硬件加速装置，提升区块链性能。混合双链治理结构，有效减轻主链拥塞，保持 SnapScale 链上工作负载均衡，提升物联网设备不同类型交易的处理效率；SnapScale 的硬件加速装置，支持将计算密集型任务从 CPU 卸载至专用硬件加速装置，动态调动任务负载，并做到按需按时执行应用程序加速。

2 设计思路

2.1 设计思路

SnapScale 是结合区块链和边缘技术的新型物联网解决方案，设计之初即聚焦于物联网数据安全、流通、共享等弊端，希望通过分布式账本技术（DLT），在 5G 网络边缘建立领先的联盟区块链技术平台及 MEC 资源管理平台，实现任意类型、任意规模的物联网设备互联互通。

SnapScale 采用云原生边缘架构，将云原生微服务管理能力延伸到边缘，并将云原生的生态和开发体验延伸到边缘，开发者可以在 SnapScale 区块链管理平台实现一键式的智能合约开发及部署。同时边缘计算在靠近用户和设备近端提供可靠、低时延的计算、存储和宽带服务。

为了提升区块链性能，SnapScale 采用混合双链治理结构和 FPGA 硬件加速装置，未来还将采用芯片级别的硬件加速装置，以软硬件合力来打破性能瓶颈，打造易用的高性能区块链平台。

2.2 设计原则

模块化

SnapScale 采用了模块化的设计原则，目的是为了降低程序复杂度，使程序设计、调试和维护等操作简单化。

解耦

区块链 3.0 时代的核心在于“解耦”，SnapScale 主链和子链的双向协作是功能解耦的有益尝试，我们也将继续探索不同功能层之间如何解耦。

兼容性

SnapScale 基本模块的设计遵循了兼容性原则，使得不同的应用开发者能够快速而方便地进行集成。例如，使用通用的数据传输标准，账户系统的设计可以满足绝大部分场景的需求等。

可插拔

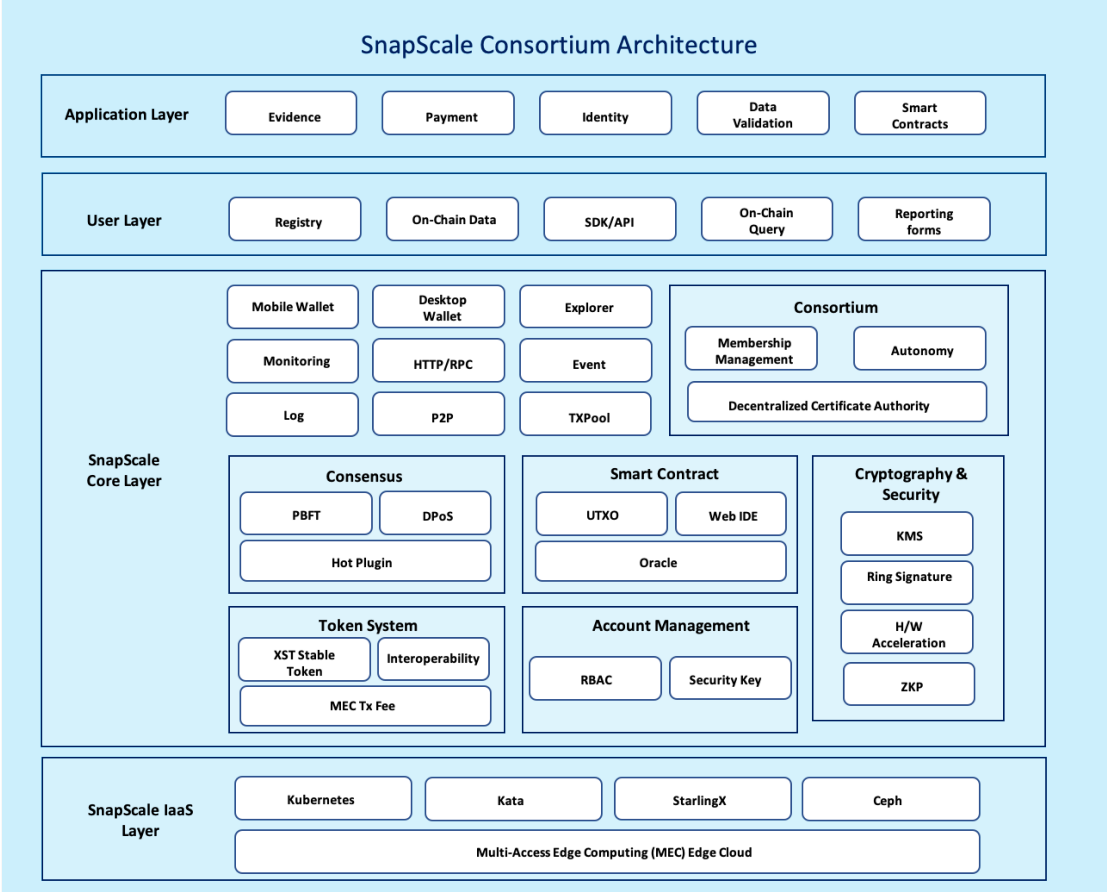
插件是可独立开发的程序模块，它能够动态地插入到系统中，并且可以被自由地删除和替换。因此它能够提高软件开发的并行性和开发效率，降低设计开发难度，缩短开发周期，增强应用程序的可运行性、可测试性和可维护性。

