『宝链生态』区块链技术实践白皮书

打造数字经济时代艺术品收藏平台信任基石

前言

文物艺术品具备市场基础和价值认定共识，本应成为不亚于房产、证券、能源投资的巨大市场。但由于缺乏公正鉴定、估值定价中心化、高仿赝品多、流通效率低等问题，一直低效运行。

传统文物艺术品交易渠道的租金费用率在 30%以上，拍卖渠道手续费在 25%以上，交易成本高达 50-90%。除此以外，文物艺术品单笔金额巨大且无法进行拆分式交易或投资，苛刻的交易门槛已经脱离了人民群众，导致也难以被流通。

文物艺术品原本有机会成为类似房产、证券、能源、黄金的硬通货，但由于高昂的交易成本、苛刻的交易门槛，现在沦落为小众参与的游戏。如果能够降低文物艺术品的交易门槛，降低交易成本并提高流动性，文物艺术品将成为比肩房地产的巨大市场，成为家庭财富和企业资产配置的重要组成部分。

由于流动性的差距，A 股主板的总市值为 50 万亿，为新三板 5 万亿市值的 10 倍以上，当下文物艺术品规模在 2 万亿人民币，如果能够通过区块链实现文物艺术品的数字化，未来的市场空间有望比肩 20 万亿人民币。

宝链（Treasure Chain）是由文物艺术品产业资深践行者创建的，面向文物艺术品产业的自主区块链底层和资产交易平台，以及由此构建的分布式经济生态。区块链与文物艺术品的结合 ,将帮助文物艺术品行业解决信息不对称和流通效率低这两大关键问题。

运用区块链技术，能有效解决中介信用问题，为艺术品防伪和防欺诈提供了新的渠

道，为文物艺术品行业树立了新的规矩。让每一件文物艺术品的重要信息（包括文物艺术品的重要属性、权威鉴定评估机构信息、鉴定时间、交易记录、证书数据）将会被记录在区块上，任何试图修改文物艺术品属性的行为，将无法施展。这击中了文物艺术品市场缺乏合适的记录保留方式和文物艺术品来源实时验证等需求痛点。文物艺术市场由此成为区块链技术最适合应用的五大行业之一。

通过区块链的去中心化信用网络，文物艺术品将实现资产的数字化、证券化，文物艺术品数字资产的数千万玩家也将真正实现文物艺术品投资梦想。去中心化信任机制以及智能合约的特性，能有效解决文物艺术品的共有权问题信任机制和在流通过程中发生的共有权变化的信任问题。通过托管机构保存文物艺术品，并发行对应的文物艺术品代币，可以帮助文物艺术品实现资本化效果。

用户可以在任何加密货币交易所交易对应的文物艺术品代币，实现低门槛，7*24 小时的随意买卖，并且只需要承担低廉的交易费用，文物艺术品代币还能够解决文物艺术品作为非标品的定价问题。

这将是一个伟大的创新，帮助文物艺术品投资走入寻常百姓家。中国有上亿藏友，多为身家底蕴深厚，这将对仅有数百万人的区块链市场带来巨大冲击。区块链与文物艺术品的结合，将中华九千年的文物瑰宝，以全新的数字资产形式，推广到全世界并发扬光大，实现中国文物艺术品资产国际化全流通，使中国文物艺术品走向全世界，实现中华民族的伟大复兴。

一、区块链技术简介

1、区块链是近年来最具革命性的新兴技术之一，该技术因其去中心化、不可篡改、可溯源等特征，逐渐引起了众人的高度关注，包括金融、保险、健康、医疗、公益等多个行业都在探索其应用前景。

区块链是比特币的底层技术，其数据块信息生成的时间戳和存在证明，可以实时记录并完整保存所有的交易记录。区块链的优势主要表现在不需要中介参与、信息开放透明且不可篡改、数据安全和成本很低。基于密码学、分布式共识协议、点对点网络通信和智能合约等技术保障，使用区块链账本系统的多个参与者，无需额外的第三方担保机构，即可构成多方交易的信任基础。

2、区块链的 1.0 时代，是由比特币这一区块链行业的元老所带领起飞，上涨的逻辑是比特币将作为一种货币在越来越多的场景下替代法币使用。伴随着接受程度的提高，2017 年比特币迎来大牛市，自 700 美金一路上涨至 15000 美金，上涨了约 20 倍。

区块链的 2.0 时代，是由以太坊这一区块链的「证券公司」带领起飞，任何人都可以便捷地依赖以太坊发行自己的代币，甚至不需要准备矿工和交易所。2017 年以太坊从 8 美元一路上涨至 800 美元以上，涨幅超过 100 倍。然而由于以太坊上募资项目一直没有出现落地应用，仅仅 2018 年的头 4 个月，以太坊便腰斩一半到 400 美元。

区块链的 3.0，将会由具备实际价值的资产上链所引领，加密货币无国界、无门槛、低费率的优势，使得一切传统世界的资产都能通过区块链重塑。然而，企业股权、房产等资产不必依赖区块链也能有完善的交易市场；专利、IP、明星时间之类的资产虽有区块链改造的空间，但是本身的参与者和资产体量都不足以成为一个大众交易市场。

文物艺术品+金融+区块链，将是区块链 3.0 中最重要的组成部分，区块链的浪潮将伴随着文物艺术品行业天翻地覆的变化，一切从业者，一切藏家，都必须快速提高认知能力而决定是否被时代弃取。

基于区块链的文物艺术品产业资产体系及相关生态的建设，极具现实意义。文物艺术品+金融+区块链产业体系搭建，将利用区块链技术的优势，弥补当前传统模式对于文物艺术品规范化方面的不足，为文物艺术品交易提供新的可信渠道，最终实现重塑文物艺术品产业价值链。

二. 宝链底层设计思想

宝链是公有链+原生应用，这是宝链和市场上其他资产上链项目的最大区别。大部分的资产上链都是单独的 DAPP 应用。一个完整的资产生态应当包含资产方、交易所、投资机构、投行、第三方鉴定机构、评级机构、数据服务机构、金融中介等多个角色，宝链就是这样一个完整的生态。

宝链底层是一条针对文物艺术品产业特别设计的底层区块链网络，除了发行宝链子币的功能外，将开放给所有有志于从事文物艺术品产业区块链应用开发的开发者，帮助他们搭建不同场景下的应用。

从而间接帮助收藏家扩展宝链子币的用户，以及帮助收藏家寻找到愿意私有化文物艺术品的大户。宝链也将由资产上链平台变成一个文物艺术品行业的操作系统。宝链和宝币的价值将拓展到产业的更多方面，与更多原有生态资源结合。宝链希望最终实现一个弱中心化的文物艺术品收藏与投资新模式，打造智能、自治、繁荣的宝链生态圈。

