WeShare 共享经济链
技术和经济白皮书

北京新宋共享科技有限公司

目录

1 项目背景

区块链(Blockchain)区块链是一种分布式账本技术，基于去中心化的对等网络，用开源软件把密码学原理、共识机制、时序数据相结合，来保障分布式数据库中各节点的连贯和持续，使信息能即时验证、可追溯、但难以篡改和无法屏蔽，从而创造了一套透明、高效、安全的共享价值体系。根据麦肯锡公司的一份区块链技术报告显示，从2016 年开始，已有超过 100 种区块链技术解决方案探索。在全球区块链产业中，中国成为最活跃的市场。工信部联合多个行业公司编写的《中国区块链技术和应用白皮书》中列举了金融服务、供应链管理、智能制造、文化娱乐、医疗健康、社会公益和教育就业等区块链可以实现的六个典型应用场景，并分析了区块链与云计算、大数据、物联网、下一代网络、加密技术和人工智能等 6 大类新技术的关系。

今天的互联网，已经近乎完美地解决了信息传递问题，人们可以非常便捷、低成本地点对点传递信息。然而，目前的互联网技术还不能实现点对点的价值传递。不同于信息传递的可复制特征，价值传递需要保证权属的唯一性，所以当前价值的传递仍然需要依赖中心机构承担记账功能。简单地说，在信息传递之后，发送方和接收方能够同时拥有信息；但是，在价值传递之后，只能受让方拥有价值，转让方不能再拥有，目前这个转移过程的权属记录是通过中心机构记账实现。那么，如果网络本身能够提供可靠的记账功能，将使得价值传递不再完全依赖于中心机构，可以实现价值的点对点转移。区块链这种分布

式总账技术（DLT, Distributed Ledger Technology），能够让参与各方在技术层面建立信任（Trust），有潜力成为构建未来价值自由流通网络的基础设施，即形成价值互联网（Internet of Value）。尽管价值互联网广泛到来的时间仍未可知，但从今天的发展状况来看，一些价值局域网已经在逐步形成。实际上，在某些特定领域，若干合作伙伴或产业链的参与方正在共同建立区块链信任网络，这种价值局域网已经在实施过程中，而不再只是概念。从价值局域网到价值互联网的一个可能的演进路径是：类比于互联网的发展历程，前期是一个个独立的、由各个行业按照自身需求形成的局部价值流通网络，后期在跨行业价值交换需求的驱动下，逐步形成大规模的、共有的价值自由流通网络。区块链的核心价值在于构建可信任的多中心体系，将分散独立的各自单中心，提升为多方参与的统一多中心，从而提高信任传递效率，降低交易成本。

区块链的核心价值在于构建可信任的多中心体系，有潜力成为构建价值互联网的基础设施。WeShare 链致力于打造企业级区块链产品并提供行业解决方案，已经开发了高性能、高可扩展的区块链基础服务平台，具备快速构建上层应用业务的能力，满足大规模用户数量的应用场景。瞄准企业级产品化运营能力，WeShare 链努力进行技术突破和创新，在性能、扩展性、安全和运维等方面形成一系列技术特色和优势。在与产业合作伙伴共同深入探索区块链应用场景的基础上，WeShare 链将应用于数字资产、贸易金融、股权债券、供应链溯源、联合征信、公示公证、物联网共享、数据安全等领域。以去中心化+

共享经济为核心，打造新一代价值流通网络，让数字资产都自由流动起来。

WeShare 链的应用场景分析：

数字资产发行流通

相比于传统中心化系统，区块链应用于数字资产领域的优势在于：资产一旦在区块链上发行，后续流通环节可以不再依赖发行方系统，在流通中，资产由单中心控制变成社会化传播，任何有资源的渠道都可能成为资产流通的催化剂。因此，区块链能极大地提升数字资产流通效率，真正达到“多方发行、自由流通”。传统的资产服务，需要相应的中间商，如资产所有者证明、真实性公证等均需要第三方的介入才可以完成，只有通过资产发行方、资产接收方、流通平台的三方介入，资产才可以完成整个流通过程。在目前的三方模式中，存在以下几个痛点：

（1）资产进入流通后，仍必须依赖资产发行方系统才能完成使用、转移，这就将资产流通范围限制在发行方系统用户群内；

（2）传统的资产流通渠道有限，几乎都依赖于大渠道，行业大渠道由于垄断地位大幅增加费用，从而导致流通成本显著提高，小渠道及个人难以在流通环节发挥作用。

图 6-1 数字资产发行与流通

如图 6-1 所示，在数字资产发行与流通网络中，区块链用于资产登记、交易确认、记账对账和清算等。区块链数字资产网络，包括资产发行方、资产交易方、交易所、流通渠道在内的各个上下游机构，他们可以按照自身角色在链上自行开展业务。

- 任何可数字化的资产都可以在平台上实现登记、发行，各种主体（个人、机构）均可以在平台上登记、发行自己的数字资产。实现资产登记即公示，利于数字资产追踪查询，可以有效减少资产纠纷问题。
- 资产流通的核心是渠道，区块链技术使资产流通由原来的单中心控制变为社会化流通，任何有资源的渠道都可以成为资产流通的催化剂，促进流通、提高流通效率。

- 区块链“交易即结算”的基本特性使得实时清算成为可能，大幅提高交易后处理的效率，实现资产流通情况的实时查询功能。
- 数字资产可以是已经数字化的资产，可以成为资产证券化和资产数字化的入口，将现实资产映射成数字资产在链上发行与流通。

WeShare 链可应用于商业积分、电子券、预付卡、游戏装备、保险卡单、资产证券化等。

贸易金融/供应链金融

贸易金融/供应链金融领域的业务链条中，天然就是多方参与协作。利用区块链，能将分散独立的各自单中心，提升为多方参与的统一多中心，打通贸易上下游各个环节，提高信任传递效率，降低交易成本，促进贸易金融的良性生态建设。在贸易金融领域，信息散落在供应链各家自有系统中，流通和融资环节存在信息重复验证，效率低下；受各个供应链圈的信息流限制，中小企业和金融机构双向选择范围有限；缺乏统一可靠的中小企业征信系统，金融机构风控难度大，风控成本全部转嫁给融资企业。区块链可以促使供应链参与方共同创建和维护一份各环节都认可的统一凭证，并保障其真实有效、不可篡改；除了凭证的共享，项目/合同执行的过程也可以完整记录和跟踪，降低金融机构的风控难度，提升中小企业融资的可行性，降低融资成本；淡化供应链固有的圈子，扩大凭证授信范围，成为资产证券化、数字化的入口，增强流通性；链信息的记录和积累，也是企业自征信的过程，基于这些征信数据，可以展开各种金融服务。

图 6-2 区块链贸易金融

- 统一凭证，保障唯一真实性，极大降低核验成本；
- 过程可视，增强履约透明度，提高融资管理能力；
- 数据记录，促进征信的体系，减小风险控制成本。

WeShare 链会应用于仓单质押融资、应收账款融资、票据托管贴现、消费金融理财、大宗商品交易等。

私有股权登记转让

应用区块链技术的加密股权、债券等证券化资产，有助于完善登记与流转服务，尤其是区块链构建的多中心体系，能够大幅地提升资产跨域流通效率，降低交易成本，使管理更安全、高效、可信、低成本、合规。目前，股权登记需要人工处理，股东名册维护繁琐、历史交易维护与跟踪十分困难。传统股权交易，以双方信用为基础，需要建立

双边授信后才可进行交易，信用风险由交易双方自行承担，而交易平台集中承担市场交易参与者的信用风险。

图 6-3 股权登记与转让

- 唯一真实的数字凭证，适于股权债券等证券化资产的登记；
- 跨域的多中心化信任，便于加密证券化资产的转让与交易；
- 增强的信息披露记录，易于符合监管满足合法合规性要求。

WeShare 链可被应用于众筹平台、区域股权交易中心、区域金融资产交易中心、私募管理平台等。

2 我们的目标

目前，区块链产品可以大致分成两个层面：一是区块链底层技术；二

是区块链上层应用。WeShare 链的产品定位是，先在共享经济领域将区块链技术真正和业务场景结合落地，并逐渐提供商业级的区块链基础设施服务，主要包括：一是打造企业级区块链基础平台（“区块链底层技术”）；二是在其上构建具有高可扩展性的应用业务支撑系统（介于“区块链底层技术”与“区块链上层应用”之间），从而结合共享经济、物联网构建更多的商业模式，打造可编程循环经济生态。