安全与性能相结合

区块链的系统设计应该遵循安全以第一的原则，SnapScale 在保证安全性的基础上，有效提升了扩展性，可以满足海量物联网设备数据的处理要求。

3 技术架构

SnapScale 可信联盟链体系架构由应用层、用户层、区块链核心层和区块链基础设施层架构组成。如下图：



3.1 DPOS+Pipelined BFT 共识机制

SnapScale 目前采用 **DPOS+Pipelined BFT** 共识机制。

DPoS 共识 - 如何成为出块节点

DPoS（Delegated Proof of Stake）是权益委托证明机制。相比于比特币的 PoW 机制，DPoS 不用浪费算力资源争夺记账权，而是通过赋予通证持有人投票权，SnapScale 将投

票选出 21 个“超级节点”来担任记账人（Block Producer：区块生产者简称 BP）的角色，保证整个网络的正常运行。

出块机制

SnapScale 每 0.5 秒生产一个区块。超级节点轮流出块，每轮每个超级节点连续出 12 个块，以 21*12 个区块为一个周期。在每个出块周期开始时，21 个区块生产者会被投票选出。同时，为了防止因网络延迟而使超级节点漏掉区块，SnapScale 采用确定的出块顺序，通信时延低的超级节点互为邻居出块者。

Pipelined BFT - 如何进行区块确认

Pipelined BFT（Pipelined Byzantine Fault Tolerance）是基于流水线的拜占庭容错机制。常规的 PBFT（Practical Byzantine Fault Tolerance）都是生产一个区块，等待共识，然后再生产一个区块。因而共识需要比较长的时间，没法满足 0.5s 出块的需求。

SnapScale 采取了不同的实现方式，出块和共识是可以流水并行工作的，区块生产完成后，不等待 PBFT 共识，继续生产同时参与并处理上一个区块的 PBFT 共识，当 PBFT 共识完成后即修改为不可逆状态。

惩罚机制

任何时刻，只有一个生产者被授权产生区块。如果在某个时间内没有成功出块，则跳过该块。如果出块者错过了一个块，并且在最近 24 小时内没有产生任何块，则这个出块者将被删除。这确保了网络的顺利运行。

会不会分叉

在正常情况下，DPOS 区块链不会经历分叉，因为区块生产者是合作生产区块而不是竞争关系。如果有区块分叉，共识将自动切换到最长的链条。具有更多生产者的区块链长度将比具有较少生产者的区块链增长速度更快。此外，应该没有区块生产者会同时在两个区块链分叉上生产块。如果一个区块生产者被发现这么做了，就可能被投票出局。