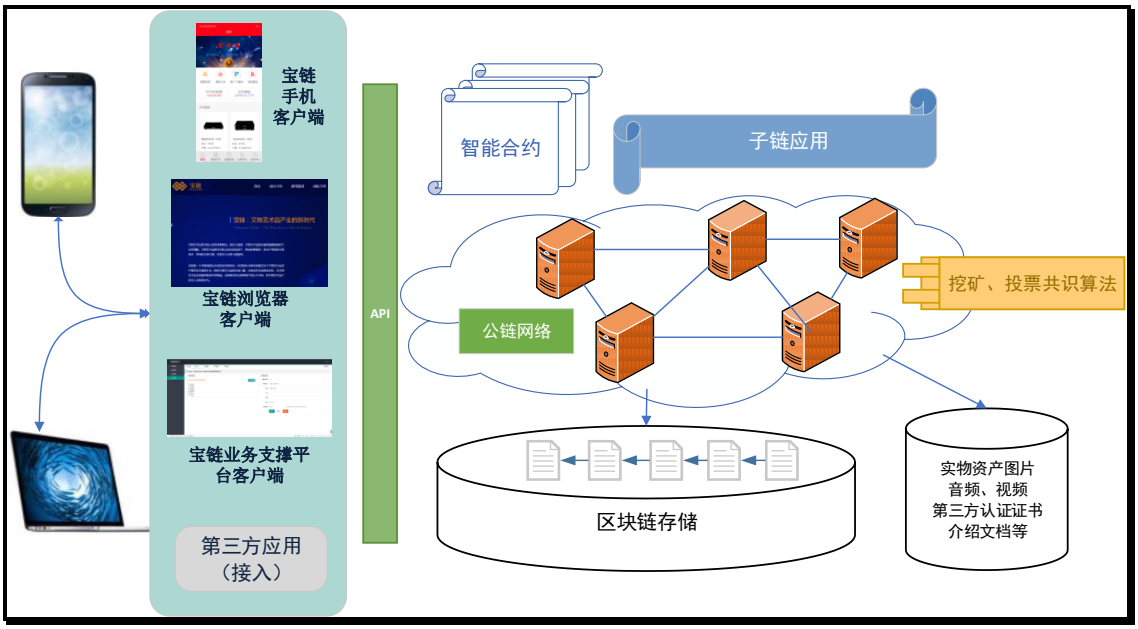
三、宝链体系架构

宝链的体系架构遵循区块链 3.0 架构，能够满足更加复杂的商业逻辑，是面向实体业务的真正的应用之链。

四、宝链技术架构

宝链的客户端应用包括移动端应用、浏览器端应用，以及后台运营管理平台，并支持第三方应用的接入。

宝链的服务端及公链网络实现了区块链存储、智能合约、共识算法等区块链功能，并支持子链应用和实物资产上链及相关业务交易。



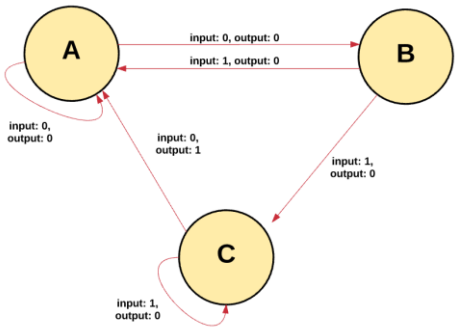
宝链子链是从宝链公有主链上派生出来的区块链，不单独存在，通过主链供的基础设施运行，免费获得主链用户

宝链子链特性： 可自定义共识方式和执行模块；快速部署子链，无需维护节点；

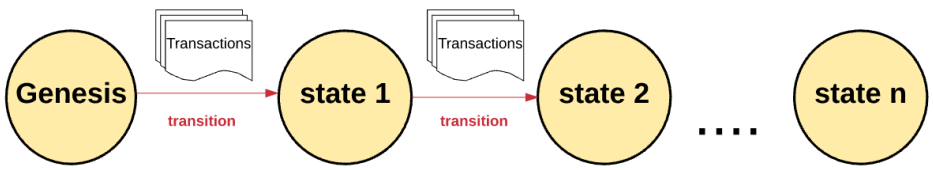
方便构建功能强大的 DAPP。

五、宝链底层技术概述

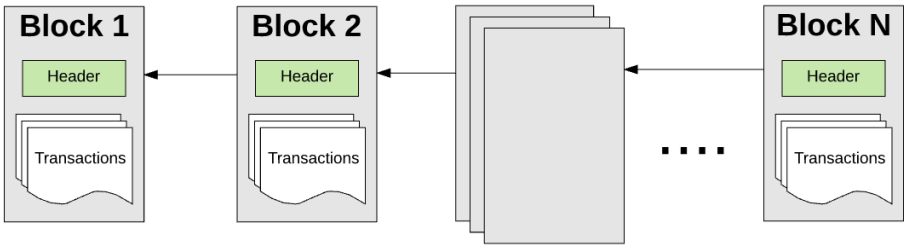
宝链的本质是基于交易的状态机(transaction-based state machine)。在计算机科学中，一个 状态机 是指可以读取一系列的输入，然后根据这些输入，会转换成一个新的状态输出。



根据宝链的状态机，我们从创世纪状态(genesis state)开始。这差不多类似于一片空白的石板，在网络中还没有任何交易的产生状态。当交易被执行后，这个创世纪状态就会转变成最终状态。在任何时刻，这个最终状态都代表着宝链当前的状态。



宝链的交易都被“组团”到一个区块中。一个区块包含了一系列的交易，每个区块都与它的前一个区块链接起来。



为了让一个状态转换成下一个状态，交易必须是有效的。为了让一个交易被认为是有效的，它必须要经过一个验证过程，此过程也就是挖矿。挖矿就是一组节点（即电脑）用它们的计算资源来创建一个包含有效交易的区块出来。

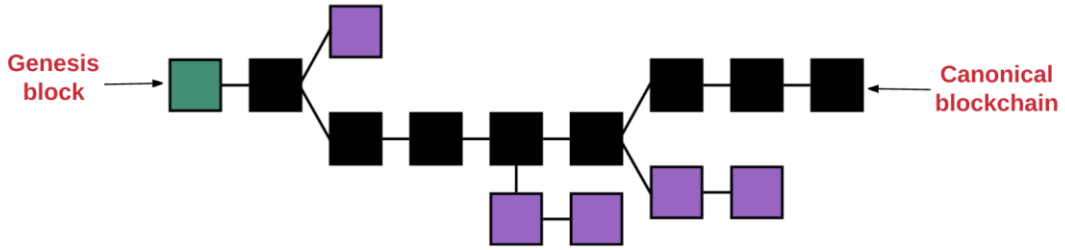
任何在网络上宣称自己是矿工的节点都可以尝试创建和验证区块。世界各地的很多矿工都在同一时间创建和验证区块。每个矿工在提交一个区块到区块链上的时候都会提供一个数学机制的“证明”，这个证明就像一个保证：如果这个证明存在，那么这个区块一定是有效的。

为了让一个区块添加到主链上，一个矿工必须要比其他矿工更快的提供出这个“证明”。通过矿工提供的一个数学机制的“证明”来证实每个区块的过程称之为工作量证明(proof of work)。证实了一个新区块的矿工都会被奖励数字代币作为奖赏。每次矿工证明了一个新区块，那么就会产生新的宝币并被奖励给矿工。

