合链科技
区块链产品技术白皮书

ECO
CHAIN
合链

目录

序言

本白皮书主要内容在于介绍合链区块链服务 BAAS 平台的系统架构、核心设计理念以及相关的产品技术与特色。北京合链共赢科技公司（简称 合链科技）以“推动科技发展，成就社会进步”为使命，致力于打造基于区块链技术的商业生态体系。合链科技核心团队都来自于世界 500 强高科技企业，自 2014 年开始即从事区块链技术及应用的研究，目前已经开发出高性能、高可扩展性、高可控的区块链底层技术产品，同时团队具备多行业的业务分析能力，并能够基于区块链底层快速构建上层应用系统以满足多样化的商用业务场景。

业务定位：打造基于区块链技术的商业生态体系

区块链的发展

有非常多的朋友是透过“比特币”这个数字货币接触到区块链这个名词。通过“比特币”在市场上广为人知，使得越来越多人开始关注到区块链技术。之后区块链技术又产生了很多虚拟货币，比如“以太币（Ethercoin）”、“莱特币（Litecoin）”、“瑞波币（Ripple）”等等。借助开源软件，开启了全世界区块链技术应用的大门，让各类应用场景可以快速的借助开源代码，引入区块链技术，

进行深入的应用开发。

上述开放数字货币的底层区块链技术，后来被发现不适用于某些特定的应用场景。至此，区块链技术开始有了变化。从原本的公开的使用环境<公有链>，慢慢的开始转化成特定的应用场景<联盟链>，或者成为一个封闭式的环境<私有链>。但不管如何，这些都只是围绕着区块链的核心概念所延伸出的“应用进化”。本质上并没有太大的区别，只是在其区块链技术架构中，在不同层级的架构中做了不同的处理罢了，在后续的内容中我们会一一做更深入的介绍。

承上，为了满足市场上不同应用场景的需求，有更多的技术开发者纷纷投入到区块链技术的开发领域，进行区块链技术的研究与开发。合链科技的使命是“以信息技术为核心，致力打造区块链生态体系，成为区块链技术领先的开拓者”。我们将在本文中介绍和分享合链科技的区块链技术，以及区块链技术在各类场景的应用和解决方案。我抛砖引玉，让各种不同的业务场景能应用区块链技术，一起打造更为多元丰富的区块链生态体系。

甚么是区块链？

区块链技术本身并不是一个单一的技术名称，更多的应该称为一个技术的架构，当中采用了各种不同的技术，在其核心概念之上结合多种的业务逻辑综合而成的一项技术应用。

区块链的核心理念如下：

- 去中心化(Decentralization)
- 分布式帐本技术（DLT, Distributed Ledger Technology）
- 数据不可被窜改与可溯源性
- 对等网络（P2P）

同时在技术的引用上，一开始的区块链网络主要的技术组合为：

- 条件式的 hash 函数
- 公私钥加密机制
- 共识算法

在区块链核心理念的基础下，区块链技术和商业应用不断的演进，导致技术组合不断的演变。从一开始的 PKC 到 PKI、各类的投票机制，智能合约的应用、各种不同的共识算法，使得区块链技术随着需求而不断的进化。所以，“什么是区块链”这个问题的答案很难一言以蔽之。

我们尝试着为区块链做一个简单的定义：互联网提供了信息的传递与连结，物联网解决的人与物的连结，而区块链网络将解决“价值与信任”的传递与流动，让互联网与物联网上的人、事、物都可以在协定的信任基础上进行各种具有价值的资产流动与转移。

区块链的价值

从技术角度出发，区块链带来的技术价值将会改变现有互联网的底层协议，可以更有效解决因为信用所产生的风险藉此保证交易安全。因此区块链就是要在互联网中创造一种特殊的交易机制，在交易对象彼此不能够互相信任的前提下，依然可以进行有价资产的交易活动，从交易的根本上改变现代市场的交易信用体系，让价值可以透过区块链网络中进行最大化的流动，并且透过点对点网络与加密机制传递，真正实现从传统互联网到价值互联网的转变。

区块链的架构

先前我们提到，区块链技术更象是一个采用了不同的技术综合而成的技术架构。在广义的区块链技术架构中，可以粗分为三个层次：

协议层：

在这一个层次当中，代表着区块链核心的内容。也就是目前市场上所泛称的底层技术。里面包含了数据存储的结构、共识算法、加密机制、网络通讯协议等等。这一切的内容都被包覆到这层当作进行运作，并且以 API 或者服务的形式提供上层调用。

扩展层：

扩展层比较象是传统 MVC 架构中的 V 层，处理部分业务逻辑。智能合约就是建构在这个层上的。因此在这个层，我们可以通过智能合约将区块链技术延伸到各种不同的场景中，例如 AI 人工智能、VR/AR、物联网<IOT>、ERP/MES、大数据<Bigdata>、云平台<Cloud>，都可以在这里进行实现。

