小牛链项目理念白皮书1.0
—价值传输协议及去中心化应用平台

Calf-Chain-white-paper version1.0

2017

目录

摘要

小牛链致力于开发比特币和以太坊之外的第三种区块链生态系统，并致力于拓展区块链技术的应用边界和技术边界，使普通互联网用户能感受到区块链技术的价值。在小牛系统中，可以通过价值传输协议来实现点对点的价值转移，并根据此协议，构建一个支持多个行业的（金融、物联网、供应链、社会公益等）去中心化的应用

小牛链通过良好的设计原则和设计策略来实现，例如兼容性原则、模块化设计策略、安全性策略和易用性策略。 从技术角度分析，致力于实现首个兼容 BIP（基于 UTXO 模型 ）的 POS 智能合约平台，并通过 Identity，Oracle 和 Data feeds 的引入。在合规性方面，符合不同行业的监管需求。在 小牛的公链系统中，在共识机制上，从去中心化程度、实用性、技术可靠性考虑，我们将以 Proof of Stake 为基础，加入节点在线激励因素（Incentive Factor），形成 IPOS（Incentive POS)的共识协议。在 小牛的联盟链中(Permissioned Blockchain)，我们将采用 小牛开发团队提出的与 Raft 融合的 Proof of Time 共识协议，使得在联盟链或者私链中，达成共识的时间大大缩短（BlockTime:250ms，Confirmation Time：750ms-3s)。

小牛系统将基于 UTXO 模型来实现基于区块链的合约，主要考虑以下因素：（1）与比特币生态的兼容性； （2）BIP 长期演进协议的兼容性 ；（3）交易的并行处理能力/隐私性/可追溯性。

在小牛系统中，我们把区块链合约（Blockchain Contract）分成 智能合约（Smart Contract）和简单合约（Simple Contract），除了支持智能合约外，我们将通过链下因素的引入，形成符合现实世界商业逻辑的区块链简单合约。另外在虚拟机方面，在 小牛的测试网络中，我们将兼容 EVM，后期通过标记不同的虚拟机类型，可以支持更多的虚拟机，包括 LLVM 和 Lua 以及 EVM2.0. 以及为 VM 开发的更严格的编程语言。

在 小牛系统中，我们通过 Oracle 和 Data Feed 的设计，可以让区块链的

智能合约更落地和更符合商业规则，搭建了现实世界到区块链世界的桥梁。另外小牛系统中，可以通过智能合约来管理参与者的身份信息，将为基于 小牛系统的金融服务提供更好的支持。最后面向移动端策略（Go Mobile）也是 小牛特别重视的一个战略，在小牛链的生态系统中，我们将会与第三方开发者，一起从技术架构支持提供移动端的服务，包括：移动端钱包、移动端 DAPP 应用、移动端智能合约服务。 我们也鼓励第三方的开发者，加入我们，一起开发区块链的移动端服务，共同推动区块链技术的落地。

第 1 章 区块链的兴起与未来之路

区块链的诞生，标志着人类开始构建真正可以信任的互联网。通过梳理区块链的兴起和发展可以发现，区块链引人关注之处在于，能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介的干扰，既公开信息又保护隐私，既共同决策又保护个体权益，这种机制提高了价值交互的效率并降低了成本。

从经济学意义来看，区块链创造的这种新的价值交互范式基于“弱中心化”，但这并非意味着传统社会里各种“中心”的完全消失，未来区块链将出现大量的“多中心”体系，以联盟链、私有链或混合链为主，区块链将会进一步提高“中心”的运行效率，并降低其相当一部分成本。家战略层面开始对区块链技术及发展趋势进行研究。

从技术角度来说，我们认为，区块链是一种由多方共同维护，以块链结构存储数据，使用密码学保证传输和访问安全，能够实现数据一致存储、无法篡改、无法抵赖的技术体系。这种技术给世界带来了无限的遐想空间，全球对区块链的关注热度持续升温，全球主要经济体从国家战略层面开始对区块链技术及发展趋势进行研究。

1.1 区块链的兴起

1.1.1 从摆脱第三方制约起步

早先，人们将区块链视为点对点网络上的一个分类账本，每笔交易自诞生起，所有转账、交易都将被记录在“区块”上，区块与区块之间首尾相连，形成链式的结构，并且公布给该网络上所有的节点，节点之间通过共识机制形成共识。节点成员可根据权限查阅相关交易记录，但任何单个节点都无法轻易控制和更改整个网络的数据。

这种设计来源于 2008 年中本聪发表的论文《比特币：一种点对点的电子现金系统》。文章提出，希望可以创建一套新型的电子支付系统，这套系统“基于

密码学原理而不是基于信用，使得任何达成一致的双方能够直接进行支付，从而不需要第三方中介参与”。该论文催生了比特币，标志着人类社会的货币体系向前迈出了一大步。比特币采用了公开的分布式账本的设计思路，真正摆脱了第三方机构的制约。随后比特币进入快速发展期。

2009 年 1 月 3 日，区块链的第一个区块诞生，该区块又名“创世区块”。

2009 年 1 月 12 日，中本聪发送了 10 个比特币给密码学专家哈尔芬尼。

2010 年 7 月，比特币交易所 Mt.Gox 的成立，比特币的价值被世界认可。

此后几年里，由于比特币的挖矿机制造成巨大的资源消耗，比特币的匿名性对传统金融监管提出了挑战，使得比特币价格随之出现了大起大落。

1.1.2 从比特币跃迁到区块链+

区块链的诞生，标志着人类开始构建真正的信任互联网。

有一种新的观点认为，区块链技术可以构建一个高效可靠的价值传输系统，推动互联网成为构建社会信任的网络基础设施，实现价值的有效传递，并将此称为价值互联网。我们注意到，区块链提供了一种新型的社会信任机制，为数字经济的发展奠定了新基石，“区块链+”应用创新，昭示着产业创新和公共服务的新方向。区块链技术已经在全球开始部署应用，美、英、日、德、加、澳等发达国家已经认识到区块链技术在公共服务和社会机制优化上存在着巨大的应用前景，开始设计区块链的发展道路。

目前主要有两大应用趋势：

从公共服务层面来看，区块链技术正在探索在公共管理、社会保障、知识产权管理和保护、土地所有权管理等领域的应用。相关实践表明，这种技术有助于提升公众参与度，降低社会运营成本，提高社会管理的质量和效率，对社会管理和治理水平的提升具有重要的促进作用。

从经济社会来看，区块链经济已经萌芽。许多基于区块链的解决方案，可以改善现有的商业规则，构建新型的产业协作模式，提高协作流通的效率。无论是各国央行和各大商业银行，还是联合国、国际货币基金组织以及许多国家政府研究机构，都对“区块链+”投入极大关注。

区块链可为经济社会转型升级提供系统化的支撑。区块链+的显著优势在于

优化业务流程、降低运营成本、提升协同效率，这个优势已经在金融服务、供应链管理、知识产权、智能制造、社会公益以及教育就业等社会各领域初步体现出来。

1.2 小牛块链的设计思想

自从 2009 年比特币代码开源以来，社区里面出现了很多 Altcoin 和其他区块链项目，有意义的 Altcoin 项目成为了区块链技术的试验田（一些毫无意义的 Altcoin 除外），对区块链技术的发展和成熟有一定的借鉴意义（例如 NameCoin 等），除此之外还有一些从不同角度拓展区块链技术边界的项目，例如 ColorCoin 协议，NXTCoin，Ripple 和 Stellar，BitShare，Dash，Maidsafe，Factom 等。 之后，还有致力于成为通用智能合约平台和去中心化应用平台的 Ethereum 项目。无数的开发者和社区人员一起参与和见证了区块链技术的快速发展，但是区块链行业不论是从技术角度，还是行业应用角度都还面临着很多挑战。