3.2 智能合约

智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。SnapScale 智能合约是用 C++ 语言开发的，目前支持调用的 API 接口有以下几种类型：

- Account API，查询账户数据的 API；
- Chain API，查询链内部状态的 API；
- Database API，存储和检索区块链的数据 API；
- Math API，定义常用的数学函数；
- Action API，定义用于查询操作属性的 API；
- Memory API，定义常用的记忆功能；

- Console API，使应用程序能够记录/打印文本消息；
- System API，定义用于与系统级内部函数进行交互的 API；
- Token API，定义用于与标准兼容的令牌消息和数据库表进行交互的 ABI；
- Transaction API，定义用于发送事务和内联消息的 API；

3.3 UTXO 交易模型

UTXO 的全称是 Unspent Transaction Output （未消费的交易输出）。这个概念首先在比特币中使用，一个钱包的余额，是追踪所有可花费的 UTXO，把它们加起来的总和。在交易时，支出方钱包花出去多个 UTXO，系统将生成新的 UTXO 到收取方钱包，如果收取方要“找零”给支出方，新的找零 UTXO 也会生成并返回到支出方钱包。所有 UTXO 显示的额度都是固定的，无法改变，用户不能只花一部分 UTXO，而是要全部花出去。

SnapScale 的交易模型同时支持账户余额模型与 UTXO 模型，不仅相同模型间可以相互转账，且支持两种交易模型间的相互转账，这也是匿名交易模型的基础。

3.4 匿名交易模型

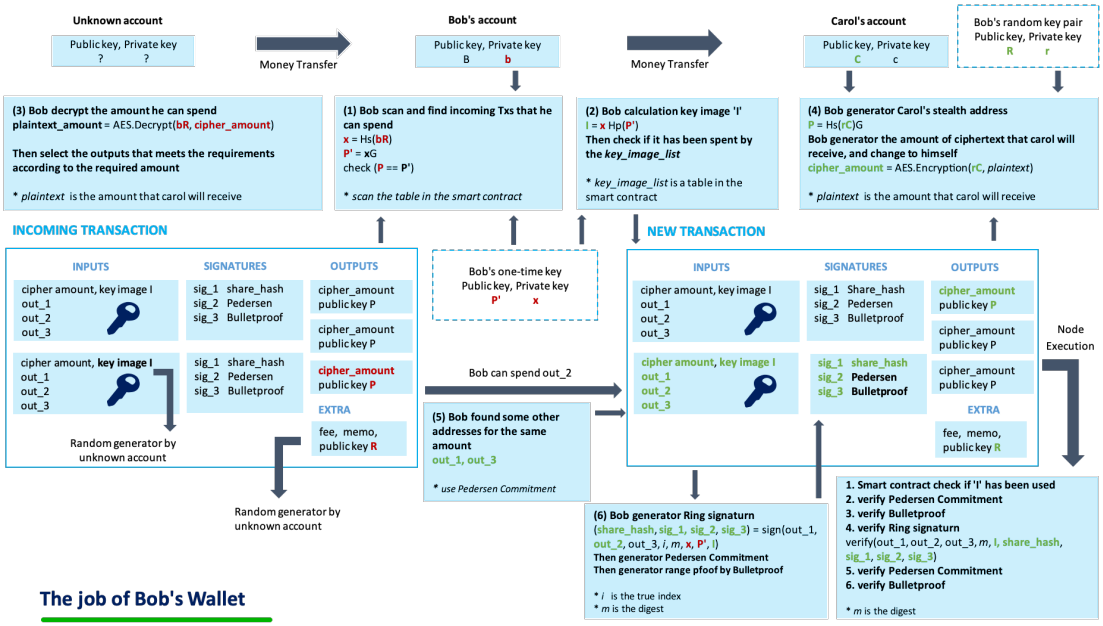
SnapScale 采用 UTXO 模式 + 环签名机制来实现匿名交易，将交易发送方、接收方和金额完全隐匿，无法追踪，且同时支持透明交易与匿名交易两种模式， 即 4 种交易方向:

交易发送方	交易接收方	交易金额	匿名程度
账户	账户	可见	透明交易
账户	地址	可见	接收方不可见
地址	地址	不可见	完全匿名交易
地址	账户	可追踪	发送方不可见

环签名解决的问题是，我对你说了一句话，但是你只知道是某一群人中有人对你说了这句话，而不知道这群人里具体哪个人说的，适用于签名方的计算能力较弱的情况。

SnapScale 还采用 Key Image 解决交易双花问题以及零知识证明解决交易金额隐匿后的范围证明问题。

下图是发送方 Bob 发送交易给接收方 Carol，Bob 使用密码学工具产生交易所需数据的过程:



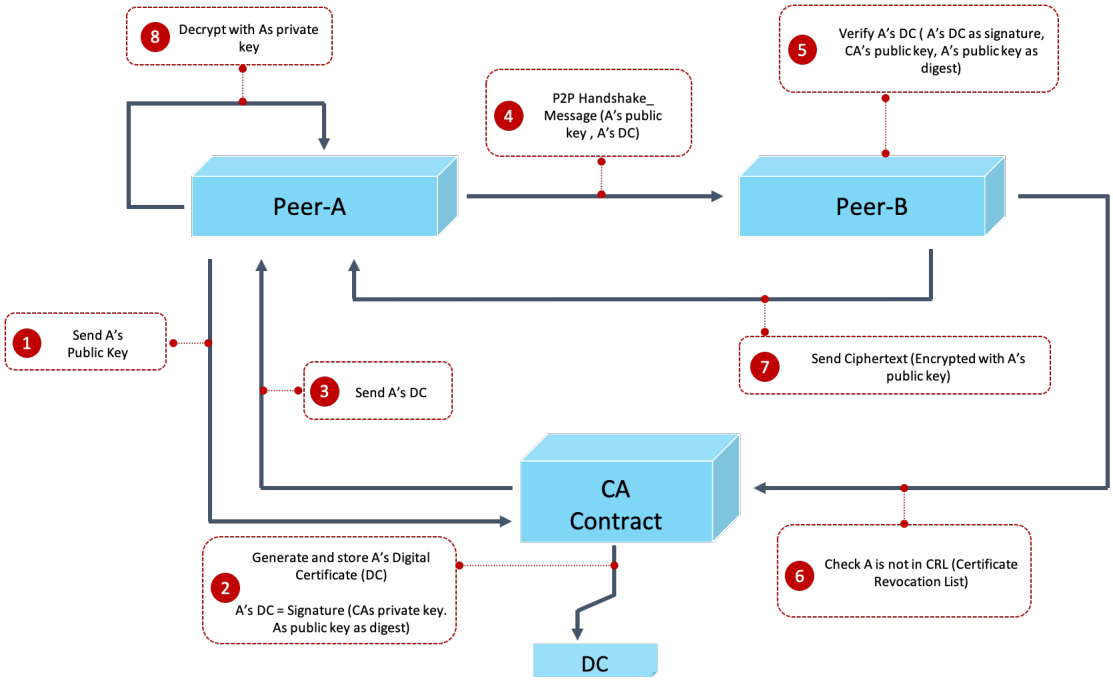
匿名交易相关的密码学算法:

- 将交易发起者隐匿: Borromean Ring Signature, Key Image
- 将交易接收者隐匿: ECDH, Stealth Address
- 将交易金额隐匿: ECDH, Pedersen Commitment, Bulletproofs(ZKP)