应用层：

应用层面向最终用户。对于有接触过虚拟货币的人来说，各种不同的“电子钱包”就属于这个层。不过在实际应用中，由于区块链技术本身的限制。应用层的开发除了要面对使用者的需求之外，同时也要兼顾扩展层与协议层的逻辑与技术要求。这导致一个区块链开发项目，将会需要更为复杂的团队协作。

从以上的架构可以发现，区块链技术在每一个架构层当中都可能是不同的编程语言与各自独立的运算逻辑。同时要配合业务自身的加密算法要求等等，这会形成一个复杂的协作过程。在其背后更是需要完整的业务逻辑，才能迎合市场的真实需求。

合链区块链平台企业服务架构

为了有效的协助企业进行区块链 BAAS 平台的导入，合链科技提供完整的企业区块链平台架构模型。在这个模型中明确定义了从区块链技术在企业整体发展的过程中，从战略到具体落地实施区的架构维度与实施路径，

在整个服务的搭建上，我们分做五个阶层来进行整个合链区块链BASS平台的搭建。

- 战略层：基于企业发展所需的区块链平台目标与对应的目标用户需求。
- 范围层：具体的功能规格与内容需要
- 结构层：整体的系统设计与信息的架构，满足各类型信息技术结构
- 框架层：在统一的信息传递基础上进行界面设计与各类型的功能与场景服务设计
- 表现层：功能与服务的设计与展现

延伸数字资产生命周期

为了保护数字资产的价值流动性，在合链区块链BAAS平台中，延伸数字资产生命周期是一个非常重要的核心概念。因此在整个合链区块链BAAS平台中，我们将数字资产的生命周期做了一个新的拆分和定义。

第一阶段：采集

在这个阶段当中，数字资产在经历过一连串传统的拆分与定义<如ABS资产证券化>之后，我们将重新进行数字编码/转码，重新赋予标签<Met-Tag>，透过各类型的代理机制<Proxies>重新进行对数字资产存储<Store>与加密<Encrypt>。为之后数字资产在区块链上平台进行流通移转时做第一阶段的准备。

第二阶段：管理

为了满足现有区块链技术无法进行高效交易的弊病，这个阶段我们对数字资产进行管理。建立元数据<Metadata>、相关的视图<View>，并且强化数据接入管理<Access control>、引入工作流<Workflow>、数字版权管理<DRM>等机制，强化与资产拥有者。加大企业在原始数字资产上的管理强度。使数字资产的发行可以被有效管控。

第三阶段：发布

本阶段将数字资产在区块链平台上进行发布和资产移转。先前两个步骤，该数字资产的元信息已经进入的一个安全的存储空间<Store>中。因此，在发布时，这些元信息会随同数字资产本身进入到区块链环境中进行转移<此时这些信息将会分门别类的各自存放到区块链上合适的位置>。抵达被移转对象后，会回到第一个阶段进行数字资产重新采集的流程，整个流程将不断的循环下去。

这样，我们会发现原先的数字资产已经在实质意义上被重新被定义拥有者和拥有权。

数字资产交易平台架构

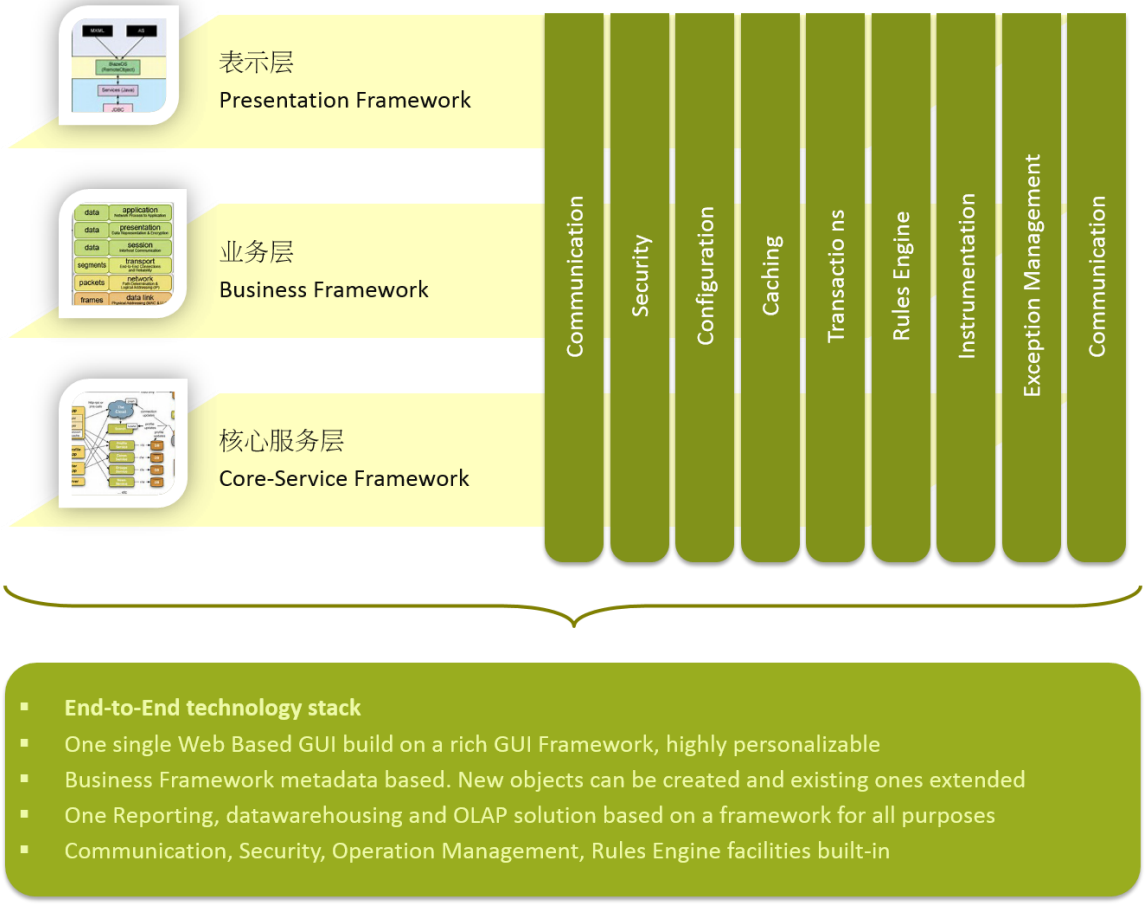
1. 数字资产在线采集并且进行初始管理同时便会进入合链区块链 BAAS 平台网络中，数字资产交易元数据便会透过区块链路由加密之后存放到一个数据库之中等待被调用。