区块链技术面临的主要问题：

1．缺乏新型的智能合约平台，目前现有的智能合约平台主要是基于 Proof of Work（POW）。

2．而 Proof of Work（POW）的共识机制很难被行业应用大规模部署。

3．不同区块链技术之间的兼容性，比如基于 UTXO 模型的比特币生态和基于 Account 模型的以太坊生态很难有兼容性。

4．共识机制本身缺乏灵活性，因为参与者的不同，在公有链中和联盟链中，对共识机制的要求是不一样的。

5．缺乏对行业合规性的考虑，例如在金融行业要求的 identity 和 KYC 部分，在现有的区块链系统中，很难保证。

6． 现有区块链系统具备很大的封闭性，目前大多数的智能合约的触发条件大多来自于区块链系统本身，很少有来着外界的触发条件，缺乏与现实世界的交互。

针对当前区块链行业的挑战，小牛链在区块链技术和理念上进行了一系列的创新：包括基于 UTXO 的智能合约模型，面向公有链和联盟链的灵活的共识机制，

区块链简单合约的理念和实现，交易账本和智能合约账本的分离，Oracle 和 Data Feed 的设计和实现等，使得小牛链成为区块链世界与现实商业世界的桥梁。

对比互联网技术的发展路径，我们发现不论是区块链技术本身，还是基于区块链技术的应用，都处于行业发展早期，有很多值得探索的方向。

因此我们希望可以构建一个全新的区块链生态系统，作为未来世界可选的互联网价值传输协议的可选项，并把整个区块链行业的易用性向前推进一步，这也是我们设计小牛链的原因。小牛链致力于拓展区块链技术的应用边界和技术边界，使普通互联网用户能感受到区块链技术的价值，并构建一个全新的基于区块链技术的开发者和用户的生态系统。

1.2.1 经济层面设计思想

降低成本，是区块链技术的一个重要的设计思想。在区块链体系中，参与者可以不需要了解对方基本信息的情况进行交易，实现了“无需信任的信任”，改变了传统模式中以第三方为中心的信任模式。

这种设计模式有许多创新性，其中两项值得关注：

第一，交易信任由机器和算法确定。区块链通过构建一个依赖于机器和算法信任的交易体系，解决在匿名交易过程中的相互信任问题。所有参与者将在无须建立信任关系的环境中，通

过密码学原理确定身份，依靠共识机制实现相互间的信任。

第二，交易过程可以由程序自动执行。区块链通过可编程的智能合约，自动执行双方所达成的契约，排除了人为的干扰因素，从制度上防止任何一方的抵赖。从而推动经济社会进入一种智能的状态，实现当前经济交易系统的质的飞跃。

基于区块链技术的“弱中心化”特性，现有的经济体系可以脱离当前通过制度约束或第三方机构背书，双方直接实现价值交付。这种“弱中心化”特性可以有效降低交易成本，提高交易效率，减少因交易一致性所引发的摩擦。

1.2.2 技术层面设计思想

通俗的说，区块链可以看成是一套由多方参与的、可靠的分布式数据存储系统，其独特之处在于：一是记录行为的多方参与，即各方可参与记录；二是数据

存储的多方参与、共同维护，即各方均参与数据的存储和维护；三是通过链式存储数据与合约，并且只能读取和写入，不可篡改。

在应用实践中，这种系统能够实现所有参与者信息共享、共识、共担，可以成为各种商业行为和组织机构的基础技术架构。具体与传统中心式系统对比如下：

系统分类 / 关键点		传统技术系统		区块链技术系统	
		特点	中心化的实现方式	特点	去中心化的实现方式
记录行为的多方参与	网络架构	中心化	主从式的B/S网络	去中心化	P2P分布式网络
	记录权及记录方式	中心节点进行	中心节点记录及维护所有交互数据	所有节点参与	共识算法确定记录权，共同维护交互数据
	交易方式	每笔交易需中心节点确认	中心节点监督和维护	点对点交易	所有节点集体监督和见证
	信任关系	中心节点见证	中心节点为所有节点进行信任背书	节点自证其信	非对称加密技术验证身份，零知识证明等方式验证信息
	交易一致性	中心节点保障交易数据的一致性	中心节点的一本账，保障交易数据的一致性	所有节点共同参与解决数据交易的一致性	所有节点通过共识算法保证交易一致性，解决双花现象
账数据存储的多方维护	交易有无欺诈	存在欺诈和造假的可能	中心节点主动欺诈的可能	不可欺诈、不可造假	分布式存储、共识算法
	信息被篡改	存在数据被篡改和抵赖的可能性	中心节点存在被攻击、数据被篡改等可能性	不可篡改、不可抵赖	分布式存储、链式数据结构、哈希算法、时间戳及数字签名
	数据存储的可靠性	中	依靠中心节点进行交易信息系统的存储和容灾备份	高	任意单个节点故障或者少数节点故障，系统能正常运行，并且故障节点数据可以恢复。
	隐私保护	交易双方身份信息存在泄露的可能性	所有参与交易者需提供身份信息，且都由中心节点保存，中心节点存在被攻击、盗取等可能，导致交易者的隐私泄露	交易双方的身份信息不会被泄露	所有参与方在区块链中通过加密后的ID进行标识。 1、不需要所有交易者提供身份隐私信息，保障交易者的隐私不被泄露。 2、同一个交易者可通过多个ID进行的多次交易来达到隐私保护的目的。

1.3 区块链的核心技术

区块链技术不是一个单项的技术，而是一个集成了多方面研究成果基础之上的综合性技术系统。我们认为，其中有三项必不可缺的核心技术，分别是：共识机制、密码学原理和分布式数据存储。

第一，共识机制

所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、行为或流程达成一致的过程。共识机制是指定义共识过程的算法、协议和规则。区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。

第二、密码学原理

在区块链中，信息的传播按照公钥、私钥这种非对称数字加密技术实现交易双方的互相信任。在具体实现过程中，通过公、私密钥对中的一个密钥对信息加密后，只有用另一个密钥才能解开的过程。并且将其中一个秘钥公开后（即为公开的公钥），根据公开的公钥无法测算出另一个不公开的密钥（即为私钥）。

第三、分布式存储

区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。

跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。数据节点可以是不同的物理机器，也可以是云端不同的实例。

第 2 章 小牛链的解决方案

小牛链在自主创新的基础上，打造了提供企业级服务的“区块链”解决方案。基于“开放分享”的理念，小牛链将搭建区块链基础设施，并开放内部能力，与全国企业共享，共同推动可信互联网的发展，打造区块链的共赢生态。

小牛链在支付与金融、虚拟资产、电商等多个领域积累了丰富的行业与技术经验，在高并发的交易处理方面取得了业界领先的突破；此外，小牛链还具备海量数据处理和分析、金融安全体系构建的能力，在云生态和行业连接的探索上也积累了丰富的经验。