为了确定哪个路径才是最有效的以及防止多条链的产生，宝链使用了一个叫做“GHOST协议(GHOST protocol.)”的数学机制。

GHOST = Greedy Heaviest Observed Subtree

简单来说，GHOST 协议就是让我们必须选择一个在其上完成计算最多的路径。一个方法确定路径就是使用最近一个区块（叶子区块）的区块号，区块号代表着当前路径上总的区块数（不包含创世纪区块）。区块号越大，路径就会越长，就说明越多的挖矿算力被消耗在此路径上以达到叶子区块。使用这种推理就可以允许我们赞同当前状态的权威版本。



宝链系统主要组成部分有：

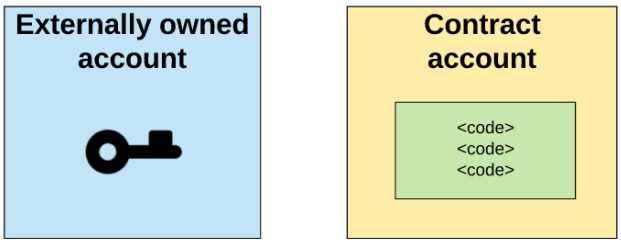
1. 账户(accounts)
2. 状态(state)
3. 损耗和费用(gas and fees)
4. 交易(transactions)
5. 区块(blocks)
6. 交易执行(transaction execution)
7. 挖矿(mining)
8. 工作量证明(proof of work)

账户

宝链的全局“共享状态”是有很多小对象（账户）来组成的，这些账户可以通过消息传递架构来与对方进行交互。每个账户都有一个与之关联的状态(state)和一个 20 字节的地址(address)。在宝链中一个地址是 40 位的标识符，用来识别账户。宝链地址使用 16 进制形式呈现，一个十六进制数字占 4 位，故 16 进制地址长度为 40，地址前面再加上 0x 以表示使用 16 进制。

这是两种类型的账户：

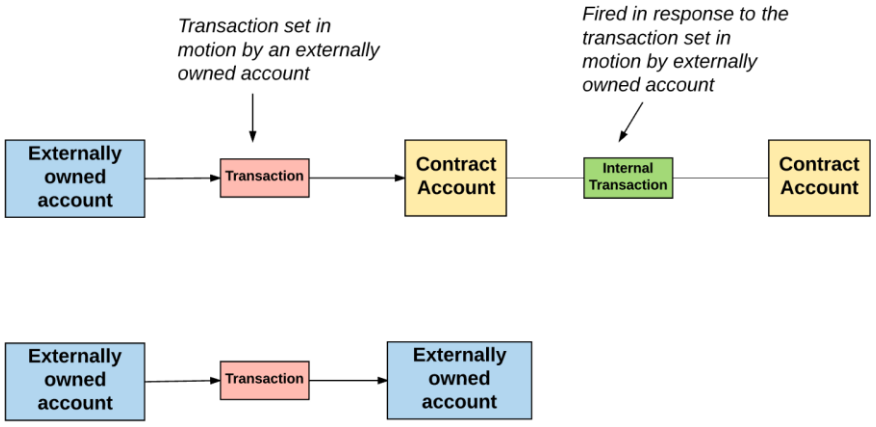
1. 外部拥有的账户，被私钥控制且没有任何代码与之关联
2. 合约账户，被它们的合约代码控制且有代码与之关联



外部拥有账户与合约账户的比较

外部拥有账户可以通过创建和用自己的私钥来对交易进行签名，来发送消息给另一个外部拥有账户或合约账户。在两个外部拥有账户之间传送的消息只是一个简单的价值转移。但是从外部拥有账户到合约账户的消息会激活合约账户的代码，允许它执行各种动作。（比如转移代币，写入内部存储，挖出一个新代币，执行一些运算，创建一个新的合约等等）。

合约账户不可以自己发起一个交易。相反，合约账户只有在接收到一个交易之后(从一个外部拥有账户或另一个合约账户接)，为了响应此交易而触发一个交易。我们将会在“交易和消息”部分来了解关于合约与合约之间的通信。

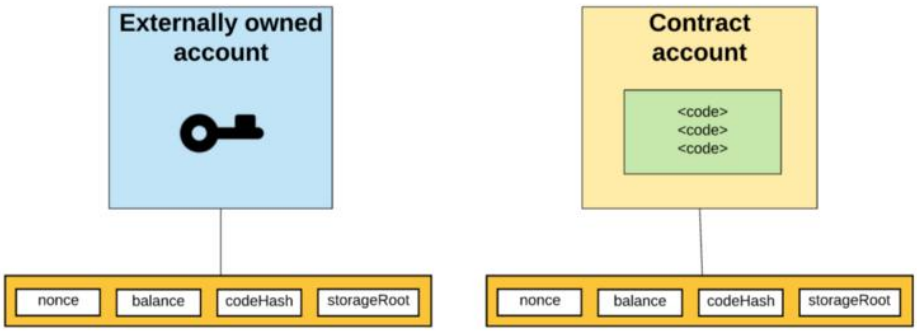


因此，在宝链上任何的动作，总是被外部控制账户触发的交易所发动的。

账户状态

账户状态有四个组成部分，不论账户类型是什么，都存在这四个组成部分：

1. nonce：如果账户是一个外部拥有账户，nonce 代表从此账户地址发送的交易序号。如果账户是一个合约账户，nonce 代表此账户创建的合约序号
2. balance： 此地址拥有 Wei 的数量。1TST=10^18Wei
3. storageRoot： Merkle Patricia 树的根节点 Hash 值（我们后面在解释 Merkle 树）。Merkle 树会将此账户存储内容的 Hash 值进行编码，默认是空值。
4. codeHash：此账户 TVM（宝链虚拟机，后面细说）代码的 hash 值。对于合约账户 ,就是被 Hash 的代码并作为 codeHash 保存。对于外部拥有账户 ,codeHash 域是一个空字符串的 Hash 值。