2. 当数字资产交易发生时，数字资产本身与相对应的元数据便会透过合链区块链 BAAS 平台网络开始进行交易，此时整个交易会交由区块链平台当中的交易管理层进行统一的管理，并且在各节点的核心账本上进行记账动作。

3. 在不同的场景下，当数字资产进行交易时，整个交易行为也会一并的透过合链区块链 BAAS 平台路由，在数据安全的情况下调用相对应的交易数据，与特定的对象进行数据交换，达到与非区块链平台上数据库的数据同步作业。

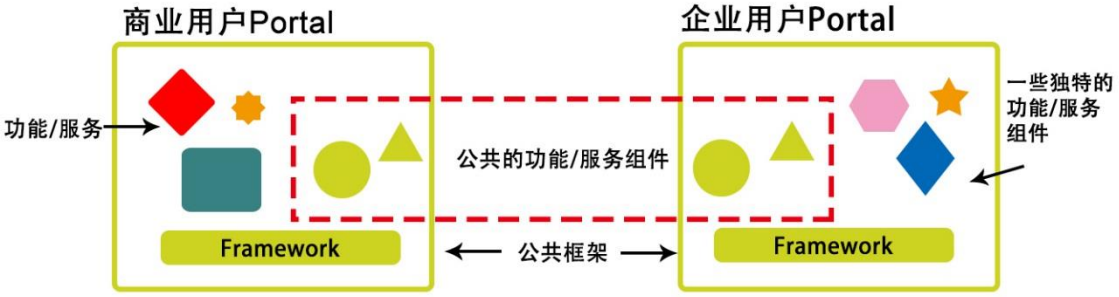
合链区块链 BAAS 平台架构

合链科技区块链 BAAS 平台的架构图：



- **表示层< Presentation Framework>：**

  为了有效提供优质的使用者体验，在公共框架<Framework>下我们重新定义了功能/服务，在这样的框架下使用了标准的设计原则，达到”即插即用”的目的性。让不同的用户体验到不同的服务。



在表示层的逻辑设计中，我们将认证、授权、Profile、管理等用户相关组件进行重新设计，抽象成公共服务组件，且对外提供标准的 restful 接口。例如用户 Profile 可结合外部 UPS/UGS<User Prolfie/Group Service>进行扩容整合，以及授权组件可以透过外部的安全系统进行功能的强化。对接 lldp，或者 OAuth2 等标准协议，也可以对接微信支付宝认证等等。