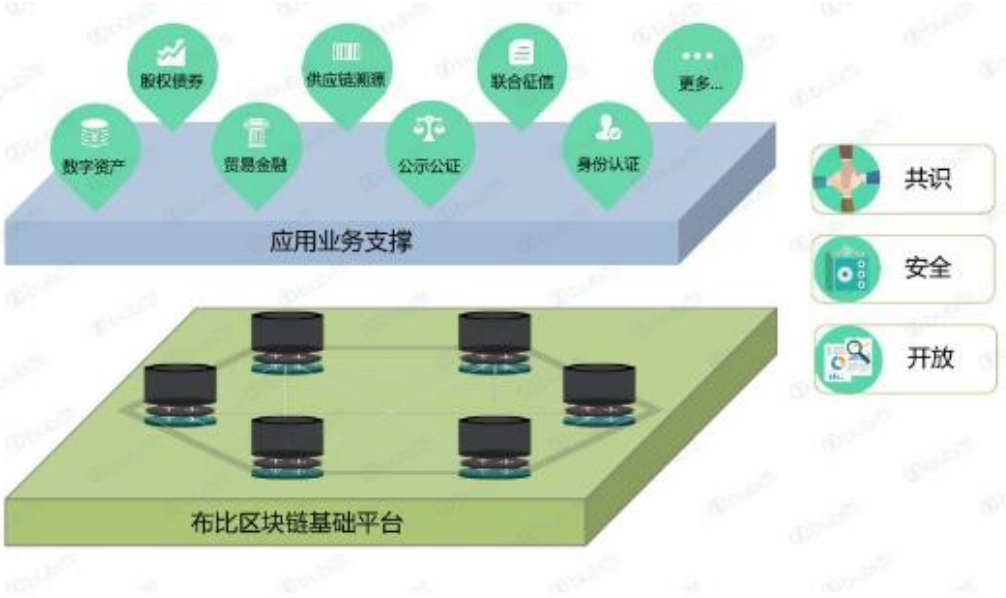


图 2-1 布比区块链的目标

WeShare 链致力于提高区块链结合实际业务的赋能程度，表现在如下几个方面：

（1）快速应用构建：多模式的账本结构及业务模型，方便快速构建应用；

（2）海量用户支撑：高效交易验证和同步，支撑千万甚至亿级用户规模；

（3）可视化运维管理：从网络、系统、业务层面提供可视化的运维

管理；

（4）隐私权限策略：丰富的权限策略配置，依据应用需求进行隐私保护；

（5）内置智能合约：支持可编程的合约开发，并提供标准化的合约模板；

（6）共享经济区块链即服务：面向共享经济各行业领域，提供可配置企业级区块链云服务;

产品和技术将实现如下三个阶段：

- 去中心化共享经济平台，实现真正业务应用数据价值流通。WeShare 将解决业务终端的信任、透明问题，通过去中心 化交易平台实现用户的数据权利和价值保护。
- 打造行业价值的公链，构建共享经济价值生态系统。 WeShare 结合共享经济、物联网特性开发去中心化价值公有链，并支持多种行业应用，提供智能硬件等多种方案，结合密码学技术，分布式架构，采用 DPOS 共识的主链，构建安全、去中心化的、支持高并发、高价值的区块链网络。
- 实现万物互联、终端价值交易。在万物互联的庞大网络通过区块链去中心化可信的环境，实现实现用户间、终端与终端之间价值透明交换。最后，WeShare 的愿景是用区块链激活巨大的共享经济行业，人和终端都成为 WeShare 区块链网络的组成，形成基于用户、终端、服务、数据的使用权和所有权为交易载体的价值生态经济社区。

WeShare 链是我们迈出的第一步，我们将与共享经济、金融、健康医疗、供应链、工业、物联网、能源服务等多个领域悉心耕耘的商业伙伴共同成长，聚焦于各种行业应用，深刻洞察市场需求，积极进行技术更迭。

3 技术特色和优势

WeShare 链遵循以下六大价值理念：

1.1 分布式商业的定义与边界

新一代分布式商业模式的兴起与涌现是社会结构、商业模式、技术架构演进的综合体现，参与者众多且分别拥有大量数据是这个时代日益凸显的基本特征，商业活动的发起与完成都

需要引入更多参与方来协同操作。最终用户的需求将不再可能单一依赖于某个服务提供方，要求更多拥有垂直领域数据的参与方按照约定的方式、公开透明的提供服务。分布式商业以多方参与、智能协同、专业分工、价值分享等为主要特征，典型的应用场景有银行联合贷款、银证信保的多方产品合作、N+N 供应链金融、分布式能源、分布式电商以及各类共享经济等。分布式商业提倡“专业分工”和“价值连接”：通过预先设定透明的价值交换或合作规则，使得分工及集群后的新商业模式产生强大力量，与传统单一中心化实体主导的商业模式相比有显著优越性。

1.2 分布式技术的特性与价值

为了实现分布式商业的对等、共享与透明规则，以开源为主要特征的分布式技术得以发挥优势，区块链技术、分布式账本技术等渐渐成为了前沿科技的核心代表。一方面，技术架构变革导致分布式架构应用价值凸显。集中式的传统技术架构因其较高的投入、较差的弹性、对少数几家厂商过度依赖而面临发展瓶颈，技术上陷入“大而不能倒”的窘境，并难以实现对新型商业模式的有效支撑。而在分布式商业模式下，参与各方具有平等地位，专注各自领域且足够成熟，在此基础上，采用基于对等架构的技术平台实时交换和共享数据，同时接入多家合作方，可以有效提升商业上的容错性，从而

避免商业上的“大而不能倒”的情况发生。另一方面，在安全可控成为国家战略的背景下,寻求区别于传统中心化架构的高性能、高扩展、高可靠且低成本的分布式架构，是新一代技术的必然选择。因此，以区块链为代表的分布式账本技术的价值逐渐凸显。区块链技术是一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理可信数据的产生、存取和使用的模式。广义上，这是由分布式架构与分布式存储、块链式数据结构、点对点网络、共识算法、密码学算法、智能合约等多种信息技术共同组成的整体解决方案。

1.3 分布式商业与技术的融合与演进

区块链技术的应用最早从金融行业起步，并逐步向各个行业渗透。由于金融行业参与者群体广泛，而不同类型的金融机构其资质、资本、资源等禀赋各异、互补性较强，因此通常是以同业合作的对等形式共同设计产品或开展业务，如银银、银信、银保、证信合作等，天然形成了较多分布式商业场景的雏形，在某种程度上，分布式商业是传统金融同业合作模式的升华。同时，健康医疗、物联网、工业互联网、能源服务、物流、供应链等多个领域也都存在类似需求与要求，这亦对区块链底层平台提出了较高的要求，为区块链技术与分布式商业的融合提供了演进的路线参考。

1.4 规模化商用的挑战

如需成功运用区块链技术，首先，需要改变传统的“中心化”商业模式的思维，走向专业分工、开放合作和价值共享，拥抱“分布式商业”这一新业务形态。其次，新的技术终究要在应用场景尤其是具备海量用户的企业级应用场景中被充分验证并推广，才能评判其成熟度。在过去几年里，区块链底层平台与应用虽然不断涌现，但大多数仍停留在实验室阶段以及小规模探索阶段，具体而言，区块链技术在中国进行大规模的商用仍然存在以下六点挑战。

- 政策可行性——是否与现有的技术监管、行业监管、技术治理、技术合规等要求符合，是否需要政策、法律、法规等的修改与支持；
- ✓性能可用性——是否满足大量用户、高并发量、快速响应时间、大量存储等的可用性要求；
- ✓业务适当性——是否能解决传统中心化技术难以解决业务痛点，带来新的分布式商业模式变革；
- ✓安全可控性——是否符合特殊行业的高安全级别要求，是否采取了各种必要的安全手段，保障链上资产和交易等信息的安全、可防范攻击等；
- ✓技术使用难度——是否通过规范开发语言、接口标准、友好平台等途径，降低应用难度，便于无技术积累的企业

也能快速灵活加入使用；

- ✓治理难度——是否对区块链系统与传统系统的结合与互补有所考虑，是否规划设计了综合型系统的治理方法，对所有资源或对象进行统筹管理等。

基于对以上挑战的考虑，WeShare 链从中国的商业可行性与监管要求出发，对场景进行了深度理解，对平台进行深度定制，是更适合国内企业的联盟链解决方案；另一方面，我们本身就具有大规模的商用业务需求，对生产环境里能达到的并发用户数、访问量、吞吐量、响应时间、可用性、安全性等要求更高，因此从生产应用落地角度在联盟链的架构上也做了深度设计。