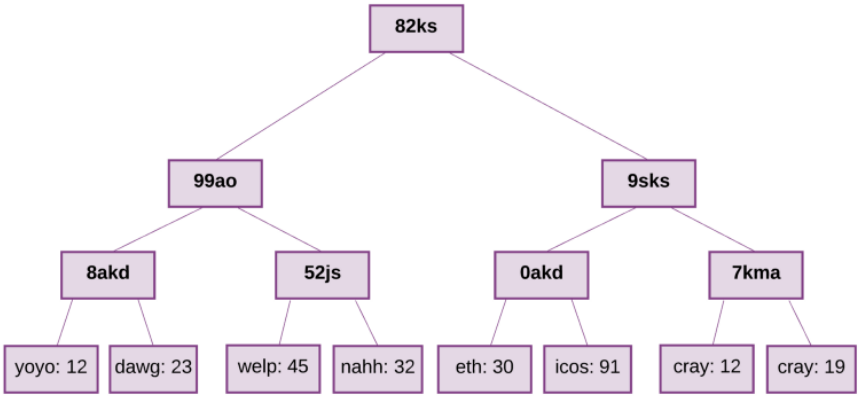


世界状态

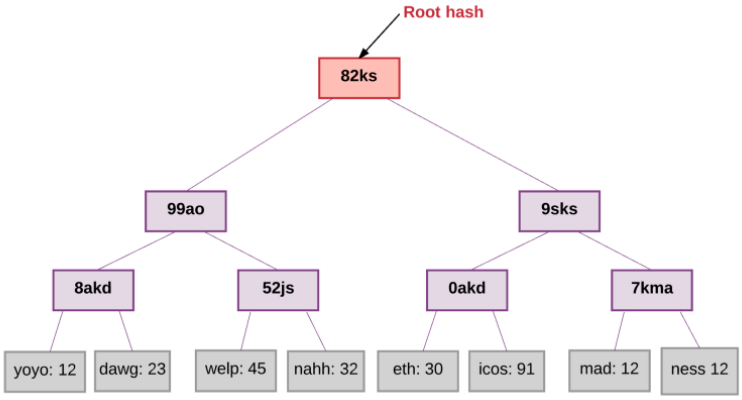
宝链的全局状态就是由账户地址和账户状态的一个映射组成。这个映射被保存在一个叫做 Merkle Patricia 树的数据结构中。

Merkle Tree（也被叫做 Merkle trie）是一种由一系列节点组成的二叉树，这些节点包括：

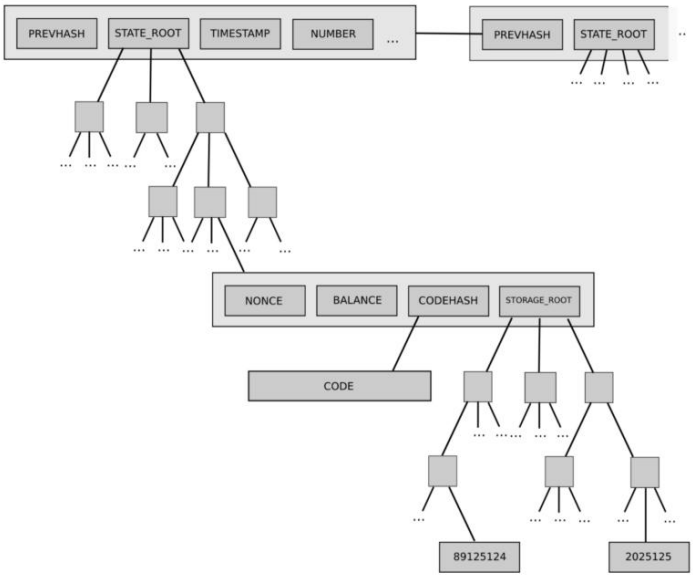
1. 在树底的包含了源数据的大量叶子节点；
2. 一系列的中间的节点，这些节点是两个子节点的 Hash 值；
3. 一个根节点，同样是两个子节点的 Hash 值，代表着整棵树。



树底的数据是通过分开我们想要保存到 chunks 的数据产生的，然后将 chunks 分成 buckets ,再然后再获取每个 bucket 的 hash 值并一直重复直到最后只剩下一个 Hash：根 Hash。

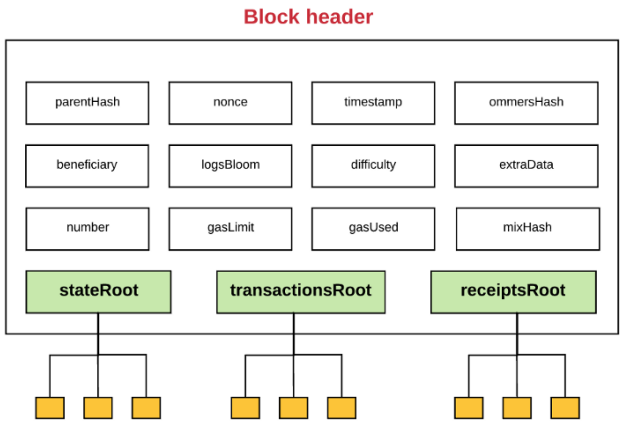


这棵树要求存在里面的值（value）都有一个对应的 key。从树的根节点开始，key 会告诉你顺着哪个子节点可以获得对应的值，这个值存在叶子节点。在宝链中，key/value 是地址和与地址相关联的账户之间状态的映射，包括每个账户的 balance, nonce, codeHash 和 storageRoot（storageRoot 自己就是一颗树）。



同样的树结构也用来存储交易和收据。更具体的说，每个块都有一个头(header)，保存了三个不同 Merkle trie 结构的根节点的 Hash，包括：

1. 状态树
2. 交易树
3. 收据树



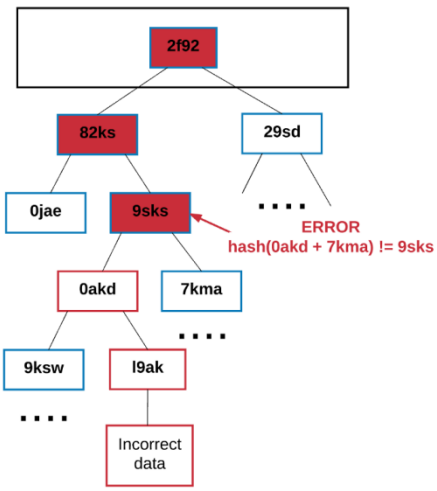
在 Merkle trees 中存储所有信息的高效性在宝链中的“轻客户端”和“轻节点”相当的有用。记住区块链就是一群节点来维持的。广泛的说，有两种节点类型：全节点和轻节点。

全节点通过下载整条链来进行同步，从创世纪块到当前块，执行其中包含的所有交易。通常，矿工会存储全节点，因为他们在挖矿过程中需要全节点。也有可能下载一个全节点而不用执行所有的交易。无论如何，一个全节点包含了整个链。

不过除非一个节点需要执行所有的交易或轻松访问历史数据，不然没必要保存整条链。这就是轻节点概念的来源。比起下载和存储整个链以及执行其中所有的交易，轻节点仅仅下载链的头，从创世纪块到当前块的头，不执行任何的交易或检索任何相关联的状态。

由于轻节点可以访问块的头，而头中包含了 3 个 tries 的 Hash，所有轻节点依然可以很容易生成和接收关于交易、事件、余额等可验证的答案。

这个可以行的通是因为在 Merkle 树中 hash 值是向上传播的—如果一个恶意用户试图用一个假交易来交换 Merkle 树底的交易，这个会改变它上面节点的 hash 值，而它上面节点的值的改变也会导致上上一个节点 Hash 值的改变，以此类推，一直到树的根节点。



任何节点想要验证一些数据都可以通过 Merkle 证明来进行验证，Merkle 证明的组成：

1. 一块需要验证的数据
2. 树的根节点 Hash
3. 一个“分支”（从 chunk 到根这个路径上所有的 hash 值）

任何可以读取证明的人都可以验证分支的 hash 是连贯的，因此给出的块在树中实际的位置就是在此处。

总之 ,使用 Merkle Patricia 树的好处就是该结构的根节点加密取决于存储在树中的数据，而且根据点的 hash 还可以作为该数据的安全标识。由于块的头包含了状态、交易、收据树的根 hash，所有任何节点都可以验证宝链的一小部分状态而不用保存整个状态，这整个状态的的大小可能是非常大的。