以下是核心的概念：

- 公共框架服务<Framework Service>

  公共框架服务于表示层中主要的目的有三：

  1. 提供所有面向客户端应用的服务
  2. 一次构建成型（基于容器统一封装），降低开发与部署的风险
  3. 功能与服务可复用，无须重新开发

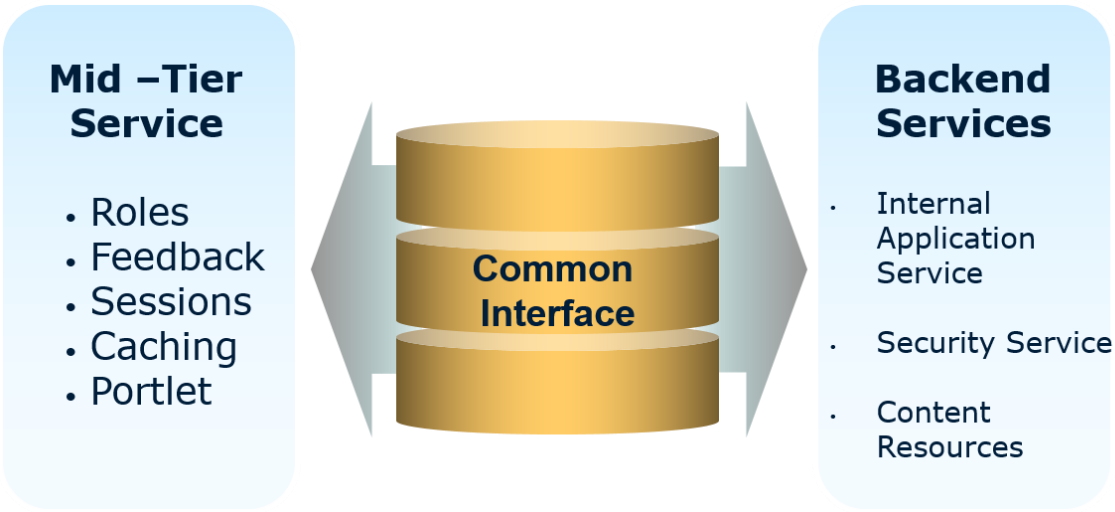
- 功能服务<Feature Service>

  功能服务于表示层中的角色即是在特定的应用当中所需要的功能，不过在这里所提的功能服务更多的是一个功能集合的概念。

  一个不同编程语言的功能服务透过 WSRP 或者 SOAP，grpc，thrift 等等协议来进行沟通。在实际应用场景上可能会因为不同的系统而面向不同的编程语言所构建的环境。因此功能服务的目的在于以下几点：

1. 注重客户原先的系统价值
2. 只开发需要的框架，而不是重新搭建
3. 使用标准方式构建<如.Net WSRP、J2EE Portlet (JSR168 / JSR286)、WPAP Framework、GPRC Thrift 等等...>
4. 快速开发、快速部署 （基于容器）

- 公共接口<Common Interface>



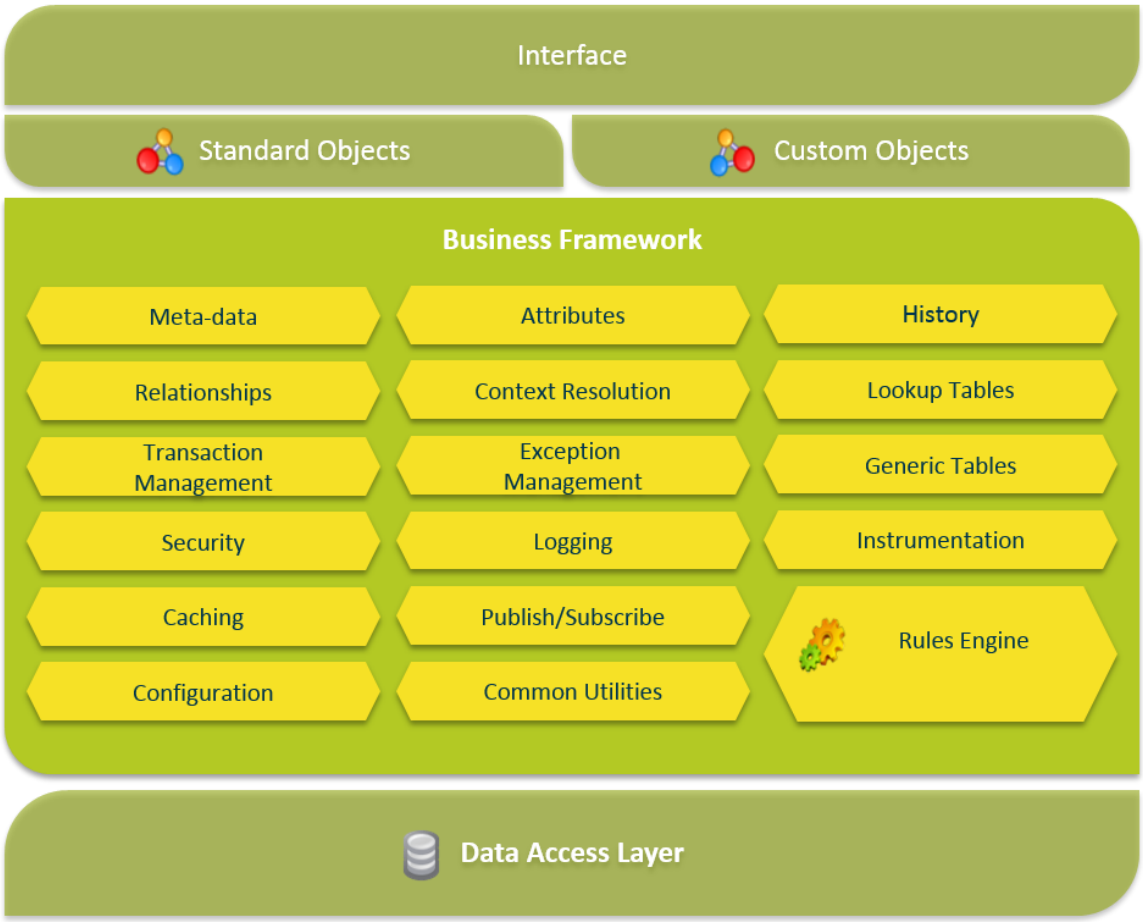
如上图，我们可以看见一个架构在公共框架服务之上的功能服务集合，在其中的每一个功能项我们会设计一个公共接口来与其他的应用服务进行对接。在维持每一个系统对于其功能服务的所有权的情况下，我们透过公共接口来进行对接。其具备以下几点特色：