2.1 设计原则及目标

区块链致力于提供企业级区块链基础设施，行业解决方案，以及安全、可靠、灵活的区块链云服务。

自主创新：小牛链注重自主创新，目前在关键领域已经拥有多项自主知识产权的独特核心技术，在共识算法、十亿级用户管理、海量数据并发处理、账户安全管理、风险控制等方面具有专利和技术积累。

安全高效：基于小牛多年在支付与金融领域的安全、可靠运营经验的积累，推出小牛可信区块链，能够有效实现信息共享，保护信息安全，提升系统效率。

开放分享：小牛将搭建区块链基础设施，开放内部服务能力，与行业伙伴共享，共同推动可信互联网的发展，打造区块链的共赢生态。

小牛可信区块链旨在为行业伙伴提供企业级区块链基础设施，行业解决方案，以及安全、可靠、灵活的区块链云服务。通过高性能的区块链服务，在实现安全可靠的交易对接的前提下，通过可视化的数据管理手段，有效降低企业运营综合成本，提高运营效率。

2.2 整体架构

在“自主创新、安全高效、开放共享”设计原则的指导下，小牛可信区块链

方案的整体架构分成三个层次：小牛链的底层是小牛自主研发的底层平台，通过 SQL 和 API 的接口为上层应用场景提供区块链基础服务的功能。核心定位于打造领先的企业级区块链基础平台。

中间是平台产品服务层为，在底层之上构建高可用性、可扩展性的区块链应用基础平台产品，其中包括共享账本、鉴证服务、共享经济、数字资产等多个方向，集成相关领域的基础产品功能，帮助企业快速搭建上层区块链应用场景。

应用服务层向最终用户的提供可信、安全、快捷的区块链应用，小牛未来将携手行业合作伙伴及其技术供应商，共同探索行业区块链发展方向，共同推动区块链应用场景落地。整体框架结构如下图：

2.2.1 底层平台

用户管理：负责所有区块链参与者的身份信息管理，包括维护公私钥生成、密钥存储管理以及用户真实身份和区块链地址对应关系维护等，并且在授权的情况下，监管和审计某些真实身份的交易情况。对数字资产等金融交易类的应用，

还提供了风险控制的规则配置，以保证系统交易安全。

基础服务：基础服务部署在所有区块链的节点上，用来验证业务请求的有效性，并对有效请求完成共识后记录到存储上。对一个新的业务请求，基础服务先对接口适配解析，鉴权处理，然后通过共识算法将交易或者合约加上签名和加密之后，完整一致的存储到共享账本上。共识机制可自适应，在网络和节点都正常情况下具有高并发性，网络异常或者节点欺骗的情况下具有强容错性。

智能合约：负责合约的注册发行以及合约的触发和执行。用户通过某种编程语言定义合约逻辑，发布到区块链上之后，根据合约条款的逻辑，由用户签名或者其他的事件触发执行，完成交易结算等合约的逻辑。

运营监控：负责产品发布过程中的部署、配置修改、合约设置以及产品运行中的实时状态可视化的输出，如：告警、交易量、网络情况、节点健康状态等。

2.2.2 平台服务层

平台产品服务层抽象了各类典型的区块链应用，提供典型应用的基本能力和实现框架，用户可以基于这些基本能力，叠加自己业务独有的特性，轻松完成业务逻辑的区块链实现。帮助用户快速搬迁已有业务到区块链上，以应对新的场景需求，或者搭建全新的业务场景，利用区块链的不可篡改、防抵赖等特性解决之前难以解决的问题。

数字资产：根据对虚拟货币、游戏装备、商业票据、积分、卡券等数字资产的分析，我们发现资产上链是一个关键环节。为此引入“资产网关”的概念，协助用户进行链下资产到链上资产的转换。资产一旦上链，转移、拆分、提现等操作就会通过帐户公私钥体系严格控制起来，并且所有的操作都会有签名校验，交易双方都会留下痕迹，不可抹除。如商业票据、卡券等存在有效期的资产，还会提供到期自动清算的能力，包括资产发行、资产转让、资产提现、资产清算、资产查询等。

鉴证服务：针对知识产权、保单保全（权益证明）、个人和企业资质证明等应用场景，区块链充分发挥不可抹除和公示的能力，让机构和个人通过一个简单的接口或 APP 客户端就可以把版权资料、投保资料、资质证明等发布到区块链上，让所有记账节点共同为自己作证。另至必须要业务运营方去垫资进行。区块

链天然的共享账本，让对账不必第二天汇总发送，而是随时都可以进行，双方只要把对账逻辑对接到区块链上，就可以完成资金的核对。基本可以实现准实时的交易确认和资金划拨，并且任意一方都不可抵赖。特别对于资金链条比较长，牵涉环节比较多的业务非常有竞争优势。同时监管机构也可以参与到共享账本记录中。

分享经济：分享经济能否走的长远，一个关键因素就是供需方之间信任的建立，保证分享行为的顺利实施，而区块链从技术层面提供了一种实现途径。技术保证能力的背书，让彼此难以达成信任的多方参与者，共同建立起公信力，不再需要中间机构或者服务平台构建强大的内部审核流程，严谨繁复的记账备份体系，以及配合监管机构做的额外设施，就可以达到相同的效果。从而节约了大量的成本，让分享更加高效可行。

2.2.3 应用服务层

应用服务层提供基于区块链方案的应用服务给最终用户的使用。小牛链解决方案中应用服务层将尽力为小牛的海量用户提供各类区块链场景的服务，未来将在数字票据、贵金属交易、知识产权保护、网络互助、机构清结算、公益等场景为用户提供可信、安全、便捷的区块链服务。小牛链也会本着开放分享的原则，未来将携手各个行业伙伴发掘更多区块链的应用场景，开放区块链底层和平台应用层的能力，共同开发新的应用服务，一同维护区块链生态。

2.3 底层平台

2.3.1 基础服务

基础服务模块由接口适配、共识管理，网络通信和记录存储四个部分组成，如下图：

接口适配

为了用户方便、低成本的接入小牛链，Trust SQL 对应用层提供 SQL 和 API 的接口，其中 API 接口支持同步和异步操作两种模式。接口适配层对业务请求进行解析，鉴权和签名校验之后，通过共识算法将业务请求记录到账本存储上。接口适配模块作为共识管理模块的客户端，也会参与共识管理。接口适配模块主要负责各个共识节点返回结果的汇总和一致性判断。另外，当使用具有自主知识产权的“改进的 bft-raft”共识算法时候，接口适配模块还会收到来自业务侧的选举切换请求，接口适配模块对选举切换请求进行汇总统计。当符合切换条件的时候，通知共识管理模块重新选举。

共识管理

共识机制是区块链中核心的技术点。多方参与的节点在预设规则下，通过节点间的交互对数据、行为或流程达成一致的过程称为共识。共识机制是指定义共识过程的算法、协议和规则。

共识机制按照共识的过程分两类，第一类是概率一致的共识、工程学上最终确认；第二类是绝对一致之后再共识，共识即确认。小牛链提供第二类的共识机制，支持自适应和用户指定配置两种模式。自适应的模式是在网络状况良好、无欺诈节点的情况下自动使用共识效率高、能够防欺诈的、具有自主知识产权的“改进的 raft”算法，当欺诈节点或者故障节点超过阈值之后自动切换到更为严格的、具有自主知识产权的“改进的 bft-raft”算法。用户指定配置模式是指用户直接配置固定共识机制，进行共识管理。