3.5 联盟模型

加入 SnapScale 联盟链的计算机节点和用户都必须要经过注册并获得 CA 颁发的证书，才能在联盟链中进行相关操作。

3.5.1 节点如何加入联盟



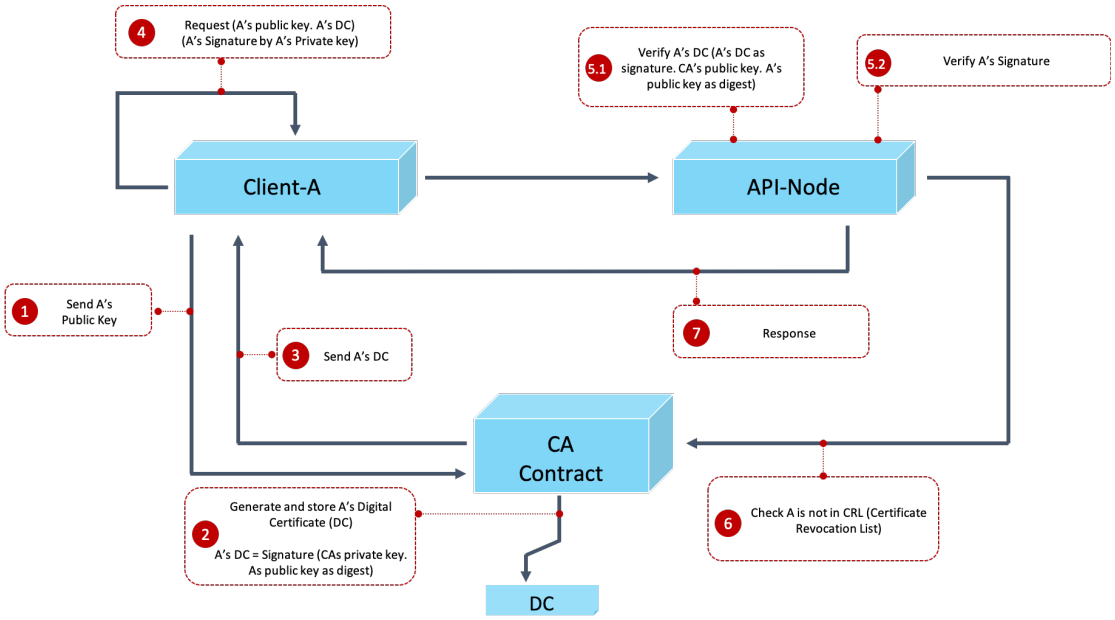
流程介绍:

某个组织 A 想要增开一个 Node

- 没有平台账号的话，得先注册平台账号；
- 组织 A 需要准备一组联盟用的密钥对，分为公钥和私钥（自己保管好）；
  - 注册账号时同时生成
  - 或者导入现有的一套

1. A 向 CA（certification authority）提出加盟申请 (提交申请信息：主要是 A 的联盟公钥)；
2. CA 处理申请请求，同意的话，为 A 的公钥生成 Digital Certificate（DC）；
3. 管理部门 CA 发送 A 的数字证明 DC；
4. A 配置 CA 的公钥,A 的公钥, A 的私钥, A 的 DC 和已知一个（或多个）联盟内节点(PeerB）的 IP, 开启自己的节点 PeerA 尝试与之建立链接；
5. PeerB 检验 PeerA 的数字证书；
6. PeerB 查看 PeerA 是否不在 CRL（Certificate Revocation List）名单内；
7. PeerA 与 PeerB 成功连接后,使用加密通道交互数据；

3.5.2 客户端如何访问联盟



流程介绍:

客户端 A 使用钱包生成公私钥对（Key Pair）

1. 客户端 A 将生成的公钥发送给证书管理部门 CA，提出加盟申请；
2. 管理部门 CA 对信息进行初步审核，审核通过则为 A 的公钥生成 Digital Certificate（DC）；
3. 管理部门 CA 发送 A 的数字证明 DC；
4. A 使用 A 的公钥、A 的私钥、A 的 DC 和要访问的联盟内 API 节点的公钥，产生 Http header token，发起 request；
5. API 节点检验；