1. 可复用的接口设计（restful）
2. 允许即插即用
3. 更快速的开发

有了这样的结构，我们可以更快速的将复杂的应用透过这样的接口进行沟通与对接，大大提高开发实施的效率。

在上述模型上我们配合实际的应用场景，结合 Web、移动端等应用，进行定制化功能的组件开发，如此我们便可在表示层中进行敏捷且高效的应用开发。

- **业务层<Business Framework>：**



在业务层当中存放了由展示层采集回来的数字资产交易的元数据，同时也存放了所有的业务逻辑。在数据与资产尚未进入到区块中进行流动时，业务层便会依照其属性进行一系列的编码、拆分、排序、加密和存放管理。

业务层也支持 Data Mining 与 OLAP，有助于开发者进行复杂的业务集程操作与分析模型。同时也提供相对应的报表<Report>与仪表板<Dashboard>。同时也提供企业级的 ETL 平台，用于建立数据仓库<DW>的高性能数据集成解决方案。

这一系列的商业组件会针对特定的业务逻辑<如智能合约 Smart Contact 提供特定的功能>，执行相关的工作流程，这一层的引入可以满足数据的实时处理和实时的区块链交易。以下是依照个组件的层次结构介绍：

- 基础组件<Base>：

  包括一些来自其他组件<Object>对象的所有基类<Class>，提供常见的广泛属性<Common Wide Properties>、方法<Methods>与元数据<Metadata>。

- 核心组件<Core>：

  这部分包含数字资产与商业规则规则本身之延伸的相关的数据。如数字资产本身的数据、索引、交易流程与历史、版本历史、属性、资产状态、风控模型等等...