通过大量业务模型、应用模型的数据测试分析，WeShare 链在性能方面可达到：秒级交易验证、海量数据存储，高吞吐量、节点数据快速同步；在扩展性方面可达到：满足多业务区块结构、权限控制策略；同时，提供安全的私钥存取服务，以及隐私保护方案。

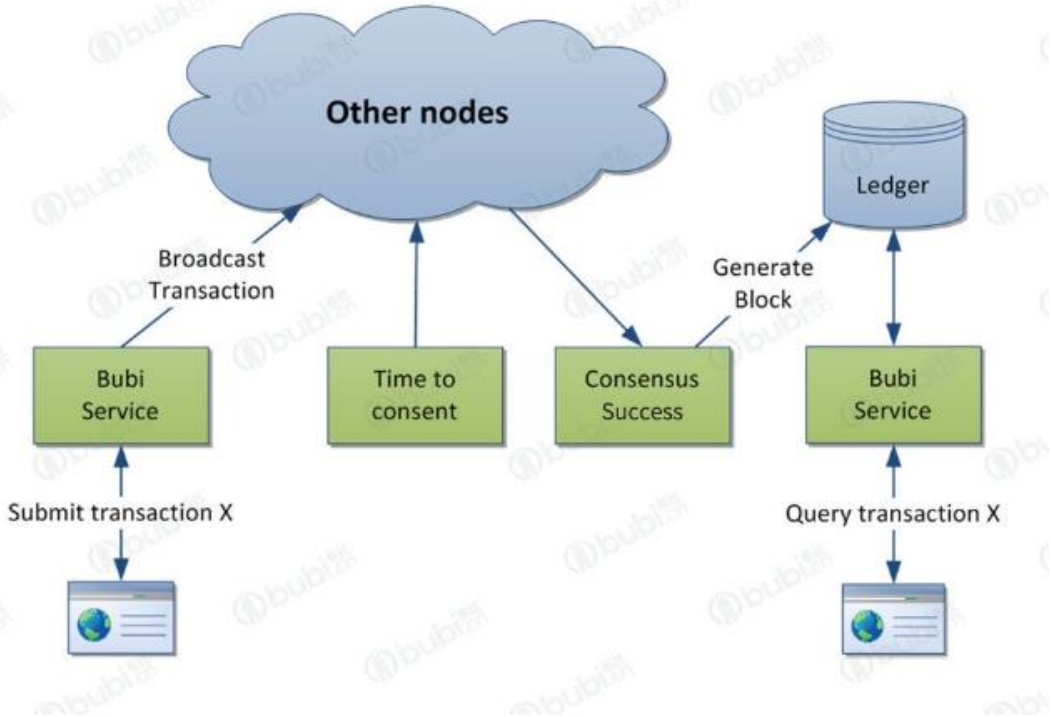


图 5-1 快速交易验证

通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，WeShare 链可以实现秒级的快速交易验证。满足绝大部分区块链应用场景的用户体验。

WeShare 链支持如下各种特性：

- 海量数据存储

区块链复式记账的模式，在系统长时间运行下，历史数据不断累积；WeShare 链借鉴传统金融系统中冷热数据分离存储、分表存储的机制，实现海量数据的有效存储。旧的交易数据，非活跃的资产数据等信息可以使用大数据存储平台进行存储（如 Hadoop，满足 PB 级别的数据存储）。

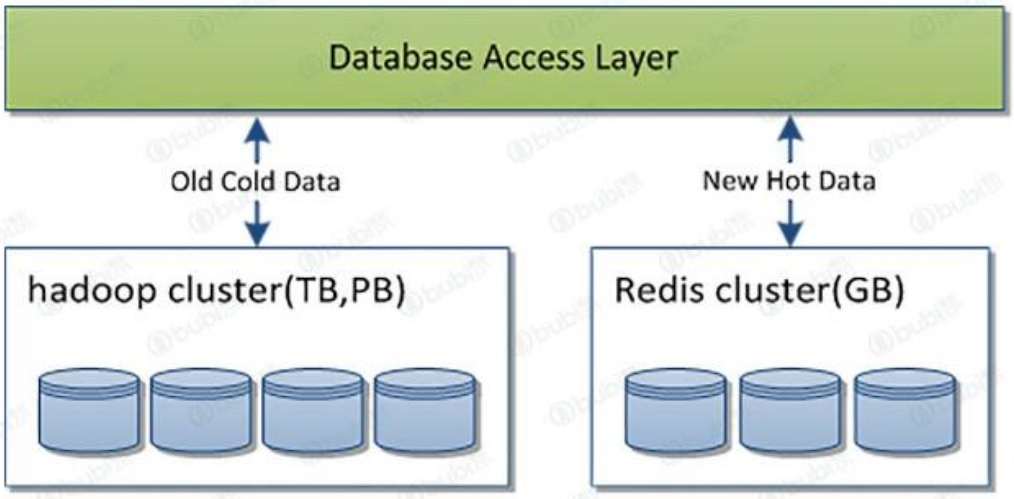


图 5-2 海量数据存储

- 高吞吐量

  区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，WeShare 链的处理性能已经能满足万级 TPS 的需求。如果再引入 Off-Chain 等机制，还能进一步大幅提高交易吞吐量。

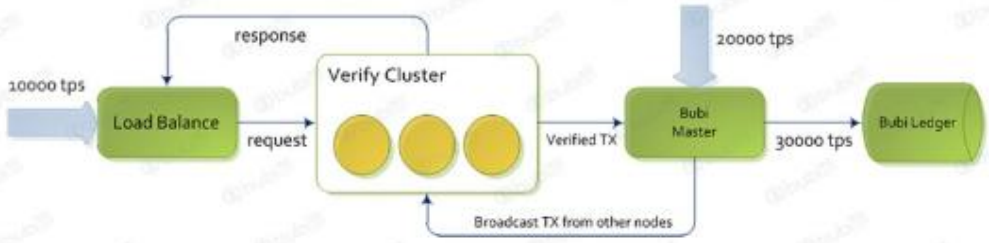


图 5-3 高吞吐量

- 节点数据快速同步

  WeShare 链支持镜像(Snapshot)机制，可以定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚；同时，缩短新加节点加入运转的周期，仅需同步最新镜像及少量近期交易集合，即可融入网络并参与共识验证。

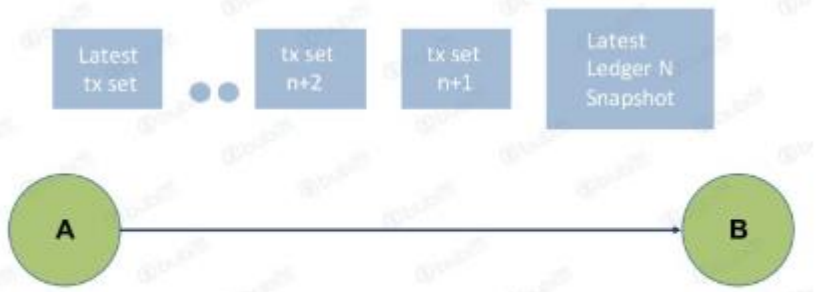


图 5-4 节点数据快速同

- 权限控制策略

提供数据信息写入与读取两类权限控制策略。数据信息写入权限，同一账户下设置多个使用用户，并针对不同的操作设置相应的权

限，满足多方签名控制的使用场景。数据信息读取权限，用户可以授予和撤回单用户或用户组对数据的操作权限，用户组可以由用户灵活配置。数据包括用户账户信息，交易信息等，粒度可以细化到交易或账户的各属性字段。

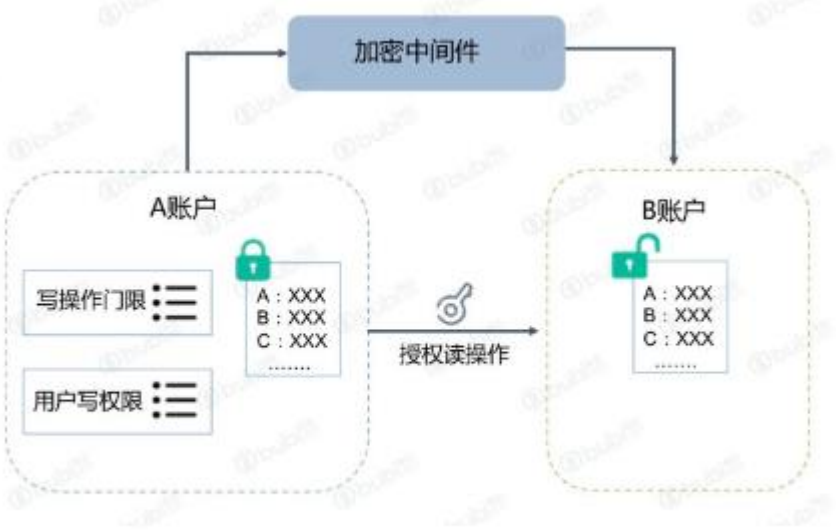


图 5-6 权限控制

- 安全私钥存取

  为了方便用户使用区块链产品服务，除了传统的客户端生成和保存的机制，WeShare 还提供网络托管存取和私钥硬件存取（U-key）两种方案。网络托管存取，即把用户名和密码通过特定算法映射成私钥并在服务端进行存储。服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；硬件私钥是为了满足金融行业及物联网行业的使用需求。

