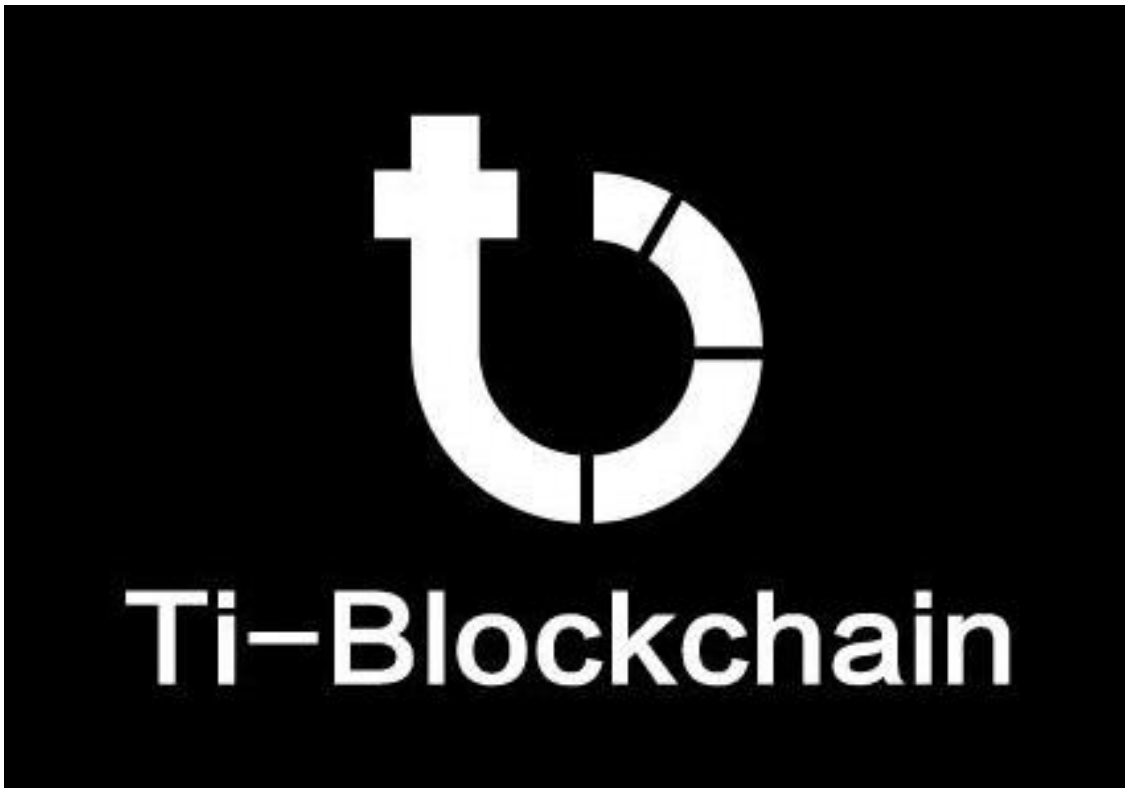


钛 链 白 皮 书

2018 年 1 月 10 日

摘　要

钛链 (Ti-Blockchain)，致力于发展现有区块链之外的公有链生态，结合 IPFS 系统解决现有金融问题和大量网络储存闲置问题。

钛链的主要特色是基于石墨烯技术开发的拥有智能合约的加密分布式存储。智能合约可以控制存储文件的加密等级，在商业应用中可以很好的保护用户的隐私。分布式存储称为永不消逝的硬盘，在有效利用闲散硬盘空间的同时，通过合理冗余的设计，达到安全存储的目的。 钛链的开发将围绕加密分布式存储继续进行，同时将落地更多的商业项目。主要从中国医院的电子病历系统、中国教育部的电子学历系统、电子合同系统、不同等级的加密通讯系统进行应用。