- 订制组件<Customer>：

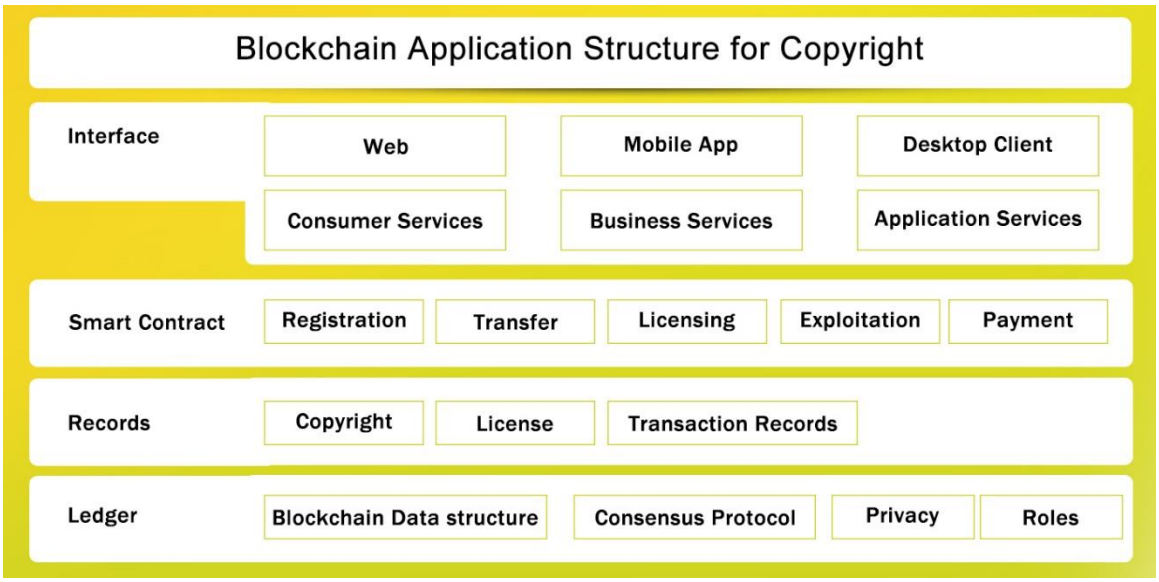
  为特殊逻辑提供一个附加的一层组件结构，以满足不同的特殊需求。

业务层将会进行一系列的商务数据与逻辑处理，并且在这个过程中协助形成智能合约来配合整个合链区块链 BAAS 平台的运行。

- 智能合约

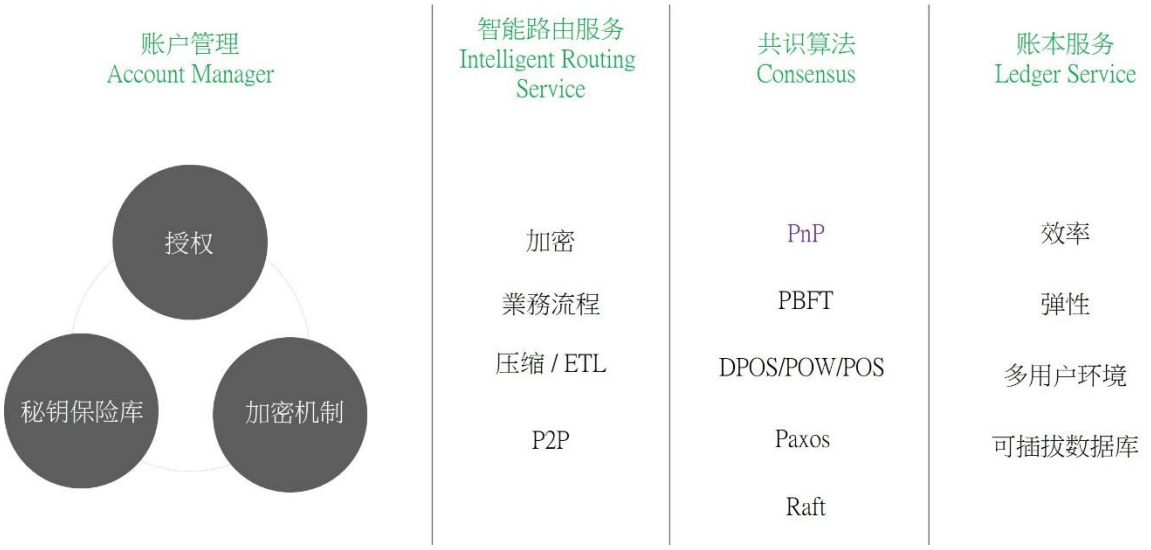
  智能合约一直是区块链平台进行交易最重要的一个要素。因此，其本身的可控性和安全性是区块链交易平台中最重要的环节。当我们进行智能合约的设计时，会先与这些业务组件中的数据和业务进行逻辑对比，确保其规则与条件均在适用范围内<重点是智能合约的内容是根据实际的业务逻辑和约束生成，而不单单由代码表示>。这阶段还只是商业流程分析师

或者交易分析师需要参与的环节。接下来在脚本代码的引入后，区块链平台系统会再一次的进行比对，确认交易与相关的规则是否符合业务组件中的数据规范<此时是一个系统行为>。如此一来便会以封闭式行为，进行智能合约的发行与应用。



在这个数字版权的范例里面我们就可以很清楚的看到，智能合约里所需要的几个讯息，而这个讯息就是从业务层这边提取出来并且加以封装实现。而其下 Record 的相关信息也是一并的存放在业务层进行统一的管理。

- 核心层<Core-Service Framework >



在核心层当中，包含以下的功能组件：

- 账户管理<Account Manage>：

动态加密-在业务层中我们将用户数据进行了一次处理，让相关的元数据进行了编码加密的处理。并且将对应的公私钥进行了保存。在核心服务层中，引入了”状态<Status>”的概念，让交易发生时，需要引用户账户信息时，授权服务会将此用户账号变更为待确认，同时调用业务层的公私钥与核心服务层中的”保险箱”公私钥进行交叉比对。如果确认无误，便会进入区块进行合约所约定的交易行为。当交易完成后，该用户于核心服务层中的信息便会重新再次加密，重新放入新的保险箱当中存放，让整个授权行为变得更安全。

比例原则秘钥保险库-在实务上当区块链网络节点多的时候，各节点上存放私钥的保险库便会增加被攻击的风险。因此在特定的场景与智能合约的约束下，将一定比例的密钥保险库布放在特定节点上，而非全部节点

都存放私钥保险库，保证特殊交易场景的安全。。

多阶层帐户服务-传统的帐户管理系统有类似树状的结构，然而在以电子账号为主的区块链平台中，原先的子账户<Child Account>亦有可能为另一交易环境的主要帐户<Parent Account>。因此容易让原先的树状结构产生出死循环状态。所以在 Account manager 中提供了多阶层账户服务< Multi-level Account Service>，让每一个账户都能有多重的子账户，并且同时具备其独立性与可分割性。

- 智能路由服务<Intelligent Routing Service>：

  由于合链区块链 BAAS 平台特殊的架构，因此在核心服务层中我们可以将交易讯息从业务层进入核心服务层中打包成区块，同时透过智能合约的约束与链上引入业务层的工作流程与业务逻辑至链服务上，之后透过 ETL 机制让整个交易与信息流动可以在一定的条件要求下结合外部信息<通过压缩与加密机制,为了支持续传作业>与直接进入到节点据库与交易对象主体，

