Huobi

HUOBI CHAIN WHITEPAPER

火币公链白皮书

火币公链

Version 1.0 / 2018.12

摘要

随着金融科技的发展，传统的信息互联网开始逐渐向以区块链技术为基础的价值互联网演变。目前，数字经济正在高速增长，并逐步渗透至其他经济领域中，或将改变现有经济发展方式、重塑世界经济格局。

火币深耕于数字资产市场，在数字资产的全周期操作中积累了丰富的经验，取得了一系列的阶段性成果。为满足用户在资产安全性、交易便捷性、投资多样性、法律合规性等方面的需求，同时也为了适应数字经济在未来的发展变化，火币将携手行业领袖共同研发一条数字经济时代的基础设施公链——Huobi Chain。

Huobi Chain 以“赋能实体经济，推动数字经济发展”为愿景，以“公开透明、共建共信”为宗旨，从火币生态业务出发，向数字化世界的无限空间进行探索。在未来业务发展上，主要集中在以下三个方面：

首要目标：在透明和可监管的前提下，实现资产交易的清结算

目前，数字资产交易所的透明度不高，用户资产的安全保障存在隐患；另外，交易所一直备受质疑的非法交易和洗钱问题，也阻碍其长远发展。因此，Huobi Chain 将通过交易上链和引入监管节点的措施解决上述问题。

未来愿景：支持复杂业务流程和多元化资产上链

数字资产市场仍处于初级阶段，资产种类相对单一、业务流程尚待规范，还无法满足更多样的需求。为此，Huobi Chain 将开发新型通证合约，以支持复杂业务流程和多元化的资产类型。

价值承载：火币的生态业务

为保证 Huobi Chain 的持续发展和经济价值， Huobi Chain 在初始阶段将以火币现有的生态业务为承载；在社区生态和技术基础发展成熟后，Huobi Chain 将面向全球拓展更为广泛的业务场景。

为实现以上设计理念，Huobi Chain 在技术上将引入以下特性：

- **资产上链，安全为先：**Huobi Chain 将安全作为架构设计的首要因素，并进行严格的安全审计和智能合约安全测试。
- **双“链”合璧，动态协同：**交易链负责交易清结算，追求交易速度更快、频次更高、手续费更低；合约链则支持金融合约、业务合约等复杂应用。
- **多元需求，生态闭环：**Huobi Chain 将借鉴传统金融市场的业务模式，为多元化的需求提供基础设施，构建并逐步完善数字身份体系，为多样的市场参与者提供精准的需求匹配。
- **透明可信，监管保障：**除了秉承区块链的分布式治理、信息公开透明等特性外，Huobi Chain 还将可监管性作为设计目标，旨在为用户提供更强有力的监管保障。

Huobi Chain 的健康发展离不开社区的治理。为了兼顾治理的去中心化和有效性，Huobi Chain 将结合链上治理与链下治理，把人与代码同时引入到公链的复杂治理体系中：

- **链上治理：**采用全体通证持有者协商投票的方式选举超级节点；设立“社区章程”，实践“代码即法律”的区块链治理理念。
- **链下治理：**在区块链社区开创性地引入“现代经理人制度”，理事会负责社区重大事项决策，执行团队负责具体工作开展，并接受专家顾问团的监督指导。

Huobi chain 将成为物理世界向数字世界的连通器，让更多可想象的场景在比特化的平行域中实现！

目录

01 背景介绍

1.1. 数字经济基础设施

数字经济是以数字化的知识和信息为关键生产要素，以数字技术创新为核心驱动力，加速重构经济发展的新型经济形态。数字经济是继农业经济、工业经济之后更高级的经济形态，也是新一轮竞争中的制高点。在数字经济建设中，区块链是重要一环。目前，区块链行业仍处在早期发展阶段，基础设施尚未成熟，基于区块链的服务、应用和商业模式仍有许多难题需要攻克。为了寻求更大的突破，火币将开发适用于数字经济环境下的基础设施公链——Huobi Chain。

作为面向未来数字经济的公链，Huobi Chain 致力于满足行业级和企业级的应用、支持各种复杂场景。为此，Huobi Chain 将由以下三大支柱构成：统一的高技术标准、跨链技术、监管与测试平台。

（1）统一的高技术标准

建立标准是基础设施要解决的核心问题。统一的技术标准能够促使行业形成集聚效应，从而推动数字经济在全球范围内的发展。从广义来看，高技术标准需要满足以下条件：

- **更高的性能**

吞吐量的局限性是现阶段区块链技术难以被大规模商业应用的主要限制因素之一。以比特币为例，比特币每秒所能承载的交易量约为 7 笔，而为确保交易被记录在链上，还需等待约一小时的确认时间，这样的交易速度很难满足大规模商业应用。为了满足数字经济时代的应用需求，基础设施公链至少需要达到每秒万级别交易处理速度。

- **更高的隐私保护**

目前，主流区块链还未实现真正意义上的匿名性。这是由于交易地址、交易时间和交易金额等链上信息对所有人公开，人们凭借种种蛛丝马迹可将用户的钱包地址与真实身份相关联。在数字经济时代，用户需要把很多重要信息、数据上传至链上才能进行交易或运行智能合约。确保信息、数据的处于匿名、非公开状态变得至关重要。因此，未来的公链可以采用非交互零知识证明技术或在数据上链前进行加密的功能，以满足用户

对隐私保护的要求。

- **更高的安全性**

数字经济时代的公链将面向更多的用户，其必须在安全审计、安全架构、编译器安全优化、虚拟机安全设计、合约安全模板等方面达到更高的标准，以满足用户对安全性的要求。

（2）跨链技术

未来，区块链技术将被运用在更多领域中。从货币到商品、从房产契约到权益类凭证，更多资产或数据信息将可以被通证化（Tokenization），并在区块链系统中进行交易和管理。随着交易量的增加和需求多样性的扩展，多链并行必将成为趋势。因此，跨链技术必不可少，以支持不同区块链的信息交互和资产转移，同时兼顾系统的效率与延展性。

（3）监管与测试平台

技术是把双刃剑，为了防止利用技术手段作恶、避免可能存在的漏洞被人滥用造成用户的大量损失，基础设施公链需有相应的设计，在保护隐私情况下实现可监管。Huobi Chain 将建立严格的 KYC（Know-Your-Customer）和 AML（Anti-Money Laundering）标准对用户数字身份信息进行审核，并且设置监管节点对链上信息进行监督。此外，Huobi Chain 还将搭建智能合约自动化验证平台以保证合约应用的安全性。

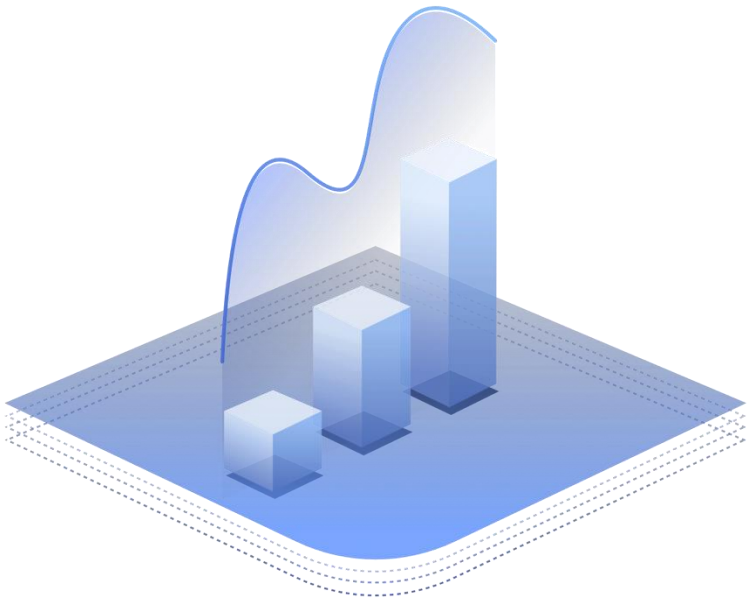
1.2. Huobi Chain 愿景

火币自 2013 年创立以来，一直秉承“让金融更高效，让财富更自由”的使命，并始终将“用户至上”作为公司发展的核心理念。经过五年与用户的风雨同舟，火币已经发展为全球领先的数字资产金融服务商，形成了以数字资产交易平台火币 Global 为核心，以各国交易所与火币生态、火币区块链应用研究院、火币资本、火币 Labs、火币矿池、火币资讯、火币钱包等为集团内生态节点，并且以火币生态火伴为集团外生态节点的全产业生态布局。

随着区块链技术的不断发展，火币未来的形态更可能进化为一种全新的分布式体系，所有资产与权证的生成、流转、公证与确权都在公链上进行。火币正在进行逐步将业务开放到社区进行自治的生态化尝试。但当前区块链底层基础设施尚未成熟，全产业依旧

处在受制于区块链技术性能与可拓展性缺陷的阶段。因此，火币在经过深入论证后，决定致力于开发出一条代表全球行业最高水准的数字经济时代公有链——Huobi Chain，以支持未来世界的底层运转。

在即将到来的数字经济时代，Huobi Chain 以“赋能实体经济，推动数字经济发展”为目标，定位于数字经济时代基础设施公链，追求更高的性能、稳定与安全，为交易清算、支付、资产管理、证券等各种复杂场景提供计算与存储等基础设施，旨在成为数字经济时代公有链的标杆。



02 技术介绍

2.1. 设计理念

“以交易为起点，以实现复杂业务流程及多元化资产上链为愿景，以火币生态业务为承载”

作为面向数字经济时代的基础设施公链，Huobi Chain 旨在利用区块链技术优化火币在不同时间段、不同领域的战略布局，为火币在数字时代中的产业发展助力。

首先，Huobi Chain 通过交易上链，实现在透明和可监管前提下的数字资产交易和清结算。具体而言，在透明度设计方面，通过技术手段，实现交易委托账本（order book）、限价单、结算的上链，使 Huobi Chain 可以自证无权使用交易资产；在监管方面，Huobi Chain 增加了监管节点，在保护用户隐私的前提下保证监管节点可追踪交易，查看资产溯源；在交易和清结算方面，为实现链上高效交易，交易链上将增加做市机器人撮合交易，以提高流动性。

其次，随着公链在交易方面的设计完成，为适应数字经济在未来的发展，Huobi Chain 将支持复杂业务流程的链上处理及更丰富的资产类型登记上链。现阶段，数字资产市场仍处于早期阶段。截至 2018 年 11 月，数字资产市场的总市值约为 1300 亿美元，而同期苹果公司的市值就达到了 8000 亿美元；同时，相比于股票市场，数字资产的设计也较为单一，可以说数字资产市场无论从规模还是从产品来讲仍有较大的发展空间。随着社会经济的进一步发展，更多资本市场的成熟模式也会逐渐与通证经济相结合。在不久的将来，从货币到商品，从房产契约到各类金融资产，将会有更多资产可以进行通证化（Tokenization）。现实世界中的资产以通证的形式映射到数字世界，可在区块链系统中进行交易和管理，数字资产的市场规模也将迅速扩大。为此，Huobi Chain 将开发新型通证合约，满足增发、并购等复杂业务场景的需要。

最后，Huobi Chain 也将会成为火币全产业生态的底层支持。火币诸多业务例如超级节点投票、火币矿池、火币钱包、火币生态基金等均可进行上链处理；而火币在人才、法律方面的业务布局，也可基于 Huobi Chain 开发相应的 DApp。在 Huobi Chain 的社区生态和技术基础发展成熟后，将面向全球拓展更为广泛的业务场景。

2.2. 技术架构

Huobi Chain 首创双链架构，构建交易链和合约链双链并行的模式，并通过跨链技术实现双主链间的信息交互。双链架构确保 Huobi Chain 系统能够兼具高扩展性、高安全性和高效率。Huobi Chain 系统架构如图 1 所示。

交易链不需要支持智能合约，对于金融领域的具体需求可以通过增加金融相关的特殊交易来实现，从而可以在一定程度上提高 TPS，以满足交易上链中高速、高频、低手续费的需求；合约链主要支持智能合约，对 TPS 的需求较低，以实现在合约上链时的复杂交易、业务合约、金融合约、逻辑和验证内容。

无论是面对高并发、高 TPS 的业务，还是面对高扩展性、强智能的业务，Huobi Chain 都能游刃有余，从而真正落实区块链赋能实体经济的理念，使 Huobi Chain 成为构建数字经济的基石。

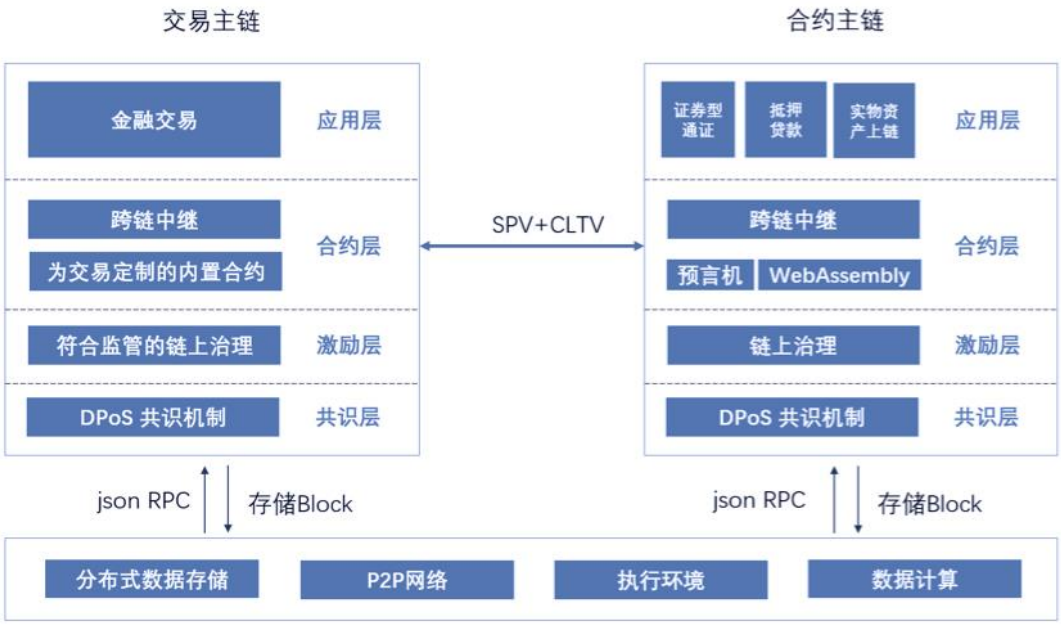


图 1　Huobi Chain 系统架构

2.2.1. 区块链系统

（1）区块链基本概念

■ **哈希函数**

密码学哈希函数是区块链的基础，保证了系统中的信息不能被篡改。简要而言，哈希函数能在合理的时间内，把任意长度的输入通过散列算法，变换成固定长度的输出。要使哈希函数达到密码层面的应用，必须满足以下特性：定义一个哈希函数 Y=H（X），①对于任何输入 X，H(X)长度永远一致；②根据输入值 X 能算出输出值 Y，但根据输出值 Y 无法算出输入值 X；③无法找出两个输入值 X 和 X'，使输出值 H(X)和 H(X')相等；④谜题友好性。