去中心化可以显著减轻数据中断的风险及其损失等，增加安全性、保密性。云存储依赖于第三方大型存储商来传输和存储数据，如 360 云盘、百度云盘等。但是受限于中心化的架构，非常容易受到各种安全威胁。冗余和去中心化的分布式存储可以有效改善这种状况，有效抵制篡改和未经授权的访问。文件在上传服务器之前就能得到加密，这样可以保护数据的内容，数据所有者保留对加密秘钥的完全控制，从而可以限制其他人对数据的访问。

传统存储与分布式加密存储

本文主要介绍钛链区块链的产品架构、技术特色与优势等。区块链的核心价值在于构建可信任的分布式多中心体系，它有潜力成为构建价值互联网的基础设施。钛链项目方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、高可扩展的区块链金融、企业服务平台，瞄准企业级产品化运营能力，钛链区块链已取得多项技术突破和创新，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，钛链区块链已应用于数字资产、贸易金融、股权债券、公示公证、数据安全等领域。其以多中心化信任为核心，打造 ABS+云存储网络，让企业信息数据更加可信。

关键词：钛链，区块链，去中心化

目 录

第一章 密码学专用术语和缩略语

1.1 密码学专用术语

密钥：分为加密密钥和解密密钥。

明文：没有进行加密，能够直接代表原文含义的信息。

密文：经过加密处理之后，隐藏原文含义的信息。

加密：将明文转换成密文的实施过程

解密：将密文转换成明文的实施过程。

密码算法：密码系统采用的加密方法和解密方法，随着基于数学的密码技术的发展，加密方法一般称为加密算法，解密方法一般称为解密算法。

密码通讯系统的模型：

对于给定的明文 m 和密钥 k，加密变换 Ek 将明文变为密文 c=f(m，k)=Ek(m)，在接收端，利用解密密钥 k（有时 k=k，）完成解密操作，将密文 c 恢复成原来的明文 m=Dk，(c)。一个安全的密码体制应该满足：①非法截收者很难从密文 C 中推断出明文 m；②加密和解密算法应该相当简便，而且适用于所有密钥空间；③密码的保密强度只依赖于密钥；④合法接收者能够检验和证实消息的完整性和真实性；⑤消息的发送者无法否认其所发出的消息，同时也不能伪造别人的合法消息；⑥必要时可由仲裁机构进行公断。

哈希算法：

哈希算法将任意长度的二进制值映射为较短的固定长度的二进制值，这个小的二进制值称为哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式。如果散列一段明文而且哪怕只更改该段落的一个字母，随后的哈希都将产生不同的值。要找到散列为同一个值的两个不同的输入，在计算上是不可能的，所以数据的哈希值可以检验数据的完整性。一般用于快速查找和加密算法。

哈希表是根据设定的哈希函数 H(key)和处理冲突方法将一组关键字映射到一个有限的地址区间上，并以关键字在地址区间中的象作为记录在表中的存储位置，这种表称为哈希表或散列，所得存储位置称为哈希地址或散列地址。作为线性数据结构与表格和队列等相比，哈希表无疑是查找速度比较快的一种。

通过将单向数学函数（有时称为“哈希算法”）应用到任意数量的数据所得到的固定大小的结果。如果输入数据中有变化，则哈希也会发生变化。哈希可用于许多操作，包括身份验证和数字签名。也称为“消息摘要”。

简单解释：哈希(Hash)算法，即散列函数。它是一种单向密码体制，即它是一个从明文到密文的不可逆的映射，只有加密过程，没有解密过程。同时,哈希函数可以将任意长度的输入经过变化以后得到固定长度的输出。哈希函数的这种单向特征和输出数据长度固定的特征使得它可以生成消息或者数据。

散列表（Hash table，也叫哈希表），是根据关键码值(Key value)而直接进行访问的数据结构。也就是说，它通过把关键码值映射到表中一个位置来访问记录，以加快查找的速度。这个映射函数叫做散列函数，存放记录的数组叫做散列表。