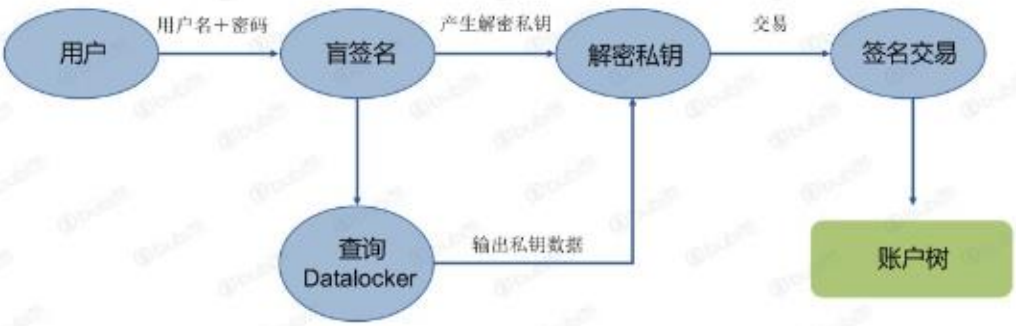


图 5-7 安全私钥存取

- 多重隐私保护方案

  提供多重隐私保护功能。首先，区块链底层提供同态加密方式，用户所有数据均加密存储，仅用户本身可见。其次，WeShareAdaptors 提供加密中间件服务，用户可根据业务需要进行选择。最后，上层应用可以在录入时对数据进行加密处理，WeShare 平台负责对用户生成的加密数据进行写入和读取。

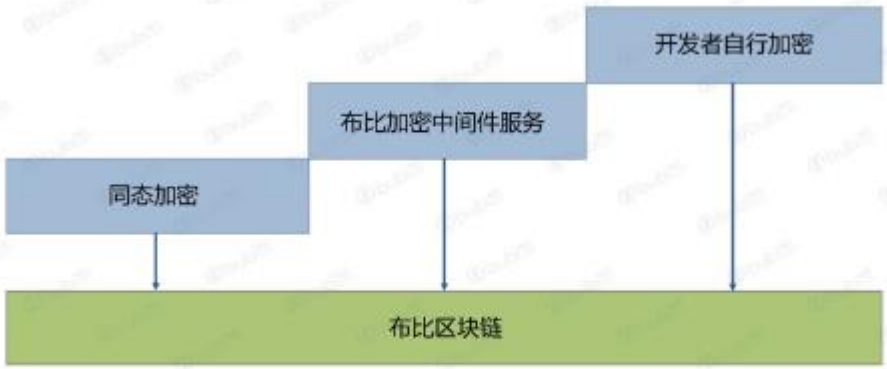


图 5-8 多重隐私保护方案

- 全平台部署支持，方便部署运维

  WeShare 链的所有代码均可跨平台编译运行，平台相关代码均

封装成基础库，业务逻辑独立于 WeShare 平台。除了 PC 及服务器的方式编译，同时支持交叉编译方式，如 ARM、MIPS 平台，方便在移动便携式系统部署，为区块链物联网化做预备支撑。同时，WeShare 已与国内几家知名云平台达成战略合作，可以实现在云平台上快速部署。

图 5-9 全平台部署

- 可视化运维

  提供运维管理所需的可视化工具。区块链节点上部署的系统监控服务（MonitorAgent）：支持业务（区块、交易、合约、共识等）、网络（组网、时延、吞吐量等）、系统层面（CPU、内存、磁盘等）的数据信息监控；同时提供完备的日志、告警与通知机制，便于商用系统的维护。

图 5-10 可视化运维

- 低成本接入方式

  WeShareAdaptors 抽象出适用于多种业务场景的 API 接口，如：资产、溯源、存证等，供这些场景相关的业务直接使用。在新的业务场景下，WeShare 链可以基于现有的框架为用户快速定制接口，满足业务功能需求。同时提供已封装的支持多种主流开发语言（JAVA、C++、node-js、PHP）的 SDK 软件开发包。目前区块链技术服务主要有两种：一种是搭建一套区块链底层，提供一套标准化的 API 并开放，然后由开发者自己对接应用；另外一种是配合上层应用解决一些行业痛点，将分布式账本内嵌到已有的应用系统中。区块链是一项新兴技术，只有不断的满足业务需求，才能走向成熟，所以我们通过对底层分布式账本的封装，降低上层应用使用的门槛，在对接和使用的过程中，不断地优化和完善底层分布式账本和共识算法，使之更加贴近商用诉求。

4 技术架构

为了解决区块链技术在应用落地过程中可能面临的各种阻碍，WeShare 链平台采用两层结构：

（1）底层 WeShare 链提供区块链基础服务；

（2）上层应用进行封装处理，对外进行统一接口，提供一系列符合应用场景的接口，降低应用对接的复杂度，如图 4-1 所示。

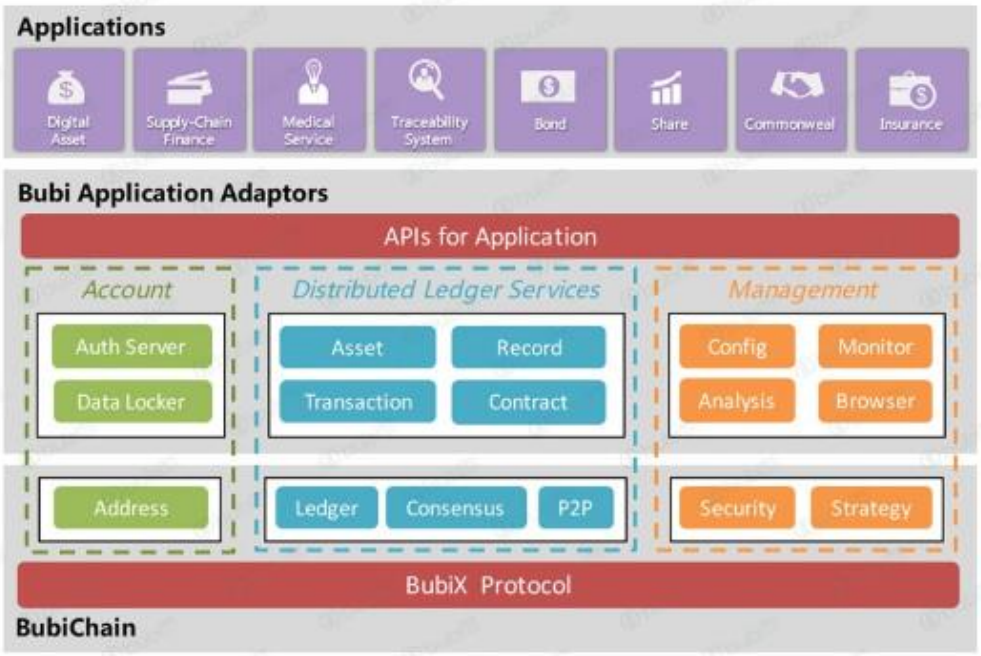


图 4-1 布比区块链平台架构图

WeShare 链产品体系架构组成部分：账户中心、分布式账本服务、策略与管理。其中，部分采用某些标准的开源组件，部分是在成熟框架上进行优化和改进，部分从头构建。

- "账户中心（Account）：公私钥生成，公钥写入，私钥签名与管理；应用层用户信息与区块链地址的映射；支持实名认证及审计的监管需求。
- "分布式账本服务（Distributed Ledger Service）：基于 P2P 协议的底层组网，各节点通过 P2P 协议进行消息分发；提供账本结构的定义和账本数据的存储；可插拔的共识模块，负责确保底层数据强一致性的同时抵抗来自“恶意”节点的攻击。针对应用的建模适配，包括对资产、记录、事务、合约等多种对象的建模和实现。
- "策略与管理（Management）：提供完备的数据隐私安全及访问策略控制的解决方案。多种可视化管理工具，底层区块链的健康监控、系统参数配置、数据分析、区块链浏览器等。

