2019

合同链白皮书

REVIEW FOR 2019

目录

2、“合同链”盈利模式

3、技术实现

4、技术创新

5、产品优势

6、“合同链”发展历程

四、社会效益及经济效益

（一）、推动经济发展、增加就业岗位

（二）、推动中国司法的进步和发展

（三）、推动中国教育的持续发展

（四）、保护环境，降低碳排放

（五）、建立社会“信用机制”

一．政策分析

近年来，区块链日益受到中国政府的重视与关注，一方面中央加大对 ICO 项目的监管，

另一方面积极推动国内区块链的相关领域研究、标准化制定以及产业化发展。

（一）、领导关注

2018 年 5 月 28 日，在北京召开的中国两院院士大会上习近平总书记指出“以人工智能、量子信息、物联网、区块链为代表的新一代信息技术加速突破应用，科学技术从来没有

像今天这样深刻影响着国家前途命运，从来没有像今天这样深刻影响着人民生活福祉……”

（二）、2019 年两会关注

2019 年的全国两会上，区块链更是频繁被提及。据公开数据表示，两会代表委员共提出至少 15 份涉及区块链场景的提案或议案，而金融、政务、商品溯源等领域成热门讨论方向。

（三）、中央及地方政策支持

1、中央政策

1).2019 年 1 月 10 日，国家互联网信息办公室发布《区块链信息服务管理规定》(以下简称“《规定》”)，自 2019 年 2 月 15 日起施行。

2).2018 年 3 月，工信部发布《2018 年信息化和软件服务业标准化工作要点》，提出推动组建全国信息化和工业化融合管理标准化技术委员会、全国区块链和分布式记账技术标准化委员会。

3).2017 年 10 月，国务院发布《关于积极推进供应链创新与应用的指导意见》提出要研究利用区块链、人工智能等新兴技术，建立基于供应链的信用评价机制。

4).2016 年 12 月，“区块链”首次被作为战略性前沿技术写入《国务院关于印发“十三五”国家信息化规划的通知》。

2、地方政策

据现在财经(caijing.io)统计，截止 3 月底，目前国内有北京、上海、广州、重庆、深圳、江苏、浙江、贵州、山东、贵州、江西、广西等多地发布政策指导信息，开展对区块链产业链布局。

1).上海 :《2018 上海区块链技术与应用白皮书》在 2018 中国（上海）区块链技术创新峰会上发布，以积极开放、主动合作的姿态向社会各界展示了上海在区块链技术和产业上的积极探索和布局考虑。

2).浙江 :2017 年浙江省在多次政府文件中提及区块链 ,如在《关于推进钱塘江金融港湾建设的若干意见》中提及积极引进区块链企业入驻，在《关于进一步加快软件和信息服务业发展的实施意见》中加快云计算、大数据、区块链等前沿领域技术研究和产品创新。

3).贵州 :2018 年 1 月 贵阳市人民政府办公厅关于印发关于支持区块链发展和应用的若干政策措施(试行)的通知筑府办发〔2017〕12 号

（四）、司法先行

1、**北京互联网法院** 天平链北京互联网法院成立于 2018 年 9 月 9 日，集中管辖北京市辖区内应当由基层人民法院受理的第一审特定类型互联网案件。法院内设立案庭、三个综合审判业务庭、执行局、审判管理办公室、政治处、综合办公室八个部门。法院将按照“网上案件网上审理”的基本思路，通过全流程一体化在线服务平台，实现案件起诉、调解、立案、送达、庭审、宣判、执行、上诉等诉讼环节的在线进行，切实做到高效便民，切实提高审判质效，从而推动我国科技强国战略的实施和网络空间治理的法治化进程。

2、**杭州互联网法院** 司法区块链杭州互联网法院，于 2017 年 8 月 18 日挂牌成立，是全国第一家集中审理涉网案件的试点法院。贯彻“网上案件网上审”的审理思维，将涉及网络的案件从现有审判体系中剥离出来，充分依托互联网技术，完成起诉、立案、举证、开庭、裁判、执行全流程在线化，实现便民诉讼，节约司法资源。融合机制创新与网络解纷，构建前置性指导化解、ODR、第三方调解、诉讼等多层次、多元化的涉网纠纷解决体系，专业、高效、便捷处理涉网纠纷。利用大数据分析技术对涉网案件数据进行多模块比对分析，梳理规律和特点，形成结构化标准化的互联网司法裁判规则，为营造

更安全、更干净、更具人性化的网络空间司法护航。

3、**广州互联网法院** 网通法链 2018 年 9 月 28 日上午，广州互联网法院正式挂牌成立，广州互联网法院是为落实中央全面深化改革委员会审议通过的《关于增设广州互联网法院的方案》，全面发挥司法在推动网络经济创新发展、保障网络安全、构建互联网治理体系方面的职能作用而增设的互联网法院。广州互联网法院将践行“网通法联，明断善治”院训，坚持“政治为本、公正为魂、创新为源、科技为基”工作方针，紧紧围绕经济社会发展需要和人民群众多元化司法需求，积极探索完善符合互联网规律的新型技术平台、新型诉讼规则、新型裁判规则、新型治理规则，努力打造维护网络安全、化解涉网纠纷、服务保障互联网经济发展的示范点和排头兵不断为走中国特色社会主义法治道路、实施网络强国战略贡献广州智慧。

二、电子合同市场分析

（一）、市场痛点及需求—电子合同能解决纸质合同高成本、高风险等问题。

原始的纸质合同在签署过程中，整个流程存在使用大量纸张、油墨打印，行业公认价格每份纸质合同签署费用达 20-25 元。纸质合同需要专人管理。异地签署需要来回快递。整个过程可能会遇到合同易丢失、隐私被泄露、合同被伪造、内容被篡改、阴阳合同、私刻萝卜章等多重风险。