给定表 M，存在函数 f(key)，对任意给定的关键字值 key，代入函数后若能得到包含该关键字的记录在表中的地址,则称表 M 为哈希(Hash)表,函数 f(key)为哈希(Hash) 函数。

1.2 数字货币专有名词

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。

以太坊：是一个有智能合约功能的公共区块链平台。

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

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。

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。

激励权益证明共识：在权益证明共识中加入了激励措施，估计节点在线，激励网络中的节点可以保持在线以维护网络的稳定性和安全性。

硬分叉：区块链发生永久性分歧，在新公式规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会产生。

图灵完备：一个能计算出每个图灵可计算函数的计算系统被称为图灵完备。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相当，这也是现代计算机语言所能拥有的最高能力。

Oracle：根据预先设定的判断条件，对输入数据进行筛选，选择最适合的数据作为输入数据。

Data feeds：数据馈送，为区块链提供数据链下数据来源。

POS：权益证明共识机制。根据每个节点所占代币的比例和时间，等比例地降低挖矿难度，从而加快找随机数的速度。

UTXO：未花费交易输出。比特币网络中使用的交易模型。

POW：工作量证明共识机制。一方（通常称为证明人）提交已知难以计算但易于验证的计算结果，而其他任何人都能够通过验证这个答案就确信证明者为了求得结果已经完成了大量的计算工作。

DAO：分布式自治组织。通过一系列公正公开的规则，可以在无人干预的和管理的情况下自主运行的组织结构。

第二章 区块链综述

区块链技术，作为金融科技的核心革命力量，随着与物联网、保险、汽车、制造、医疗、能源、航运等多个领域的有机结合，联同云计算、大数据、人工智能、移动互联网等新技术，为新一轮的技术和产业创新革命提供动能。

2.1 区块链的起源和发展

区块链技术引发了人们关于摒弃效率低下陈旧系统，开启颠覆多行业运营和贸易崭新思路的思考。它作为一种分布式账本，在诸多领域，特别是在金融行业能发挥出极大潜力。由于存储在区块链的数据不可能被篡改，因此，我们相信区块链技术能够将数据的真实性和安全性推向一个全新的高度。

2.1.1 背景

2008 年末，名叫中本聪的人在比特币论坛发表了一篇题为《Bitcoin: A Peer-to-Peer Electronic Cash System》（比特币：点对点的电子现金系统）的论文。在文中，区块链的概念被首次提出，作为构建比特币网络与交易信息加密传输的基础技术，它能够支持比特币的采挖与交易。

中本聪认为，如果借助中心化手段（第三方机构）来处理交易数据，不仅无法克服商家和客户之间的不信任问题，而且交易成本高昂，交易规模也会受到限制。为解决此类问题，中本聪创造了区块链，并在其基础上发明了比特币。

2.1.2 定义

区块链的本质是一个共享、公开、共同参与记录的数据库。在没有中央服务器的情况下，它允许链接其中的计算机等设备使用“共识机制”相互通信，所有联网（点对点网络）设备（节点）都会保持数据一致且持续更新。由于采用这种模式，区块链又被称为“分布式账本”，分布意味着去中心化，而账本则是记录数据的载体，因此，可将区块链理解为“去中心化的数据生态系统”。

2.1.3 发展历程

2008 年，中本聪发表比特币论文。2009 年，比特币虚拟货币平台建立。在近 9 年的时间里，比特币系统运行稳定，能够自动实现比特币发行、流通、交易

和支付。作为区块链技术的第一个应用，其成就有目共睹。

2015 年，作为基础支持技术，区块链的概念逐渐从虚拟货币中独立出来。它被转化为智能合约可编程平台，通过它，各种不同类型的资产及合约可以实现注册、确认和转移，数字资产发行流通平台的概念也由此成形。