Gas 和费用

宝链网络上的交易而产生的每一次计算，都会产生费用。对每个交易，发送者设置 gas limit 和 gas price。gas limit 和 gas price 就代表着发送者愿意为执行交易支付的 Wei 的最大值。

gas 不仅仅是用来支付计算这一步的费用，而且也用来支付存储的费用。存储的总费用与所使用的 32 位字节的最小倍数成比例。

存储费用有一些比较细微的方面。比如，由于增加了的存储增加了所有节点上的宝链状态数据库的大小，所以激励保持数据存储量小。为了这个原因，如果一个交易的执行有一步是清除一个存储实体，那么为执行这个操作的费用就会被放弃，并且由于释放存储空间的退款就会被返回给发送者。

交易和消息

宝链有两种类型的交易：消息通信和合约创建(也就是交易产生一个新的宝链合约)。

不管什么类型的交易，都包含：

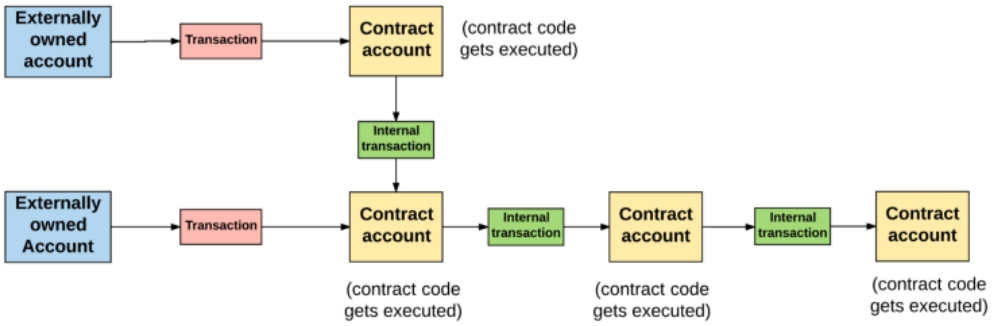
1. nonce：发送者发送交易数的计数

2. gasPrice：发送者愿意支付执行交易所需的每个 gas 的 Wei 数量
3. gasLimit：发送者愿意为执行交易支付 gas 数量的最大值。这个数量被设置之后在任何计算完成之前就会被提前扣掉
4. to：接收者的地址。在合约创建交易中，合约账户的地址还没有存在，所以值先空着
5. value：从发送者转移到接收者的 Wei 数量。在合约创建交易中，value 作为新建合约账户的开始余额
6. v,r,s：用于产生标识交易发生着的签名
7. init（只有在合约创建交易中存在）：用来初始化新合约账户的 TVM 代码片段。init 值会执行一次，然后就会被丢弃。当 init 第一次执行的时候，它返回一个账户代码体，也就是永久与合约账户关联的一段代码。
8. data（可选域，只有在消息通信中存在）：消息通话中的输入数据(也就是参数)。例如，如果智能合约就是一个域名注册服务，那么调用合约可能就会期待输入域例如域名和 IP 地址

在宝链状态全局范围内的合约可以与在相同范围内的合约进行通信。他们是通过“消息”或者“内部交易”进行通信的。我们可以认为消息或内部交易类似于交易，不过与交易有着最大的不同点—它们不是由外部拥有账户产生的。相反，他们是被合约产生的。它们是虚拟对象，与交易不同，没有被序列化而且只存在与宝链执行环境。

当一个合约发送一个内部交易给另一个合约，存在于接收者合约账户相关联的代码就会被执

行。



一个重要需要注意的事情是内部交易或者消息不包含 gasLimit。因为 gas limit 是由原始交易的外部创建者决定的（也就是外部拥有账户）。外部拥有账户设置的 gas limit 必须要高到足够将交易完成，包括由于此交易而长生的任何”子执行”，例如合约到合约的消息。如果，在一个交易或者信息链中，其中一个消息执行使 gas 已不足，那么这个消息的执行会被还原，包括任何被此执行触发的子消息。不过，父执行没必要被还原。

区块

所有的交易都被组成一个”块”。一个区块链包含了一系列这样的链在一起区块。

在宝链中，一个区块包含：

1. 区块头
2. 关于包含在此区块中交易集的信息
3. 与当前块的 ommers 相关的一系列其他区块头

由于宝链的构造，它的区块生产时间（大概 15 秒左右）比其他的区块链例如 Bitcoin（大概 10 分钟左右）要快很多。这使得交易的处理更快。但是，更短的区块生产时间的一个

缺点就是：更多的竞争区块会被矿工发现。这些竞争区块同样也被称为“孤区块”（也就是被挖出来但是不会被添加到主链上的区块）。

Ommers 的目的就是为了帮助奖励矿工纳入这些孤区块。矿工包含的 ommers 必须是有效的，也就是 ommers 必须在父区块的第 6 个子区块之内或更小范围内。在第 6 个子区块之后，陈旧的孤区块将不会再被引用(因为包含老旧的交易会使事情变得复杂一点)。

Ommer 区块会收到比全区块少一点的奖励。不管怎样，依然存在激励来让矿工们纳入孤区块并能从中获得一些报酬。

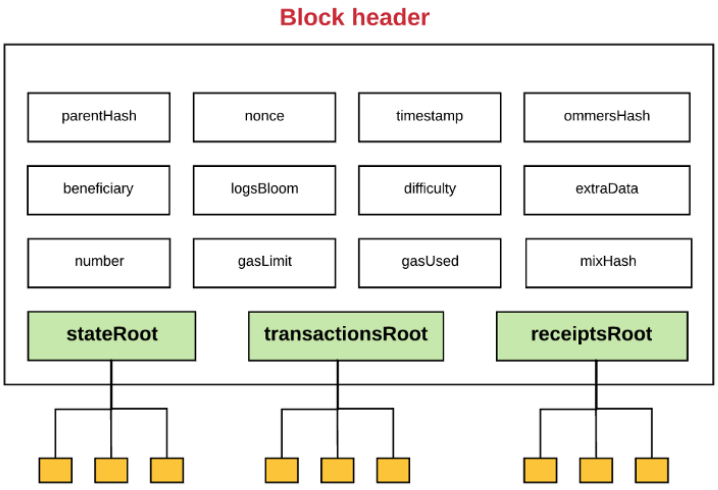
区块头

让我们再回到区块的问题上。我们前面提到每个区块都有一个“区块头”，但这究竟是什么？

区块头是一个区块的一部分，包含了：

1. parentHash：父区块头的 Hash 值（这也是使得区块变成区块链的原因）
2. ommerHash：当前区块 ommers 列表的 Hash 值
3. beneficiary：接收挖此区块费用的账户地址
4. stateRoot：状态树根节点的 Hash 值（回忆一下我们之前所说的保存在头中的状态树以及它使得轻客户端认证任何关于状态的事情都变得非常简单）
5. transactionsRoot：包含此区块所列的所有交易的树的根节点 Hash 值
6. receiptsRoot：包含此区块所列的所有交易收据的树的根节点 Hash 值
7. logsBloom：由日志信息组成的一个过滤器