电子合同优于纸质合同的是，不仅在于能大量节省合同打印，快递、存储和管理成本，更在于合同电子化后，能大幅提升交易效率，降低交易成本，推动协作和价值交换，推动资源的优化配置。签署纸质合同，从达成共识到双方完成合同签署，不仅会消耗大量的人力物力，而且需要很长时间，少则 1 天，多则 10 天半月，而显得社会，日新月异，过长的交易周期，不仅对先签署方不公平，而且也会失去更多交易机会。

所以电子合同代替纸质合同是社会经济信息化、数字化的必然趋势，是电子商务的基础设施，它不仅能降低成本，更能驱动交易，保障安全，简化管理，促进社会经济的繁荣和发展。

（二）、电子合同市场份额分析：是一片千亿级高利润的蓝海

1、目前中国“电子合同”市场巨大，但尚处于初级发展阶段，整个行业的渗透率还非常低。

	B2B	B2C	C2C	总额
商务部数据	50 亿份	50 亿份	20 亿份	
行业公认电子合同单价	12 元	8 元	4 元	
电子合同总市场额度	600 亿	400 亿	80 亿	1080 亿
税收分析（15%）	90 亿	60 亿	12 亿	162 亿

2、当前市场份额分析 目前尚有 95%的电子合同市场份额，即 1026 亿元的一个千亿级市场待开发待发展，整个行业渗透率极低，几大平台的营收合计仅在亿元级别。电子合同是一个全新且高利润行业，更是一片蓝海市场。谁拥有更尖端技术，谁能迅速抢占巨额市场，谁将成为行业领袖和规则制定者。

3、竞品分析据行业报告分析，2018 年中国有近 50 家第三方电子合同提供商，占据整体合同市场份额 5%左右。

1) .目前中国排名前三名的电子合同服务提供商:

A.法大大：于 2015 年获天使轮融资 1500 万元，2016 年 12 月获得 6000 万人民币 B 轮融资。

2018 年 6 月完成亿元级别的 B+轮融资，由元璟资本领投，汇付创投基金、和盟创投、博将资本跟投。

2019 年 3 月，“完成 C 轮 3.98 亿元融资，此轮融资由老

虎环球基金和腾讯联合领投，锐盛投资、元璟资本跟投。2018 年，法大大平台合同签署量超 4.2 份日均合同签章数超 930 万次。

B.e 签宝：成立于 2002 年，2015 年完成 PreA 轮 1000 万元融资，由浙银绩优领投。

2016 年 12 月完成 A 轮 4500 万元融资，由东方富海领投，清控银杏跟投。

2017 年 12 月完成 B1 轮 1.5 亿元融资，由前海梧桐领投，清控银杏继续跟投。目前 e 签宝签约总量超过 60 亿份，日签约量超过 2000 份，企业用户超过 190 万家，个人客户超过 1.9 亿。

C.上上签：成立于 2014 年，2015 年上上签完成了两轮融资，分别是经纬中国 700 元的 Pre-A 轮，以及 DCM 领投、经纬跟投的 2930 万元 A 轮。2018 年 8 月 获老虎环球基金领投，经纬、DCM、晨兴跟投的 C 轮融资 3.58 亿人民币。上上签平台目前的日签署量已突破 1100 万，服务超过 50 万家企业客户。

2) .国外-DocuSign

DocuSign 成立于 2003 年，是一家诞生于美国硅谷的电子签约解决方案和数字交易管理公司，能够帮助用户快速创建、获取 具有法律效力的电子签约。2018 年 4 月，DocuSign 在纳斯达克 IPO，上市当日市值突破 60 亿美元。2019 年 5 月，市值约 90 亿美金。目前每天合同签署量达 15 万份。

（三）、市场需求：

“电子合同” 2019 年预计 134.7%复合增长率 。当前国内第三方电子合同市场仍处于发展的起步阶段，在起步阶段已经呈现出高速增长的态势。据知名研究机构 T 研究 2018 年报告说明，

2017 年国内第三方电子合同市场规模则高速攀升，年复合增长率连续多年高于 130%。新技术、新概念的引入，也有力推动了第三方电子合同向更安全、更高效、更智能发展，

2018 年复合增长率可达 146.6%，

2019 年将持续保持高速增长，达到 134.7%的复合增长率。

图表来源：T 研究《2018 年第三方电子合同市场分析报告》

图表来源：T 研究《2018 年第三方电子合同市场分析报告》

（四）、电子合同市场环境分析：使用电子合同的大环境已然成熟

1、用户互联网习惯—人们已经形成用电脑和手机处理任何事情在当前大互联网环境下.

已经实现全民皆互联网。人们可以在任何时间、任何地点通过各端上网进行信息交流和互换。人们也已经非常习惯通过支付宝、微信等工具，进行沟通、支付、传送文件、视频、语音、处理工作等行为。

2、**区块链思维—区块链解决了互联网带来的各类弊端**

区块链技术已经发展 10 多年，近两年技术发展已经十分成熟，开始进入飞速发展时期。区块链技术的灵魂在于它有有别于传统互联网的运行机制：通过技术的精巧组合，完成资源的公平分配，从而确保社区目标一致，成员的行为规范。传统的互联网，已经使人们形成了一切用电脑或手机来处理工作和生活日常事务。但是会造成信息泄露，文件丢失、非实名制导致人们相互之间不信任等多重风险。区块链技术正好弥补了这块安全缺失。