因此，比特币可称作“区块链 1.0”，即可编程的虚拟货币。以太坊开源项目可认为是“区块链 2.0”，即智能合约平台。而区块链 3.0，目前还属于构想阶段，它超越了经济领域，可在全球范围内，实现物质资产和人力资源的自动化配布，同时能促进政府、健康、科学、文化、艺术等领域的大规模协作。

2.2 区块链的特征和应用

区块链技术具有去中心化、开放性、自制与自治性、信息不可篡改、匿名性等主要特征，因此它在转账与支付、泛金融业务、征信领域都有着广泛的应用发展空间，还可以与云计算、物联网、大数据等创新技术结合应用。

2.2.1 特征

去中心化

传统的网络交易支付，在商家和客户之间存在第三方（中心）机构来协助资金确认和结算等，但使用区块链技术，在分布式网络共识机制的作用下，交易数据可实现“自动”辨别和验证，第三方参与因此可以“下课”。

开放性

除了交易各方的私人信息被加密保护以外，区块链中的数据能够实现全网公开，所有联网设备均可以随时查看相关信息。

自制与自治性

基于共识机制等网络规则的确立，区块链网络中的所有设备能够自动、安全地进行数据记录、更新和交换，任何组织和个人都无法对此进行干预。

信息不可篡改

通过验证的数据一旦录入到区块链，便会永久性存储。除非区块链网络超过51%的设备数据被同时更改（几乎不可能），否则无法被局部篡改。

匿名性

区块链网络中的各节点可在相互非公开身份的情况下，进行数据交换。也就是说，交易双方可以在不知道对方相关信息的情况下完成支付、转账等交易。

2.2.2 应用方向

转账与支付

目前，这是区块链技术最成熟的应用方面。区块链技术能够避开繁杂的系统，节省银行间对账和审查流程，加速资金的结算速度，同时，极大降低交易手续费。

泛金融业务

区块链技术可以用于资产交易、快速审计等领域。用户双方达成交易意向，随着交易信息被添加到区块链，交易即宣告完成。这无需登记结算机构的多方数据核对，不仅提高了效率，而且也会方便日后的审计工作。

征信领域

区块链技术特点能够低成本地解决金融活动中的信任问题。信任是金融活动的根基，金融活动的监管，包括产品登记、信息披露、资金托管、征信体系建设等都是为了解决这一问题。在全社会都在积极建设征信体系的背景下，区块链技术的逐步成熟为创造了一个共信、互信的金融环境提供了绝佳的条件。

结合创新技术

区块链技术还可与云计算、物联网、大数据等创新技术结合，应用前景极为广阔。

相对传统技术，区块链能帮助金融业有效地提高效率、降低成本与风险。由于无需第三方机构参与，中间成本有效降低，而伴随着操作自动化水平的提升，结算速度更快，人力成本也大大降低。同时，区块链可以通过多重签名等技术精简服务流程，提升工作效率，而记录的信息不可篡改、可追溯，这也为监管、审计等工作提供了便利。

此外，由于交易确认、清算与结算同步完成，可能的风险大大降低。数字化交易过程还能有效解避免人工输入错误等问题。同时，由于区块链具有分布式网络和共识机制等特征，黑客网络攻击以及服务器宕机等系统风险问题也能得到有效避免。未来，在能源行业，包括居民用电、购电支付等也可以通过智能合约来自动执行。而碳交易市场也可以采用区块链技术来提高透明度、公平性，避免重复计算等问题。此外，土地确权和流转交易也可以采用该技术。

第三章 钛链概述

3.1 钛链诞生的背景

点对点价值传输网络的出现有其历史必然性，而中本聪则是加速这个历史进程的人。从上个世纪 80 年代，TCP/IP 协议的开发，到 90 年代，网页浏览器的应用和服务器的应用，一直到今天，互联网技术从不同侧面和维度改变了数据交换的模式和人类的生活。互联网技术的发展得益于基础设施的完善，从早期的信息高速公路到各种智能终端的普及，这些也构成了互联网 OSI 七层模型中，应用层无限拓展的基础。