网络通信

网络通信模块负责各节点间以及业务侧的消息数据传输。小牛链采用可以多路复用、连接共享的动态自组织的网络。可以跟现有的防火墙、代理服务器等安全设施很好的兼容，提供点对点的组网和安全可靠的数据传输。

记录存储

小牛链记录存储可以支持多种的介质的存储，存储介质可以是数据库、文件系统，也可以是云存储介质，如云 DB，云 KV 等。记录存储采用块链的结构，任何对历史数据篡改都能被自校验发现，并进行告警和自动修正。

2.3.2 用户管理

用户管理主要解决用户身份到区块链地址的映射关系、用户隐私的保密性以及监管审计的可追踪性。从业务场景上看，有些场景是需要匿名、交易不相关性，如股票交易、数字货币等，有些场景则不需要匿名和不相关性，如互助保险、源头跟踪等。要兼顾这两大场景，密钥管理需要很强的适应性和兼容性。小牛链提供了用户灵活自由选择的多种配置方式。

从用户接入的角度看，一种是原有系统改造接入区块链，存在原有安全级别较高的密钥管理体系，如机构清算，银行保理等，另外一种是新应用场景接入区块链或者原有系统没有完善的密钥管理体系，如一些供应链业务和一些 B2C 业务等。为继承原有安全级别较高的密钥管理系统、同时又能保留原有用户的使用习惯，小牛链提供了传统密钥系统集成、全托管和部分托管三类模式。

传统密钥系统集成：适用于原有私钥系统安全级别较高的用户，如：金融机构、银行原有的 U 盾、电子签名等，对于此类用户，小牛链只需要将原有用户的私钥系统跟区块链地址关联起来即可。

部分托管：适用于接入区块链服务的部分主体有较高安全级别的密钥系统或者多种区块链技术互通的场景。部分托管情况下，小牛链来保证参与的多方区块链地址关联关系和一致性。

全托管：适合全新接入的场景以及原有互联网习惯程度较高的场景。将原有的以用户名、密码的体系，通过安全的密钥生成和管理系统对应起来，使用户信息跟区块链地址隔离开来，保护用户隐私安全。对于全托管的模式，小牛链的用户管理系统由账户管理、密钥管理、权限管理和风控审计四个部分组成，如图：

账户管理

账户管理负责用户的账户管理，包括账户的注册、登录、注销以及账户跟密钥的不相关性处理。账户注册时，将原来用户习惯的用户名、密码等身份信息映射到小牛链地址。账户登录之后，才可以发送区块链相关的业务请求。对交易保密程度较高的场景，用户可以选择小牛链地址不相关性处理，使得同一个用户的不同交易在区块记录存储中不具有关联性，提高了用户安全性和交易保密性。

密钥管理

在全托管的模式下，密钥管理系统负责用户密钥跟账户的关联、密钥安全管理和丢失找回。用户密钥在客户端生成，用户可以选择将密钥保存在密钥保险箱或者委托给关联账户的方式以便密钥丢失后找回。为了保证用户账户跟密钥关联关系可靠性，密钥管理系统将关联关系的签名采用多节点链式存储。

权限管理

权限管理模块负责用户账户、密钥系统、节点加入和退出、数据访问等权限的控制和管理。包括审计权限、账户委托权限、节点共识权限以及用户数据访问权限等。审计权限是为监管机构提供审计的功能，对访问权限和数据范围做严格的控制，对共享账本上交易不相关性的用户可以做到用户关联。账户委托权限用来控制用户账户委托关系的访问控制。共识权限对参与或者新加入节点进行共识权限管理。访问权限用来管理客户端对区块链上的数据查询权限。

风控审计

风控模块负责对区块链中数字资产类的交易行为进行风险控制，小牛链提供风控专家模型系统，通过分析和捕捉海量数据间的深层关系，自适应调整风控规则，及时发现风险、管理风控和控制风险，做到防患于未然。审计模块为审计机

构提供审计能力，通过严格的权限控制来保证审计能力只能被审计机构使用。

2.3.3 智能合约管理

小牛链合约部分包括标准合约以及业务定制的合约两种类型。标准合约包括资产一致性检查、自动成交撮合、多方共同确认的转账、到期自动清算等逻辑相对简单的合约，是小牛链内置合约，可以直接挂在区块链上使用。用户定制的智能合约包括通过合约模板修改配置和添加其他业务逻辑的形式，也可以支持更加复杂的用户自编程的合约，在独立的环境里运行。

智能合约包括合约的注册、触发、执行以及注销四个部分，如下图：

合约注册

合约注册是将用户编写好的合约安全检查处理之后，共识存储到区块链的过程。小牛链未来计划支持多种语言来编写智能合约。

发是在合约注册之后，通过外部条件来触发合约执行的过程，支持定时触发、事件触发、交易触发和其他合约触发的方式。定时触发是指满足合约中预设的时间之后，节点就触发时间共识之后，自动触发合约调用的过程。事件、交易和其他合约调用都是一次新的请求共识过程中触发合约执行。

合约执行

合约执行是合约代码在独立的环境中运行的完整过程，包括对合约构造镜像环境、代码执行、执行代码中状态修改的共识以及共识的异常处理。

合约注销

合约注销，是对已经执行过、过期作废或者业务需求变更不再需要的合约进行转存，清理，清理的过程需要多节点共识之后才能完成。

2.3.4 运营监控管理

为了客户快速接入以及接入之后能够快速准确地识别系统的运行状态以及

在运行中满足其他的运维需求，如存储账本扩容、程序升级等。小牛链提供了完整、快捷、可视化的运营监控系统，运营监控主要包括配置，监控、告警、发布和业务分析等功能。

配置

负责处理网络节点的相关配置，如共识算法的选择、自适应阈值、存储账本的存储方式、网络路由方式等，配置的本身可以作为区块链中的一个交易的形式下发，通过共识算法达成一致之后再生效。

监控

负责收集系统中运行的状态数据，并且可视化的呈现出来。系统中的状态数据包括系统的访问量、耗时、节点的健康状态以及比较底层的机器资源（CPU、内存、硬盘）使用状况等，