其中，性质②保证了信息的隐密性。性质③保证了哈希函数值具有不可篡改的特性。信息如果被篡改，那么整个哈希值会完全不同。在性质②③的前提下可以引申出性质④谜题友好性。我们设输出值为 Y，已知的输入值 M，要找到谜题的未知输入值 X，使 Y=H（M || X）成立，唯一的方法是尝试所有的可能输入值 X。例如 Y 是一个 200 位的二进制数，如果使用暴力破解，Y 所有的情况共包括 2^200 中，对 X 进行随机选取，在最差的情况下，要经过 2^200 次哈希运算，才能得到一个满足要求的哈希值。X 的随机性特征保证了求解过程除上述方法外，没有更好的办法。

■ **区块链**

区块链是使用哈希指针形成的一种链式数据结构，区块之间互相链接一直延续到创世区块，一个区块包含一段时间内的交易信息，因此区块链包含了所有的历史交易信息，如果黑客想篡改区块链中的数据，那么前一区块的哈希值将不会与该区块的哈希指针匹配；当然，黑客也可以通过篡改前一个区块的哈希指针来进行掩盖，但他会发现修改到区块链的头部——创世块时会遇到麻烦，因为创世块一般存储在黑客无法改动的地方。

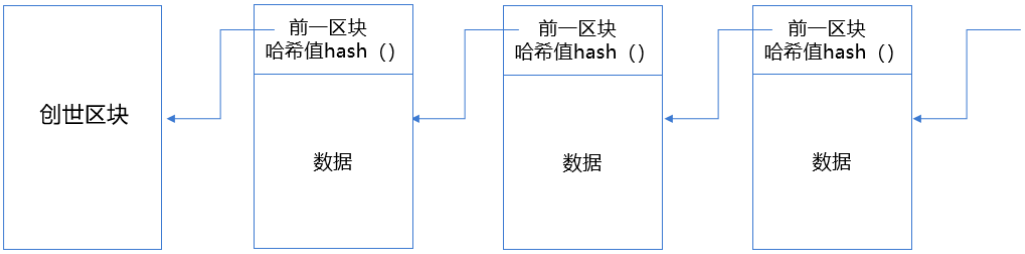


图 2 区块正常生产流程示意图

■ **账户设计**

不同于比特币区块链，Huobi Chain 引入了多重签名账户模型的设计。比特币没有账户概念，每个用户的余额都是从区块链上的 UTXO（未花费的交易输出）计算出来的，所有合法的比特币交易都可以追溯到前一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。所有的未花费输出即为整个比特币网络的 UTXO。在 Huobi Chain 上，每一个地址对应一个账户，而全局状态就是由账户地址和账户状态的一个映射组成，该映射被保存在 Merkle 树的数据结构中。由于 Huobi Chain 拥有账户的概念，使得它在交易的可视化和查询账户状态方面具备实时性，可根据一个地址情况实时查看当前账户情况以及交易状态。

（2）数字签名技术

数字签名是区块链的重要组成部分，保证了区块链系统的安全性。数字签名有两个重要特性，第一，只有所有者可以制作自己的签名，但任何看到它的人都可以验证其是否有效；第二，该签名只与某一特定的文件发生联系，该签名不能用于表明所有者支持另一份不同的文件。

数字签名方案由以下三个算法构成：

- ✓ （sk，pk）：=generateKeys（keysie）；generateKeys 方法把 keysize 作为输入，来产生一对公钥和私钥。私钥 sk 被安全保存，并用来签名一段消息；公钥 pk 是任何人都可以找到的，可以用来验证签名。
- ✓ sig：=sig（sk，message）；签名过程是把一段消息和私钥作为一个输入，对应的消息输出是签名。
- ✓ isValid：=verify（sk，message，sig）；验证过程是通过把一段消息和签名消息与公钥作为输入，如果返回的结果是真，证明签名属实；如果返回的结果为假，证明签名消息为假。

同时，要求有以下两个性质，

- ✓ 有效签名可以通过验证，即： Verify（pk，message，sign（sk，message））==true
- ✓ 签名不可伪造。

（3）共识机制的选择

公链共识机制的选择会考虑多方面的因素。首先，共识机制一般遵循 CAP 原则，即一致性（Consistency）、可用性（Availability）和分区容错性（Partition tolerance）三者难以同时达到最优。其次，在选择和设计共识时，也需要考虑共识的基础性质：(a)可认同（agreement），所有诚实节点都认同一个结果；(b)值合法（validity），认同的结果必须是一个合法的；(c)可结束（termination），在一定时间内一定达成共识，而不会无休止地进行下去。

从理论与实践相结合的角度出发，Huobi Chain 的合约链和交易链均选择 BFT-DPoS（Byzantine Fault Tolerance - Delegated Proof of Stake，拜占庭容错式的委托权益证明机制）作为共识机制，具体考量因素如下：

一是基于火币业务具体需求。

Huobi Chain 为实现支持交易清算、资产上链等多功能的目标，其系统的可用性需要排在首要的地位。具体在 CAP 原则中，Huobi Chain 的设计需要保证系统的可用性和分区容错性，对于一致性可以做适当的妥协。对于强一致性方面不需要保证，只需要最终保证一致性即可，BFT-DPoS 机制的特点正与之相契合。

二是出于提高效率、降低能耗考虑。

现有区块链项目的主要共识机制为 PoW（Proof of Work，工作量证明机制）、PoS（Proof of Stake，股份证明机制）和 DPoS（Delegated Proof of Stake，委托权益证明机制）。从效率和能耗角度考虑，PoW 和 PoS 机制在设计层面均存在部分问题。

PoW 机制的问题主要存在于算力中心化以及能耗。一方面，PoW 机制是通过节点的计算能力来进行算力竞争，随着 CPU 挖矿逐渐升级到 ASIC 矿机挖矿，出现了算力中心化的趋势，这与区块链去中心化的理念相冲突；另一方面，PoW 浪费了大量的电力进行运算。PoS 机制在能耗方面有所改善，但是在中心化方面仍然存在隐患。具体而言，PoS 机制会出现持有币越多的人会获得更多的币奖励的趋势，整个网络可能会随着运行时间的增长而越来越趋向于中心化。因此，PoS 机制虽然相对于 PoW 节省了能源，但是其底层依然依赖于 PoW，同时也没有很好地提升性能和安全性。

DPoS 机制类似股东大会选举产生董事会的制度，引入了超级节点选举机制。这一设计机制使得区块的生成更为快速、节能。此外，DPoS 机制充分利用了持币人的投票，

以公平民主的方式达成共识。投票选出的 N 个超级节点，权利完全相等，并且持币人可以随时通过投票更换超级节点。尽管 DPoS 机制仍然存在中心化，但是这种中心化是受到控制的，因为每个用户都有权利决定哪些节点可以被信任。DPoS 机制理论上能达到万次每秒的交易速度，在网络延迟高的情况下亦可达到千次每秒级别，更适合企业级的应用。由于 Huobi Chain 旨在服务数字经济，对于可信环境下的数据交换和计算及其稳定性要求极高，因此 DPoS 是更合适的选择。

三是性能提升需求。

DPoS 虽然在性能方面较其他机制相对优越，但是其高性能是建立在低故障和低延迟的基础上。然而现阶段的应用场景很难保障长时间的低故障和低延迟。因此，非 BFT 的 DPoS 机制可能出现潜在的问题。

在 DPoS 算法中，区块生产者们在一定时间内轮流生成一个区块。假设没有节点错过自己的轮次，那么将产生最长链。区块生产者在被调度轮次之外的任何时间段出块都是无效的。

不过可能存在恶意或故障节点创建少数分叉的情况。为了确保诚实节点所在的链成为最长链，要求诚实节点的数量占总数的 2/3 以上。例如，一共有三个节点 A、B 和 C，其中 A 和 C 是诚实节点，而 B 是恶意节点，在 DPoS 下产生一个区块需要 2 秒，那么恶意节点 B 每 6 秒只能产生一个区块，而诚实节点每 6 秒能产生 2 个区块，因此诚实节点所产生的链永远比攻击链更长，具体如图 3、图 4 所示。

图 3 一般 DPoS 共识机制下区块正常生产流程示意图

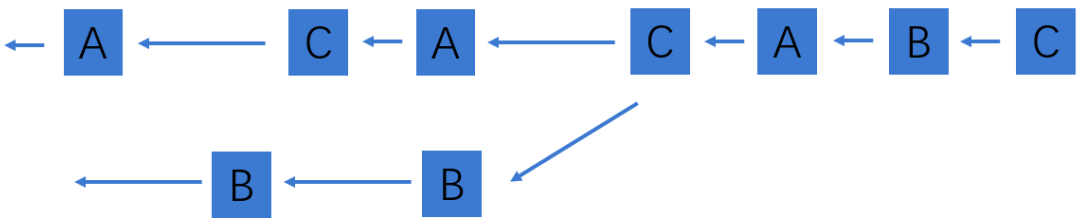


图 4 一般 DPoS 共识机制下少数节点分叉示意图

同样地，考虑其他故障场景：比如离线少数节点的双重生产、网络分片化、在线少数节点的双重生产、法定超级节点数不足、多数生产者舞弊等场景[1]，均要求诚实节点的数量需要占总数的 2/3 以上。

因此，在传统的 DPoS 机制下，为了防止出现分叉，保证交易的不可逆，需要 2/3 的超级节点通过在该区块后继续生产区块的方式进行确认，比如一个系统中有 18 个超级节点，每两秒产出一个区块，那么要达到交易不可逆就需要继续在后面产出 12 个区块，共需要 26 秒（1+12 个区块）。

为了提升 Huobi Chain 系统的性能，可以在原 DPoS 的基础上引入 BFT 协议，实现在产生区块时完成对区块签名的确认，缩短交易不可逆所需要的时间。具体而言，超级节点将交易打包成区块后用自己的私钥对该区块签名，并广播到所有节点，当超级节点收到至少 2/3 的其他超级节点的签名区块后，该区块就完成了所有节点的验证成为不可逆区块加入到区块链中。由于每次区块在生产后立即进行全网广播，新区块链的生产和旧区块确认的接收可以同时进行，因此，一个区块从产生到成为不可逆区块，最长只需要区块产生的时间加上其他超级节点签名确认的时间（据 EOS 团队测试该过程可在 1 秒内完成），继续上文的例子，则仅需 3 秒的时间。

在 BFT-DPoS 机制下，系统的出块间隔的缩短，使跨链通信的时延减小，同时单位时间内可确认的交易数量得到提升，提高了区块链系统的整体性能。

超级节点数量的确定

在实际操作中，关于 Huobi Chain 超级节点数量的确定，在交易链和合约链上有不同的标准：

A. 交易链由 Huobi 自有节点和监管节点组成，根据吞吐量需求来配置相应数量的节点，节点设备配置的性能以及节点的通信方式都受到吞吐量的制约；

B. 合约链通过社区投票选举超级节点，节点数量可参考 EOS 的设计初步设定为 21 个，或者根据 Huobi 社区对出块节点设备性能的考虑以及对通信方式的选择来确定最终的节点数量。

[1] DPoS 下每种故障场景的分析详细可见 Dan Larimer 所写的《DPoS 共识算法 - 缺失的白皮书》。

（4）合约层设计

Huobi Chain 的合约层由多个为交易而定制的内置合约、智能合约构成，并在此基础上实现跨链中继，从而使得 Huobi Chain 双链之间实现可信的跨链交互。

Huobi Chain-VM 使用 WebAssembly（WASM）执行智能合约。WASM 可支持多种编程语言，采用二进制编码，占用存储空间更小，且在程序执行过程中的性能优越。

WASM 会生成中间语言——字节码，可以使用 Huobi Chain 提供的编译工具进行编译。调用合约时，部署接口将字节码部署在链上。成功部署后，区块链上会创建一个智能合约账户，账户中存储了合约的字节码和对应的 ABI（Application Binary Interface）。用户通过指定的合约账户名以及合约方法，利用 ABI 和智能合约交互，实现对智能合约的调用。

最后，为了防止合约逻辑执行失败产生的问题，Huobi Chain 将参考以太坊的流程，使用 require 和 assert 解决。

2.2.2. 双链架构

双链结构主要是根据现有工程实践案例的相关设计，例如 thunder network 的快慢链解决方案，该方案可以追溯到 BTC 时期。BTC 的主要功能为支付结算，但受限于 10 分钟的出块时间，在实际应用中用户体验较差，因此需要一层 hub-based network 来做相对更快的结算。lightning network 作为第二层解决方案在保障 BTC 主链结算功能的同时，也增加了可扩展性。可以看到 lighting network 通过 4000 多节点以及 12000 多个通道维护了 450 个 BTC 的网络交易。基于这个技术解决案例，我们可以在公链的初始设计中，通过双链结构保障结算功能的同时增添可扩展性，而在其中，就需要设计相关的结算公链以及扩展公链的功能，并在连接通道上使用到 SPV（Simplified Payment Verification）和 CLTV（Check Lock Time Verify）作为主要跨链方式。

由于 Huobi Chain 的首要目标是保证高速交易，但智能合约对系统内有效资源的消耗较大。为了在快速结算的同时保证合约的广度，Huobi Chain 在设计中将采用双链架构，分成交易链和合约链两部分：

交易链：提供支付结算功能，如挂单、撮合、深度等功能都由其负责；

合约链：支持智能合约，满足复杂场景的应用，提高公链的扩展性。

其中，合约链上的交易需要登记到交易链上，Huobi Chain 会提供跨链中继来实现，而合约链上会提供一个统一记账的内置合约来负责接收。

具体而言，在区块链中，要保证高速特性就需要对交易 KV 对（Key Value Pair）进行精简，同时对相关节点的机器进行优化，否则区块链网络的交易处理能力（TPS）就会因为在传输、打包时间上的损耗而降低。由于 Huobi Chain 在设计上要求引入多种功能特性，需要基于非图灵 script 或者更高级的虚拟机部分的支持，以及将一些可内置化的特殊交易以较低的成本在终端实现。如果采用 gas limit 或者控制节点机器的方式，当任何 DApp 受市场追捧而大热时，势必将会影响到整个公有链的运行，因此 Huobi Chain 将采用双链架构设计。此外，为了保证双链数据的可用性（尤其是合约链上数据的可用性），Huobi Chain 将使用 SPV 验证+类 HTLC（Hashed Timelock Contracts）主链锁定的跨链技术方式，在合约上将使用主链的 Token，交易链主要保障 KV 对，合约链上的 balance 只有交易链通过 SPV 后才会产生，但合约链只有返回的交易，交易链只有进入合约链的交易。综上，Huobi Chain 将通过双链的架构设计和上述跨链技术，保证合约链的使用对交易链的 TPS 不会产生影响。