在互联网的各种协议栈中，我们用的较多有 TCP/IP，HTTP，HTTPS，FTP，TELNET，SSH，SMTP，POP3 等网络层、传输层、应用层的协议，并且借助这些协议，我们已经比较完美地搭建了各种各样的互联网服务。但如果我们深思，我们会发现，在比特币网络出现之前，我们一直无法在互联网上在不借助于第三方的情况下，较好地进行点对点的价值的转移和传输。其实我们并不是缺少一种特定的方法，而是缺少基于信息高速公路（Information Super Highway）的价值高速公路（Value Super Highway），以及如何实现 Value Super Highway 的价值传输（VTP 协议），而比特币网络恰恰是运行于信息高速公路上面的第一个 VTP 协议。

随着互联互通技术的发展（互联网、物联网、VR/AR），人与物体、人与信息的交互方式更加多样化，更多的实体被数字化（Digitalize）和令牌化或者代币化（Tokenize）和符号化（Symbolize），一旦实体被数字化或者代币化之后，就完成了实体资产在互联网上面的映射和切分，马上面临的一个问题就是：如何点对点传输这些资产和价值？因此可以推测，随着互联网服务的进一步深入，实体和虚拟的边界也会开始模糊，点对点价值转移的需求会被凸显出来，因此在互联网上面的 Value Super Highway 和 Value Transfer Protocol 必然会出现，而比特币网络加速了这一历史进程。

3.2 钛链的发展愿景

钛链(Ti Blockchain) 将为投资者、公司和监管者建立一个可信赖的商业生态系统。投资者可以在钛链上查阅资产负债表、损益表、现金流量分析等财务文件；公司可以利用钛链来发布公司的文件，例如：白皮书、预算、代码开发、管理结

构、财务报表等都可以发布在钛链上，让感兴趣的投资者查阅。在未来版本的钛链中，文件能够通过智能合约检查审阅。

对于个人消费者来说，钛链可以作为数字保险箱使用，消费者可以上传文档在区块链上加密。除了将文档加密的人之外，其他任何人都不能解密该文档。从技术上讲，利用公钥和私钥很容易实现。用户使用公钥对文档进行加密。由于公钥/私钥的非对称属性，只有持有私钥的人才能解密文档。因此，其他任何人，包括钛链都无法解密文档。

对于业务用户来说，钛链可以用作协作空间，供用户在单个文档上协同工作。智能合约具有访问限制，可以只允许具有实际权限的用户查看文件。

钛链也支持资产证券化，资产证券化（Asset Backed Securitization，ABS）作为一种金融创新，近几年在国内外得到迅猛发展，是国内外资本市场的热搜词之一。资产证券化是以特定资产组合或特定现金流为支持，发行可交易证券的一种筹资形式，通俗来讲，资产证券化指将缺乏流动性但具有稳定收入（或可预期收入）的资产，通过在资本市场上发行证券的方式予以出售，以获取发展资金的一种筹资方式。资产证券化在一些国家运用非常普遍。目前美国一半以上的住房抵押贷款、四分之三以上的汽车贷款是靠发行资产证券提供的。资产证券化最大的优势在于，对于发行方而言，不但降低了筹资门槛，还提供了资产流通性，对于投资者而言，能够突破投资限制，降低风险，提高收益。

钛链还具备图灵完备的智能合约。通过智能合约把链上的资产自动进行管理，并且在不改变链代码的情况下灵活扩展业务功能。结合钛链提供的分布式存储服务，智能合约可以发挥更大的作用。比如：通过合约实现有偿文件存储、分享，通过合约实现机密文件有限范围传播，通过合约实现合同、文书公证，通过合约实现遗嘱等时效性文档的管理等等