4.1 账户中心

在区块链技术自有的公私钥体系下，账户中心负责：公私钥生成，公钥写入，私钥签名与管理；保存应用层用户信息与区块链地址映射关系；支持实名认证及审计的监管需求。为应用适配层提供两类接口：非托管型接口和托管型接口。

非托管型接口：适合有能力在应用端实现安全级别较高的私钥生成和使用的企业机构。例如，在金融领域，将私钥的生成与管理跟现有的 U 盾、电子签名等安全的客户端体系相结合。

托管型接口：适用于互联网化程度较高的应用场景。公私钥直接作为用户名和密码使用对普通用户来说识记成本高体验差，大多数用户习惯用手机号、邮箱、昵称等作为用户名。因此，在托管型接口里，通过安全的私钥生成与管理的体系，应用层用户信息与区块链地址映射，使上层应用和底层区块链平台都无法触碰到用户的私钥。

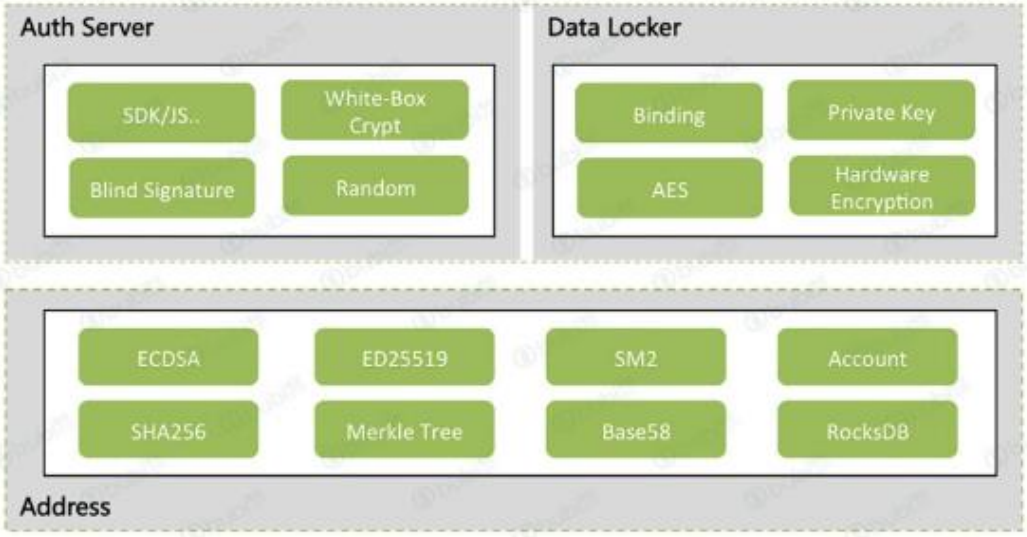


图 4-2 账户中心

托管型接口使用账户中心架构，由鉴权服务（Auth Server）、私钥保险箱（Data Locker）、区块链账户树（Address）三部分构成，如图 4-2 所示。

- 鉴权服务

  鉴权服务主要解决第三方应用与账户中心的安全问题。通过在交互过程中加入随机数和盲签名技术，增强密钥安全，降低暴力破

解的可能性；同时利用白盒加密技术强化客户端的访问安全。

- 私钥保险箱

  私钥的写入和读取在保险箱体系里以密文的方式传输和存储。用户与密钥一一对应。密钥在客户端侧生成且客户端不用保存，每次需要使用私钥签名时，客户端能够通过盲签名流程得到加密过的私钥以及解密的密钥。

- 区块链账户树

  WeShare 链上存储完整的账户树，每个叶子节点记录一个账户的资产信息和身份信息(可选)；每个账户可以支撑多维资产的使用。支持多种加解密算法，依据不同场景选择使用。

4.2 分布式账本服务

WeShare 链底层服务由 P2P 组网、分布式账本、共识服务三部分组成；同时，为方便应用层理解和对接，在分布式账本服务适配层抽象出应用组件。（如图 4-3 所示）

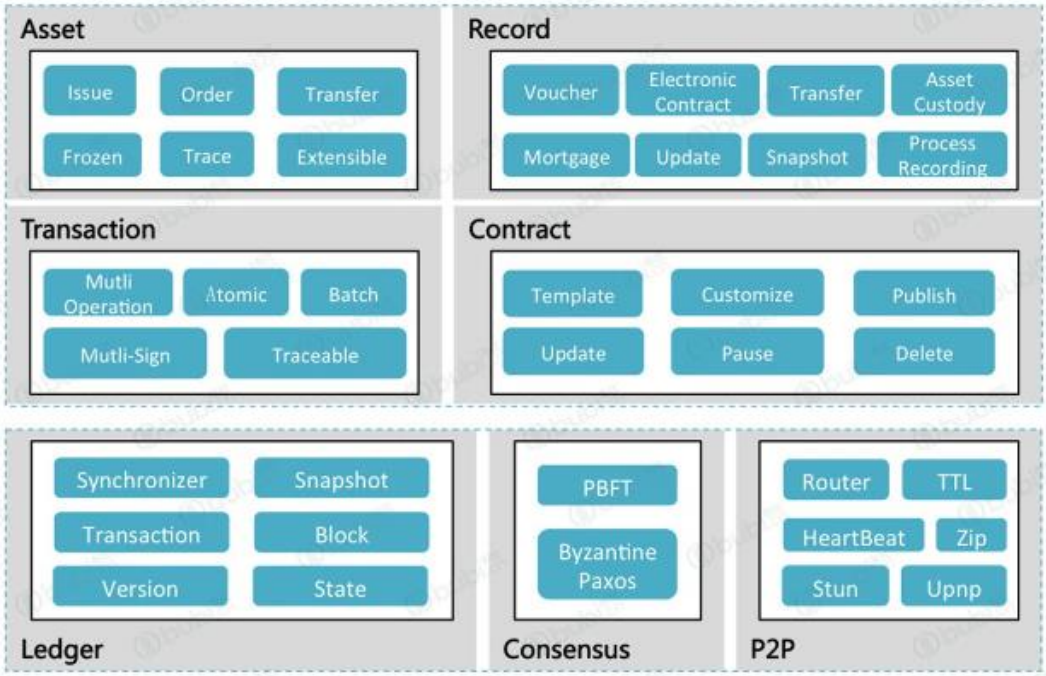


图 4-3 分布式账本服务

底层架构

- P2P 组网：对等协议（Peer-to-Peer）实现基础组网和通信，每个节点维护一张邻居列表，实现动态自组织网络；并可与现有的安全防护设施配合使用，确保商用网络的安全性。
- 分布式账本：解决数据格式、数据记录、数据存储问题，通俗的说就是“记什么账和如何记账”。因此分布式账本设计的好坏决定了区块链底层对外提供服务的能力。
- 共识服务：是区块链的核心，也是区块链与传统分布式系统的最大区别之处。它保障底层数据的强一致性的同时，能抵抗“恶意”坏人的影响。WeShare 链的共识服务提供一组抽象的共识接口，

用于连接共识算法和其它 WeShareChain 模块。它负责接受和处理 Transaction，并给出共识结果。共识服务采用开放式框架，可支撑不同种类的共识算法，目前 WeShare 链已经开发 Byzantine Paxos、Byzantine Raft 商用共识算法，同时支持 PBFT 等共识算法，可以根据上层应用对性能、安全性、容错能力等需求选择不同的算法。

- 应用组件

  为方便应用层理解和对接，在分布式账本适配层抽象出：资产（Asset）、记录（Record）、事务（Transaction）、合约（Contract）等各类组件。

  - ✓ 资产（Asset）：支持目前已经数字化的资产，以及未来可以通过资产证券化、资产数字化的资产。
  - ✓ 记录（Record）：需要利用区块链增加信息记录的真实性和信任的场景，例如：金融领域的凭证、供应链的溯源信息等。
  - ✓ 事务（Transaction）：与区块链底层交互的原子级操作，一个上层应用可以对应一个事务，也可以由一组事务共同完成。
  - ✓ 合约（Contract）：提供两种合约——标准化合约、可编程合约。标准化合约，它主要针对场景相对简单、标准化程度较高，同时对执行效率有很高要求的业务需求。例如资产交换时的交易一致性保障、资产交易的挂单与撮合等。标准化合约可以通过配置生成直接挂在链上，无需编程，也不用通过虚拟执行，降低上层应用使用的成本，提升合约执行的效率。为了应对用

户复杂的业务逻辑，WeShare 链也支持用户自编程，并且提供丰富的组件供用户针对特定的需求快速构建应用，如加密组件、权限管理组件等。同时 WeShare 链对于通用的场景如资产、存证提供相应的模板，用户不需要从头编写代码，只需要更改模板的关键参数，加上自己业务的特性就可以建立成熟的合约应用。