通过可视化监控可以实时了解整个区块链系统的状态。

告警

对系统中比较严重的情况如欺诈节点、账本篡改、机器故障等情况通过短信、电话、微信、邮件等方式通知到相关人员，以便及时处理。

发布

对系统初次部署、运行中程序升级以及运行过程中节点扩展等场景下的操作可以通过发布模块来支持。发布模块保证接口、共识算法等重要模块的可执行程序的一致性。

业务分析

业务分析包括各个节点间数据一致性检测以及交易数据多维度的统计和分析，可以给特定授权用户提供业务统计分析以及业务发展趋势的图表。

云适配

云适配提供目前云主流运营商的接口适配，可以让小牛链更加方便的部署在云上，方便维护和扩展。

2.4 技术特色和优势

在“自主创新、安全高效、开放分享”的设计原则下，小牛链打造的企业级基础设施服务，具有如下特点：高性能、高安全性、高速接入、高效运营：

1、高性能：依托小牛的海量并发经验，交易支持秒级确认；提供海量数据存储，具备每秒万级的处理能力；

2、高安全性：提供丰富的权限策略、安全的密钥管理体系和用户隐私保密方案，保障数据安全。

3、高速接入：丰富的应用开发框架和灵活的部署方式，方便不同类型的用户快速接入，构建应用；

4、高效运营：提供全面、实时、可视化的运维管理系统，快速识别系统状态，满足多个层级的运营管理需求。

2.4.1 高性能

高效自适应共识算法

在企业级区块链解决方案中，单个区块链的并发处理的能力主要受制于共识算法。实际的联盟链应用中，绝大部分时间里，各节点间网络状况是良好的，节点故障或者是拜占庭节点的概率小，这样，在绝大部分时间里，只需要解决多个节点数据一致性，高效完成交易即可。只要在发现有节点故障或者欺诈的时候，能够自动切换到具有拜占庭容错的算法就可以保证业务顺利进行。小牛链提供的自适应的区块链共识算法，在网络状况良好、无节点故障或者欺诈的情况下处理效率很高，并且可以准确检测节点故障或者节点欺诈；当检测到节点故障或者欺诈，系统自动启用拜占庭容错的算法特性，保证容错节点在小于 1/3 总节点数的情况下，系统正常运转；当所有坏节点修复或者拜占庭容错节点解决之后，所有节点数据能全一致的时候，自动切回到高效的算法上。自适应算法很好保证联盟链绝大部分时间内高效的并发处理，并且精准处理了节点错误的问题。

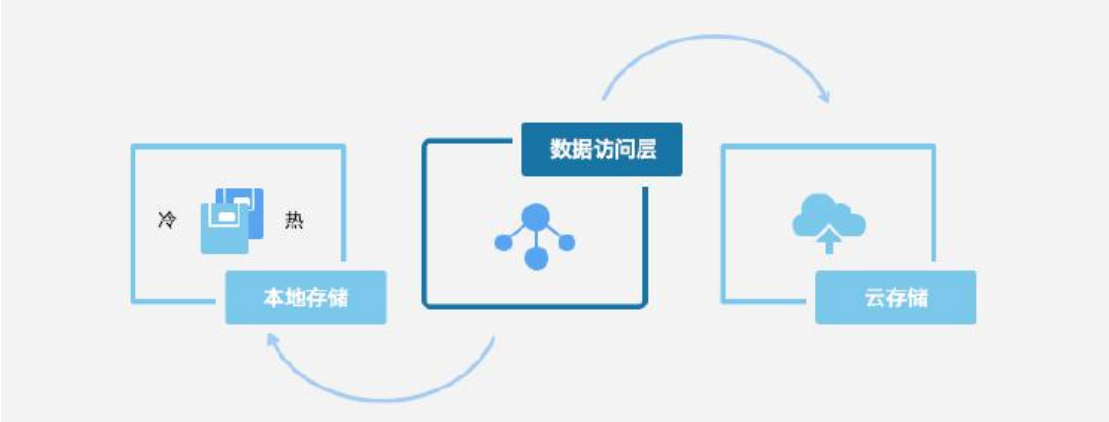
交易快速确认

小牛链采用高效自适应的共识算法，保证了共识完成即交易确认，并且对交易确认过程中的其他环节，如签名算法、账本存储方式等进行了优化，实现了秒级确认交易。

海量存储

小牛链支持本地数据库存储、文件系统存储以及云存储多种方式。本地存储实现冷热分离，数据库存储使用分库分表的模式，云存储支持按照云的集群规则

扩展。

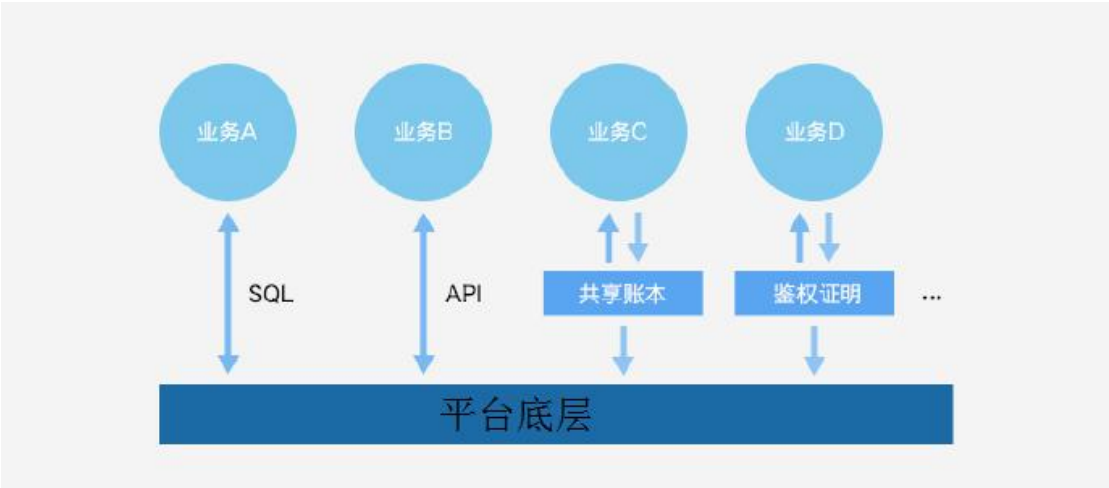


2.4.2 高速接入

在实际的业务对接场景大致分为三类：第一类，原有系统改造后接入区块链，第二类，原有系统上新的需求使用区块链开发，第三类，在全新的系统和场景使用区块链。小牛链为了适应于上述三类场景，本着业务开发工作量尽量少、尽量满足用户原有开发习惯、方便的部署、保持原有的安全体系的原则，在用户业务开发方式、部署方式以及安全性继承上做了大量的兼容性设计，可以实现各种场景、各种开发习惯的用户能以较低的代价、较快的速度对接到区块链上来。

满足多种用户习惯的方式接入

小牛链平台产品层提供丰富的应用开发的框架，应用类型包含了数字资产、共享账本、鉴证证明、股份众筹及所有权交易等基本应用模型。用户可以基于这些应用开发框架进行业务开发，也可以直接基于小牛链底层提供的 SQL 和 API 进行开发。对业务开发中使用的底层 API 的库提供了多语言支持，可以满足不同的用户的开发习惯，降低用户接入难度。



跨平台的部署方式

小牛链针对不同的用户需求，可以支持云部署、服务器部署等多种部署方式，适应多种用户部署环境。

可选的密钥管理对接机制

小牛链提供了原有密钥系统关联、部分托管和全托管三类对接机制，跟现有系统对接时，可以根据现有系统的密钥管理系统的实际情况选择合适的对接机制。原有密钥系统安全程度较高的，可以复用的直接使用原有密钥关联的方式；全新的业务可以选择密钥管理全托管的方式；也可以根据业务情况选择部分托管的方式。

2.4.3 高安全性

可靠一致的记录存储

小牛链通过非对称加密的数字签名保证业务请求在传输过程中不能被篡改，通过共识机制保证各节点的数据一致的存储。对于已经存储的数据记录通过节点内的自校验性和准实时多节点数据校验来保证已经存储的数据记录不能被修改。

节点的自校验性：

小牛链采用块链结构存储数据记录，其中部分记录的修改会破坏块链结构的完整性，可以快速校验出来并从其他节点将数据恢复。另外小牛链每个记账节点都有自己的私钥，每个区块头中包含了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。