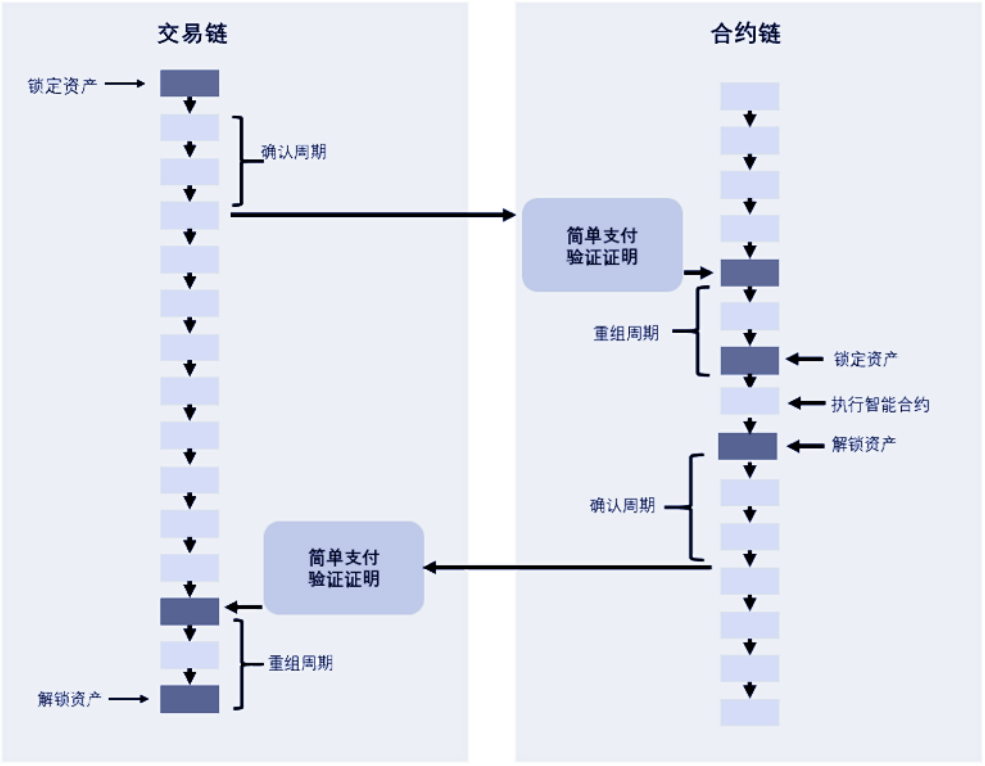


图 5　Huobi Chain 跨链交易实现示例

Huobi Chain 的双链架构优势显著：首先，基于链中的所有交易，都可以看作全局变量的更改，此时可采用静态的方式来保证一定作用域，在未来有更多的作用域时就可

以用同样的跨链协议进行联系；其次，在合约链拥有 SPV 之后，支付在合约链和主链进行验证的步骤可异步，大幅加强了使用性以及延展性。例如，当一个合约链被几个应用占满时，可通过同样的结构开启另一条合约链。

2.3. 技术实现

2.3.1. KYC&AML

（1） 数字身份

在 Huobi Chain 的交易链上实现 KYC 和 AML 管理，首先必须在链上建立一个可信的数字身份标准 H-UID(Huobi Chain - User Identity)。H-UID 具有唯一性，各国公民经过 KYC 身份验证后将个人信息登记上链，用户可基于 H-UID 对自己的个人信息和数字资产进行管理。

H-UID 由以下几个部分组成：

A. 基础信息，如姓名、性别、国籍、证件类型、证件号码、联系方式等；

B. 高级信息，如信用、教育、工作、社交等相关数据；

C. 数字资产信息，个人持有的数字资产情况；

D. 账户公私钥，用于对 H-UID 的数据进行签名、加密和授权。

注：机构账户须与法人身份相关联，一个法人可以注册多个机构账户。

（2）H-UID 的创建和验证

用户自行提交信息创建 H-UID，由监管节点对信息真实性进行验证，验证通过后对验证内容进行签名，个人信息经过加密后登记上链。在 H-UID 的验证周期上，在需要用到的 H-UID 的时候触发验证判断，重新验证周期为 6 个月，一般情况下则不需要验证。

（3）数据授权

为了更好的保护个人隐私，除监管节点有权查看 H-UID 的个人数据外，其它任何

人或机构只有在获得本人授权的前提下方可查看他人 H-UID 的数据。用户在授权他人查看数据时，可以将授权用户、授权时间、具体用途等要素在智能合约中进行设置，并且要求被授权人只能在可信执行环境中使用相关数据。所有查询记录都会在链上登记，以便追责。

（4）安全保护

为了保护用户的身份信息安全，在 Huobi Chain 上，用户丢失了数据私钥不会丢失身份，可以通过监管节点验证身份后并重置数据私钥；为了防止私钥被盗取后在全网公开，用户本人也可以对私钥进行修改。

2.3.2. 跨链技术

Huobi Chain 采用的是双链结构，因此涉及跨链技术。Huobi Chain 将开发 H Protocol，即使用 SPV 验证+类 HTLC 主链锁定的跨链技术方式，传统的 SPV 验证模式往往存在确认时间太长而造成效率低下的现象，但 Huobi Chain 采用了 DPoS 机制，巧妙地改善了这一问题，可完成对跨链交易的极速验证。

以交易链上的两个用户 UserA 和 UserB 为例，其中 UserA 和 UserB 拥有一定数量的 Token。UserA 和 UserB 达成了某个协议（如跨链数据转移），随后 UserA 需要抵押一定数量的 Token，并利用一个侧链完成此协议。协议中约定， UserB 在完成某项任务之后（如完成跨链数据转移）可以在侧链上获得 UserA 所抵押的 Token。在该过程中，UserA 可随时查看所抵押 Token 的剩余数量， UserB 也可随时可以查看自己可改范围内的剩余数量。且 UserA 可随时决定终止整个协议，在 UserA 终止协议后，抵押剩余将返回到 UserA 的主链账户中，UserB 也将获得在这个协议过程中所扣除的 UserA 的 Token。

例如，初始情况下， UserA 和 UserB 拥有的通证数量为{UserA:1000, UserB:0}。首先， UserA 启动该协议并生成一个侧链；然后，UserA 和 UserB 达成一个跨链数据转移协议， UserA 抵押 100 枚通证到侧链中。UserB 完成了部分跨链数据转移之后扣除了侧链上的 10 枚通证。完成了上述过程之后， UserA 发现不需要继续转移了，选择终止这一次协议，侧链上通证的转移将会同步到主链上。最后，UserA 撤销了整个侧链。整个过程中 UserA 和 UserB 的资产变化如图 6 所示：

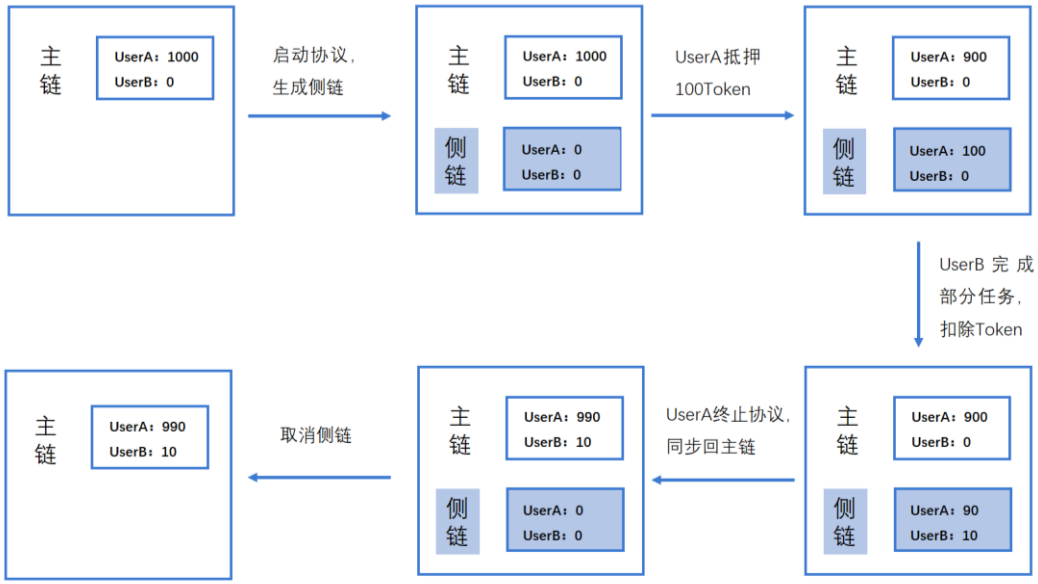


图 6 跨链协议工作流程图

上述示例是简单的 UserA、UserB 之间的合约。我们可依照相同的方法将该协议应用到多方角色中（UserB 可以是多个用户）。下面以一个具体的示例来描述整个协议工作的过程：

A. 初始化：假设有四个用户 A,B,C,D，用户 A 发送特殊交易 Tx.init ，初始化一个数据，包括权限表 {用户 B: modify，用户 C: modify，用户 D: readonly} 和抵押列表 {用户 B: 100,用户 C: 50 }（即面向用户 B 抵押 100Token，面向用户 C 抵押 50Token）。特殊交易过程中 用户 A 的 150 枚 Token 被锁定(扣除)，其值即为抵押列表的和；

B. KDC（Key Distribution Center，密钥分发中心）取这条 Tx.init， 保存好文件 ID， 包括权限表{用户 B: modify，用户 C: modify，用户 D: readonly}和抵押列表{用户 B: 100，用户 C: 50}；

C. 用户 B 向 KDC 发送修改 HTTP 请求 req-write，KDC 根据权限表判断拥有权限，将 用户 B 的修改记录，返回成功；

D. 用户 C 向 KDC 发送读取 HTTP 请求 req-read，KDC 根据初始值和所有的修改，计算出最终的值，返回给 用户 C；

E. 用户 A 向 KDC 发送终结 HTTP 请求 req-terminate，KDC 停止为请求的 fileid 服务，然后，KDC 发特殊交易 Tx.terminate，将 用户 A 剩余的抵押金额返还，将抵押列表的用户金额增加。

2.3.3. 分布式存储

目前，分布式存储是新公链的必备模块。由于 EVM 的 4700000 的 gas limit per block 只能容纳 62kb 的存储空间，远不能满足用户建立静态链接或存储文档原件上链的使用需求，而分布式存储可为不同场景下的需求提供适当的选择，通过把数据在链外进行分布式存储的方式，既能做到主链存储资源的合理利用，也能让数据在隐私存储和公开访问上有所选择。

为此，Huobi Chain 使用第三方开发的去中心化存储来加快开发。为了保障用户的安全与隐私，Huobi Chain 要求第三方提供的去中心化存储使用无服务器交互系统的存储架构方案。

选择上述方案主要基于以下几点：(1)若只涉及用链，则需要提供能被验证的明文，即公开整份文件给全体用户；（2）若仅用 A 的密钥对进行加密，则只能每次对 A 进行询问后才能查阅合同，会存在合同不被承认的单点故障风险；（3）若只用分布式存储，则文件（作为分布式网络资源）还是以明文的形式存储在各个节点中，这种场景一般发生在网页资源分布式存储当中，针对直接访问资源的场景，通过明文访问可以保证无服务器的资源服务系统，但在交互上依旧存在全部明文可见或是只对 A 可见的问题，A 的文件还是存在出现单点故障的风险。

在第三方提供的分布式存储实现路径上，Huobi Chain 要求使用 DHT（分布式哈希表）作为 P2P 通信结构，这也是分布式存储非常成熟的技术解决方案。具体而言，Huobi Chain 要求使用 PoR（Proofs of Retrievability）中的 sentinel（SPoR）来提供定时存储心跳，保证文件可以在上传之后被取回；通过对 sentinel 进行区块链版本的工程优化生成指纹组，并通过相关的心跳产生时间属性提供给链端以保证区块演进。DHT 作为解决 trackerless 运用的最广的方案，已经成熟使用在 BitTorrent、电驴 (kad network)、以太坊（只包含通信寻找邻居部分）中。

Huobi Chain 将沿用第三代 DHT—Kadmilia 作为 P2P 覆盖网络的结构，全网采用分布式存储 Key Value 的方式进行设计，通过 Key 进行精确查找，通过多次异或距离跳转寻址最终进行下载，能保证具有 2 的 n 次方个节点的 Kad 网络在最坏的情况下最多通过 n 步就可以找到被搜索的节点或值。而在保证下载方面，PoR 也是云存储中保证数据完整性的方法。相较于 PDP，PoR 除了确保数据的完整性之外，还能确保数据的可恢复性。

2.3.4. 监管节点

监管节点主要存在于交易链中，合约链中不引入监管节点。区块链的节点可以简单分为两大种类：全节点（非挖矿）以及出块节点。全节点主要功能是为签名方交易和下载区块以保证区块链系统的可用性。出块节点的主要功能是验证、打包区块，并允许其他全节点下载区块。

基于技术特点，在设计时监管节点只能放在出块节点中。因为全节点已经下载了区块，即便是对区块的读取做一些特殊操作，对于不希望被监管的交易也可以通过技术方法回避。针对写入节点的监管相对容易，只要区块在打包之前将相关需要监管的模块用监管密钥进行加密即可：通过对 memory pool 的设置，普通出块节点和监管节点在打包的过程中都能看到源交易，而上链后，普通出块节点只能看到监管节点区块内容的子集合。这样既满足监管节点能查看所有信息，且仅有监管节点能查看这些信息（非监管节点不能查看），也保证了相关信息的每一次记录都在链上，以方便不同监管机构进行监管。

在 Huobi Chain 的交易链上，出块节点主要由火币和监管部门的节点构成，而一般出块节点为火币控制的节点。在具体实现上，监管节点主要有以下三个功能：

- ✓ 监管节点可查看 KYC 信息与区块链地址的对应关系，通过 KYC 信息本身（例如姓名、照片、身份证号等）去中心化存储以及 KYC 生成相应的一系列区块链地址，实现对应关系上链；
- ✓ 监管节点可对交易委托账本（order book）进行验证，主要通过涂污上链的方式实现，即将数据先加密再上链，监管节点有相关密钥可以随时查看，而没有密钥的节点无法查看相关信息；
- ✓ 监管可查看资产溯源，其余节点无权限，主要通过结算涂污上链的方式实现，由监管节点验证。

为保障监管节点的接入、证实、证伪及安全性，监管节点在设计上秉持独立原则，并计划使用两套网关。在信息数据的查询和追踪上，监管节点将设计一套安全合理的管理分发机制。具体而言，Huobi Chain 会设置一个特殊的监管节点来负责其他监管节点的公钥认证授权，同时每个监管节点有自己的一套公私钥。KYC 由监管节点完成验证、签名，不需要本人授权就可以在监管节点本地的离链数据库查看用户的基础信息，但更多的链上数据如高级信息、资产数据等都需要获得用户本人的授权才可以查看。