3.3 钛链代币的分配

TV 总量为 2.1 亿个，具体分配比例如下：

1.6 亿释放作为市场流通，

剩余 0.5 亿作为团队所有，之后十年内将于每年 1.1 号解冻十分之一即 500 万代币作为：

开发费用： 平台的开发需要技术研发、招募人才、团队建设，足够的开发费用使得项目得以按计划推进。

咨询费用： 我们将留出一定费用来详细咨询相关领域的专业人士和机构，保

证充分的市场调研。

法律费用： 针对未来可能出现的某些突发法律事件，我们需要保留一部分应急资金。保证项目可以在正确的道路上得到长远的发展。

市场营销费用： 由于 TV 是一个非常广泛的项目，可以垂直涉足多个领域，因此 TV 需要和多领域内的多家机构和用户保持良好的关系，同时我们也会把一部分代币回馈给社区内的支持者们。

其他费用： 除以上之外的各种杂项开支。

第四章 钛链技术

4.1 钛链的技术特征

4.1.1 数据存储

钛链将提供一种 DPOS 模式的代币来支撑钛链的运行。钛链将提供智能合约+多场景应用+在线云存储功能。钛链将在智能合约的基础上，提供存储空间，在公司运营过程中，保存公司的基本信息，例如：营业执照、税务、人员以及每个月的财务报表。

文件和数据能够储存在利用分片技术构架的系列片段中，数据所有者可以单独确定文件如何分片以及碎片在网络中的位置。如果没有事先了解碎片的位置，随着网络的扩散，找到任何给定的分片的难度是指数级增长的。这意味着该文件的安全性与网络大小的平方成比例。碎片尺寸是可协商的合同参数。标准化大小劝阻侧线试图确定给定分片的内容，并且可以屏蔽通过网络的分片流。分割大型文件，如视频内容，并分发碎片节点，减少内容传递对任何节点造成的影响。云状存储系统中的所有设备对使用者来讲都是完全透明的，任何地方的任何一个经过授权的使用者都可以通过一根接入线缆与云存储连接，对云存储进行数据访问。通过各种数据备份和容灾技术及措施可以保证云存储中的数据不会丢失，保证云存储自身的安全和稳定。

钛链利用 Kademlia(简称 Kad)来为分布式存储提供数据索引和快速路由的支持。Kademlia 协议是美国纽约大学的 PetarP. Maymounkov 和 David Mazieres. 发布的一项研究结果《Kademlia: A peerto -peer information system based onthe XOR metric》。它是一种分布式哈希表（DHT）技术，不过和其他 DHT 实现技术比较，如 Chord、CAN、Pastry 等，Kad 通过独特的以异或算法（XOR）为距离度量基础，建立了一种全新的 DHT 拓扑结构，相比于其他算法，大大提高了路由查询速度。Kademlia 属于一种典型的结构化 P2P 覆盖网络(Structured P2P OverlayNetwork)，以分布式的应用层全网方式来进行信息的存储和检索是其尝试解决的主要问题。在 Kademlia 网络中，所有信息均以哈希表条目形式加以存储，这些条目被分散地存储在各个节点上，从而以全网方式构成一张巨大的分布式哈希表。我们可以形象地把这张哈希大表看成是一本字典：只要知道了信息索引的 key，我们便可以通过 Kademlia 协议来查询其所对应的 value 信息，而不

管这个 value 信息究竟是存储在哪一个节点之上。在 eMule、BitTorrent 等 P2P 文件交换系统中，Kademlia 主要充当了文件信息检索协议这一关键角色，但 Kad 网络的应用并不仅限于文件交换。

在 Kad 网络中，所有节点都被当作一颗二叉树的叶子，并且每一个节点的位置都由其 ID 值的最短前缀唯一的确定。对于任意一个节点，都可以把这颗二叉树分解为一系列连续的，不包含自己的子树。最高层的子树，由整颗树不包含自己的树的另一半组成；下一层子树由剩下部分不包含自己的一半组成；依此类推，直到分割完整颗树。