多节点准实时的数据校验

当节点的私钥被盗取，恶意用户是存在修改账本链上所有数据的可能性的，小牛链提供了多节点间准实时的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。

用户隐私和交易保密

小牛链中用户信息和区块链地址是隔离的。从各节点的记录存储中，无法获取到相关联的用户信息。用户信息存储有权限控制，访问认证，加密存储等多层保护。对交易保密程度较高的用户还可以选择交易不相关性机制，同一个用户的每次交易都映射到区块链上不同的地址上，从而保证了在交易账本上无法获取一个用户的多笔交易的关联性。

安全的密钥管理体系

在小牛链的密钥管理解决方案中，提供了密钥保险箱和用户账户委托的功能来保证密钥的安全。密钥保险箱使用用户信息对密钥加密并分割存储在多个不同的节点上，正常业务流程下不会访问密钥保险箱，当用户密钥丢失后，可以通过对用户信息认证之后将密钥找回。账户委托是通过委托账户来操作被委托账户来实现账户找回的功能，小牛链所有委托账户操作会独立记录在区块链上，并且对委托账户的操作有严格的频度限制和独立的风控策略，可以严格控制委托账户的操作风险。

2.4.4 高效运营

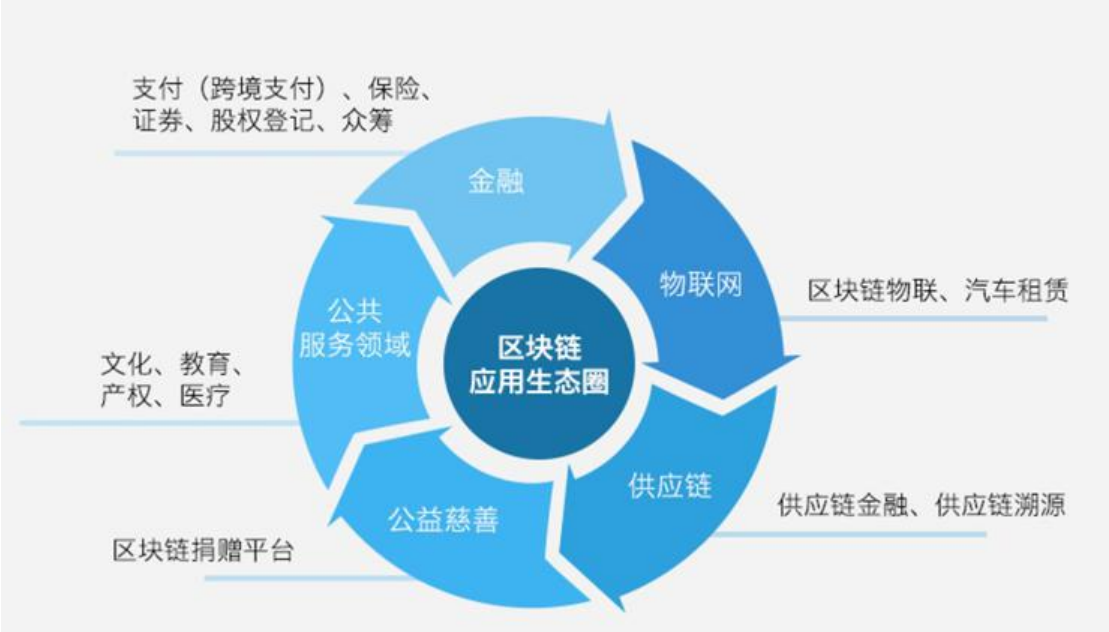
小牛链实现了可视化的服务交付和可视化的服务度量。在服务交付方面，从代码编译、测试、灰度环境验收到正式环境部署，整个服务交付流程实现可视化管理。在服务度量方面，对数据进行了标准化的分层归类，从基础设施、上层组件、应用服务、到用户侧，基于应用的拓扑架构，收集各类指标，统一到一个分

析平台中展现。

小牛链提供通用高效的信息采集组件，部署在业务层、共识节点层以及账本存储层，信息采集组件把机器的系统信息（如，CPU，内存、硬盘、网络等状态）、节点使用状态（如节点访问量、访问时耗、节点健康状态等）以及业务使用情况（业务访问量、成功率、耗时分布等）实时展示到监控界面上，便于整个系统的管理。

2.5 行业应用前景

第 3 章 区块链发展的重点行业



3.1 金融领域

金融服务产业是全球经济发展的动力，也是中心化程度最高的产业之一。金融市场中交易双方的信息不对称导致无法建立有效的信用机制，产业链条中存在大量中心化的信用中介和信息中介，减缓了系统运转效率，增加了资金往来成本。

区块链技术公开、不可篡改的属性，为去中心化的信任机制提供了可能，具备改变金融基础架构的潜力，各类金融资产，如股权、债券、票据、仓单、基金份额等均可以被整合进区块链账本中，成为链上的数字资产，在区块链上进行存储、转移、交易。使其在金融领域的应用前景广阔。例如，在跨境支付、保险理赔、证券交易、票据等方面有了典型的应用。

在（跨境）支付方面，通过区块链技术，实现资金转移，尤其在跨境支付业务上的潜在优势格外突出，在跨国收付款人之间建立直接交互，简化处理流程，实现实时结算，提高交易效率，降低业务成本，由此推动跨境微支付等商业模式的发展。典型的应用案例是 Visa B2BConnect。国际银行卡组织 Visa 与区块链公司 Chain 共同开发的 B2B 跨境支付项目，计划于 2017 年推出服务，目前已

经在 10 个国家的 30 家银行中进行了测试。Visa 和 Chain 联合开发的区块链系统可以实现支付交易的实时处理，从而提高效率，降低成本。

在保险理赔方面，保险机构是传统保险业务的核心，负责资金归集、投资、理赔，往往管理和运营成本较高。通过智能合约的应用，既无需投保人申请，也无需保险公司批准，只要触发理赔条件，实现保单自动理赔，支付理赔金额。区块链上数据真实、难以篡改的特点，可有效简化保单理赔处理流程，降低处理成本，降低索赔欺诈的概率。此外，通过区块链技术，实现个人数据的数字化管理，简化信息认证，有助于更为清晰地披露历史情况。

典型的应用案例是 LenderBot,是 2016 年由区块链企业 Stratumn、德勤（Deloitte）与支付服务商 Lemonway 合作推出，它允许人们通过 Facebook Messenger 的聊天功能，注册定制化的微保险产品，为个人之间交换的高价值物品进行投保，而区块链在贷款合同中代替了第三方角色。

在证券交易方面，传统证券业务需中介机构深度参与，才能有效完成股票发行与交易。将股权整合进区块链中，成为数字资产，可实现无需通过中介机构，直接发起交易。资产发行可根据需要，采取保密或公开方式进行。股票资产交易通过区块链代码表达相关各方一致达成的合约，实现合约的自动执行，保证相关合约只在交易对手间可见，而对无关第三方保密。

此外，通过相应机制确保证券发行和交易符合监管要求和框架，进一步降低监管合规成本。典型的应用案例是 Linq 平台，由纳斯达克与区块链企业 Chain 合作，于 2016 年 1 月上线的私募股权交易平台，促进私人股权以一种全新的方式进行转让和出售。