8. difficulty： 此区块的难度级别
9. number：当前区块的计数（创世纪块的区块序号为 0，对于每个后续区块，区块序号都增加 1）
10. gasLimit：每个区块的当前 gas limit
11. gasUsed： 此区块中交易所用的总 gas 量
12. timestamp：此区块成立时的 unix 的时间戳
13. extraData：与此区块相关的附加数据
14. mixHash：一个 Hash 值，当与 nonce 组合时，证明此区块已经执行了足够的计算
15. nonce：一个 Hash 值，当与 mixHash 组合时，证明此区块已经执行了足够的计算



每个区块包含三个树结构（Merkle Patricia 树），分别对应：

1. 状态（stateRoot）
2. 交易（transactionsRoot）

3. 收据（receiptsRoot）

区块头合法性

确定区块是否合法除了整体性的合法校验，还需要对区块头进行更进一步的校验。主要校验规则有以下几点：

- parentHash 正确。即 parentHash 与其父区块的头的 hash 一致。
- number 为父区块 number 值加一。
- difficuilty 难度正确。区块合理的难度跟父区块难度，以及当前区块时间戳和父区块时间戳间隔以及区块编号有关。难度可以起到一定的调节出块时间的作用。，可以看出当出块变快（也就是出块间隔变小之后）难度会增加，相反难度会减小。
- gasLimit 和上一个区块的差值在规定范围内。
- gasUsed 小于等于 gasLimit
- timestamp 时间戳必须大于上一区块的时间戳。
- mixHash 和 nonce 必须满足 PoW。
- extraData 最多为 32 个字节。

交易执行

首先，为了可以被执行所有的交易必须都要符合最基础的一系列要求，包括：

- 交易必须是正确格式化的 RLP。”RLP”代表 Recursive Length Prefix，它是一种数据格式，用来编码二进制数据嵌套数组。宝链就是使用 RLP 格式序列化对象。
- 有效的交易签名。

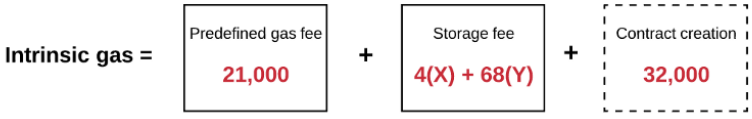
- 有效的交易序号。回忆一下账户中的 nonce 就是从此账户发送出去交易的计数。

如果有效，那么交易序号一定等于发送账户中的 nonce。

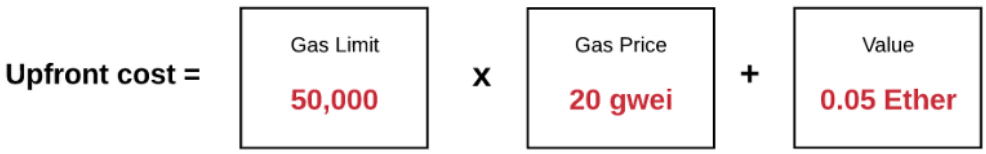
- 交易的 gas limit 一定要等于或者大于交易使用的 intrinsic gas，intrinsic gas

包括：

1. 执行交易预订费用为 21,000gas
2. 随交易发送的数据的 gas 费用（每字节数据或代码为 0 的费用为 4gas，每个非零字节的数据或代码费用为 68gas）
3. 如果交易是合约创建交易，还需要额外的 32,000gas

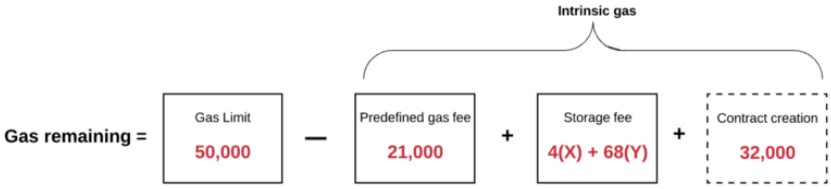


- 发送账户余额必须有足够的 TST 来支付”前期”gas 费用。前期 gas 费用的计算比较简单：首先，交易的 gas limit 乘以交易的 gas 价格得到最大的 gas 费用。然后，这个最大 gas 费用被加到从发送方传送给接收方的总值。



如何交易符合上面所说的所有要求，那么我们进行下面步骤。

第一步，我们从发送者的余额中扣除执行的前期费用，并为当前交易将发送者账户中的 nonce 增加 1。此时 ,我们可以计算剩余的 gas ,将交易的总 gas 减去使用的 intrinsic gas。



第二步，开始执行交易。在交易执行的整个过程中，宝链保持跟踪“子状态”。子状态是记录在交易中生成的信息的一种方式，当交易完成时会立即需要这些信息。具体来说，它包含：

1. 自毁集：在交易完成之后会被丢弃的账户集（如果存在的话）
2. 日志系列：虚拟机的代码执行的归档和可检索的检查点
3. 退款余额：交易完成之后需要退还给发送账户的总额。回忆一下我们之前提到的宝链中的存储需要付费，发送者要是清理了内存就会有退款。宝链使用退款计数进行跟踪退款余额。退款计数从 0 开始并且每当合约删除了一些存储中的东西都会进行增加。

第三步，交易所需的各种计算开始被处理。

当交易所需的步骤全部处理完成，并假设没有无效状态，通过确定退还给发送者的未使用的 gas 量，最终的状态也被确定。除了未使用的 gas，发送者还会得到上面所说的“退款余额”中退还的一些津贴。

合约创建(Contract creation)

在宝链中，有两种账户类型：合约账户和外部拥有账户。当我们说一个交易是“合约创建”，是指交易的目的是创建一个新的合约账户。

为了创建一个新的合约账户，我们使用一个特殊的公式来声明新账户的地址。然后我们使用下面的方法来初始化一个账户：

1. 设置 nonce 为 0
2. 如果发送者通过交易发送了一定量的 TST 作为 value，那么设置账户的余额为 value
3. 将存储设置为 0
4. 设置合约的 codeHash 为一个空字符串的 Hash 值

一旦完成了账户的初始化，使用交易发送过来的 init code（查看”交易和信息”章节来复习一下 init code），实际上就创造了一个账户。init code 的执行过程是各种各样的。取决于合约的构造器，可能是更新账户的存储，也可能是创建另一个合约账户，或者发起另一个消息通信等等。

当初始化合约的代码被执行之后，会使用 gas。交易不允许使用的 gas 超过剩余 gas。如果它使用的 gas 超过剩余 gas，那么就会发生 gas 不足异(OOG)常并退出。如果一个交易由于 gas 不足异常而退出，那么状态会立刻恢复到交易前的一个点。发送者也不会获得在 gas 用完之前所花费的 gas。

不过，如果发送者随着交易发送了 TST，即使合约创建失败 TST 也会被退回来。

如果初始化代码成功的执行完成，最后的合约创建的花费会被支付。这些是存储成本，与创建的合约代码大小成正比（再一次，没有免费的午餐）。如果没有足够的剩余 gas 来支付最后的花费，那么交易就会再次宣布 gas 不足异常并中断退出。