3、法律环境--电子签名是法律认可的真实有效的

1) .法律条文

A.《**中华人民共和国合同法**》：认可以数据电文作为合同书面形式的合法载体

第十条：当事人订立合同，有书面形式、口头形式和其他形式。

第十一条：书面形式是指合同书、信件和数据电文（包括电报、电传、传真、电子数据交换和电子邮件）等可以有形地表现所载内容的形式。

B.**《中华人民共和国电子签名法》**：认可可靠电子签名的合法效力

第十三条：电子签名同时符合下列条件的，视为可靠的电子签名：电子签名制作数据用于电子签名时，属于电子签名人专有；签署时电子签名制作数据仅由电子签名人控制；签署后对电子签名的任何改动能够被发现；签署后对数据电文内容和形式的任何改动能够被现。当事人也可以选择使用符合其约定的可靠条件的电子签名。

第十四条：可靠的电子签名与手写签名或者盖章具有同等的法律效力。

C.**《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》**：认可电子数据为法定证据种类的合法地位

第一百一十六条：视听资料包括录音资料和影像资料。电子数据是指通过电子邮件、电子数据交换、网上聊天记录、博客、微博客、手机短信、电子签名、域名等形成或者存储在电子介质中的信息。 存储在电子介质中的录音资料和影像资料，适用电子数据的规定。

D.**《最高人民法院印发〈关于互联网法院审理案件若干问题的规定〉的解释》**：认可区块链存证的法律效力

第十一条：当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认.

2) .司法案例

2019 年 4 月 成都市郫都区法院 上线区块链电子证据平台

2019 年 1 月合肥市蜀山区人民法院上线区块链电子证据平台

2018 年 11 月 杭州余杭人民法院 采信电子合同证据

2018 年 10 月 北京市东城区人民法院 区块链取证判决知识产权

2018 年 10 月 广西兴业县人民法院 采信电子合同证据

2018 年 8 月 云南省红塔区人民法院 采信电子合同证据

2018 年 8 月 天津市武清区人民法院 采信电子合同证据

2018 年 6 月 杭州互联网法院 全国首例区块链存证案

2017 年 6 月 上海市嘉定区人民法院 采信电子合同证据

2017 年 6 月 衢州仲裁委 采信电子合同证据

三、基于区块链的电子合同产品—“合同链”

（一）、什么是“区块链”？

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机应用技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。比起之前传统的数据库，区块链除了解决信任问题，还有以下主要优点：

1、完全非中心化：读 / 写数据库是分散和安全的，单独某个人或某个组无法控制区块链。

2、逻辑化，让每个人共享数据库来验证其变化。

3、独立验证：交易可以由任何人验证，无须第三方，这有时也被称作脱媒。

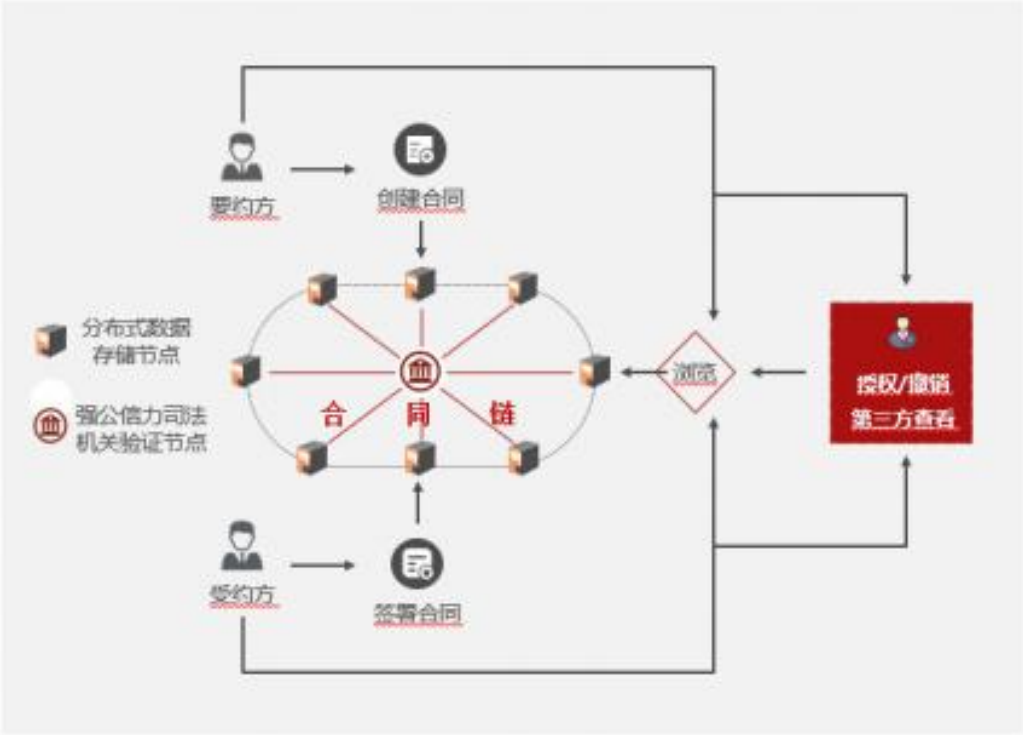
（二）、核心产品：“合同链”

合同链是通过智能合约实现合同的创建、签署、补充、交付、关闭等的一站式处理与区块链存证的非中心化处理系统。企业客户用源代码公开的 sdk 集成至已有 OA 或业务系统,个人客户用非中性化电脑端及移动端网页。

1.“合同链”流程“合同链”的要约方和受约方，分别在系统中创建账户，获取地址和私钥(私钥为具有法律效益的唯一的电子签章)，进行实名认证后，以其私钥 (符合《中华人民共和国电签名法》中关于可靠电子签名定义) 共同完成合同的签署。合同内容分布式存储于全球各数据节点，结合国密系列算法，可做到数据无法删除、不可篡改，确保隐私和安全。同数据由如法院、公证处、仲裁委等权威司法机构的验证节点进行记录和验证。整体流程要约方和受约方基于数字身份可授权给第三方浏览、取证或撤销。整个过程，高效便捷、合法有效、安全可靠。