4.1.2 共识机制

目前主流的共识机制有：Pow、Pos、DPos。

Pow 工作量证明，即挖矿，通过与或运算，计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储；

优点：完全去中心化，节点自由进出；

缺点：目前 bitcoin 已经吸引全球大部分的算力，其它再用 Pow 共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长，不适合商业应用

Pos 权益证明，Pow 的一种升级共识机制；根据每个节点所占代币的比例和时间；等比例的降低挖矿难度，从而加快找随机数的速度。

优点：在一定程度上缩短了共识达成的时间

缺点：还是需要挖矿，本质上没有解决商业应用的痛点

DPos 股份授权证明机制，类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证

缺点：整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的

钛链决定使用 DPOS 共识机制。POW 算法对算力的要求很高，并且由于利益的驱动，算力最终会集中到少量的矿池中，因此并不能达到完全去中心化的目的。DPOS 则无需消耗大量的计算资源，提供快速的共识方式。投票选举代理出块的方式确保了网络不会被少数人控制（在后期代币大量分散的情况下）。这个和现实中的选举机制非常类似，并且更加公平，只要代理能够提供足够的稳定性，那么大家自然愿意选举他出块。

4.1.3 多重签名

多重签名是采用多个私钥持有人共同管理一个账户的方式。

不同于传统的加密货币主要使用明确的签名来验证交易，多重签名使用多个私钥签名的方式来对某一个账户进行操作。多重签名采用 n/m(m >= n > 0)的方式管理账户。在创建账户的 m 个私钥中，只要有 n 个私钥签名，就可以对账户进行转账等操作。这可以在很多场景下得到应用。例如：

防止单个用户的私钥丢失导致账户无法使用；

对于公司等组织集体的资产可以共同管理，防止个人或少数人私自动用；

可以应用到投票/选举等场景。

4.1.4 合约和共识机制

合约语言：我们使用类 Lua 语言作为钛链上智能合约使用的默认编程语言，支持静态编译成字节码然后在区块链网络中根据需要执行字节码。Lua 是一种图灵完备的编程语言，编译器和字节码虚拟机为在区块链中做了针对性设计和优化。

合约解释器：合约解释器是 Lua 的字节码的解释器，在区块链网络中涉及到智能合约的操作或块同步验证中，区块链节点需要时会从区块链中取出合约字节码，用 Lua 字节码解释器加载字节码，然后使用合适的参数调用需要的 API，得到的运行结果和上下文状态变化会被区块链使用。

一次对智能合约的操作，可能在很多不同节点不同时间调用不定次数，但是同一个操作在不同节点不同时间每次调用的结果和对上下文状态的改变都是一样的。智能合约的操作，因为需要不同节点的计算机资源进行执行以及占用区块链容量和网络流量，所以智能合约的操作需要扣除一定的执行花费。

4.2 钛链的安全性

DPOS 模型

安全性是我们设计钛链的主要关注点。钛链使用所谓的 "可证明安全的 DPOS 区块链协议"。该算法具有以下五个特性，使其成为一个非常安全的 DPOS 模型。

第一，该模型侧重于持久性和活跃性，这是一个健康的交易分类帐的两个正式属性。持久性是指，一旦系统的某个节点宣布某一交易为 "稳定"，其余的节点(如果被查询和如实响应) 也将报告其为稳定的。在此，稳定性将被理解为一个谓语，它将被一些安全参数 k 参数化，并影响财产持有的确定性。(例如，"超过 k 个区块那么深"。) 活跃性保证了一旦将一个真实生成的交易提供给时间足够多的网络节点，比如说 u 时间步骤，那它将变得稳定。活跃性和持久性的结合保证了一