通过 Linq 平台私募的股票发行者享有数字化所有权，同时 Linq 平台能够极大缩减结算时间，降低资金成本和系统性风险。且传统发行和申购材料所需的审批流程也进一步得到简化，提高交易和管理效率。交易方身份、交易量等信息被实时记录在区块链上，有利于证券发行者提高决策效率；公开透明、可追踪的系统有利于证券发行者和监管部门进行市场维护，减少暗箱操作、内幕交易等的发生。

在票据方面，基于区块链技术架构建立新型数字票据业务模式，借助分布式高容错性和非对称加密算法，可实现票据价值的去中心化传递，降低对传统业务

模式中票据交易中心的依赖程度，降低系统中心化带来的运营和操作风险。通过区块链的可编程性，有效控制中介市场中的资产错配，借助数据透明特性促进市场交易价格对资金需求反映的真实性，控制市场风险。区块链技术不可篡改的时间戳和全网公开的特性，有效防范“一票多卖”、“打款背书不同步”等问题。

3.2 物联网领域

目前的物联网生态体系，依赖中心化的网络管理架构，所有的设备都是通过云服务器连接。随着网络规模的扩大，中心化云服务器、大型服务器和网络设备的基础设施和维护方面将占用高昂成本。在去中心化的物联网愿景中，区块链是发生互动的设备间促进交易处理和协作的框架，网络上的每个设备都可以作为一个独立、微型的商业主体运行。

2015 年，IBM 与三星联合打造 ADEPT 系统展示了人们在这一方向上的探索：IBM 和三星希望 ADEPT 系统可以让物联网里的各种设备自动运转，从理论上讲，家电的运转出故障

时它们可以自动发送信号，并可以自动更新软件。甚至设备本身可以通过 ADEPT 来与周边的设备“沟通”，从而提高能源的利用效率。在 ADEPT 系统中，当数十亿个设备自动交互信息时，区块链将发挥分布式账本的作用，通过在系统中植入协议，还可以大大降低 ADEPT 系统作为设备间的沟通桥梁时的成本。

此外，Visa 与 DocuSign 联合发起了区块链汽车租赁项目。2015 年 10 月，Visa 与数字交易管理公司 DocuSign 联合推出概念证明项目，使用区块链技术记录、保管租车数据，推动汽车租赁过程的数字化。该项目在区块链上为客户创建数字指纹，在链上进行登记，通过分布式账本记录交易，租车协议、保险项目等内容实时更新，简化传统汽车租赁过程中的繁琐步骤。

3.3 公共服务领域

公共服务是促进经济增长和社会进步的因素，公共服务的供给对政治、经济、社会发展过程中各类主体及制度、文化、态度、行为等都会产生重要影响。传统的公证依赖政府，而有限的数据维度、未建立的历史数据信息链常常导致政府、学校无法获得完整有效的信息。利用区块链可以建立不可篡改的数字化证明。在

数字版权、知识产权、证书以及公益领域都可以建立全新的认证机制，改善公共服务领域的管理水平。

文化：利用区块链技术，将文化产业链条中的的各环节加以整合、加速流通，有效缩短价值创造周期。通过区块链技术，对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品在区块链上被确权，后续交易都会进行实时记录，实现文娱产业全生命周期管理，也可作为司法取证中的技术性保障。数字化证明可以保障数据的完整性、一致性，保护知识产权。例如，Ujo Music 平台借助区块链，建立了音乐版权管理平台新模式，歌曲的创作者与消费者可以建立直接的联系，省去了中间商的费用提成。

教育：利用区块链技术，解决现有的学生信用体系不完整、数据维度局限、缺乏验证手段等问题，简化流程和提高运营效率，并能及时规避信息不透明和容易被篡改的问题。在区块链中记录跨地域、跨院校的学生信息，追踪学生在校园时期的行为记录，构建良性的信用生态体系。此外，通过区块链为学术成果提供不可篡改的数字化证明，可为学术纠纷提供举证依据，降低纠纷事件消耗的人力与时间成本。例如 BitProof 推出区块链学历认证项目。BitProof 是一家专门利用区块链技术进行文件认证的初创公司，该公司与加州软件工程师培训学校 Holberton School 开展合作，利用区块链技术向学生颁发学历证书，实现学历记录真实性。同时通过区块链学历验证体系，招聘者在进行学生背景调查时，通过在线区块链系统,可以快速获得学生学历及毕业证书信息,降低学历伪造风险。

产权登记：目前，房地产交易市场在交易期间和交易后流程中，存在缺乏透明度、手续繁琐、欺诈风险、公共记录出错等问题。区块链技术的应用可实现对土地所有权、房契、留置权等信息的记录和追踪，并确保相关文件的准确性和可核查性。此外，可借助区块链技术实现无纸化和实时交易。例如，美国房地产区块链公司 Ubitquity 研发出适用于房地产行业的文件安全存储区块链平台。从具体的操作上看,区块链技术在房屋产权保护上的应用,可以减少产权搜索时间，实现产权信息共享，避免房产交易过程中的欺诈行为，提高房地产行业的运行效率。

医疗健康：医疗机构面临着无法跨平台安全共享数据的问题。在医疗服务商之间建立良好的数据协作，有助于进一步提高诊断准确率，改善治疗效果，降低

医疗成本。基于区块链技术，医疗产业链中的参与方实现对网络访问权限的共享，同时也不会对数据的安全性和完整性造成威胁。此外，随着个人健康数据的不断增长，以中心化方式存储基因、指纹等重要健康数据，一旦发生大规模泄露，将产生灾难性后果。而通过算法确保数据库的安全性，避免单点故障导致数据库整体性崩溃，区块链技术有望为医疗健康行业带来金融级的数据安全保障。例如 Guardtime 医疗档案管理项目。安全初创企业 Guardtime 与爱沙尼亚电子卫生基金会合作，利用区块链技术保证病人医疗记录的安全。敏感数据保护中存在的安全隐患包含信息篡改、删除、错误升级，区块链技术可以保证数据的真实完整，并能完全记录数据变更过程，从而实现医疗记录和健康档案的实时保护。

3.4 慈善领域

慈善机构要获得持续支持，就必须具有公信力，而信息透明是获得公信力的前提。公众关心捐助的钱款、物资发挥了怎样的作用。既要知道公益机构做了什么，也要知道花了多少，成本有多高。这种公信度的高低和公益的成效决定了公益机构能否获得公众的认同和持久支持。然而，在过去几年里，公益慈善行业时不时地爆发出一些“黑天鹅”事件，极大地打击了民众对公益行业的信任度。公益信息不透明不公开，是社会舆论对公益机构、公益行业的最大质疑。公益透明度影响了公信力，公信力决定了社会公益的发展速度。信息披露所需的人工成本，又是掣肘公益机构提升透明度的重要因素。

区块链从本质上来说，是利用分布式技术和共识算法重新构造的一种信任机制，是用共信力助力公信力。区块链上存储的数据，高可靠且不可篡改，天然适合用在社会公益场景。公益流程中的相关信息，如捐赠项目、募集明细、资金流向、受助人反馈等，均可以存放于区块链上，在满足项目参与者隐私保护及其他相关法律法规要求的前提下，有条件地进行公开公示。

为了进一步提升公益透明度，公益组织、支付机构、审计机构等均可加入进来作为区块链系统中的节点，以联盟的形式运转，方便公众和社会监督，让区块链真正成为“信任的机器”，助力社会公益的快速健康发展。