➢ 服务流程

➢ 布局构架



2.“合同链”盈利模式合同链依靠向用户收取合同签约手续费获得盈利。

同时与验证节点共享收入。用户签署前向合同链预存合同服务费，用户在发起或签署合同后，作为权威公信的验证节点将收到合同链向其支付的验证节点利润分成。

3.技术实现

1). 系统概述

传统的电子合同虽然能在一定程度上解决线下合同签署流程繁琐等问题，但其采用的是第三方中心化存储的方式，该种模式下数据是可篡改的，无法保证数据的真实性。

而基于块链技术的电子合同系统，通过结合区块链技术不可篡改、可溯源等特性，对合同签署的每一个过程都实时记录上链存证，有效的保障了合同数据的完整性和真实性，合同签署记录可溯源。

你一定很好奇这跟区块链存证有什么关系？在区块链存证出现之前，利用云存证是我们常用的方式，

但是云存证有一个弊端：太过中心化，没有办法证明存储的就是之前的证据，数据也容易被篡改。

为了解决这个问题，电子合同结合区块链技术，让需要存储的证据通过哈希运算生成一串字符后上链存储。然后再将源文件本身上传至云端进行加密存储，这样两者之间就有了可以验证的关系，这也是在法律上得到认可的原因。

在区块链存证中，哈希加密只是其中一种超级保险库级别的保障措施。

除了它，还有共识机制以及去中心化存储两大核心底层技术。通过国密 SM3 算法在本地生成源文件证据的哈希，并将其写入区块链

某一区块中，之后源文件证据的哈希就被永久进行保存了，而后一区块在新生成时，又会将前一区块的哈希包含进去，以此类推。

2）.公链设计策略

★账户

我们抛弃了UTXO的方案，转而使用更简单的方法：采用状态(state)的概念存储一系列账户，每个账户都有身份认证信息以及自己特有的数据（代码或内部存储器）。某些情况下，接受账户内有需要执行的代码，则交易会触发该代码的执行，那么账户的内部存储器可能就会发生变化，甚至可能会创建额外的信息发送给其他账户，从而导致新的交易发生。

★默克尔帕特里夏树

默克尔帕特里夏树(Merkle Patricia tree/trie),由 Alan Reiner 提出设想，并在瑞波协议中得到实现，是“合同链”的主要数据结构，用于存储所有账户状态，以及每个区块中的交易和收据数据。MPT 是默克尔树和帕特里夏树的结合缩写，结合这两种树创建的结构具有以下属性：

1.每个唯一键值对唯一映射到根的 hash 值；在 MPT 中，不可能仅用一个键值对来欺骗成员（除非攻击者有~2^128 的算力）；

2.增、删、改键值对的时间复杂度是对数级别。

MPT 为我们提供了一个高效、易更新、且代表整个状态树的“指纹”。

★RLP 编码

RLP 旨在成为高度简化的序列化格式，它唯一的目的是存储嵌套的字节数组③。不同于 protobuf、BSON 等现有的解决方案，RLP 并不定义任何指定的数据类型，如 Boolean、20floa、double 或者 integer。它仅仅是以嵌套数组的形式存储结构，并将其留给协议来确定数组的含义。RLP 也没有明确支持 map 集合，半官方的建议是采用 [[k1, v1], [k2, v2], ...] 的嵌套数组来表示键值对集合，k1,k2 ... 按照字符串的标准排序。

与 RLP 具有相同功能的方案是 protobuf 或 BSON，它们是一直被使用的算法。然而，我们更偏向于使用 RLP，因为：

1、它易于实现；

2、绝对保证字节的一致性。

★虚拟机

简单：操作码尽可能的少并且低级；数据类型尽可能少；虚拟机的结构尽可能少；

结果明确：在 VM 规范语句中，没有任何可能产生歧义的空间，结

果应该是完全确定的。;

节约空间：VM 组件应尽可能紧凑；

预期应用应具备专业化能力:在 VM 上构建的应用应能处理字节的地址，以及 32 位的自定义加密值，拥有用于自定义加密的模数运算、读取区块和交易数据与状态交互等能力；

简单安全：为了让 VM 不被利用，应该能够容易地让建立一套 gas 消耗成本模型的操作；

优化友好：应该易于优化，以便即时编译（JIT）和 VM 的加速版本能够构建出来。

同时我们也有如下特殊设计：

临时/永久存储的区别：

临时存储：存在于 VM 的每个实例中，并在 VM 执行结束后消失；

永久存储：存在于区块链状态层。

假设执行下面的树（S 代表永久存储，M 代表临时存储）:

1. A 调用 B；

2. 2.B 设置 B.S[0]=5，B.M[0]=9；

3. B 调用 C；

4. C 调用 B。

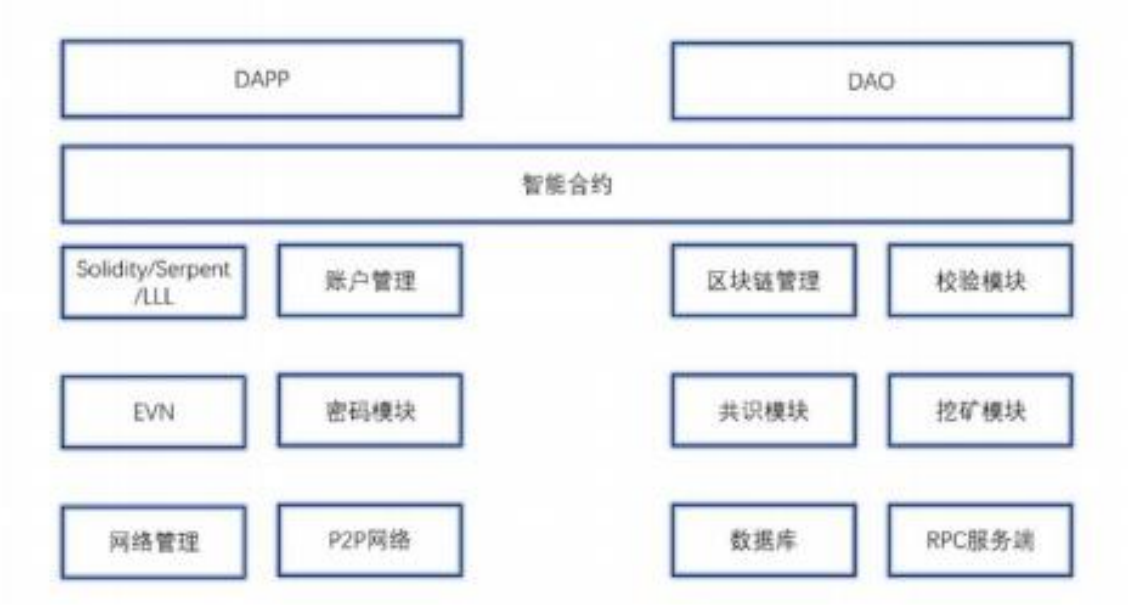
此时，如果 B 试图读取 B.S[0]，它将得到 B 前面存入的数据，也就是 5；但如果 B 试图读取 B.M[0]，它将得到 0，因为 B.M 是临时存储，

读取它的时候是虚拟机的一个新的实例。

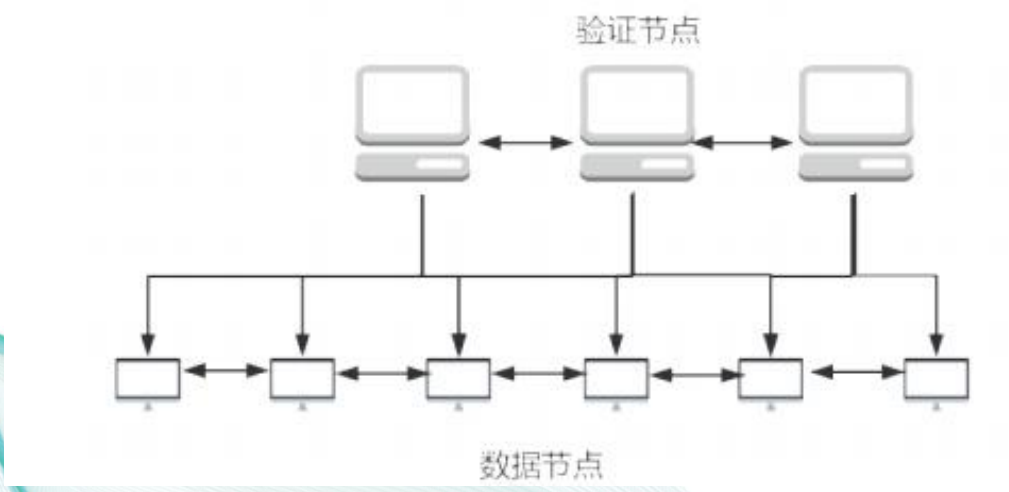
在一个内部调用中，如果设置 B.M[0] = 13 和 B.S[0] = 17 ，然后内部调用和 C 的调用都终止，再执行 B 的外部调用，此时读取 M,将会看到 B.M[0] = 9(此值在上一次同一 VM 执实例中设置的)，B.S[0] = 17 。如果 B 的外部调用结束，然后 A 再次调用 B，将看到 B.M[0]= 0，B.S[0]= 17 。这个区别的目的是：1.每个执行实例都分配有内存空间，不会因为循环调用而减损，这让安全编程更加容易。2.提供一个能够快速操作的内存形式：因为需要修改树，所以存储更新必然很慢。

3) .公链技术构架

★基础架构



★节点架构



★什么是节点?

区块链中的节点，通常是指下载了相关区块链数据的软件，以参与对等网络的计算机。

加密货币区块链的结构是对等点(P2P)之间的网络架构。P2P 是指参与网络的计算机彼此相等。P2P 这个词并不新鲜，P2P 网络的第一次大规模使用是由音乐文件共享网络 Napster 完成的。

这样，在 P2P 网络中，参与网络的每一台计算机都可以接收节点的名称。在网络中，所有的节点都有责任提供网络服务。这是因为网络节点的互连性，允许进行互操作性。

区块链网络是指执行给定区块链 P2P 协议的节点集。整个网络以完全联合、去中心化和分布式的方式编排和协调每个用户在网络中所做的操作。

这意味着全世界的计算机网络以不断地相互传输新的事务。这个网络中的每台计算机都是一个节点，它已经下载了完整的区块链。这样，网络就变得冗余了，而协同工作使其在扩展方面具有可伸缩性。

由于区块链的分散化，任何人都可以参与其中。只需从下载节点软件并执行它即可。通常，每个项目的主钱包都支持此功能。最初，网络从区块链的起源开始，直到与网络同步为止。

此时，节点开始全面运行，不仅允许验证事务，而且支持区块链的整体映像。通常节点可以执行以下功能:路由、区块链数据库、挖

掘和钱包服务。

这些节点是一个区块链最大数据结构中的单个部分。当节点所有者自愿贡献自己的计算资源来存储和验证事务时，他们就有机会收取交易费用，并在潜在的加密货币中获得奖励。

处理这些事务可能需要大量的计算和处理能力，这意味着计算机的平均能力是不够的。一般来说，专业的矿商倾向于投资被称为CPU(中央处理单元)或 GPU(图形处理单元)的非常强大的计算设备，以满足对验证事务所需的处理能力的需求，从而获得相应的回报。