如果所有的都正常进行没有任何异常出现，那么任何剩余的未使用 gas 都会被退回给原始的交易发送者，现在改变的状态才被允许永久保存。

消息通信(Message calls)

消息通信的执行与合约创建比较类似，只不过有一点点区别。

由于没有新账户被创建，所以消息通信的执行不包含任何的 init code。不过，它可以包含输入数据，如果交易发送者提供了此数据的话。一旦执行，消息通信同样会有一个额外的组件来包含输出数据，如果后续执行需要此数据的话就组件就会被使用。

就像合约创建一样，如果消息通信执行退出是因为 gas 不足或交易无效（例如栈溢出，无效跳转目的地或无效指令）,那么已使用的 gas 是不会被退回给原始触发者的。相反，所有剩余的未使用 gas 也会被消耗掉 ,并且状态会被立刻重置为余额转移之前的那个点。

没有任何方法停止或恢复交易的执行而不让系统消耗你提供的所有 gas，直到最新的宝链更新。例如，假设你编写了一个合约，当调用者没有授权来执行这些交易的时候抛出一个错误。在宝链的前一个版本中，剩余的 gas 也会被消耗掉，并且没有任何 gas 退回给发送者。但是拜占庭更新包括了一个新的“恢复”代码，允许合约停止执行并且恢复状态改变而不消耗剩余的 gas，此代码还拥有返回交易失败原因的能力。如果一个交易是由于恢复而退出，那么未使用的 gas 就会被返回给发送者。

执行模式

协议实际操作交易处理的部分是宝链自己的虚拟机，称之为宝链虚拟机（TVM）。

像之前定义的那样，是图灵完备虚拟机器。TVM 存在而典型图灵完备机器不存在的唯一限制就是 TVM 本质上是被 gas 束缚。因此，可以完成的计算总量本质上是被提供的 gas 总量限制的。

此外，TVM 具有基于堆栈的架构。TVM 中每个堆栈项的大小为 256 位，堆栈有一个最大的大小，为 1024 位。TVM 有内存，项目按照可寻址字节数组来存储。内存是易失性的，也就是数据是不持久的。

TVM 也有一个存储器。不像内存，存储器是非易失性的，并作为系统状态的一部分进行维护。TVM 分开保存程序代码，在虚拟 ROM 中只能通过特殊指令来访问，此架构将程序的代码存储在内存或存储器中。

TVM 同样有属于它自己的语言：“TVM 字节码”，当一个程序员比如你或我写一个在宝链上运行的智能合约时，我们通常都是用高级语言例如 Solidity 来编写代码。然后我们可以将它编译成 TVM 可以理解的 TVM 字节码。

在执行特定的计算之前，处理器会确定下面所说的信息是有效和是否可获取：

1. 系统状态
2. 用于计算的剩余 gas
3. 拥有执行代码的账户地址
4. 原始触发此次执行的交易发送者的地址
5. 触发代码执行的账户地址（可能与原始发送者不同）
6. 触发此次执行的交易 gas 价格
7. 此次执行的输入数据

8. Value(单位为 Wei)作为当前执行的一部分传递给该账户
9. 待执行的机器码
10. 当前区块的区块头
11. 当前消息通信或合约创建堆栈的深度

执行刚开始时，内存和堆栈都是空的，程序计数器为 0。

1 PC: 0 STACK: [] MEM: [], STORAGE: {}

然后 TVM 开始递归的执行交易，为每个循环计算系统状态和机器状态。系统状态也就是宝链的全局状态(global state)。机器状态包含：

1. 可获取的 gas
2. 程序计数器
3. 内存的内容
4. 内存中字的活跃数
5. 堆栈的内容

堆栈中的项从系列的最左边被删除或者添加。

每个循环，剩余的 gas 都会被减少相应的量，程序计数器也会增加。在每个循环的结束，都有三种可能性：

1. 机器到达异常状态（例如，gas 不足，无效指令，堆栈项不足，堆栈项会溢出 1024，无效的 JUMP/JUMPI 目的地等等）因此停止，并丢弃任何的更改
2. 进入后续处理下一个循环

3. 机器到达了受控停止（到达执行过程的终点）

假设执行没有遇到异常状态，达到一个“可控的”或正常的停止，机器就会产生一个合成状态，执行之后的剩余 gas、产生的子状态、以及组合输出。

块的完成机理

如果是个新块，就是指挖这个块所需的处理。如果是已存在的块，就是指验证此块的处理。不论哪种情况，一个块的“完成”都有 4 个要求： 1）验证（或者，如果是挖矿的话，就是确定）ommers 在区块头中的每个 ommer 都必须是有效的头并且必须在当前块的 6 代之内

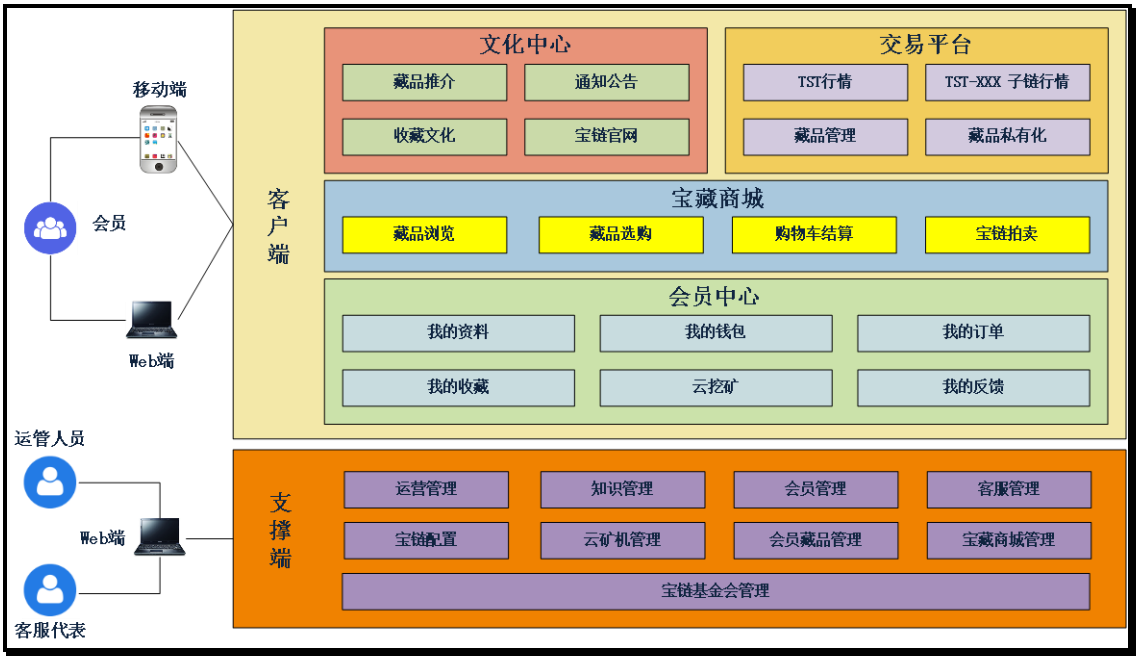
2）验证（或者，如果是挖矿的话，就是确定）交易 区块中的 gasUsed 数量必须与区块中所列交易使用的累积 gas 量相等。（回忆一下，当执行一个交易的时候，我们会跟踪区块的 gas 计数器，也就跟踪了区块中所有交易使用的 gas 总数量）