a. API 节点检验 A 的数字证书

b. API 节点检验 A 的签名信息

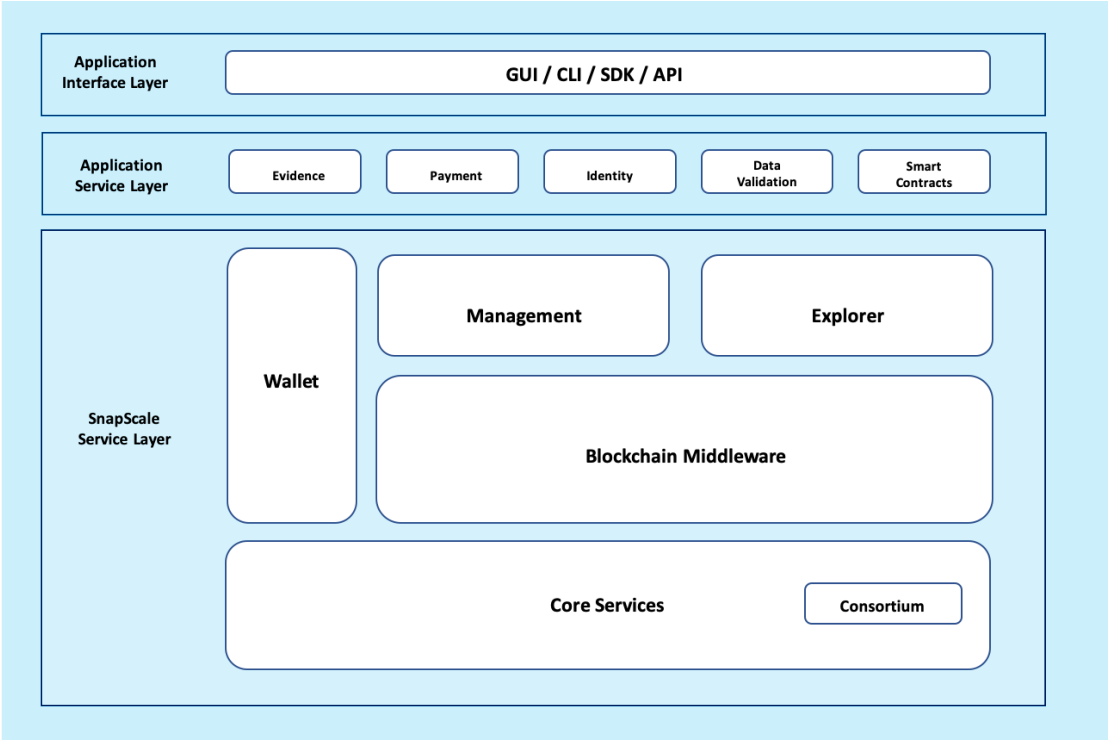
6. API 节点查看 A 是否不在 CRL（Certificate Revocation List）名单内；
7. API 节点响应 A 的请求；

3.6 计费（奖励）模型

SnapScale 基于配置和事务的计费方式可以灵活多变，具体根据每个事务所消耗的链上资源（CPU、MEM、NET）进行计费。每笔交易费分为两部分，一部分为作为对边缘节点的奖励，另一部分作为对出块节点的奖励。初步的计费模型将在下一版本的白皮书中展示。

4 产品模块架构

SnapScale 产品模块由 SnapScale 服务层、区块链应用层和区块链接口层组成。其中服务层包括：核心服务（分布式账本、共识机制、加密和授权技术、智能合约）、钱包、浏览器、区块链中间件和区块链管理平台；应用层产品包括凭证服务，支付服务和身份验证服务等；接口层针对不同的用户提供各种接口，如 GUI、CLI、SDK、API 等。