节点可以是通信端点，也可以是通信的重分发点，链接到其他节点。网络中的每个节点都被认为是相等的，但是，某些节点在支持网络的方式上扮演着不同的角色。例如，并非所有节点都会存储区块链的完整副本。

一个完整的节点下载一个区块链的完整副本，并根据该特定加密货币或实用代币所使用的共识协议检查产生的新事务。所有节点都使用相同的共识协议来保持相互兼容。网络中的节点负责确认和验证事务，并将它们放入块中。对于一个事务是否有效以及是否应该添加到带有其他事务的块中，不管其他节点如何行动，节点总是可以得出自己的结论。

当用户试图通过协议的某种机制向区块链添加一个新的事务块时，它将该块传输到网络的所有节点。根据块的合法性(签名和事务

的有效性)，节点可以接受或拒绝块。

当一个节点接受一个新的事务块时，它保存它并将它存储在它已经存储的其他块上。

综上所述，节点的作用是：他们可以检查一个事务块是否有效，并接受或拒绝它。存储和存储事务块(存储区块链事务历史)。将此事务历史传输并扩展到可能需要与区块链同步的其他节点(它们必须在事务历史中更新)。

4) .数据安全

A. 区块链的固有结构可增强安全性

仅仅是区块链的基本结构，不加上基于此的任何应用和平台，区块链就可以增加数据安全性。从整体安全角度考虑，区块链的零信任本质就意味着用户无需依靠第三方来完成交易。最重要的是，从数据角度看，区块链上发生的一切都是加密的。黑客悄悄篡改区块链上数据而不被他人发现这种事绝对不可能发生。

作为高度去中心化的系统，区块链天生比传统数据安全系统更安全。在大多数现有数据安全系统都集中放置的时候，区块链的分布式特性就代表着其更难以被黑。没有单一组织管控，意味着不会发生单点故障。

B. 区块链的分布式特性引领数据存储革命

数据安全与数据存储紧密相关，而后者正是区块链革新的领域。与将数据存放在云端不同，区块链利用的是分布式存储：

将数据打散成无数小块

加密数据以防黑客获得真正信息

将数据文件分散存储

这一分布式存储过程以两种方式保护数据安全：

a. 因为存储在多个位置而不是在单一位置存放，数据不会受到某一网络掉线的影响，即便一部分网络被黑客致瘫，用户仍能从其他地方获取到数据。

b.加密过程也有效防止了无权用户对数据的访问，可确保隐私及敏感个人数据免遭黑客毒手。一旦有人篡改了记录，数据签名也就失效了。

如果是传统存储模型，黑客只需攻破某个服务器即可。而在区块链模式下，想要进行欺诈交易或伪造余额，你得搞定网络中绝大部分节点才行。只黑一台服务器都已经让网络罪犯费神费力了，黑掉网络中足够多的节点以形成“共识”来篡改记录这种事，有脑子的黑客都不会去干。更遑论，黑客没准儿还得同时搞定网络中所有节点呢。

C. 区块链可证明数据未受污染

除了分布式数据存储，区块链还可以保存特定文档的加密签名。只要文件有签名，用户就可以保证无法被篡改。该方法可以让用户文件存哪儿存哪儿，无论存放文件的系统是基于云的还是本地系统，且同时还能保证无论在哪儿都看到的是同一份未经篡改的文件。