在 Huobi Chain 上，监管方想要获取监管节点的权限和执行能力，必须对监管节

点进行维护。因为监管节点需要用自己的监管公私钥对涂污源数据进行可控的监管。若监管方不维护节点，则安全性和可控性均难以保证。

出于现实情况的考虑，初始阶段监管节点的维护由火币来代为执行。火币将会主动向监管机构提供数据，以便其进行监督。

2.4. 安全性

在数字经济时代，基础设施公链的安全性尤为重要。Huobi Chain 在安全性的设计上，主要围绕安全架构、安全审计、智能合约安全性和安全赏金计划四个方面展开。

2.4.1. 安全架构设计

在架构设计上，Huobi Chain 的核心目标是保护出块服务器的正常通信与运行，增强初始主网整体抗攻击能力与保护节点安全。为此，Huobi Chain 在架构设计上采用超级节点服务器隔离、多跳转节点和多链路通信的布局，防止 DDoS 攻击，确保超级节点不间断通信，具体架构设计如图 7 所示。

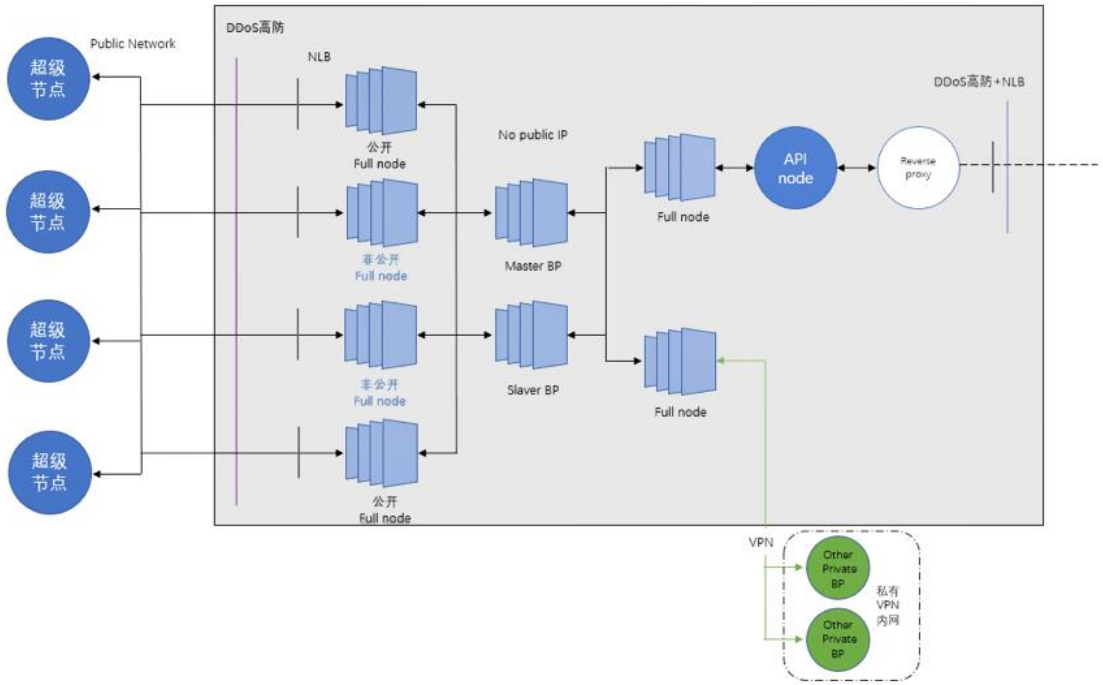


图 7 Huobi Chain 安全架构设计

正常情况下，外围节点通过对外公布的公开节点进行通信；当攻击者通过公开的节点列表攻击公开节点造成公开节点不可用时，则可通过私密节点进行通信；当公网节点均被发现，并且攻击者进行攻击导致对公网 full node 服务器全部阻塞，最后则由私有 VPN 网络在隔离的虚拟内网进行通信，保证最基础的出块正常；查询用 RPC 所在全节点与超级节点完全隔离并架设防御，保证外网对 RPC 的攻击不能影响到超级节点。

2.4.2. 安全审计

（1）审计的核心目标

在安全审计上，Huobi Chain 的审计核心目标如下：

A. 审计超级节点在公网暴露服务的安全状况，查找传统安全中的常见安全问题；

B. 审计超级节点架构的抗 DDoS 能力；

C. 针对本条公链的特性，进行定制化载荷攻击测试，检测整体框架稳健性。

（2）审计的核心方向

Huobi Chain 的核心审计方向主要包括以下四点：

A. 查找可造成整个节点停止出块的漏洞问题；

B. 架构缺陷造成的单点阻塞攻击就能导致节点瘫痪的问题；

C. 服务错误配置导致服务器可被远程攻击及控制的问题；

D. 节点敏感信息泄露（特别是服务器 SSH 连接私钥在 GitHub 上泄漏）等问题。

（3）审计内容

Huobi Chain 将以节点的自我审计为主（许多敏感的服务器与操作不应该直接暴露给第三方，需要依赖节点自我审计），安全团队提供专业的指导与协作配合，以达到最全面且高效的审计效果。

- **节点自我审计**

A. 架构审计

- ✓ 超级节点服务器是否达到与外网的充分隔离，保证若有外网恶意攻击不会直接影响超级节点服务器出块；
- ✓ 超级节点是否多链路设计，防止出现单点故障（或针对单点的 DDoS ）导致超级节点无法与其他节点同步；
- ✓ 节点是否有必要的安全加固（如是否在核心通信节点外围正确的部署高防抵御 DDoS 攻击，以及适当的部署 HIDS）。

B. RPC 安全审计

- ✓ 是否有对非必要的节点 RPC 服务进行限制；
- ✓ 若开启 RPC 服务，是否有禁用不必要的 wallet_plugin 、wallet_api_plugin 及 producer_api_plugin；
- ✓ RPC 是否启用 SSL。

C. 安全配置审计

- ✓ Active 多签密钥是否配置正确；
- ✓ 是否开启日志记录，有条件下是否开启更多安全日志记录插件等；
- ✓ max-clients 参数配置是否合理，是否易遭受 P2P 连接打满连接数，导致无法同步；
- ✓ 是否使用非 root 权限启动节点程序；
- ✓ 是否更改 SSH 服务默认端口，服务器 SSH 是否配置白名单，并且设置只允许 key（并对 key 加密）登录，禁止密码登录。

■ **安全团队审计**

A. 基础设施审计

- ✓ 服务器提供商是否是优质的安全供应商，；
- ✓ 节点公网 IP 真实开放端口服务审计，防止运维人员未正确配置服务与安全规则导致脆弱点暴露。

B. 节点脆弱性审计

- ✓ 审计节点对抗全网扫描，隐藏真实公网 IP 的能力；
- ✓ 审计节点敏感信息是否在公网上泄漏，如在 GitHub 上暴露等；
- ✓ 审计 RPC 端口是否可进行恶意调用；
- ✓ 若节点部署除区块链网络主程序外的其他程序，则针对第三方程序进行脆弱性攻防审计；
- ✓ 审计节点是否有定制合适的应急响应方案。

C. 抗 DDoS 能力审计

- ✓ 针对 P2P 端口的抗 UDP Flood 、TCP Flood 等（含各种主流反射型攻击）进行实战型测试，利用真实的攻击流量，来检验节点的的稳定性；
- ✓ 针对 RPC 端口的抗 CC 攻击进行实战型测试，利用大量攻击节点高并发请求消耗服务器性能来检测节点稳定性。

2.4.3. 智能合约安全性

为提供智能合约的安全性，Huobi Chain 将结合业务需要，开发相关合约模板，开发者可以按照合约的接口参数进行调用，对于不符合接口要求的请求会直接拒绝调用，在舍弃一定程度灵活性的基础上极大提高合约的安全性。

此外，在智能合约安全测试方面，Huobi Chain 将开发专门针对 Huobi Chain 的智能合约验证平台，做到常规漏洞自动检测，快速、准确地查找智能合约常规安全问题。在实施层面，智能合约的安全测试包括两部分：

A. 事前、事中：Huobi Chain 鼓励社区开发一个标准化 IDE，该 IDE 会进行代码自动补全和语法提示，并且能够自动整合已发现的安全漏洞并及时检查代码并指出可能存在的安全风险；

B. 事后：通过自动化扫描 Huobi Chain 的所有 DApps 的合约代码，利用自动化测试将漏洞库规则和 DApps 的合约代码进行匹配检测，并及时公布 DApps 合约代码漏洞。

2.4.4. 威胁情报赏金计划

Huobi Chain 将考虑与专业的区块链安全团队合作，实行安全赏金计划，为提供威胁情报报告的团队或个人给予一定数量的通证奖励。

■ **处理流程**

A. 报告阶段：

✓ 报告者访问安全网站，进入“赏金漏洞提交”页面，提交威胁情报；

B. 处理阶段：

✓ 一个工作日内，安全团队就收到的威胁情报进行确认并持续跟进评估；

✓ 三到十个工作日内，技术团队处理问题、给出结论并计分，必要时会与报告者沟通确认，请报告者予以协助；

C. 修复阶段：

✓ 业务部门修复威胁情报中反馈的安全问题并安排更新上线，修复时间根据问题的严重程度及修复难度而定，一般来说，严重和高危问题 24 小时内，中危问题三个工作日内，低危问题七个工作日内。客户端安全问题受版本发布限制，修复时间根据实际情况确定；

✓ 报告者复查安全问题是否修复；

✓ 报告者确认安全问题已修复后，技术团队告知安全团队处理结论和漏洞得分，并发放奖励。

■ **严重漏洞**

严重漏洞是指，发生在核心系统与业务系统（核心控制系统、域控、业务分发系统、等可管理大量系统的管控系统），可造成大面积影响的，获取大量（依据实际情况酌情限定）业务系统控制权限或核心系统管理人员权限并且可控制核心系统。包括但不限于：

A. 区块重放校验，区块不因为任何因素导致重放失败；

B. 系统智能合约溢出、条件竞争漏洞、权限控制缺陷、双花、共识层漏洞；

C. 沙箱逃逸造成节点命令执行或系统文件读取；

D. 沙箱超时检测机制绕过，造成 DDoS 本地节点；

E. 内网多台机器控制；

F. 核心后台超级管理员权限获取且造成大范围企业核心数据泄露，可造成巨大影响；

G. 通信层以较小的代价大面积 DDoS 其他全节点。

■ **高危漏洞**

A. 系统的权限获得（getshell、命令执行等）；

B. 系统的 SQL 注入（后台漏洞降级，打包提交酌情提升）；

C. 敏感信息越权访问，包括但不仅限于绕过认证直接访问管理后台、重要后台弱密码、获取大量内网敏感信息的 SSRF 等）；

D. 任意文件读取；

E. 涉及金钱的越权操作、支付逻辑绕过（需最终利用成功）；

F. 严重的逻辑设计缺陷和流程缺陷。包括但不仅限于任意用户登录漏洞、批量修改任意账号密码漏洞、涉及企业核心业务的逻辑漏洞等，验证码爆破除外；

G. 大量源代码泄露；

H. 智能合约权限控制缺陷；

I. 异常智能合约攻击，避免耗尽节点资源；

J. 通过全节点程序入侵服务器获取控制权限。

■ **中危漏洞**

A. 需交互方可影响用户的漏洞，包括但不仅限于涉及核心业务的 CSRF 等；

B. 普通越权操作，包括但不限于绕过限制修改用户资料、执行用户操作等；

C. 拒绝服务漏洞，包括但不限于导致网站应用拒绝服务等造成影响的远程拒绝服务漏洞等；

D. 由验证码逻辑导致任意账户登陆、任意密码找回等系统敏感操作可被爆破成功造成的漏洞；

E. 本地保存的敏感认证密钥信息泄露，需能做出有效利用。

■ **低危漏洞**

A. 本地拒绝服务漏洞，包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由 Android 组件权限暴露、普通应用权限引起的问题等；

B. 普通信息泄露，包括但不限于 Web 路径遍历、系统路径遍历、目录浏览等；

C. 普通 CSRF；

D. 反射型 XSS（包括 DOM XSS / Flash XSS）；

E. URL 跳转漏洞；

F. 短信炸弹、邮件炸弹（每个系统只收一个此类型漏洞）；

G. 其他危害较低、不能证明危害的漏洞（如无法获取到敏感信息的 CORS 漏洞）；

H. 无回显的且没有深入利用成功的 SSRF。

2.5. 技术优势

在技术优势上，Huobi Chain 将做到“易用性+支持活跃度+可监管+安全”，在可监管和安全的基础上，保持高性能以及增加易用性。

（1）易用性

✓ 对于用户：目前主流公链 keystore 生成本地私钥的方式会给用户使用带来一定难度，Huobi Chain 在做区块链 account 前端的时候，将采用类似于双登陆机制——keystore 针对开发人员与专业从业者，中心化的邮箱/电话账户对应 keystore 生成对应从互联网转过来的用户；

✓ 对于开发人员：为使技术人员在开发智能合约时能使用更简单的组件，即通过简单地拼接 template 就能写出常用的智能合约，Huobi Chain 将在设计上把常用智能合约进行分类，通过模块化的方式提供在 template 中。

（2）支持活跃度

- ✓ 开发环境和工具：基于 WASM，用户可使用 C、C++、Rust 等多种语言编写智能合约，并且存储成本低，性能高效；
- ✓ 高 TPS：Huobi Chain 通过 BFT-DPoS 机制，有望实现万级 TPS，实现低延迟的实时区块写入和查询，出块速度可达秒级；
- ✓ 资产上链：实现各种资产的上链。

（3）可监管性

- ✓ KYC&AML：监管节点可以查看 KYC 信息；
- ✓ 资产溯源：监管节点可以知道每个交易的溯源细节，其余节点只进行交易信息的溯源。

（4）安全性

- ✓ 采用安全架构设计，保证网络正常通信与运行；
- ✓ 与专业的区块链安全团队合作进行安全审计；
- ✓ 开发智能合约自动化验证平台，保证智能合约的安全。

03 社区生态及应用

3.1. 社区生态

历史经验表明，每一次经济形态的重大变革，必然催生并依赖于新的生产要素。如同农业经济时代以劳动力和土地为新的生产要素、工业经济时代以资本和技术为新的生产要素一样，数字经济时代，数据将成为新的关键生产要素，有价值的数据将成为一种稀缺资源。用户主体掌握大量的数据资源，但由于缺乏数据共享交换协同机制，容易形成“孤岛”。数字经济要达到一定的规模效应，必须要突破自身的个体界限，打通内部与外部的数据信息。而内外部数据信息的打通需要两个条件：一是数据的真实性、有效性能得到广泛认同；二是数据的内涵能得到一致的认同理解。而区块链技术恰好能解决这两个问题，借助区块链对信用体系的重塑，实现高度的信息对称和真实有效的共识。

Huobi Chain 将打造一个数字经济生态社区。在数字经济时代，用户的经济活动范围是基于信息与数据的优势。用户对自身数据和信息的掌握具有优势，但对外界的信息和数据的掌握处于空白状态，用户与外界主体之间缺乏信任与了解，无法对数据和信息的真实性和有效性达成共识，因此生态化的数字经济要求能够形成一个面向所有用户的社会信用体系。而 Huobi Chain 将利用区块链技术不可篡改和公开透明的优势重塑信用体系，提高数字经济活动的效率。具体而言，Huobi Chain 作为未来数字经济的基础设施平台，在社区生态上将提供以下三个功能：一是利用平台连接所有服务对象，收集和处理所有经营交易、场景活动的数据，并提供支付结算功能；二是根据服务对象的需求提供服务匹配，包括资金与资产的匹配、增值服务的匹配；三是连接外部服务机构，为用户的经济活动提供法律、会计、咨询、增信等服务。