4.3 策略与管理

WeShare 链平台提供的安全与策略机制，既可以管理维护区块链系统本身的配置和安全，也可以管理区块链存储数据的访问策略和隐私安全。

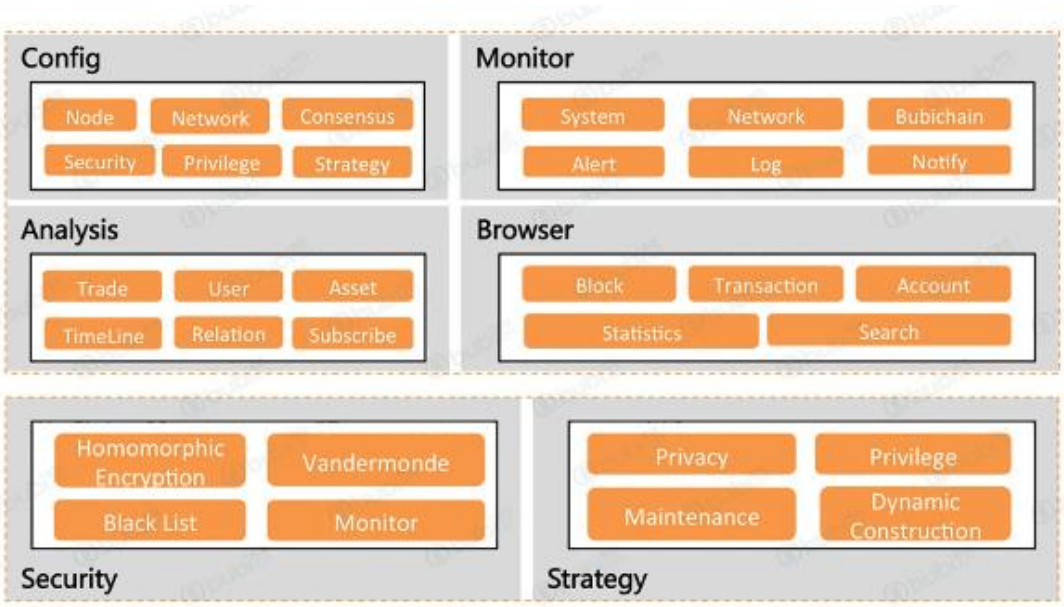


图 4-4 策略与管理

如图 4-4 所示，区块链底层提供安全（Security）与策略（Stratery）两个基础功能，应用适配层提供一系列可视化的管理工具，有配置管

理（Config)、健康监控（Monitor)、数据分析（Analysis)、区块链浏览器（Browser)。

- 安全(Security)底层安全服务负责解决系统组网、接口访问、共识算法、数据隐私等安全问题。目前，大多数行业应用都是联盟链和私有链。
  - ✓ 系统组网安全：组网方面可以用传统的一些安全措施进行加固：例如接入 IP 控制、专线、节点授权才能接入、节点信任列表等。
  - ✓ 接口访问安全：在接口层可以引入 CA 机制，只有授权的机构才能访问区块链平台的接口。
  - ✓ 共识算法安全:不同的共识算法都有一个安全边际,以PBFT为例，N/3 的安全问题是由配置决定的，安全性和容错能力在 2/3 阀值处于极大值。如果为了追求共识算法的安全，可以牺牲一部分容错能力，将投票通过阀值设置在 90%，甚至更高。同时还可以加入恶意节点发现与处理、黑白名单制等，加强共识算法的安全。
  - ✓ 数据隐私安全：区块链作为一个数据仓储的解决方案，它能提供的隐私保护与传统的数据库没有太大区别：对称加密和非对称加密，常用的技术有同态加密和 RSA；隐私保护与区块链的数据共享信任之间的平衡是由业务场景来决定的。
- 策略（Stratery）策略服务除了提供上述的安全策略外，还包

括节点部署策略、数据访问权限策略、多签名（Multisign）联合控制策略、合规性策略、性能策略等。

- 配置管理(Config)配置管理服务主要提供可视化的配置操作，针对上述的安全、策略、权限、区块链节点、分布式账本结构、共识算法、系统参数等进行灵活设置；配置本身也可以作为一种区块链的事务，由节点共同投票确定生效。
- 健康监控（Monitor）WeShare 链的区块链健康监控平台提供三个维度的监控：物理层（CPU、内存、磁盘等）、网络层（时延、断线）和业务层（区块生成、交易验证）；并且提供完善的告警、日志、消息通知机制体系，便于商用系统的运维。
- 数据分析（Analysis）分布式账本内存储的大部分是原数据，还有少量标准化的关联关系。为了满足上层应用各种复杂的数据分析需求，数据分析服务除了提供标准的数据查询接口，还支持批量导出和订阅式两种定制化的接口服务。
- 区块链浏览器（Browser）在不涉及隐私的情况下，区块链浏览器可以实时看到整个区块链底层存储的数据信息，包括区块信息(Block)、账户信息(Account)、交易信息(Transaction)、合约信息（Contract）等。

5 产品规划和路线图

5.1 产品规划

• 2019 年 3 月

WeShare 链项目启动；

• 2019 年 8 月

WeShare+共享经济应用发布；

• 2020 年 5 月

WeShare 公链上线运行；

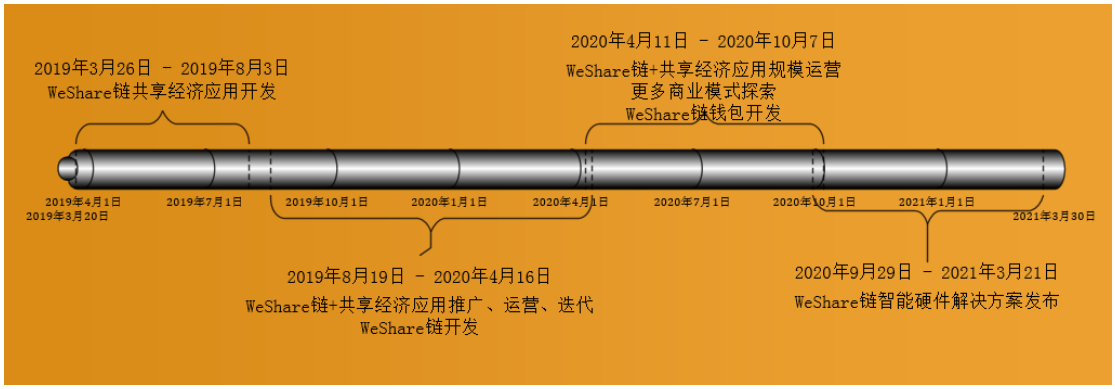
• 2020 年 10 月

WeShare 链钱包客户端上线；

• 2021 年 3 月

WeShare 链智能硬件解决方案发布，与物联网、智能硬件厂商战略合作推出产品，共建共享经济生态；

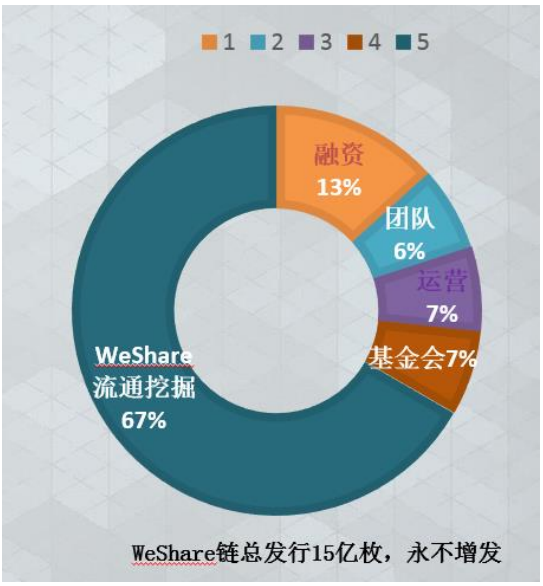
5.2 路线图和里程碑



6 WeShare 链原生资产介绍

6.1 加密数字黄金 WSG 发行

WSG 是 WeShare 链共享经济平台运作的基础代币（加密数字黄金，WeShareGold），基于以太坊区块链底层发行，发行总量为 15 亿枚（永不增发），接受智能合约限定。



1 亿用于早期种子轮和天使轮融资；早期投资人为私募阶段，为 WeShare 链提供资金、资源、技术等方面的支持；1 亿用于后续融资使用，充当股权凭证；
1 亿用于团队激励；团队持有的 WSG，分三年共计 6 期进行解禁;
1 亿用于商业合作与市场。用于 WeShare 链社区的维护、运营、品牌、公共关系等，提升用户体验，维护粉丝圈对社区的信任；
1 亿用于基金会管理和社区建设，用于 WeShare 链基金会的运营，包括代码安全审计、市场、法务、财务、第三方审计等；
WSG 流通挖矿预留 10 亿，WeShare 链共识采用 POT（交易量证明）机制，挖矿激励根据共享经济平台产生的增值来奖励。