4.1 SnapScale 服务层

4.1.1 核心服务

分布式账本

区块链的本质是一个去中心化的分布式账本，账本由联盟的节点共同维护，且每一个节点记录的都是完整的账目，有益于节点之间的相互监督，保证数据不可篡改以及使用的合法性。

共识机制

共识机制是区块链节点就区块信息达成全网一致共识的机制，共识机制可以保证最新区块被准确添加至区块链、节点存储的区块链信息一致，并可以抵御相当规模的恶意攻击。

加密和授权技术

存储在区块链上的部分交易信息是公开的，但是账户身份信息是高度加密的，数据使用者只有在获得数据拥有者授权之后才能进行数据调用或查验，从而保证了数据安全和个人隐私。

智能合约

基于这些可信的不可篡改的数据，可以自动化的执行一些预先定义好的规则和条款。

4.1.2 钱包

钱包是用户管理密钥和数字资产（通证）的工具，用户将使用通证获取 SnapScale 生态中的服务。钱包中包含成对的私钥和公钥，用户用私钥来签名交易，从而证明该用户拥有交易的输出权；公钥则用来验证交易的签名，一个私钥签名的数据，只有对应的公钥才能对其进行验证。

4.1.3 浏览器

个人用户、企业用户、移动网络运营商、Hyperscale 云服务商等利益相关方可以使用区块链浏览器查询记录在区块中的交易信息，这些区块信息包括：ChainInfo、BlockInfo、TransactionInfo 、ContractInfo 等。物联网设备发生的每一笔交易（在获得授权的前提下）都可以在浏览器进行查询，实现了交易数据透明、可追踪。

4.1.4 区块链中间件

区块链中间件包含如下几点功能：

- 与区块链核心服务交互更便利；
- 访问区块链核心服务更安全；
- 提供更多维度的区块链统计信息；

4.1.5 区块链管理平台

SnapScale 提供一键式区块链管理部署平台，开发者无需进行进行复杂的开发环境配置，即可一键进行智能合约的开发、部署、测试和源码调试等操作，极大提高了开发效率。

SnapScale 支持联盟链的开发和部署。移动网络运营商、云服务商可以作为节点加入联盟链网络，整个网络由成员机构共同维护，其他节点（如企业）必须经过授权后才能加入。更多的联盟链管理架构和细则将会在下一个版本发布。

4.2 应用层

凭证服务

SnapScale 依托区块链的时间戳和哈希加密技术，可提供数据以及文件的凭证服务。数据或文件一经上链，就会生成一个特定的“数字指纹”记录在区块链上，且永久不可篡改。区块链凭证系统可监控电子数据的全生命周期，适用于司法存证、电子凭证、溯源等应用场景。

支付服务

SnapScale 将为智能设备之间的数据交易和共享提供一套基于区块链的可靠、安全、互操作的支付系统。该支付系统采用友好、灵活的计费标准，同时 SnapScale 高性能、高可靠、高安全的平台特性，可以支持海量物联网设备的高并发快速交易。

身份验证服务

接入 SnapScale 的智能物联网设备将通过分布式身份标识与可验证声明，实现去中心化的身份管理。数字签名和零知识证明等密码学技术，可以进一步保障用户隐私不受侵犯，使用户真正掌握数据所有权。

4.3 接口层

通过接口层可获得 SnapScale 相关的所有功能，开发者或应用系统仅需调用相关接口即可搭建区块链应用，无需关心复杂的区块链技术实现过程。

结语

SnapScale 致力于在网络边缘探索“5G+ 分布式账本（DLT）”的无限潜能，与运营商和 Hyperscale 云服务商一起打造新的物联网生态。

SnapScale 利用分布式账本技术（DLT）和协议在移动网络边缘为运营商打造高性能、高扩展的联盟区块链平台，其标准化的架构和接口集合让边缘基础设施运营商在为 IoT 设备提供数据流通、交易和共享服务的同时，确保分布式数据系统的安全性和扩展性。SnapScale 将在网络边缘催生大量分布式应用程序（DApps），从而振兴 IoT 社区，并为运营商和云服务商开拓收入来源，5G 网络技术也会随着新的服务和应用而逐步完善。预计到 2025 年，会有超过 70％的应用程序在移动网络边缘进行处理和执行。移动网络运营商正加快在 MEC 平台向开发者提供 API 服务接口，以部署更多的分布式应用程序（如人工智能、机器学习、游戏、虚拟现实、工业、医疗保健等应用），并基于 SnapScale 分布式账本获得收益。

访问 SnapScale 基金会网站获得更多详细信息：
https://snapscale.org/