- 共识算法<Consensus>：

  共识算法决定了整个区块链网络交易的核心规则与效率。为了配合各种不同的应用场景与需求，在共识算法上我们将这个结构调整为可配置的功能模块，以配合市场各应用场景的主流算法，合链区块链 BAAS 平台共识算法模块特殊之处除了会结合业务层的业务流程与逻辑之外，同时也配合智能路由的功能动态的调整自身算法的结果，让整体交易效率可以大为提高。

- 账本服务<Ledger Service>：

  在区块链账本服务当中除了最基本各节点” 数据同步”之外，就是账本本身的”效率”与”弹性”。由于合链区块链 BAAS 平台采用多重服

务的分布式架构，因此在核心服务层的账本服务本身就变得非常优雅。除了主要的同步机制之外，更多的是关注在节点数据库本身的架构。当数据经由区块进入到对象节点时，经由智能合约等条件约束下开始进入数据库，同时会调用帐本服务接口以验证安全性，之后才能进行一系列与数据库交互的动作。此时还需要保证在数据写入当前节点数据库，也能够与其他外部的数据库进行同步作业<亦满足大型文档存放于外部服务器的场景>，除此之外也能够判断区块本身与共识计算后的状态来决定是否写入数据库。当然数据在进出数据库的同时也会调用该用户的密钥管理机制进行数据加解密。因此在核心服务层中形成一个死循环的流程作业。

而数据库本身的规划与设计当然也就会直接影响到数据的吞吐量是否能满足业务场景的需求以及区块链网络平台的效率。所以合链科技区块链BAAS平台的数据库架构除了可以结合主流云平台数据库之外，同时也引入采用了多用户环境、可插拔数据库、各类检索算法等等数据库技术，透过规则引擎与优化器，彻底强化数据库账本的稳定度与效能。

- 瞬捷<Agile>：

我们希望在区块链平台上提供交易服务的服务端都能透过区块链平台的价值提升自身的核心竞争力，因此我们提出瞬捷服务<Agile>的概念，目标如下：

- ✓ 不中断的网络服务
- ✓ 保护企业的营业资料
- ✓ 提高执行效率
- ✓ 扩展服务
- ✓ 加强数据交易稽核与维护

因此在瞬捷服务架构下，我们提供企业级的区块链数据交易管理平台，让服务端可以透过这样的平台在有条件的情况下进行区块链平台上的交易与相关状态。

其主要的特色如下：

- 强大的数据采集处理
  - ✓ 跨平台、多数据源的统一采集
  - ✓ 灵活、高效的自主采集与其他多种数据采集方式相结合
  - ✓ 丰富的采集接口，强大的扩展功能
  - ✓ 动态控制采集引擎的采集任务的执行

- 智能化数据处理
  - ✓ 精准、高效的告警信息过滤与压缩，提高运维人员的工作效率
  - ✓ 知识自学习功能，结合告警处理的工具，便于定位故障根源，以及进行影响性分析
  - ✓ 强大、稳定的告警处理引擎，支持大数据量的并发处理

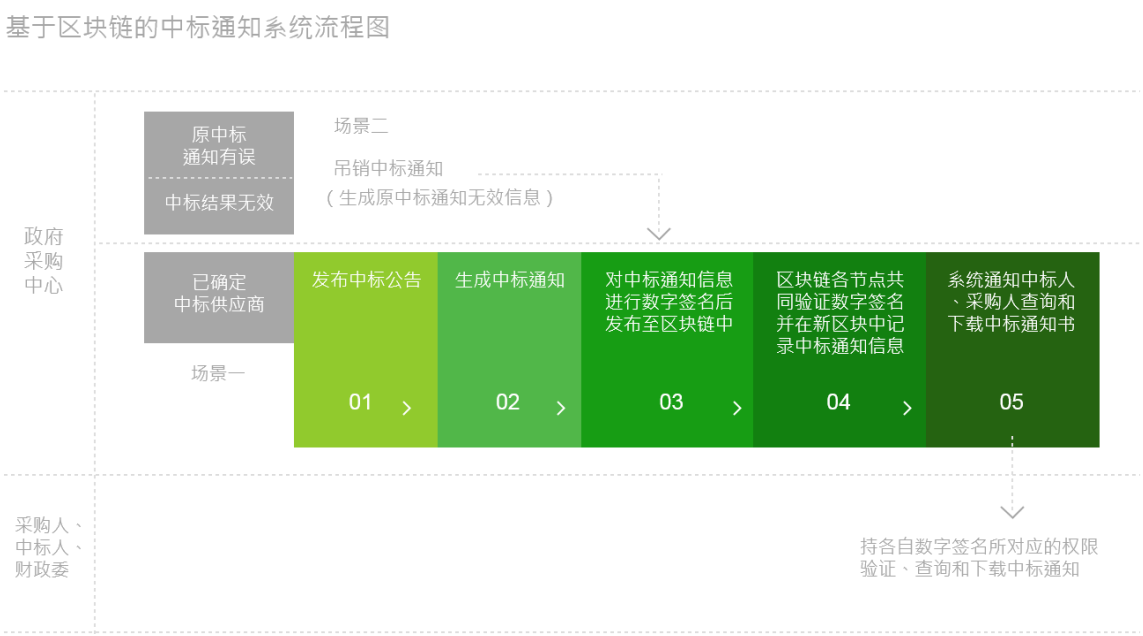
- 丰富的可视化展示
  - ✓ 统一、灵活、丰富的视图展示
  - ✓ 实时、精美的展示界面
  - ✓ 面向多重角色，从不同的纬度， 即时、准确的展现系统状态
  - ✓ 强大、灵活的报表功能