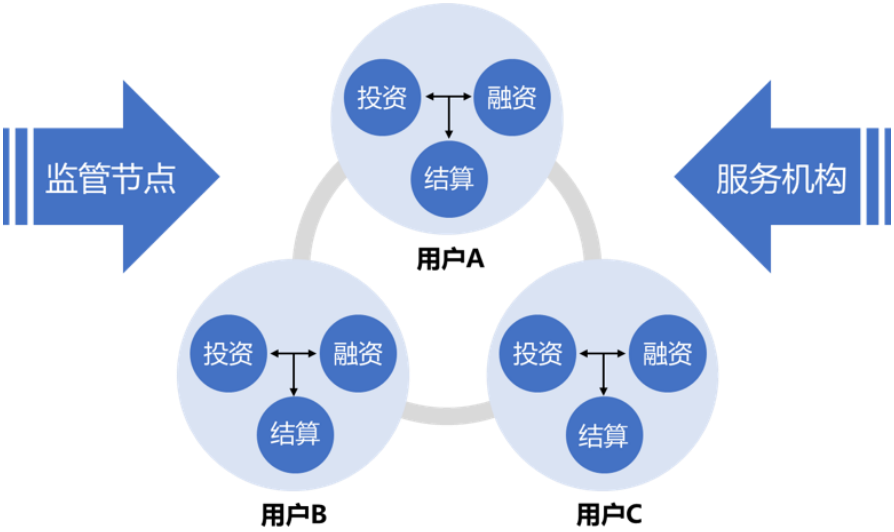


图 8 生态化的数字经济社区

因此 Huobi Chain 的社区生态将呈现以下三大特征：一是参与主体众多，各用户均可在社区内自主完成数字资产和上链资产的投资、融资和支付结算等经济活动，实现规模效应；二是交易上链实现了一定程度的信息对称，可在保证隐私和监管的前提下，让所有社区用户最大限度地发挥其在生态中的职能和价值；三是服务成本的降低，在规模效应和信息对称的基础上，通过区块链技术实现去中介化，可以大幅降低用户获取服务的成本。

在 Huobi Chain 上，数字资产和上链资产将在所有用户个体形成的生态网络体系中流转，任何一个融资需求都会与生态网络中具有相同风险收益偏好的资金进行自动匹配；资金也是如此，一个投资需求在生态网络中总能找到与之匹配的资产。当网络足够大、参与者足够多、需求足够多元化时，资金和资产将在用户之间打通，交易的清结算将在生态中普及，Huobi Chain 的数字经济生态也将形成良好的循环。

图 9 数字经济社区生态参与者

在 Huobi Chain 数字经济生态社区中，参与者包括三大类型：用户、基础设施服务方、外部服务方。各类型参与者在数字经济生态体系中的角色、职能、权责、价值各有差异。

■ **用户**

用户是数字经济生态的重要参与者。一方面，用户在生态中产生融资或投资需求，利用公链基础设施进行匹配交易，使用增值服务工具获得更大的价值。另一方面，用户更是数据输出的提供者，作为数字经济的核心生产要素，其数据对于迈向更高阶层的数字经济生态而言至关重要。为此，Huobi Chain 的用户即产生需求、接收服务，同时输出数据、完善生态。他们既是数字经济生态的参与者，也是构筑者。

■ **基础设施服务方**

基础设施服务方在数字经济生态中处于核心角色，其主要职能包括：一是运用公链平台连接所有用户，提供支付清结算功能，收集和处理所有经营交易、场景活动的数据；二是根据服务对象的需求提供匹配服务，包括资金与资产的匹配、增值服务的提供等；三是连接外部服务机构，提供法律、会计、征信、咨询等活动。在 Huobi Chain 上，火币负责提供支付清结算服务（交易链）；开发者主要在合约链上开发相关服务产品，满足各复杂应用场景需求。

■ **外部服务方**

在未来，Huobi Chain 将连入外部服务方，为社区的用户提供专业化和个性化服务。服务内容主要包括以下三大类：

✓ **增值服务**

在数字经济时代，增值服务主要以咨询服务和信息服务为代表，主要包括宏观经济分析咨询服务、行业趋势分析咨询服务、信用评级信息服务等。上述增值服务的应用场景广泛、意义深远。

在未来，当股票类、债权类、大宗商品、房产等资产实现上链交易，Huobi Chain 将接入宏观分析咨询机构，为用户提供大类资产配置咨询服务和融资方案指导服务。同时针对这一新兴行业提供行业趋势分析咨询服务，精准分析行业上下游情况，及时把握消费者信息。此外，随着数字资产规模扩大，不同数字资产的风险收益存在较大差异，为此 Huobi Chain 还将引入相应的数字资产评级机构，完善数字资产评级体系。

✓ **增信服务**

无论是在信息不完全对称还是高度对称的业务环境下，风险永远存在，只是风险程度以及违约概率不同。为此，Huobi Chain 将引入如保险公司等增信机构提供增信服务，为用户的交易活动、投融资活动提供保障，以促进社区生态发展壮大。

✓ **合规服务**

数字资产合规化是未来发展的必然趋势。数字资产依托于网络，天生具有全球流通性，然而不同国家和地区的监管要求存在较大差异。因此，Huobi Chain 也将接入专业的律师事务所、会计师事务所等，为有需求的用户提供法律合规和审计合规服务。

3.2. 应用场景

随着社会经济的发展，在未来将会有更多的企业或个体参与数字经济活动，Huobi Chain 将提供一个标准化、规模化的平台，帮助用户在去中介的条件下低成本地获取各类数字经济信息服务。

3.2.1. 数字货币交易结算

Huobi Chain 最重要的功能即为交易结算。目前的数字资产交易所存在许多问题，首先是透明度问题，交易所无法自证交易数据的可信度，资产的持有情况并不公开，用户在交易所的资产安全得不到保障；其次是合规问题，要实现交易的合规，需要保证交易的可监管性。

为此，Huobi Chain 在技术上通过交易上链的方式，大大增加交易的透明度，降低用户的信任成本；引入监管节点，进行交易追踪和资产溯源，防止非法交易；同时，为了保证交易速度，Huobi Chain 还设计独特的双链结构，由 TPS 性能高的交易链来专门处理交易。

3.2.2. 新型合规通证

在未来，Huobi Chain 将着重打造新型合规通证一站式服务平台：从咨询到担保，从法律到会计，从发行到 KYC 审查，Huobi Chain 都将接入相关专业机构，使项目方

能够在合规的前提下便捷地发行通证，允许个人和机构投资者完成合格投资者认证，合格投资人在符合政府规定的前提下参与。

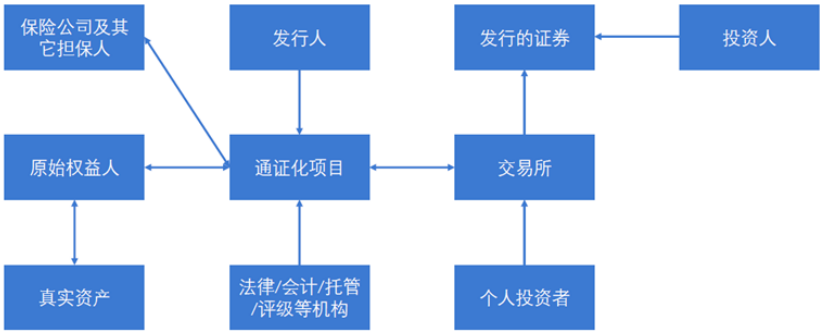


图 10 Huobi Chain 新型合规通证业务

■ **新型通证合约标准**

目前市场上主要有以 ERC-20 标准为代表的同质通证（Fungible Token）和以 ERC-721 标准为代表的非同质通证（Non-fungible Token）。前者产生的通证都是一样的，可随意交换，拆分整合；后者产生的通证是独一无二的，不可替代。然而，上述两种合约标准均无法适用数字经济时代各类资产上链业务的需求，比如 KYC/AML 限制、出入账限制、冻结名单、最小保留额以及通证内部的分级处理等。原因在于，尽管通证代表相同的标的资产，但需要有与之相关的差异化数据，这些差异化数据隐含地要求通证在不同子集间不可置换，因此要求通证具有介于同质化和非同质化之间的特性。

第一阶段，Huobi Chain 将参考 ERC1404 标准，开发难度较小的通证标准——简单的受限通证标准（Simple Restricted Token Standard），该通证标准可以依据地址进行限制，允许发行人实行对于转账的监管与限制，初步满足合规资产通证发行的基本需求。从技术角度而言，新型通证标准在基本功能接口上与 ERC20 标准一致，但会新增两个函数：

- ✓ detectTransferRestriction：该函数是发行者强制执行通证传输的限制逻辑，比如可以检验通证接收者是否在白名单内、检查发送者的通证是否在锁定期内被冻结或受相关法律的出售限制等等。该函数实现仅面向发行者，同时第三方可以公开调用该函数来检查转移的预期结果。
- ✓ messageForTransferRestriction：该函数是一个“消息”访问器，负责以人类可阅读的方式解释一笔交易为什么会被限制。通过规范消息查找，开发者授权用户界面构建器，可向用户报告错误。

第二阶段，Huobi Chain 将参考 ERC-1400，开发难度较高的部分可互换通证（Partially-Fungible Token）。新的通证标准将描述一个接口，以支持将通证分组到多个分支（tranches）中，每个分支由标识键（identifying key）和余额（balance）表示，以此实现部分操作上的限制（例如：某些操作只限定于指定分支上的通证，某些操作优先消耗指定分支的通证）。

■ **业务流程**

在合约标准开发完毕后，Huobi Chain 将搭建相关业务平台，具体流程如下：

（1）项目方在平台完成发行通证的注册；

（2）项目方在平台上双向选择法律服务机构（如要求审计还需选择会计师事务所），完成通证发行地的所需要的合规手续；

（3）项目方在平台上生成通证；

（4）用户在平台内完成 KYC 审查服务，通过 KYC 审查后，可购买与自己情况相符的通证。

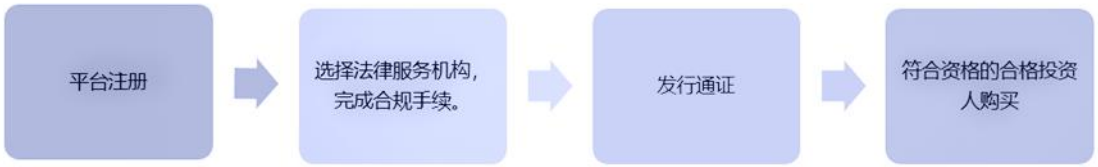


图 11 业务流程

■ **通证增发**

通证的增发主要满足项目在发行通证后，在未来可能存在融资需求。这类的融资需求主要面向定向投资者，发行的价格主要根据发行前某一阶段的均价或指定交易平台现价的某一比例。在传统金融市场中，增发需求较为普遍，其有助于企业进一步扩展业务、缓解资金压力。

现阶段，通证的定向增发操作仍处于早期阶段。技术方面，在以太坊智能合约开发中，可通过创建 owned 合约并确保通证合约对前述 owned 合约予以继承；实操方面，目前还存在社区共识、监管以及投资者不明确等问题亟待解决。

Huobi Chain 将参考现有的通证增发案例，结合股票市场上的监管规定，制定出一

套全方位、社区认可并符合监管的增发计划。现阶段的方案如下：

A. 社区共识阶段。通证增发首先需社区达成共识，项目方就增发通证方案、资金使用计划以及定向投资者等相关信息在社区中表决通过。其中，增发方案中，项目方应明确增发通证的发行方式、配售方案、定价方式等具体事宜。

B. 保荐机构推荐。火币生态中的保荐机构针对项目具体情况，为项目增发编制申请文件，并向监管机构报送。申请文件包含项目增发计划、财务规划、合规文件等材料。

C. 监管部门审批。增发材料由监管部门按照程序审核，包括对定向投资者的资质以及合规进行审查，最终进行审批核准。

D. 项目增发通证。项目在获得核准之后，经过火币确认与 Huobi Chain 进行对接，增发通证，并与投资人进行资产交割。

■ **项目的合并重组**

随着区块链行业市场的完善，产业的架构也出现一系列的变化。项目并购与重组的数量在今年也达到高峰。根据摩根大通统计，截止到 2018 年 11 月，并购与重组项目的数量相比去年已经翻倍。作为火币生态的重要一环，Huobi Chain 也将在通证的合并重组方面着手进行探索。

在技术实现方面，项目合并重组主要涉及到资产的转移，涉及到区块链中的跨链技术，具体方案将在技术黄皮书中披露。

在业务层面，由于通证涉及到监管合规、安全性方面的问题。在并购流程方面设计应该更多的参照传统证券市场的经验，保证并购项目双方利益的同时，也保证通证的投资者在过程中没有利益损失。现阶段的具体流程如下：

A. 并购方社区表决。并购方需首先达成社区共识，项目方就并购方案、被并购项目基本信息通过社区表决通过。其中并购方案中，项目方应具体提供并购价格、资产情况以及并购形式等相关信息。

B. 并购意向书的发布。并购方在进行充分调研、制定可行性报告的基础上，向被并购方发出意向书，并在 Huobi Chain 上公示，保证消息的公开透明。监管节点也会根据意向书进行审查，核实信息的真实性，并确定交易价格和条件是否符合监管要求。

C. 被并购方社区表决。与并购方形式一致，根据项目发行时的规划中社区治理的规定，满足社区表决的要求后，项目的并购方案方可被认为得到社区的认同。

D. 达成协议，签订合同。

E. 监管部门审批。并购材料由监管部门按照程序审核，包括对于项目并购的情况以及是否存在内幕交易进行审查，最终决定核准或者不核准增发的方案。

F. 项目进行并购。项目在获得核准之后，经过火币确认与Huobi Chain进行对接。根据并购协议中的内容，将被收购方的通证进行映射或进行通证互换，完成项目并购。

3.2.3. 实物资产上链

在数字经济时代，通过区块链进行交易和管理的实物资产将超过万亿美元。资产上链是将现实世界中的实物资产映射到区块链网络上，并在链上实现登记、交易、结算等环节，链下将由合规机构依照链上要求进行交割。

■ **实物资产上链的优势**

资产上链业务在未来将有大量的需求，主要原因有三点：

资产易确权，降低信息不对称。登记在区块链上的资产信息公开透明、难以篡改且便于查询，能有效降低市场参与者的信息不对称问题。

资产易审计，减少中间成本。登记在区块链上的信息易于追溯，资产权益所有者可以实时掌握资产的状态，便于进行资产审计。相对于传统方式，记录的安全性和有效性得到了极大的提升，也可以减少因资产不透明而产生的中间成本。