6.2　加密数字黄金种子轮、天使轮募资

早鸟阶段总共融资 1 亿个 WSG，时间 2019.4.2 9:00-2019.4.30 18:00
本次融资接受法币、BTC、ETH（美元按即时汇率；BTC、ETH 按即时的交易所价格进行相应兑换）；
募资过程透明，可以通过官网即时查看过程；
欢迎投资人、推广合作伙伴、创业合伙人沟通联系；
具体价格如下：

6.3 团队组成

团队具体组成包括：

- 区块链技术开发中心：负责 WeShare 链技术管理工作，具体工作包括开源代码管理、代码开发、代码修改、代码测试、代码审核、代码上线、漏洞修复等。
- 区块链商业应用中心：负责 WeShare 链上线后的应用场景落地工作，上链资产尽职调查、上链资产合规性审核、上链资产信息披露、上链资产交易管理等。
- 财务管理中心：负责整个项目募集资金的使用和审核、开发人员薪酬管理、日常运营费用审核等。
- 法务及风控部：负责境内外公司的注册登记、审核各类协议，对法律事务给出专业意见，开展法律知识的培训，提高各部门人员的法律意识。
- 综合事务管理中心：负责 WeShare 链相关文件起草、会议安排等

行政事务类工作；负责整个项目的人员招聘、薪酬福利、学习培训等工作；塑造、推广 WeShare 链的品牌形象，建立良好的社会公共关系。

- 基金会：基金会作为 WeShare 链治理的主体，全面负责管理 WeShare 链技术开发和应用开发，维护 WSG 持有人权益，宣传推广 WeShare 链品牌等。

6.4 WeShare 链基金会

WeShare 链基金会（以下简称“基金会”）致力于项目的研发和运营，积极推进区块链+共享经济发展。

基金会将通过制定良好的治理制度，管理 WeShare 链生态。基金会每月公布项目进展，每年审计并公布审计报告。 WeShare 链基金会将由技术部、商务合作部、运营部、财务部、人力资源部、法务部、顾问团等各个相关负责人组成。

基金会负责 WeShare 链的各种基本管理制度；决议 WeShare 链开源代码重大问题和资金使用重大问题的解决方案；应对 WeShare 链出现的紧急事件。

基金会成员 3~11 名，设主席委员一名。基金会成员任期 3 年，可以连任。基金会主席由委员会投票选举产生。

基金会会议做出决议，必须经委员会的投票通过。基金会每年至少召开一次会议，每次召开十五日以前通知全体成员。基金会会

议由半数以上委员或主席提议后召开，基金会的所有决议将在WeShare链官网公告。

基金会主席行使以下职权：

1）主持持有人大会和召集、主持基金会会议；

2）检查基金会决议的实施情况；

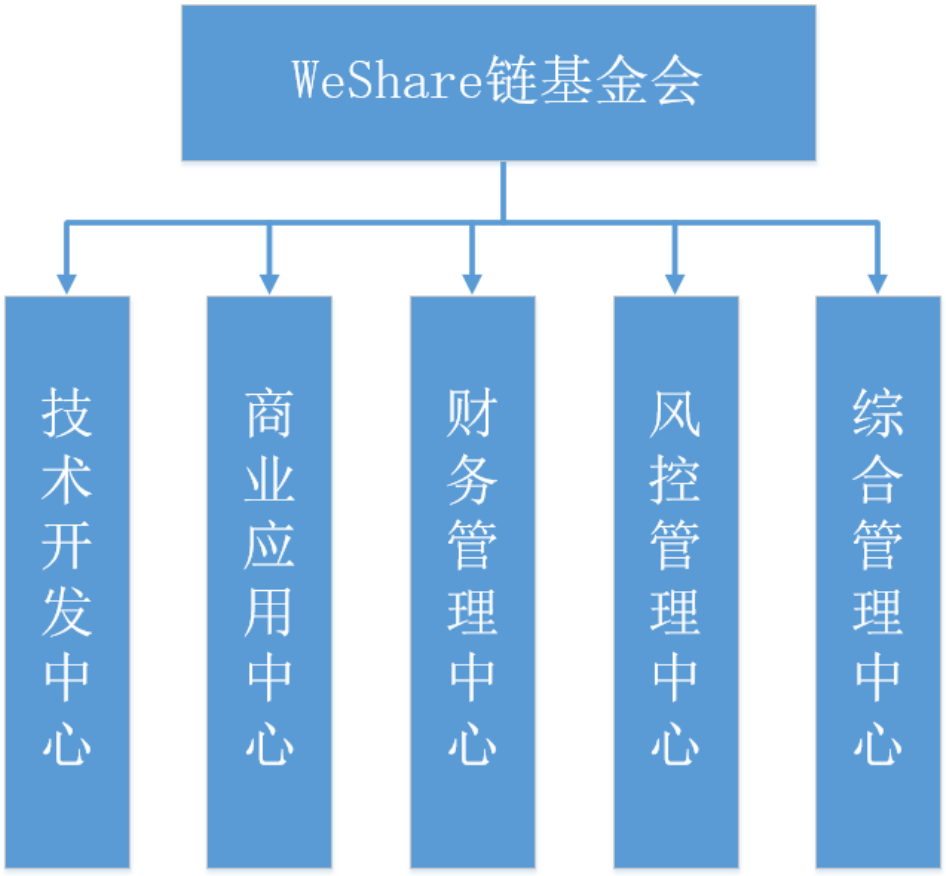
3）拥有对基金会会议决议的一票否决权；

4）拟定WeShare链开源代码问题和审核资金使用情况；

基金会机制说明WeShare链对分布式自制机构的治理提出开创性的方案，WeShare 链是一种分布式商业区块链，建立在区块链世界里，用区块链技术来构建的治理方式。

WST 持有人大会让 WSG 持有人可通过预设的代码规则参与到WeShare链的治理中。

基金会对WSG持有人大会负责，基金会监督WeShare链的相关工作。



6.4.1 财务管理

说明 WeShare 链基金会财务管理的原则 :统筹安排, 综合管理；勤俭节约，讲求实效；精打细算，量入为出。WeShare 链基金会资产管理纳入全面预算管理，根据实际运营情况，编制财务收支预算。年度财务收支预算报自制委员会审议，月度财务预算由执行委员会审议，财务管理中心负责编制和执行。在官网 https://bytom.io/披露每个季度的财务报告。数字资产使用权限：单笔支出超过 50 个比特币，需要执行委员会首席执行官同意；单笔支出超过 100 个比特币，需要基金会会议同意。WeShare

链基金会将引入第三方审计，监督项目的财务运作，进行资金审计和提供审计报告，审计报告将在年度信息披露中公告。

1.资金来源维持 WeShare 链项目运作的资金主要来源于 ICO 和原生资产 WST。在需要的时候部分加密数字资产会转换为法币，以拥有必要的支付资金。2.私钥管理说明 WeShare 链通过 ICO 筹集到的加密数字资产及原生资产，将由专业的加密资产管理服务商提供资金管理服务，采用多重签名的形式管理私钥，在项目发展的过程中逐步完善私钥管理制度。项目初始阶段 WeShare 链基金会多重签名私钥在由项目联合创始人多人持有，采取 2/3 多重签名。管理多重签名人的增加或减少，由执行委员会决议。随着项目的发展和资产规模的扩大，多重签名私钥的控制方将逐步包括但不限于：WeShare 链基金会代表，WeShare 链持有人代表、专业硬件钱包服务商，专业加密资产管理服务公司、审计公司等。

6.4.2 风险警示

参与 WeShare 链 WSG 的购买者，请请仔细阅读 WeShare 链技术和经济白皮书，全面认识 WeShare 链 WSG 的风险收益特征和 WeShare 链技术特性，购买者应明白 WeShare 链项目不会在任何情况下提供退款。WeShare 链项目团队将按照所披露的白皮书内容，合理运用筹集的数字资产，规范管理项目，尽管

WeShare 链项目团队将恪尽职守，履行诚实、信用、勤勉尽责管理的义务，购买者也存在损失的风险，风险主要包括：

1、政策风险由于目前国家监管机构对 ICO 项目尚未出台明确的监管措施，因此随着政府有关 ICO 项目的政策发生重大变化或是有相关的政策、法规出台，将引起 ICO 市场的波动，从而给 ICO 参与者带来风险。