4、技术创新

1).公链：

目前市面上传统电子合同大多数是建立在联盟链之上，而“合同链”是真正建立在公链之上的电子合同系统。

A.基于联盟链的传统电子合同：非全链各节点加密，仍有商业泄密风险

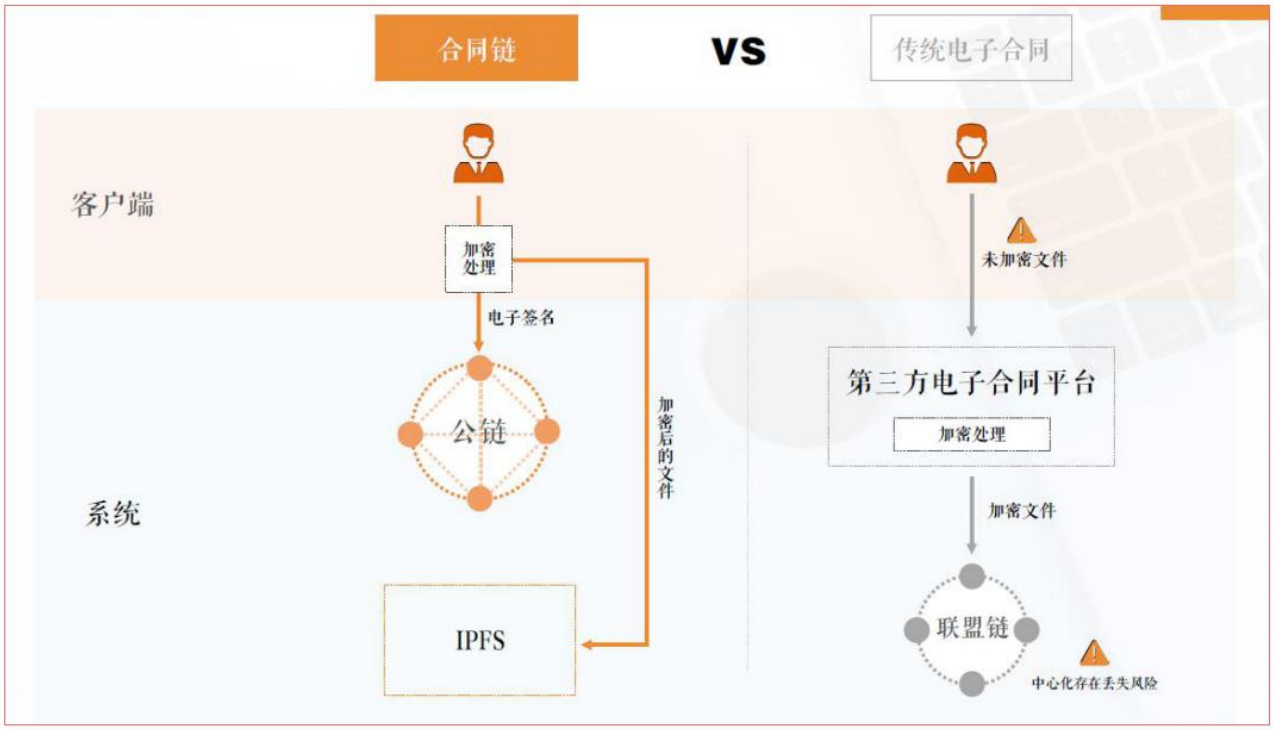
目前市场上大多数电子合同系统是基于传统互联网架构（SaaS）或联盟链架构的传统电子合同，数据被中心化的存储在备份有限且不开源的服务器当中。若服务器出现火灾、停电、黑客入侵等自然因素或人为意外，极易导致数据丢失、损毁，数据有可能永远无法找回，造成极大的经济损失。而通过中心化节点签署合同的另一个风险是，当数据传送至第三方电子合同平台时，加密度低或加密滞后，无法保

证合同数据的隐私性。

B.而基于公链的“合同链”:全链加密，即使是第三方技术方仍无法看到内容，商业机密泄露 0 风险

数据存储于无数个数据节点组成的也公有链上。每个节点相互应证，数据无法删除、不可篡改。所有数据通过高级别加密算法，每个环节均呈现为加密数据，即使是作为技术提供方也无法看到任何合同内容。整个合同签署过程，全生命周期完整，数据不可逆，无法被改，全程每个环节数据保密，绝对保护了合同的安全和隐私。

目前“合同链”是中国第一家真正使用区块链技术，将数据存储于公链之上的新一代电子合同系统。



2).IPFS 分布式加密存储：“非中心化”加密存储，数据不可篡改、无法丢失

IPFS 全名叫星际文件系统（InterPlanetary File System，缩写 IPFS)是一个旨在创建持久且分布式存储和共享文件的网络传输协议。它是一种内容可寻址的超媒体分发协议。在 IPFS 网络中的节点将构成一个分布式文件系统。它能解决现有云存储下的带宽，设备需持续投入的高成本问题，又能提出传播不良内容的行为风险，是一种 颠覆传统集中机房高额运维成本的运作模式，合理利用闲置资源，利益回归用户，根本上降低存储使用成本。

“合同链”部署了数台 IPFS 节点建设专用集群，对文件分布式

加密存储。

3).共识机制：可将数据传输速度提高 600 倍

合同链采用 DPOA（Delegated Proof-of-Autthority）共识机制。它的原理，指的是让每一个节点都可以进行投票，由此产生一定数量的代表 ,或者理解为一定数量的节点或矿池，他们彼此之间的权利是完全相等的。节点可以随时通过投票更换这些代表，以维系链上系统的“长久纯洁性”。

DPOA 的优势就在于能将维系网络运行的能源消耗降到最低，以一种低成本的方式来管理整个链上的运行 ,这就很大程度上解决了

POW 的能源耗损问题。同时，更加“非中心化”的管理方式，将区块链网络运行的决定权分散到全网的各个节点手中，这就很大程度上避免了 POS 容易出现的被庄家操纵的“控股”现象。DPOA 共识机制的出现，将通过实施区块链上的“民主”来对抗“中心化”所产生的负面效应，用被公选的“弱中心化”的方式来提高全网运维的效率。

4).认证机制：保证客户的绝对隐私

“合同链”用户，在创建账户后，必须进行实名认证。基于这种统一身份认证服务系统的认证模式，在用户登录统一身份认证服务后，即可使用所有支持统一身份认证服务的管理应用系统。这种数字身份上链的模式，所有用户上链身份唯一，行为可追溯。所有数据不可篡改，所有协议第三方需被授权才能查看，确保所有用户的绝对隐私。区块链技术发展 1 多年来，其多重技术和算法交替重叠，至今无人破解，保证了所有用户安全 0 风险。

4、产品优势:

1).真正的区块链技术：

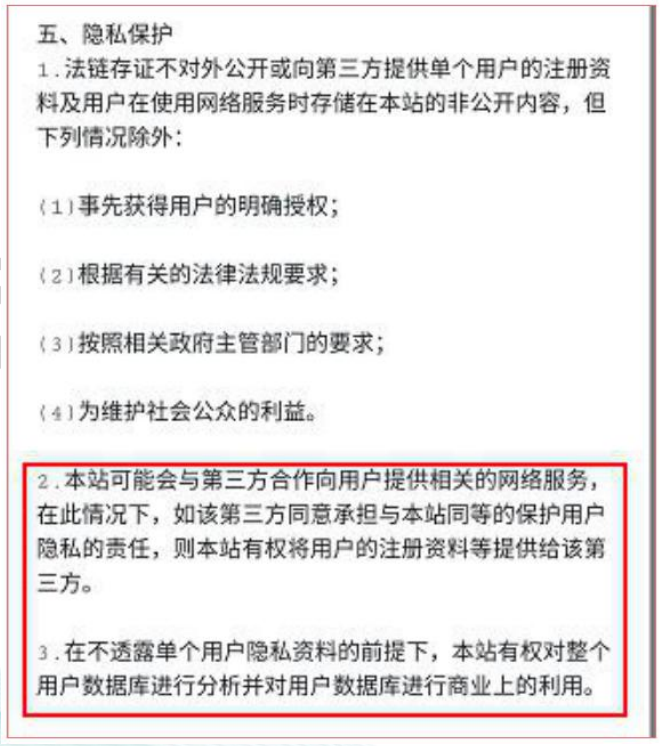
是中国第一家将自主研发的 DPOA 共识公链技术应用于司法合同领域上的公司。

2).**金融级别的安全**：

合同内容加密后存储于持久且分布式存储和共享文件系统(IPFS)中，确保数据无法篡改、无法删除、永不丢失，实现了合同的绝对安全和隐私保密。

3).**商业机密泄密 0 风险**：

目前大多数电子合同提供商，可以做到部分节点加密，无法做到全链数据节点整个闭环加密，商业机密还存在泄密风险。甚至有些服务商还在合同中明确说明链上合同可能会被做商业使用。



五、隐私保护

1.法链存证不对外公开或向第三方提供单个用户的注册资料及用户在使用网络服务时存储在本站的非公开内容，但下列情况除外：

(1)事先获得用户的明确授权；

(2)根据有关的法律法规要求；

(3)按照相关政府主管部门的要求；

(4)为维护社会公众的利益。

2.本站可能会与第三方合作向用户提供相关的网络服务，在此情况下，如该第三方同意承担与本站同等的保护用户隐私的责任，则本站有权将用户的注册资料等提供给该第三方。

3.在不透露单个用户隐私资料的前提下，本站有权对整个用户数据库进行分析并对用户数据库进行商业上的利用。

图片来源：某传统的第三方电子合同 SaaS 平台数据存证服务的用协议截图而合同链”采用了区块链上交错重叠的技术手段，确保在链上传输的数据，在每个点，每个时间都是加密文件。除非授权，任何第三方（包括技术方）也看不到任何内容，确保了商业机密绝对隐私。

4).节约成本、提高效率：

电子合同实现了无纸化和全球化，成几何化的减少了纸张、人力、快递、管理等的时间和经济成本。同时技术的革新，保证了数据的传输速度，极大的提高了工作效率。

5).**法律保障、取证容易：**

基于区块链技术的数字身份上链，确保身份唯一合法性，交易可追溯和可追回，整体证据链完整，法律上可信度、可采纳程度高。同时链上交易数据输入不可逆性，整个过程完整记录，无法被篡改、删除、永不丢失。能做到取证完整、取证容易。

6、“合同链”发展历程

1).2019 年 5 月 0.9 版本已上线试运营

“合同链”自 5 月份试运营以来，已与招商银行、兴业银行、遵义播州农商行、贵州遵义市科技局、贵州黔南州大数据局、遵义红花岗高科技局、贵州省高院、台州中级人民法院、深圳盈科律所、复旦大学、同济大学、柏丽培训、上汽、移动贵州省公司、柯沃、邦呈、兴彬国旅等近 200 家各行业客户达成意向，或签署战略合作协议。根据公司的部署战略，“合同链”预计 2019 – 2020 年每周增加 500+B 端用户，2020 – 2021 年持续推动无纸化办公生态，实现 B 端用户过百万，C 端用户过千万，2021 – 2022 年占领电子合同市场 5-10%市场份额。

2).2019 年 7 月 1.0 版本发布正式运营

3).2019 年 8 月发布第三方接入 SDK

4).未来应用延伸：

“合同链”未来将在数字身份应用、供应链金融服务、企业个人征信查询、版权资质存证、信托基金管理进行扩展和延伸。

四、社会效益及经济效益

（一）、推动经济发展、增加就业岗位

从前述表格数据可以看出，整体电子合同市场是个千亿级大市场，可为国家增加税收 162 亿元。同时也可以增加多个高技术含量的就业岗位和配套岗位，是个利国利民的、推动中国经济发展的好项目。

（二）、推动中国司法的进步和发展基于区块链电子合同系统

能确保合同签署整体流程和数据内容完整、数据隐私度极高，整体过程不可篡改，真正解决了司法取证中证据链不完整，取证不容易

等多个痛点。同时，区块链技术为整体电子合同服务创造了全新链上“公平、安全、可靠、保密”的信任体系，如若多数行业同时使用合同链，势必全面推动司法的发展，建立更多的互联网法院，实现“智慧司法”。

（三）、推动中国教育的持续发展：技术的发展带来社会的进步，社会的革新需要更多的人才和新鲜血液。市场需求的增势必会带来人才的培养需求。当更多技术岗位需求增加，更多人看到了区块链技术的实用性，随之配套而来的大学教育、社会培训需求也会激增。区块链的全球化布局，也会将全球化思维、管理方式、全新技术引进至各层级城市和地区，从而推动整体教育和经济的发展。

（四）、保护环境，降低碳排放

将合同签署电子化，可极大的减少纸张数量，树木的砍伐数量，快递包裹的数量。减少碳排放，保护更多的森林，净化美丽的地球。

（五）、建立社会“信用机制”

电子合同的使用，可以避免合同内容被篡改、不会再有萝卜章的出现，合同纠纷将大大的减少。全新区块链技术，为链上客户与客户之间搭建了安全可靠环境，用技术手段解决“信任缺失”问题，全面推

动了“信用机制”的革命。

感谢您的观看