3）申请奖励（只有挖矿时） 受益人的地址会因为挖矿而获得 3TST。另外，对于每个 ommer，当前块的受益人会获得额外的 1/32 当前块奖励金的奖励。最近，每个 ommer 区块的受益人能够得到一定量的奖励（有个特殊公式可以进行计算）。

4）校验（或者，如果是挖矿的话，就是计算一个有效的）状态和 nonce 确保所有的交易和改变的结果状态都被应用了，然后在区块奖励被应用于最终交易结果状态之后定义一个新块为状态。通过检查最终状态与存储在头中的状态树来进行验证。

六、宝链提供的业务功能

宝链是真正面向实际业务的区块链应用，支撑下图所示的各项业务功能模块。



七、宝链生态区块链特点

宝链是一个自主区块链底层，开放是宝链最基本的使命之一。开放能力主要依靠技术体系中的应用接入层来实现，更细节来说有两种实现方式。第一，利用宝链的底层框架中的应用接入模块；第二，独立的应用接入 SDK 及 API，这是一种较轻的方式，背后由某一些特定的节点提供服务。

不管哪种方式，都将提供强大的开放和可扩展能力， 输出能力包括：数据、交易、钱包账户服务、智能合约等。应为宝链本身面向文物艺术品产业，这些能力或服务也都将具备针对文物艺术品产业的特殊性来构造，实现「简洁在表，智能在芯」。

宝链的搭建需要多个功能组件的有效协作，这些组件包括网络通信、区块链数据结构、账本状态存储、交易模块、智能合约执行环境、共识机制等。宝链在设计上遵循可

扩展的架构设计和可插拔的模块化实现。

宝链结合自身承载应用的特性和未来生态建设的考量，对多个组件进行了自主开发和扩展，包括账户和代币模块的开发、账本数据结构的改进、状态存储模块的扩展等。

与比特币和以太坊不同，宝链的初始目标并非构造一套去中心化数字货币系统或智能合约平台，而是会专注于文物艺术品行业的基本应用需求。这些应用更看重各个参与主体的信誉，因此宝链的底层架构将尽量使得每一个公钥对应现实世界一个参与主体。当然，由于宝链平台可扩展的架构设计，未来完全可以开发或引入更多基本组件和扩展插件，以支持更为丰富的区块链应用。

宝链的底层由多个节点组成 P2P 分布式网络，每个节点都在网络中担任一定职能或提供服务。节点和节点之间通过 GRPC 进行交互，通过 Gossip 协议进行状态同步和数据分发。在宝链中，所有节点并非完全对等。根据所属组织或个人的资源条件和权限区别，节点可包含以下一个或多个功能。:

背书功能：对未验证交易进行检查，对其进行背书。 背书节点会独立对收到的交易进行检查，并按照自身逻辑给出背书结论。每个交易需要满足一定条件的背书才被认为合法。这个条件往往由智能合约的背书策略指定，策略可以由智能合约开发者灵活设置，如必须获得超过一定数目背书节点的支持、或必须获得某个特定背书节点的支持等。

记录功能：对交易进行打包，并生成区块。对经过全局排序的交易进行检查，执行交易并维护区块链和账本结构。每个节点独立验证交易，并按照统一的公开规则进行共识，尝试作恶或遭受攻击的节点会被实时探测到，受到隔离或惩罚。同时，宝链将提出成为记账节点的准入标准，任何满足准入标准的第三方或用户都可以申请成为记账节点，

参与维护宝链网络。

代理和路由功能：提供带宽和储存网络，作为用户应用的接入节点，并转发信息给其他相应节点。提高整个区块链网络的吞吐量和响应速度。

上述各节点和过程的配合可以保证网络对交易的合法性、发生顺序、对账本状态的更新结果达成共识。不同节点功能解耦，能够为宝链应用支撑起商用级的交易吞吐量。

宝币拥有者账户将对应到某公钥，账户信息将记录在宝链账本的状态中，所有账户信息的数字摘要将记录在区块中。宝币拥有数字货币基本的技术特性，包括发行曲线固定、可自由交易、抗双重花费攻击、交易历史可追溯等，这些特性将通过宝链的账本结构和核心通道的智能合约保证。用户使用链上应用时，通常也涉及宝币的支付或获取。宝链团队会为用户开发宝币钱包 ,可以存储宝币或宝链子币 ,同时具备对应的其他功能。

八、结语

如今，中国已经成为当今世界第二大经济体与第一大贸易国。「中国需求」和「中国价格」已经在文物艺术品上反映得淋漓尽致，文物艺术市场的影响力也与日俱增。然而，中国却始终无法参与到定价的过程中。文物艺术品的定价权长期被国际大拍卖行主导，因为资金和流动性的优势，大量中国的文物艺术品流出到国际大拍卖行交易。

作为文物艺术品最大的消费方，中国文物艺术品定价权的缺失，不仅与中国历史大国的地位明显不匹配，更严重损害了国家利益。在中国文物艺术品无序之时，海外占据文物艺术品的定价权，扭曲中国的价值观和审美标准，同时向中国大量倾销失去艺术价值的天价艺术品，掠夺中国改革开放 30 年以来积攒的财富。

「建立一个具有充沛流动性的文物艺术市场，向欧美等国建立的定价体系提出挑战，是争夺文物艺术品定价权的有力途径。这就势必要打造良好的金融环境和制度环境，允许区块链等机制创新。」有高层专家表示。

一直以来，市场监管落后，原有利益势力强大，行政力量无法遏制文物艺术品的混乱现象。国家支持文化艺术发展的政策非常多，文化产业上升为国家的战略方向，然而配套服务跟不上，无法落地。

监管滞后的连锁反应是艺术品金融服务配套政策严重滞后，跟不上社会创新的步伐，监管机构的水平跟不上“互联网+”的时代需要。既然国家提倡“互联网+”，就要允许交易在线化、数据化，只有在线，才能使数据沉淀，挖掘和使用才能带动产业，监管应该在国家提出的创新政策的大背景下进行有效的监督管理。

懂金融的不懂艺术，特别是金融机构从业人员严重缺乏文化艺术素养和情怀，导致中国艺术品资产证券化、金融化、大众化很难向前推进。中华民族九千年的文明历史，有大量传承有序的文化艺术资产，一旦资产证券化，对中华民族伟大复兴将是战略力量。习近平总书记一再强调让沉睡在博物馆、祖国大地上的文化产品活起来，目的就是要借助全社会的力量、社会大众的力量，推动其文化价值实现倍增。3

当国家政策落实以后，宝链将以全新的模式，创造出符合中国国情的金融环境、文化环境、市场环境，带领「优质艺术品」集体回归国内金融资本市场。宝链将代表中国，争夺国际文物艺术品的定价权，可提高中国的国际影响力，提升中国在文化、旅游、出口等市场的竞争力，最终体现在提升中国的综合国力。