案例分享-公益项目

给公益项目涉及的利益相关方，建立各自独立的公益钱包账户，公益钱包中的资产以中间结算货币“XX 币”的形式体现，捐款人通过充值的方式购买“XX 币”，账户中资金的流转变动信息全部记录在区块链中以验证操作的合法性及记录的不可篡改性。当需要提现兑付时，公益钱包才发送指令给 XX 指定银行账户转账

到兑现人银行账户。

案例分享- 基于区块链的中标通知系统



- 场景一：

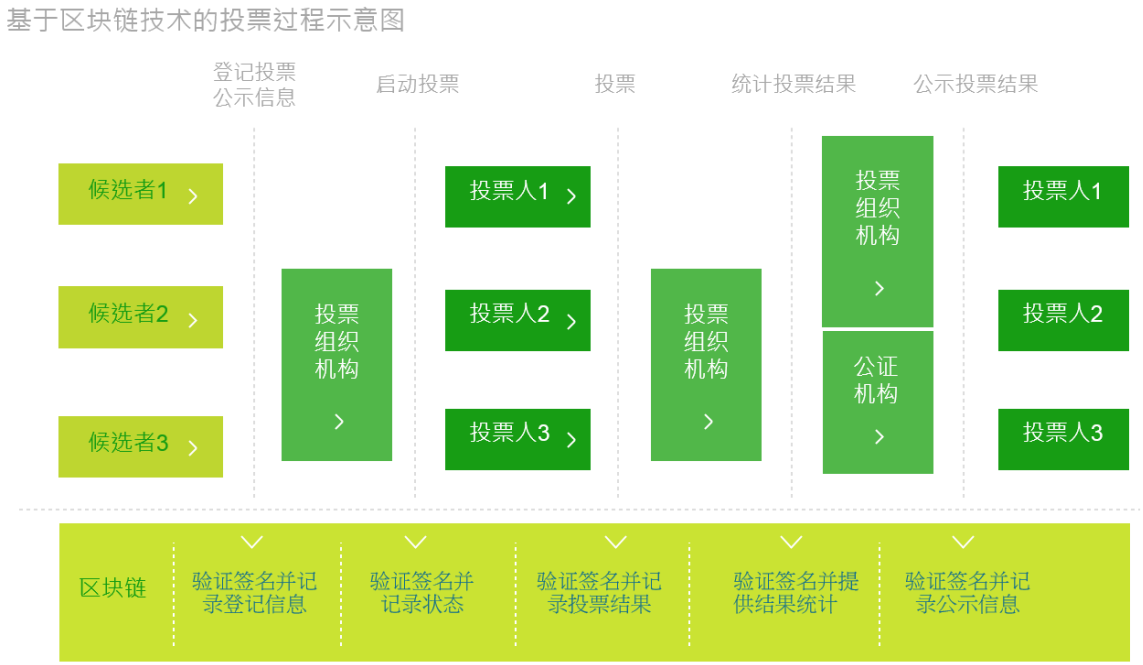
政府采购中心在中标系统中按模板录入中标通知，并通过U盾等数字签名手段确认后广播至区块链中，区块链中各参与节点验证数字签名有效性，验证通过后区块链基于共识算法确定记账节点，记账节点在新生成区块中加密记录本次中标通知信息，其他节点同步记账节点的新区块信息完成数据备份。中标系统在区块链完成数据记录后发送短信等通知至对应的中标人和采购人查询下载中标通知。中标人或采购人在系统发出查询或下载指令并通过U盾等数字签名手段确认后发布至区块链中，区块链各参与节点验证数字签名有效性，验证通过后基于对应的公钥解析并返回中标通知信息至中标系统，此时可以进行针对性的查询和下载。

- 场景二：

政府采购中心在中标系统中将原中标通知状态从有效设置为无效，并通过U盾等数字签名手段确认后广播至区块链中，区块链中各参与节点验

证数字签名有效性，验证通过后区块链基于共识算法确定记账节点，记账节点在新生成区块中加密记录本次中标通知信息，其他节点同步记账节点的新区块信息完成数据备份。中标系统在区块链完成数据记录后发送短信等通知至对应的中标人和采购人查询下载中标通知。中标人或采购人在系统发出查询或下载指令并通过U盾等数字签名手段确认后发布至区块链中，区块链各参与节点验证数字签名有效性，验证通过后基于对应的公钥解析并返回无效通知信息至中标系统，此时可以进行针对性的查询和下载。

案例分享- 投票系统



案例分享- IOT 與设备接入

IOT 设备整合控制优化方案