2. 经济周期风险受经济周期的影响，ICO 项目开发进度及数字资产管理将会相应受到直接或间接影响，项目方将会相应调整项目推进进度，并及时进行公开披露。

3. 网络黑客风险项目团队已经建立起技术安全架构防范外部侵入，但黑客攻击、病毒木马等攻击手段的更新或衍变，将会威胁到项目开发及数字资产管理，从而给项目推进带来难以预测的风险。

4. 技术风险 ICO 项目在启动时已完成概念证明，并公开部分代码框架及明确的里程碑设计，但是并不排除由于技术测试及技术路线预估不充分，从而给项目开发进度带来一定影响。

5. 代币风险 WST 的使用范围受用户和市场的认可度限制，在 WeShare 链完成测试并上线使用后，最终 WST 在链上的接受度和普及度存在不确定性。WST 并非代表持有人对 WeShare 链项目享有任何权益，并且 WeShare 链团队将不会回购，及对 WST 作出任何收益承诺。

6. 币价波动风险

WST 进入数字资产交易市场后，由于并不像中国股市那样的涨跌停限制，交易所 24 小时开放，价格易受到庄家控制以及全球政府政策的影响而大幅波动。因此，WeShare 链团队不对 WST 的市场、价值及价格等不做任何明示或暗示的保证，持有人理解并了解数字资产交易市场是不稳定的，价格和价值随时会大幅波动或崩盘。用户应慎重考虑上述风险并用清晰的判断能力去评估 WeShare 链项目、自身财务状况及风险承受能力而作出投资决策，并承担由此产生的全部损失。

6.4.3 披露义务

为保护投资人利益，加强加密数字资产的管理和高效使用，促进 WeShare 链项目的健康发展，WeShare 链项目设置信息披露制度。WeShare 链项目发起团队承诺将恪尽职守、诚实信用、谨慎勤勉的原则管理和运用ICO所众筹的加密数字资产。WeShare 链希望能通过自身的示范作用，规范 ICO 项目数字资产的管理，增加区块链行业的自律，提升区块链加密数字资产管理的透明度，维护好区块链行业的长远发展。定期信息披露，在每个会计年度之日起三个月内编制并披露年度报告，每个季度结束后的两个月内披露季度报告。报告内容包括但不限于 WeShare 链项目的技术开发里程碑及进度、应用开发里程碑及进度，数字资产管理情况，团队履职情况，财务情况等。临时信息披露，WeShare 链基金会应及时报告 WeShare 链项目的重大合作事项、核心团队

成员变更、涉及到 WeShare 链的诉讼等。WeShare 链将在官网 https://bytom.io/披露信息报告。

7 附录

7.1 术语解释

1)比特币：比特币是一种加密数字货币，在 2009 年由化名的开发者中本聪（Satoshi Nakamoto）以开源软件形式推出。

2)以太坊：英文名 Ethereum，是一个有智能合约功能的公共区块链平台。

3)超级账本：英文名 Hyperledger，是 IBM 发起的专注于联盟链的开源社区。

4)以太坊虚拟机：以太坊虚拟机设计运行在点对点网络中所有参与者节点上的一个虚拟机，它可以读写一个区块链中可执行的代码和数据，校验数据签名，并且能够以半图灵完备的方式来运行代码。它仅在接收到经数据签名校验的消息时才执行代码，并且区块链上存储的信息会区分所做的适当行为。

5)图灵完备语言：一个能计算出每个图灵可计算函数（Turing-computable function）的计算系统被称为图灵完备的。一个语言是图灵完备的，意味着该语言的计算能力与一个通用图灵机（Universal Turing Machine）相当，这也是现

代计算机语言所能拥有的最高能力。

6)智能合约：智能合约是由时间驱动的、具有状态的、运行在一个复制的、分享的账本之上的、且能够保管账本上资产的程序。

7)代币：除了比特币以外的数字货币。

8)公有链：公有链是任何人在任何地方都能发送交易且交易能获得有效确认的、任何人都能参与其中共识过程的区块链。

9)联盟链：与公有链相比在开放程度和去中心化程度上有所限制，参与者均早已达成共识并互相信任。

10)POW：(Proof of Work，工作证明)，就是说，你获得多少货币，取决于你挖矿贡献的有效工作，大部分的虚拟货币，比如比特币、莱特币等等，都是基于 POW 模式的虚拟货币（算力越高、挖矿时间越长，你获得的货币就越多)。

11)POS：(Proof of Stake，股权证明)，就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明 POS 模式下，有一个名词叫币龄，每个币每天产生 1 币龄，比如你持有 100 个币，总共持有了 30 天，那么，此时你的币龄就为 3000，这个时候，如果你发现了一个 POS 区块，你的币龄就会被清空为 0。

12)PBFT：Practical Byzantine Fault Tolerance 的缩写，意为实用拜占庭容错算法。该算法是 Miguel Castro(卡斯特罗）和 Barbara Liskov（利斯科夫）在 1999 年提出来的，解决了

原始拜占庭容错算法效率不高的问题，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行。

13)QOS：（Quality of Service，服务质量）指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。

14)RSA：Rivest、Shamir、Adleman 于 1978 年首次发表的国际通用的公钥密码算法，公钥密码系统与只使用一个密钥的对称传统密码不同，算法是基于数学函数而不是基于替换和置换。公钥密码学是非对称的，它使用两个独立的密钥，即密钥分为公钥和私钥，因此称双密钥体制。双钥体制的公钥可以公开，因此称为公钥算法。

15)国密算法 :国家密码局认定的国产密码算法。主要有 SM1，SM2，SM3，SM4。密钥长度和分组长度均为 128 位。SM1：对称加密。其加密强度与 AES 相当。该算法不公开，调用该算法时，需要通过加密芯片的接口进行调用；SM2:非对称加密，基于 ECC。该算法已公开。由于该算法基于 ECC，故其签名速度与秘钥生成速度都快于 RSA。ECC 256 位（SM2 采用的就是 ECC 256 位的一种）安全强度比 RSA 2048 位高，但运算速度快于 RSA；SM3:消息摘要。可以用 MD5 作为对比理解。该算法已公开。校验结果为 256 位；SM4:无线局域

网标准的分组数据算法。对称加密，密钥长度和分组长度均为 128 位。

16)P2P：对等网络，即对等计算机网络，是一种在对等者之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。“Peer”在英语里有“对等者、伙伴、对端”的意义。因此，从字面上，P2P 可以理解为对等计算或对等网络。

7.2 参考文献

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song. Remote data checking using provable data possession. ACM Trans. Info. & System Security, 14(1), May 2011.

[2] M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia. Privacy-preserving group data access via stateless oblivious RAM simulation. In SODA, 2012.

[3] H. Shacham and B. Waters. Compact proofs of retrievability. Proc. Asiacrypt 2008.

[4] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin. Erasure coding in Windows Azure storage. In G. Heiser and W. Hsieh, editors,

Proceedings of USENIX ATC 2012. USENIX, June 2012.

[5] L. Rizzo. Effective erasure codes for reliable computer communication protocols. ACM SIGCOMM Computer Communication Rev., 27(2):24–36, Apr. 1997.

[6] M. Liskov, R. Rivest, and D. Wagner. Tweakable block ciphers. J. Cryptology, 24(3):588–613, July 2011.

[7] V. Buterin. Ethereum, Apr. 2014.

[8] V. T. Hoang, B. Morris,and P. Rogaway. An enciphering scheme based on a card shuffle. In R. Safavi-Naini, editor, Proceedings of Crypto 2012, LNCS. Springer-Verlag, Aug. 2012. To appear.

[9] Nakamoto, S. 31 October 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System". Also known as the Bitcoin whitepaper.

[10] Kyle Randolph. "A Next-Generation Smart Contract and Decentralized Application Platform". Also known as the Ethereum whitepaper.

[11] Christopher Ferris. "Hyperledger fabric Protocol Specification".

[12] Miguel Castro,Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery".

[13] Hal, F. "Reusable proofs of work"

http://www.finney.org/~hal/rpow/.

[14] Tushar Deepak Chandra, Vassos Hadzilacos, Sam Toueg. "The Weakest Failure Detector for Solving Consensus".

[15] Manos Kapritsos, Yang Wang, Vivien Quéma, Allen Clement, Lorenzo Alvisi, Mike Dahlin: All about Eve."Execute-Verify Replication for Multi-Core Servers"

[16]ZMWorm[CCG]. ECC 加密算法入门介绍

[17] Michael Rosing. Chapter5《Implementing Elliptic CurveCryptography》, Softbound, 1998