资产易分割，提高流动性。登记在区块链系统中的资产，被赋予可编程的特性，可以通过智能合约进行分割，从而极大的提高资产流转效率。

■ **现阶段实物资产上链问题**

不同于权益类资产，不同实物资产上链的要求差异较大。实物资产的上链必须提取其数字特征，并以此作为其与区块链通证进行映射的标准。然而，区块链技术并不能解决源头上的信任问题，即区块链技术只能保证链上数据的真实可靠，却无法保证实物资产是否被伪造。

为此，Huobi Chain 在实物上链业务部分主要面向价值高昂且具有稀缺性的资产（如艺术品），采用 RFID 射频识别技术、红外感应技术以及生物特征识别技术等，采集

实物资产专属特定的物理信息，容易辨别真伪并实现链上管理。

■ **技术方案**

Huobi Chain 将对有上链需求的资产提供上链服务。在资产上链的技术上，Huobi Chain 的方案如下：

A. 标识唯一性：Huobi Chain 将开发非同质化通证标准，将资产权益或特征映射到非同质化通证上，并保证每个通证都拥有独立唯一的编号；

B. 交易：基于非同质化通证，结合密钥分发便可进行所有权的交易；

C. 交易委托账本（order book）：主要通过涂污上链的方式实现，监管节点有相关密钥可以随时查看，而没有密钥的节点看不到相关信息；

D. 限价单：采取和 order book 同样的处理方式；

E. 结算上链：采用 open ledger 方式支持跨链资产交易（优点是跨链全资产交易，缺点是需要卖方进行对资产的 1:1 抵押）。

3.2.4. 资产抵押贷款

Huobi Chain 将提供资产抵押借贷业务。即借方使用手中的数字货币作为抵押向贷方借款，在借贷双方确定借贷金额、质押率、利率等合同细节后，借方可以将数字资产质押在智能合约内并获取贷款，待借贷结束时，智能合约根据不同的条件触发完成合同。

■ **质押率的确定**

质押率，简单理解为 “折扣”。数字资产的抵押会按照当前数字资产的价格再乘以一定的比率进行放款，这一比率则被称为“质押率”。根据数字资产的流动性和市值，Huobi Chain 在提供数字资产质押贷款服务时，参考以下基准质押率：

A. 稳定币（如 USDT、GUSD）的质押率为 80%；

B. 主流币种（仅包括 BTC、ETH 两款数字货币）质押率为 60%；

C. 市值排名前 10（不含 BTC、ETH 及稳定币）的数字货币质押率为 50%；

D. 市值排名前 10 至前 15 的数字货币质押率为 40%；

E. 针对其他项目代币，根据市场表现确定质押率。

数字货币排名每周一更新一次，全周按周一的排名确定质押率。

■ **抵押品管理**

Huobi Chain 将开发相关的智能合约管理被抵押的数字资产。在进行管理时，最重要的两个指标是警戒线和平仓线。智能合约会根据市场价格重新计算抵押品的价值，当抵押品价值下跌至借贷双方约定的警戒线时，智能合约会自动签发要求借方追加保证金的通知，要求借方提供额外的抵押品，使抵押品价值高于警戒线；当抵押品价值下跌至双方约定的平仓线时，智能合约会提前终止合约并清算抵押品。

■ **数字资产融资成本定价**

Huobi Chain 的数字资产抵押贷款业务，秉持“公正、公平、公开”的原则，将对数字资产融资利率给予一定的参考标准定价。在平台上，数字资产抵押贷款的融资成本由三部分组成：购回价差率 (利息)、交易费用、质押登记费。其中后两者由 Huobi Chain 平台收取，而购回价差率将由同类产品风险溢价、交易期限等确定，具体定价方式如下图所示，基准利率将参考贷款当月银行贷款的同期基准利率，风险溢价根据不同时期数字资产的风险情况确定：

期限	同期银行基准利率	风险溢价	购回价差率	交易费率	融资利率
6个月内	A1	B	A1+B	C	A1+B+C
6-12个月	A2	B	A2+B	C	A2+B+C
1-3年	A3	B	A3+B	C	A3+B+C
3-5年	A4	B	A4+B	C	A4+B+C
5年以上	A5	B	A5+B	C	A5+B+C

图 12 融资成本定价参考

■ **案例**

客户需要使用手中的数字货币（如：100 个 BTC）作为抵押向贷方借款，将需要完成以下步骤：

步骤 1：数字资产评估

根据 BTC 对应的质押率进行计算评估客户可借贷的金额，例如 BTC 与人民币的对价为 20,000 元，质押率为 60%，那么 100 个 BTC 可借贷的金额为 1,200,000 元。

步骤 2：质押品管理

基于 Huobi Chain 开发的智能合约对质押品进行管理，在质押的数字货币价格触及警戒线和平仓线时，自动进行相关对应操作，确保借贷双方权益。

由于数字货币市场波动性大，为确保借方利益，系统可增加自动抵押品追加功能，以避免抵押品在触及平仓线时因无法及时追加抵押品而造成损失。为此，用户需在账户中留出一定额度的资金并予以授权，在触及平仓线时，Huobi Chain 可自动划账作为抵押品追加。

步骤 3：数字资产清算

抵押合约到期时，在确认借方将借贷金额按约定归还后，智能合约自动将所抵押的数字资产进行清算并返还至借方账户。

3.2.5. 数字资产衍生品交易

衍生品作为金融市场中一种重要的金融工具，其价格主要由基础产品决定，其具备高收益、高风险的特性。同时，衍生品也是专业金融投资者进行风险控制的一项重要工具。在实际应用中，衍生品具备对冲和投机套利两项重要功能。

现阶段，数字资产的衍生品主要集中在数字通证的期货，但交易品种相对较为单一。伴随着更多的资产上链、通证产品的创新，数字资产衍生品将会更加丰富。Huobi Chain 在早期将开发数字资产期货、期权，在数字资产债券、票据等多项产品发行后，将会开发更多的数字资产衍生品。

数字资产衍生品的开发需要确立合约标的、合约期限、交易保证金以及交割方式。具体介绍如下：

合约标的：指数字资产衍生品双方的权利和义务的对象。

合约期限：指数字资产衍生品可交易的时间段，衍生品合约期限的最后一天结束即开始进行资产交割。

交易保证金：即在投资数字资产衍生品时，投资者需要存入交易所结算账户以保证合约可以履行的资金。

交割方式：即投资双方在结算日进行交割时采用的方式。在数字资产交易中，一般交割方式有两种：数字资产交割和法币交割。

3.2.6. 智能风控系统

在数字经济时代，数据是金融应用的核心，大部分的金融产品都是围绕数据进行的。

风险是金融的核心要素，而风险的控制依赖于海量的数据。风险管理主要指在项目中如何将潜在的风险减少至最低的过程。随着金融产品体量和复杂性的增加，对于风险控制的要求也逐步提高，其管理的范围也涵盖了金融产品的发行、流通等各个环节。巴塞尔协议将风险主要分为市场风险、信用风险和操作风险三类。

区块链金融作为现代金融的一个创新的产品，其高风险高收益的特点也意味着对于风险管理有着更严谨的要求。Huobi Chain 也将引入 AI 和大数据技术，为整个社区生态提供最后的风险控制支撑和资产投后监管服务。链上数据的不可篡改与公开透明更好的保证了金融风控模型中输入数据的真实性与一致性。

具体而言，Huobi Chain 将项目风控方面开发智能评级系统，对项目的风险进行评测，产品的设计也会基于智能评测的数据进行调整；对于数字资产衍生品的设计也会充分考虑风险的因素，最大程度上保证投资者的权益；Huobi Chain 的架构设计也会运用风控系统进行评测，对于系统的安全以及操作风险进行合理评估。

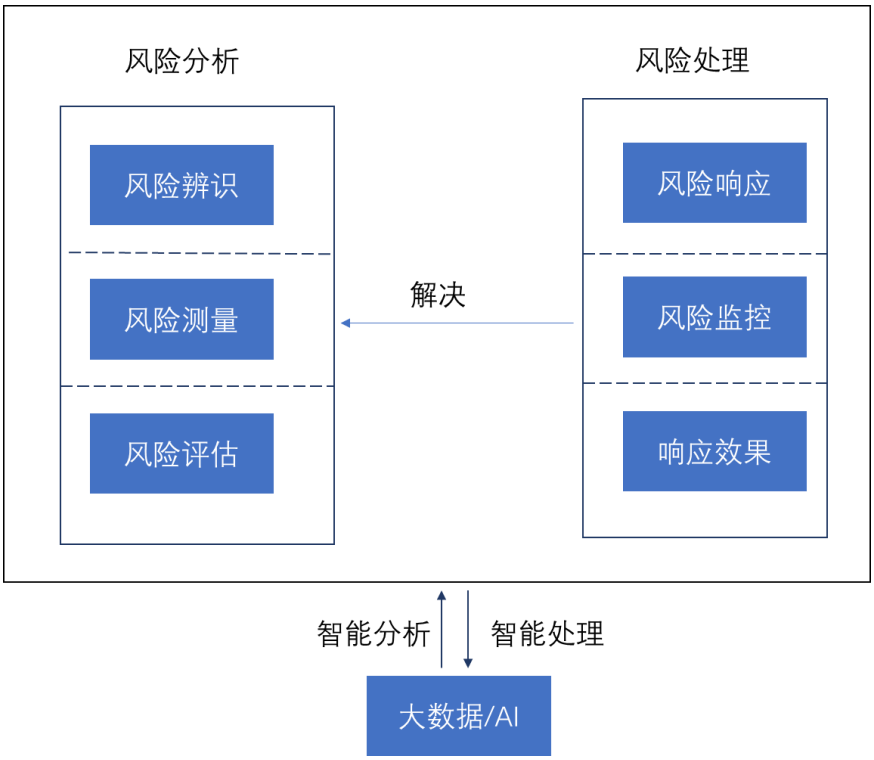


图 13 Huobi Chain 风险控制模型

04 社区治理

良好的社区治理机制能够凝聚内部力量、推动自身发展并吸引外部支持。综合考察全球的区块链社区，一套成功的区块链社区治理模式需要做到以下几点：

一是建立健全社区的激励机制。只有给予社区成员足够的激励，才能形成正反馈，吸引更多的社区成员加入。在区块链社区中，常见的激励机制即“挖矿”活动。因此，为提高社区成员的积极性，在社区治理设计时必须充分保障超级节点的收益。

二是充分的“社区自治”。“社区自治”的理念已经成为区块链社区的“共识”，然而在实践过程中很多区块链社区很大程度上是由项目方主导完成的，为充分贯彻区块链的社区自治，Huobi Chain 将采用分布式社区的模式，由社区成员自主建立。

三是实践“代码即法律”。Huobi Chain 将会把社区治理的基本规则写入智能合约，由系统自动执行，并通过治理权的合理分配以保证社区规则的连贯性和稳定性。

公链生态中的重大事件和战略决策，由 Huobi Chain 上全体的通证持有者以协商投票的方式来决定。Huobi Chain 的治理方案也将根据社区发展在不同阶段的要求逐步进行完善。

4.1. 链上治理

（1）Huobi Chain 超级节点

Huobi Chain 采用双链结构，分为交易链和合约链。双链均采用 DPoS 机制，由超级节点提供网络、存储和计算等基础设施，并负责 Huobi Chain 网络的交易验证、交易记账、区块打包和确认等工作。超级节点成功打包区块将获得对应的奖励，同时也须接受 Huobi Chain 社区的监督。

为保证交易更高的安全性和可监管性，交易链主要由火币的节点以及监管节点组成，而合约链是通过社区投票选举超级节点来实现链上治理。

- **竞选规则**

超级节点由全体社区成员采用持币投票的方式选举产生。每一个通证视为一票，所

有通证持有者均可参与投票，且可同时为多个候选节点投票。通证持有者在参与投票时需将通证将质押在自己的钱包中，若期间转出，则视为撤票。

为了保障节点竞选的高效进行，Huobi Chain 将会针对竞选者制定一系列的标准和规则。

参与超级节点竞选的基本条件：

A. 合法设立的组织主体，具备官网或经认证的官方自媒体平台；

B. 持有一定数量的 Huobi Chain 通证，参与竞选过程中，需将规定数量的通证转入选举专用的智能合约内进行抵押；

C. 具有可供社区成员测试的节点；

D. 具备符合标准的服务器和足以维护节点正常运行的技术；

E. 已制定未来一年的预算支持、技术方案、硬件扩容计划以及社区支持计划；

F. 具有一定程度的社区影响力。

抵押品及其处理：

A. 参与竞选的超级节点，须抵押一定数量的通证，具体金额由理事会决定，第一次竞选时由 Huobi Chain 提议并由社区投票通过后生效；

B. 竞选节点在退出竞选后可在 30 天（系统动态参数，可由理事会投票调整）可将抵押通证取回；

C. 若候选节点在竞选中作恶，其抵押的通证可由理事会组织社区投票处理。

（2）分布式社区

Huobi Chain 采用分布式社区的模式，由社区成员自行组织并实施自治，每个社区均可竞选超级节点。

（3）“社区章程”

尽管在区块链世界提倡“代码即法律”的理念，但社区治理是社区成员对主观问题

达成共识的一个过程，很多问题无法通过代码算法来实现。为了实现社区在一定规则下进行治理，Huobi Chain 将在区块链上绑定特殊的协议，即 Huobi Chain 社区的“社区章程”。“社区章程”规定了用户的权利和义务，以及其他重要规则，任何用户都要遵从“社区章程”。

在首次制定“社区章程”时，由理事会和专家顾问团共同商议起草完成。在对“社区章程”进行修改时，需要经过以下过程：

A. 社区成员提议修改“社区章程”，并提交给社区理事会投票，理事会成员一人一票，赞同票数超过总投票数的 2/3 视为通过，则进入社区投票环节；

B. 在社区投票环节中，由社区全体成员投票，投票不消耗通证，根据投票开始前通证持有量分配票数，赞同票数超过总投票数的 3/4 视为通过；

C. 节点通过修改源代码来反映社区章程的变化，并将新章程的哈希值向区块链网络公布；

D. 所有普通节点在一周的时间里完成升级，未升级到新代码的节点将会自动关闭。

社区治理规则、节点竞选及投票的具体细节及操作流程以官方公布的最新信息为准。

4.2. 链下治理

Huobi Chain 的链下治理由理事会主导，负责重大事项的决策，由领袖战队作为执行团队负责 Huobi Chain 的日常运营，包括但不限于技术开发、产品设计、社区运营、市场推广等内容，并接受专家顾问团的专业指导和监督。Huobi Chain 链下治理的初始组织架构如图 14 所示：