区块链中智能合约技术在社会公益场景也可以发挥作用。在对于一些更加复杂的公益场景，比如定向捐赠、分批捐赠、有条件捐赠等，就非常适合用智能合

约来进行管理。使得公益行为完全遵从与预先设定的条件，更加客观、透明、可信，杜绝过程中的猫腻行为。

区块链与公益的结合，有很多的应用场景和想象空间，目前已经有真实的应用案例投产上线。2016 年 7 月，支付宝与公益基金会合作，在其爱心捐赠平台上线设立了第一个基于区块链的公益项目，为听障儿童募集资金，帮助他们“重获新声”。在这次的项目中，捐赠人可以看到一项“爱心传递记录”的反馈信息，在进行了必要的隐私保护基础上，展示了自己的捐款从支付平台划拨到基金会账号，以及最终进入受助人指定账号的整个过程。以上所有的信息，都来源于区块链上的数据，既从技术上保障了公益数据的真实性，又能帮助公益项目节省信息披露成本，充分体现出了区块链公益的价值。

3.5 供应链领域

区块链技术有助于提升供应链管理效率。由于数据在交易各方之间公开透明，从而在整个供应链条上形成一个完整且流畅的信息流，这可确保参与各方及时发现供应链系统运行过程中存在的问题，并针对性地找到解决问题的方法，进而提升供应链管理的整体效率。区块链技术可以避免供应链纠纷。所具有的数据不可篡改和时间戳的存在性证明的特质能很好地运用于解决供应链体系内各参与主体之间的纠纷，实现轻松举证与追责。区块链技术可以用于产品防伪。

数据不可篡改与交易可追溯两大特性相结合，可根除供应链内产品流转过程中的假冒伪劣问题。例如，伦敦的区块链初创企业 Provenance 为企业提供供应链溯源服务，通过在区块链上记录零售供应链上的全流程信息，实现产品材料、原料和产品的起源和历史等信息的检索和追踪，提升供应链上信息的透明度和真实性。通过 Provenance 的区块链平台，整合产品制造、运输、交易环节过程中的全部信息，重建供应链条中的信用体系，促进体系的良性发展。

我们注意到，区块链技术已在世界各地呈现方兴未艾的发展态势。从业务上看，借助区块链的安全特性与信任机制， 将成为发展数字经济的重要技术引擎，可以在多行业领域发挥作用，行业应用领域发展潜力巨大。但从行业 IT 系统需求的角度来看，要在区块链上构建应用，需要区块链解决方案具备强大的三个底层能力：一是完善的新旧系统兼容/切换能力，二是全新的系统安全能力，三是

适用多场景的用户隐私保护能力。

基于上述需求，小牛链提供了高可用性、可扩展的区块链应用基础平台，通过此平台，各领域的合作伙伴可以快速搭建上层区块链应用，帮助企业将精力聚焦在业务本身和商业模式的运营上，让用户、商户、机构在多样化的应用场景中受益。

第四章 团队介绍

小牛团队是一支有梦想，有情怀，执行力超强的年轻团队。小牛团队已经有多年的项目运作经验。在团队雄厚的实力及广阔扎实的人脉资源下，小牛团队与多个虚拟币界大咖携手合作，经过刻苦钻研虚拟货币的区块链技术，目前，小牛旗下项目将会包含小牛币交易平台，小牛云平台，小牛资讯和小牛国内、国际交易平台。力争打造最新型区块链智能合约应用，进行深度数据挖掘，分布式布局，高度智能，贴身感受场景。

第五章 免责声明及风险声明

此章所包含的信息为风险提示，请相关意向爱好者仔细阅读。

该文档只用于传达信息之用途，并不构成任何形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。

在参加小牛币的 ICO 计划中，必须用户本人了十分了解和清楚小牛的发展路线以及明白区块链行业的相关风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。加密货币是一种早期并且高风险的的行业，投资和参与，都需要非常谨慎，本项目可能会因其合法性、市场需求、技术性或者其它不可控的原因导致项目开发失败，项目失败的最差结果可能会导致您投入的所有比特币或者其它币无法收回。在参与小牛投资项目前，这些风险用户必须悉知。

小牛（xiaoniucoin.com）明确表示不承担任何参与小牛项目造成的直接或间接的损失包括：

（1）本文档提供所有信息的可靠性；

（2）由此产生的任何错误，疏忽或者不准确信息

（3）或由此导致的任何行为

（4）小牛币不是一种所有权和控制权，持有小牛币并不代表对小牛项目或小牛应用的所有权，小牛币并不授予任何个人或任何参与、控制，或任何关于小牛项目及小牛应用的决策权力。

9.2 风险声明：

（1）区块链底层技术核心协议相关的风险

小牛币和小牛应用程序基于区块链底层技术协议开发，因此任何区块链底层技术核心协议发生的故障，不可预期的功能问题或遭受攻击都有可能导致小牛币或小牛项目以难以意料的方式停止工作或功能缺失。

（2）司法监管相关的风险

区块链技术已经成为世界各个国家的监管主要对象，如果监管主体插手或施加影响则小牛项目或小牛币可能受到其影响，例如法令限制使用，销售，电子代币诸如小牛币有可能受到限制，阻碍甚至直接终止小牛项目的发展。

（3）小牛项目缺少关注度的风险

小牛项目存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能会对小牛币和小牛项目造成负面影响。

（4）黑客或盗窃的风险

黑客或其他组织或国家均有以任何方式试图打断小牛项目或小牛币功能的可能性，包括服务攻击，Sybil 攻击，游袭，恶意软件攻击或一致性攻击等。

（5）漏洞风险或密码学科突飞猛进发展的风险

密码学的飞速发展或者科技的发展诸如小牛计算机的发展，或将破解的风险带给加密代币和小牛平台，这可能导致小牛币的丢失。

（6）小牛币挖矿攻击的风险

就如其他去中心化的密码学代币和加密代币一样，用于小牛币项目的区块链也很容易受到挖矿攻击，例如双花攻击，高算力比例攻击，“自利”挖矿攻击，过度竞争攻击，任何成功的攻击对小牛应用，对小牛币来说都是一种风险，尽管小牛非常努力提升系统的安全性，但以上所述的挖矿攻击风险是真实存在的。

（7）无法预料的其他风险

密码学代币是一种全新的且未经测验的技术，除了本白皮书内提及的风险外，

此外还存在着一些小牛团队尚未提及或尚未预料到风险，此外，其他风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现

结束语

区块链技术的应用，目前尚处于萌芽阶段，但随着基础知识的普及和众多创业团队的研发改进，区块链技术在未来全面铺开应用是势在必行的，也可能成为21 世纪最伟大的互联网创新技术。小牛开发团队希望能为区块链技术的发展应用添砖加瓦。如果您对我们的区块链应用项目有合作或投资意向，可与我们联系；如果您是有意向参与区块链技术开发的程序员，也可与我们联系。

联系我们

小牛官方网址：www.xiaoniucoin.com

邮箱：xiaoniucoin@126.com

注：该白皮书为小牛理念白皮书的 1.0 版本，后面根据小牛平台的发展需要和战略调整，将推出小牛理念白皮书的 2.0 版本，另外小牛的技术白皮书正在积极筹备中，敬请期待。