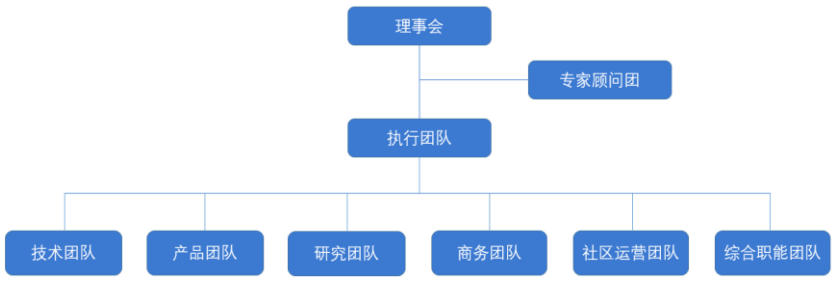


图 14 Huobi Chain 链下治理组织架构

根据《火币公链领袖征选规则征求社区意见稿》拟定如下治理制度，未来将依据项目开展情况及社区表决意见进行修订。

（1）理事会

■ **理事会组成**

Huobi Chain 理事会应当由 7 位理事组成，其中常务理事 3 人，2 位由火币指派相关人员担任，1 位由胜选公链领袖指派人员担任（当领袖发生变更时，领袖指派的理事也随即变更）。剩余 4 位非常务理事，初始由公链领袖竞选中排名 2 至 5 位的 4 位候选人担任。

白皮书完成后，以季度为单位，由社区投票确定非常务理事人选。每个季度末，根据投票情况进行理事成员更换，每次最多更换 2 名理事。投票程序和方式另行规定，以 Huobi Chain 的官方公告为准。

■ **理事会的权责**

理事会应当拥有以下权责：

✓ 听取并审议公链领袖汇报、专家顾问意见及社区意见；

✓ 对社区意见、公链发展方向等一般事项进行表决；

✓ 就重大事项进行表决。

■ **重大事项范围**

理事会所述之重大事项应当包括以下事项：

✓ 公链开发重大变革；

✓ 公链相关管理机构设置事宜；

✓ 公链相关管理机构基本制度设立事宜；

✓ 执行总裁弹劾及选举事宜；

✓ 理事会全体理事以三分之二以上通过定为重大事项的其他事项。

■ **程序性规范**

理事会应当遵循以下程序性规范：

- ✓ 理事会应当每月至少召开一次会议，会议召开日 10 日前通知全体理事和专家顾问；
- ✓ 理事会有过半数理事出席方可举行；
- ✓ 理事会决议实行一人一票制，当所表决事项与理事成员个人利益相关时，相关理事不参与投票；
- ✓ 一般事项须由全体理事过半数通过，重大事项须由全体理事三分之二以上通过；
- ✓ 代表十分之一以上投票权的社区群体、三分之一以上的理事或专家顾问会可以提议召开临时理事会议；
- ✓ 理事会形成的决议等记录，出席的理事应在记录上签名；
- ✓ 弹劾执行总裁的提案需至少 2 位（包括 2 位）理事同时提出；
- ✓ 执行总裁卸任或被弹劾时，由理事会投票内部产生继任执行总裁，获得 3 票以上者成为继任执行总裁。

■ **理事的权利和义务**

理事应履行下述义务，并享有相应的权利：

- ✓ 理事应当出席理事会议，并勤勉地履行理事会赋予的职责；
- ✓ 理事可以提出自行领导开发公链中的模块，并提议相应激励方案，交理事会审议表决，且该开发任务不应因理事去职而变化。

（2）专家顾问团

■ **专家顾问团的组成**

Huobi Chain 专家顾问团由国内外著名业界技术精英、高校学者、行业领袖及知名投资人组成。

■ **专家顾问权责**

- ✓ 促成公链事业健康发展；
- ✓ 根据本规则对 Huobi Chain 的建设进行外部监督；
- ✓ 根据本规则对 Huobi Chain 的建设提供顾问；
- ✓ 就与 Huobi Chain 相关的重要问题提出议案，且针对顾问三分之一的成员形成的提案，理事会必须审议并做出决议。

■ **专家顾问团的人数**

专家顾问团初始人数由 Huobi Chain 确定。自确定之后的第一个自然年之后，每年由 Huobi Chain 组织社区投票决定是否增加专家顾问人数。为免疑义，若投票决定增加专家顾问人数，则当年增加人数不得超过原有顾问数量的 50%。

■ **专家顾问的聘用与解聘**

- ✓ 专家顾问身份确定后，与火币指定的主体签定合同，确定权利义务。
- ✓ 当专家顾问出现不称职情形，或违合同义务时，由火币指定的主体进行解聘。

（3）执行团队

执行团队负责 Huobi Chain 的开发建设及基金会的日常运营，下设子团队若干，分别负责不同的业务条线。

■ **执行团队的组成**

- ✓ 火币公链领袖团队成员作为执行团队的初始成员；
- ✓ 一般团队成员可由领袖提名，向理事会备案后，加入执行团队；
- ✓ 子团队负责人需参加社区竞选，在社区投票中获胜者当选。

执行团队下设 6 个子团队：

技术团队：负责 Huobi Chain 的技术架构搭建、技术升级、代码审计等，根据业务需求积极探索提升公链性能的技术解决方案，以确保 Huobi Chain 的稳定运行与持续发展。

产品团队：负责 Huobi Chain 产品层设计及相关功能实现，并根据业务开展情况进行产品迭代。

研究团队：负责对监管政策进行追踪，对行业发展进行研判，对通证经济模型进行研究。

商务团队：负责 Huobi Chain 的对外商务合作以及公共形象建立与维护，推动 Huobi Chain 获得市场认可和更多的外部资源支持。

社区运营团队：负责社区建设及运营，就 Huobi Chain 的发展情况与社区成员进行及时沟通，了解社区成员的意见和建议，组织 Huobi Chain 超级节点竞选等社区活动。

综合职能团队：综合职能团队负责基金会的法律合规、财务预算、内部人事管理及行政事务管理。

■ **执行总裁的职责**

- ✓ 向理事会汇报工作；
- ✓ 组织执行团队开发和维护公链，并对执行团队进行日常管理；
- ✓ 设计和/或领导设计公链技术路线；
- ✓ 拟订执行团队基本管理制度，并将方案交理事会批准；
- ✓ 列席理事会议；
- ✓ 履行理事会赋予的其他职权。

■ **执行团队的职责**

- ✓ 执行团队成员与火币指定的主体签定合同，确认执行团队成员在公链开发建设中的权利义务。

- ✓ 根据执行总裁的要求，进行系统开发；
- ✓ 在执行总裁的指导下，进行系统维护；
- ✓ 履行合同约定的其它义务。

■ **其他**

- ✓ 执行团队成员须向执行总裁申请，经执行总裁同意，并解除加入执行团队时签订的合同后方可退出。
- ✓ 执行总裁的变更不影响执行团队成员合同项下的权利义务。

05 发展规划

■ **竞选期**

2018 年 6 月 – 2018 年 9 月，由火币组织行业专家开展火币公链领袖竞选，各战队提出初步设计方案，通过社区投票与专家评审相结合的方式选拔公链领袖。

■ **启动期**

2018 年 10 月 – 2019 年 1 月，公链领袖组建执行团队，明确业务发展需求，确定公链设计思路，制定初步开发及运营方案，完成白皮书、黄皮书和 demo。

■ **开发期**

2019 年 1 月 – 2019 年 8 月，执行团队按照规划推进项目，包括开发双链基础组件、应用模块以及智能合约标准，逐步完善社区治理相关制度等。

■ **发展期**

2019 年 9 月 – 2019 年 12 月，上线测试链，完成测试与升级。

节点建设：包括购置自由节点服务器、扩展社区节点等。

开发者社区建设：开展宣传活动，设置赏金计划，吸引全球技术开发人才。

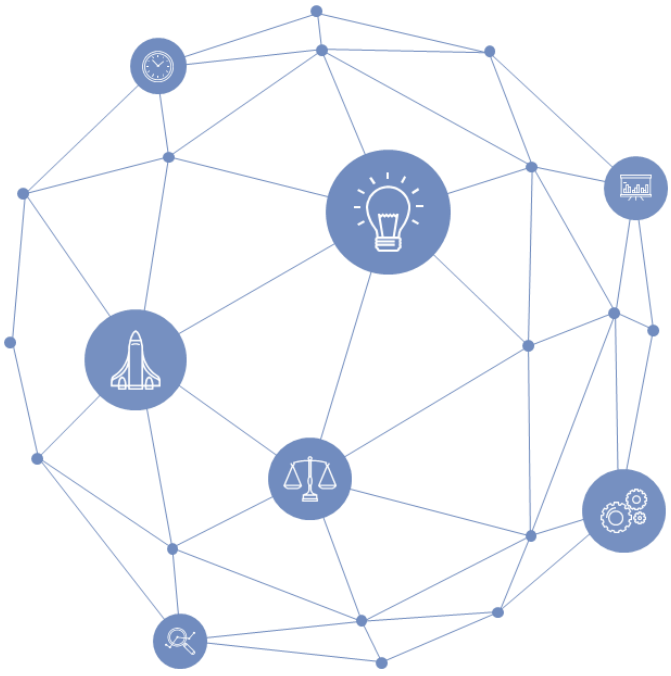
金融业务扩展：完成新型合规通证功能、数字资产抵押功能的开发，并根据监管形势，丰富新型通证发行、增发等各项功能，扩展数字资产衍生品交易功能，探索更多的金融衍生品上链可行性，基于前期数据开发智能风控功能。

应用建设：公链启动时理想状态为支持不少于 10 个杀手级应用，以及上百个 DApp，并通过黑客马拉松等大型比赛的方式，吸引更多智能合约在链上部署。

生态工具建设：为提高公链的易用性，对于开发者提供钱包、浏览器、开发环境一键部署方案等各项应用工程，对于用户开发手机对接等易用环节，对于专业人士提供金融合约模版等。

■ **成熟期**

2020 年 1 月 – 2020 年 6 月，持续对公链功能进行迭代升级，进一步深化节点建设、开发者社区建设、应用建设等，将火币生态业务对接上链，将各类合作伙伴资产上链等。



06 团队介绍

2018 年 6 月 6 日火币公链全球领袖竞选活动正式启动（关于活动详情请关注火币公链官网 www.huobichain.com），收到了来自中国、美国、日本、韩国、荷兰、新加坡等 20 多个国家近 400 人报名，经过 3 个多月的激烈角逐，最终 G 咖战队胜出，成为火币公链领袖战队。

6.1. 领袖团队

刘昱

Larry Liu，Genaro Network 创始人，趣派科技 CEO，Cofounders' Fund（创始人基金）发起人，中国移动通信联合会国际区块链创新应用联盟副秘书长，区块链先驱者，是一名具备工程师背景的创业家。Larry 硕士毕业于美国西北大学计算机专业，曾任硅谷惠普公司安全工程师，后在区块链领域进行创业与投资，拥有丰富的区块链底层构架与研发以及社区化企业运营与管理经验，同时也是 SPoR + PoS 可持续共识机制发明人，《公有链七大挑战与解决方案》作者。

徐坤

徐坤女士，TLAB 创始人，中国电子学会区块链专家委员，天风证券区块链研究中心研究总监，JRR 全球合伙人，广州黄埔区块链培训学院首位女教官，数字货币市场早期参与者，国内首个 IP 区块链项目创始人，曾为坐拥百万粉丝的财经大 V，连续两年在金融机构间女神评选夺冠，拥有丰富的金融市场从业经验与区块链产业资源积累。证券业协会优秀课题《区块链在我国证券市场的关键应用与监管研究》主要参与成员，《金融监管研究》、《证券时报》区块链专题文章第一作者，金色财经、火星财经等知名区块链媒体专栏作家， CCTV、第一财经特邀嘉宾，并接受各大媒体的专题采访。

黄敏强

黄敏强，公信宝创始人，核心设计者和开发者，在数据交换、互联网金融和区块链领域有超过 10 年的从业和研究经验。从 2012 年开始研究数字货币和区块链，参与并发起多个区块链项目，对区块链产品设计和数字货币经济模型设计有深度研究和实践。于 2016 年创办的公信宝有“国产公链三驾马车”之称，旗下“GXChain”获得工信部赛迪公链评测全球第四；“布洛克城”区块链用户超过两百万；“去中心化数据交易所“则是最早商用的企业区块链应用。同时也是超级马拉松、越野跑、山地自行车等耐力运动爱好者。

吴为龙

吴为龙，Genaro Network 创始人，趣派科技 CTO，第一批区块链开发者，无服务器交互系统架构设计第一人，是一名具备丰富创新经历的技术极客。吴为龙曾是硅谷美信集成公司的核心开发者并为三星提供算法；后投身于区块链研发，在溯源防伪与供应链金融等领域开发过十余个智能合约，实战经验涉及区块链虚拟机、P2P 存储、共识算法等诸多底层技术。SPoR+PoS 可持续共识机制发明人，Genaro Virtual Machine 缔造者。

肖艺伟

肖艺伟，币达资本创始人，数字货币资深投资管理人。币达资本为火币交易所超级节点，团队擅长量化交易与资产管理，币达社区成员持有超过 2000 万 HT。自 2013 年起，肖艺伟所带领的团队已投资数十个一级、二级市场项目。

蔡栋

蔡栋 Charles，麦当劳（中国）CDO/CIO，InfiniVision 深见 iABC 实验室创始人，前万达网络科技集团总裁助理兼 CDO / 首席架构师。20 年技术和业务创新经验：伦敦投行、能源交易首席架构师，创建大数据、云计算卓越中心（预算 1 亿美金）；西欧最大的数据科学社区 CTO；全英 2015/16 年度前 50 名数据领袖和影响者。复旦大学电子工程系信息系统专业。

6.2. 顾问团队

2018 年 8 月 15 日，火币正式发布火币公链专家顾问团成员名单。共 9 位来自区块链及科技领域的重量级专家加入，组成了跨学术、投资、产业等多维背景的强大跨界智囊团。

Steve Hoffman

Steve Hoffman，天使投资人、连续创业者，人称“硅谷创业教父”，畅销书《让大象飞：激进式创新》作者。Hoffman 是福布斯和企业家杂志评选出的排名全球第一的海外初创企业孵化器 Founders Space 的创始人和 CEO。同时他也是 Founders.VC 合伙人，投资并孵化了包括人工智能、大数据、机器人、SaaS、医疗等领域在内的大量科技类初创公司。Hoffman 也创立过三家媒体、游戏和娱乐初创公司，并获得了风投机构的大力支持。除此之外，Hoffman 还是好莱坞的电视节目制作人，也是美国制片人协会硅谷分会的创始人。

黄铭钧

黄铭钧，新加坡国立大学计算机科学系杰出教授、浙江大学长江讲座教授、 新加坡国立大学智能系统中心主任。其研究团队发布了世界上首个区块链测评套件 BLOCKBENCH，以及高性能的区块链数据存储系统 FORKBASE. 与此同时，他与工业界密切合作，致力于运用 IT 提高各种应用领域的效率。他先后创办了 MediLOT 健康数据区块链以及铭之慧科技。黄铭钧先生还是新加坡科学院院士、世界计算机协会（ACM）会士、世界电气电子工程师学会（IEEE）会士、浙江省人工智能发展专家委员会委员。

刘晓蕾

刘晓蕾，北京大学光华管理学院金融学系及会计学系教授，北大光华区块链实验室主任。她的研究方向包括资本市场和实证公司金融，并在众多学术期刊上发表论文，在加入光华管理学院之前，刘教授在香港科技大学任职，并取得了终身教职。

Don Tapscott

Don Tapscott，Tapscott 集团 CEO，“数字经济”之父，著名新经济学家和商业策略大师，对技术给商业和社会的影响具有很深刻的认识和理解。同时，他也是一名畅销书作家。除此之外，Don 还获得过加拿大勋章奖，担任特伦特大学荣誉校长。2017 年，Don 和他的儿子共同创立了区块链研究所，对区块链战略，应用场景，实施挑战和组织变革进行深入且独一无二的研究。

Jeffrey Wernick

Jeffrey Wernick，Airbnb 和 Uber 的早期投资者，自 2009 年起便开始投资并持有比特币，芝加哥大学经济与金融系博士，受教于多个诺贝尔奖得主。在职业生涯的早期，他曾在所罗门兄弟公司工作，后成为底特律国家银行最年轻的高级管理人员。Jeffrey 在各个资产领域均有丰富的投资经验，并以提倡比特币哲学和数据主权而闻名。同时，他也是多个行业通证化项目的投资人和开发团队领导者，以及多个著名区块链项目的顾问。

Lon Wong

Lon Wong，区块链技术的长期倡导者，是区块链项目 ProximaX 的创始人兼首席执行官。ProximaX 是区块链和分布式账本技术的高性能拓展，具备丰富的实用性、行业级标准服务及协议接口。在创立 ProximaX 之前，Lon 是全球开源区块链项目 NEM.io Foundation, Ltd 的创始成员及第一任总裁。Lon 还是 Dragonfly Fintech 的创始人，一家专注于使用区块链技术解决移动支付问题的金融科技公司，并拥有超过 30 年的从工程咨询到软件应用的业务建设经验。

吴忌寒

吴忌寒，比特大陆联合创始人及 Co-CEO，比特币早期布道者，比特币现金（BCH）支持和推动者。吴忌寒早在 2011 年便接触比特币，并第一个翻译了中本聪的比特币白皮书。他早年参与创立的巴比特论坛，目前已成为国内最大的区块链资讯社区门户。2013 年，他与詹克团一起创立比特大陆，经过多年的发展，比特大陆也已成为一个涵盖矿机、矿池、矿场、交易平台等全产业链的综合型区块链公司，业务覆盖全球 100 多个国家和地区。

Randi Zuckerberg

Randi Zuckerberg，企业家，投资者，畅销书作家和科技媒体人士，毕业于哈佛大学。她是新兴媒体公司 Zuckerberg Media 的创始人兼首席执行官，前 Facebook 高级管理人员，Facebook Live 缔造者。同时，Randi 也是 SiriusXM 电台的科技商业秀节目“Dot Complicated”主播，以及电视节目“DOT”（曾获 Kidscreen 最佳新学前系列奖项）和“American Dreams”的制作人。除此之外，Randi 还是畅销书“Dot Complicated”，“Dot”和“Missy President”的作者。

张首晟

张首晟，斯坦福大学物理系、电子工程系和应用物理系终身教授、美国科学院院士、中国科学院外籍院士、丹华资本创始董事长、曾投资多个知名区块链项目。

6.3. 理事会

火币公链理事会暂由 3 名常务理事和 4 名非常务理事组成。第一届非常务理事由火币公链领袖竞选中第 2-5 名战队指定队内成员代表担任，后期将由社区投票决定；其主要职责在于协助及监督公链领袖的开发和运维工作。

常务理事 李林

李林，火币董事长、创始人，毕业于清华大学自动化系，连续创业者，曾就职于全球最大的数据库厂商 Oracle。李林先生极具互联网行业前瞻眼光，2013 年创办了火币网，并将火币网打造成为全球领先的区块链资产金融服务商。

常务理事 袁煜明

袁煜明，清华大学自动化系毕业，曾任兴业证券研究所所长助理，TMT 研究中心总经理，计算机互联网行业首席分析师，2013-2017 连续 5 年上榜新财富最佳分析师。现任火币中国 CEO，火币区块链研究院院长，火币公链事业部总经理，清华 x-lab 区块链公开课程导师，北大创业孵化器区块链创业导师，2018 年 4 月提出了基于供给的区块链商业体系设计。

常务理事 刘昱

Larry Liu，Genaro Network 创始人，趣派科技 CEO，Cofounders’ Fund（创始人基金）发起人，中国移动通信联合会国际区块链创新应用联盟副秘书长，区块链先驱者，是一名具备工程师背景的创业家。Larry 硕士毕业于美国西北大学计算机专业，曾任硅谷惠普公司安全工程师，后在区块链领域进行创业与投资，拥有丰富的区块链底层构架与研发以及社区化企业运营与管理经验，同时也是 SPoR + PoS 可持续共识机制发明人，《公有链七大挑战与解决方案》作者。

刘威战队代表 黄连金

黄连金，核聚链创始人。
刘威战队成员：刘威，360 创新研究院院长；Anita Xie，Netta/Fractals 创始人及 CEO；吴思进，复杂美科技创始人；钟庚发，链上科技创始人；Steve Melnikoff Penta 首席科学家。

周硕基战队代表 周硕基

周硕基，FBG 创始人。
周硕基战队成员：余弦，慢雾科技联合创始人；马昊伯，Aelf 创始人；董沫，Celer Network 联合创始人。

A 战队代表 崔萌

崔萌，AChain 创始人。
A 战队成员：祝雪娇，Kcash 创始人；李万才，EOS 引力区联合创始人；李晨，优币资本 CEO。

极智战队代表 赵美军

赵美军，极光链的创始人。
极智战队成员：高镇硕，韩国 Davinci Foundation 首席信息官。

参与白皮书编撰及修订者（排名不分先后）：

TLAB 团队（徐坤、李炼炫、Reina Guan、Rabbi Jiang、梁晨、Lynn Huang、何志博），Genaro 团队（Larry Liu，Waylon Wu，Sophia Zhai），黄敏强，余弦，杨霞，李万才，代炜琦，Jiangshan Yu，黄连金，赵美军，崔萌，刘晓蕾，黄铭钧，林吓洪，曹辉宁，董心书，孔华威，Yaoqi Jia，王东临，王聪。

07 风险提示

除本白皮书所载明的内容之外，火币不对 Huobi Chain 或项目通证作任何陈述或保证（尤其是对其适销性和特定功能）。本项目采取自愿参加、风险自担、责任自负、费用自理的原则。

在 Huobi Chain 的开发、维护和运营过程中存在着风险，其中或有超出火币的控制。除本白皮书所述的其他内容外，用户需知悉下述风险，并评估己方是否有承担下述风险的能力。Huobi Chain 项目的开发过程中，或将存在下述风险：

(1) 不充分的信息提供

截止到本白皮书发布日，Huobi Chain 仍在开发阶段，其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了 Huobi Chain 最新的关键信息，其并不绝对完整，且仍会被火币因特定目的而不时进行调整和更新。火币将尽可能的为社区成员提供关于公链开发的各种信息，但无法确保所有信息向每位通证持有者的实时传递。

(2) 司法监管相关风险

加密数字资产正在被或可能被不同国家的主管机关所监管。火币可能会不时收到来自于一个或多个主管机关的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何关于 Huobi Chain 的开发或行动。Huobi Chain 的开发、营销、宣传或其他方面，因此可能受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家现有的对于 Huobi Chain 的监管许可可能只是暂时的。

(3) 密码学

密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明）可能给基于密码学的系统（包括 Huobi Chain）带来危险。火币无法保证 Huobi Chain 在任何时候都具有绝对的安全性。在合理范围内，火币将采取预防或补救措施，升级 Huobi Chain 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。

(4) 开发失败或放弃

Huobi Chain 仍在开发阶段，而非已准备就绪随时发布的成品。由于 Huobi Chain 系统的技术复杂性，火币可能不时会面临无法预测和/或无法克服的困难。因此，Huobi Chain 的开发可能会由于任何原因而在任何时候失败或放弃（例如由于不可抗力）。

(5) 源代码瑕疵

无人能保证 Huobi Chain 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能导致用户无法使用特定功能，暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害 Huobi Chain 的可用性、稳定性、安全性，并因此对通证的价值造成负面影响。公开的源代码以透明为根本，以促进社区对代码的鉴定和问题解决。火币将与 Huobi 社区紧密合作，今后持续改进、优化和完善 Huobi Chain 的源代码。

(6) 源代码升级

Huobi Chain 的源代码是开源的且可能被 Huobi 社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对 Huobi Chain 的运行或通证的价值造成重大不利影响。

(7) 竞争

Huobi Chain 的底层协议是基于开源电脑软件。没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用 Huobi Chain 的源代码和/或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台或虚拟机从而与 Huobi Chain 竞争，或甚至赶超或取代 Huobi Chain，火币对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台与 Huobi Chain 产生竞争关系。火币在任何情况下均不可能消除、防止、限制或降低这种旨在与 Huobi Chain 竞争或取代 Huobi Chain 的竞争性努力。

(8) 通证的流动性及价格波动

通证的交易仅基于相关市场参与者对其价值达成的共识。没有任何人能够在任何程度上保证任何时刻通证的流通性或市场价格。该通证若在公开市场上交易，其价格可能

波动剧烈。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。通证交易价格所涉风险需由交易者自行承担。

（9）不可预期风险

区块链技术是一种正在快速发展的技术，除了本白皮书提及的风险外，或将存在一些 Huobi Chain 团队尚未提及或尚未预料到的风险，抑或多种已提及的风险以组合的形式出现。

08 术语表

双链结构	分为交易链和合约链两条链组成，既满足交易上链又能实现合约上链。
交易链	又称“快链”，负责交易清结算，追求交易速度更快、频次更高、手续费更低。
合约链	又称“慢链”，支持金融合约、业务合约等复杂应用。
PoW 机制	Proof of Work，工作量证明，是一种对应服务与资源滥用、或是阻断服务攻击的经济对策。一般是要求用户进行一些耗时适当的复杂运算，并且答案能被服务方快速验算，以此耗用的时间、设备与能源做为担保成本，以确保服务与资源是被真正的需求所使用。
PoS 机制	Proof of Stake，权益证明，试图解决 PoW 机制中大量资源被浪费的情况。这种机制通过计算参与者持有占总通证数的百分比，包括参与者占有通证数的时间来决定记账权。
CAP 原则	CAP 原则又称 CAP 定理，指的是在一个分布式系统中，Consistency（一致性）、 Availability（可用性）、Partition tolerance（分区容错性），三者不可兼得。其中，一致性（Consistency）是指分布式系统中的多个服务节点，给定一系列的操作，在约定协议的保障下，使它们对外界呈现的状态是一致的；可用性（Availability）是指每次请求都能获取到非错的响应，但不保证获取的数据为最新数据；分区容错性（Partition tolerance）是指当节点之间的通信出问题时，相关的操作仍旧能够正常完成。
BFT-DPoS	Byzantine Fault Tolerance - Delegated Proof of Stake，拜占庭容错式的委托权益证明机制。BFT-DPoS 在充分提升系统性能的基础上，避免了网络延迟问题。主要的实现方式是将随机出块顺序更改为见证人上以后确定的出块顺序，让网络延迟较低的见证人实现相邻出块，从而避免了因为地理位置造成的网络延迟可能造成的区块链分叉。
智能合约	是一种旨在以信息化方式传播、验证或执行合同的计算机协议。

SPV	Simplified Payment Verification，即简单支付验证。这一概念最早出现于比特币的白皮书之中，其提供了一种方式来使得转账的执行不需要运行整个区块链网络节点加以验证。使用简单支付验证的钱包主要通过复制区块链网络最长的链，之后将转账通过 Merkle 分支链接到区块之上从而实现交易的验证。
CLTV	Check Lock Time Verify，即锁定时间验证代码。这一代码会实现在交易中锁定资金，只有在某个时间之后，资金才可以解除锁定。CLTV 的主要用途是在交易中设定交易条款，以实现双方有条件的智能交易。
HTLC	Hashed Timelock Contracts，哈希时间锁定协议。这一协议可以在去中心化的前提下，实现不同区块链项目之间通证的交易互换的技术。
WASM	WASM 是便携式的抽象语法树，被设计来提供比 JavaScript 更快速的编译及运行。WASM 将让开发者能运用自己熟悉的编程语言（最初以 C/C++作为实现目标）编译，再藉虚拟机引擎在浏览器内运行。
KYC	Know Your Customer，对账户持有人的强化审查，是反洗钱用于预防腐败的制度基础。
AML	Anti-Money Laundering，反洗钱，是指为了预防通过各种方式掩饰、隐瞒毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪等犯罪所得及其收益的来源和性质的洗钱活动。常见的洗钱途径广泛涉及银行、保险、证券、房地产等各种领域。反洗钱是政府动用立法、司法力量，调动有关的组织和商业机构对可能的洗钱活动予以识别，对有关款项予以处置，对相关机构和人士予以惩罚，从而达到阻止犯罪活动目的的一项系统工程。
H-UID	Huobi Chain - User Identity，Huobi Chain 用户身份，具有唯一性，各国公民经过 KYC 身份验证后将个人信息登记上链，用户可基于 H-UID 对自己的个人信息和数字资产进行管理。
质押率	根据数字资产的流动性和市值所制定，抵押贷款本金利息之和与所抵押数字资产估价价值之比。

09 参考文献

[1] Back, Adam, et al. "Enabling blockchain innovations with pegged sidechains." URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (2014).

[2] Bandara, H. M. N. D. and Jayasumana, A. P. (2012). Collaborative Applications over Peer-to-Peer Systems Challenges and Solutions. Peer-to-Peer Networking and Applications. arXiv:1207.0790.

[3] Maymounkov, P. and Mazieres, D. (2002). Kademlia: a peer-to-peer information system based on the XOR metric, International Workshop on Peer-to-Peer Systems, 53-65.

[4] Naor, M. and Rothblum, G. N. (2009). The Complexity of Online Memory Checking. Journal of the ACM (JACM), 56(1).

[5] Bentov, I., Gabizon, A. and Mizrahi, A. (2016). Crytocurrencies without Proof of Work. International Conference on Financial Cryptography and Data Security.142-157.

[6] Kshemkalyani A D, Singhal M. Distributed computing: principles, algorithms, and systems[M]. Cambridge University Press, 2011.

[7] 宁小军，《自金融》，中信集团出版社.

[8] 中国信通院，《中国数字经济发展白皮书（2017 年)》.

[9] 中国信通院，《G20 国家数字经济发展报告（2017 年)》.

[10] Dan Larimer，《DPoS 共识算法 - 缺失的白皮书》.

[11] EOS.IO，EOS.IO Technical White Paper v2.

[12] Genaro，《Genaro 技术黄皮书》.

[13] Genaro，《GSIOP 文档》.

[14] 公信宝 GXChain，《公信链 GXChain 白皮书 3.0》.

[15] 慢雾安全团队，《超级节点安全审计方案》.

[16] 慢雾安全团队，《安全漏洞与威胁情报赏金计划》.

[17] 链安科技，《关于区块链智能合约安全漏洞类型连载分析》.