个健康的交易分类帐，其意义是采用真实生成的交易并使其恒定。

第二，我们描述了一种新的基于 DPOS 的区块链协议。我们的协议假定参与方可以自由地创建帐户、接收并付款，而这些利权随时间推移而变化。我们利用一个非常简单的、安全的、多方实施的投票协议来达成首项选举过程中的随机性。这能够防止所谓的研磨式攻击，将我们的方法和以前的其他解决方案区分开来（之前的方案要么定义此价值基于当下的区块链或使用集体掷币这种方式引入熵[4]）。此外，我们方法的独特点在于，系统忽略了一轮又一轮的利权修改。相反，当前的利权人群被有间隔规律地记录下来，称为纪元；在每个这样间隔内，一个安全的多方计算会发生，利用区块链本身作为广播频道。具体地说，在每个纪元中，一组随机选择的利权人组成一个委员会，然后负责执行掷币协议。该协议的结果决定了下一纪元执行协议的下一个利权人的集合，以及该纪元所有首项选举的结果。

第三，我们提供了一套正式的论据，证明没有任何对手能够打破持久性和活跃性。根据一些合情推理的假设，我们的协议是安全的:

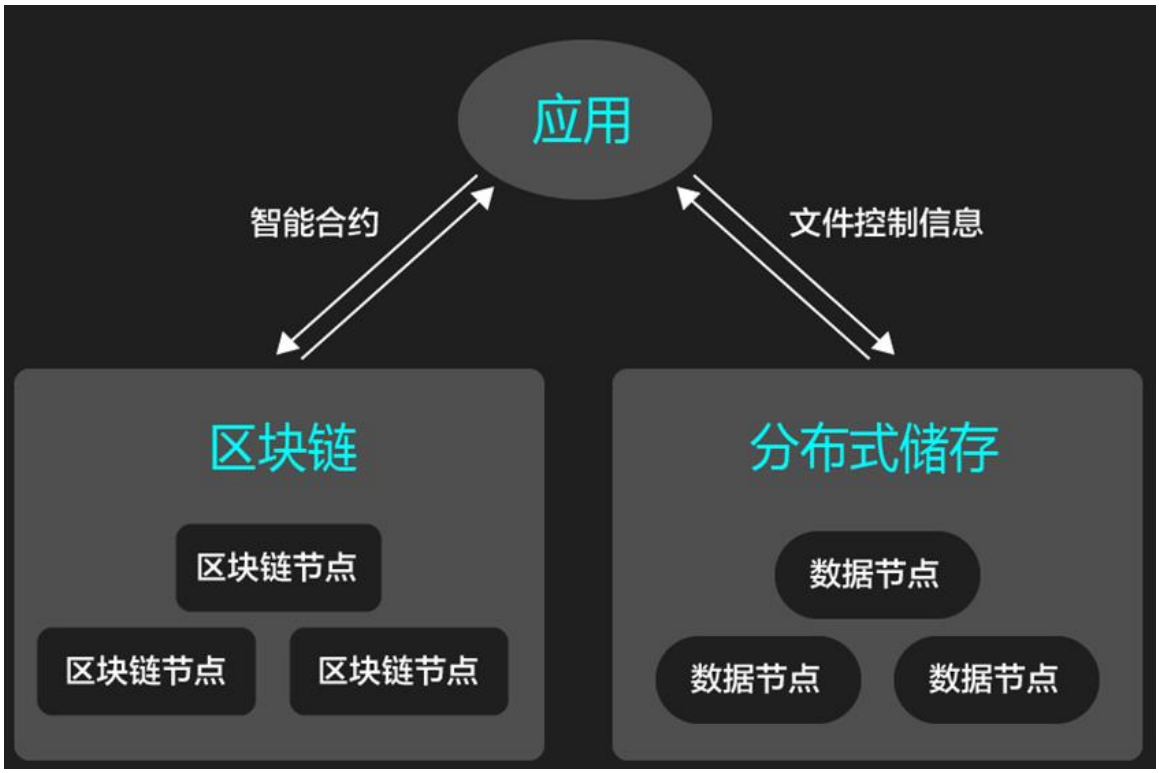
1. 网络高度同步；
2. 所选择的大多数利权人可根据需要参与每个纪元；
3. 利权在很长一段时间内不会一直处于离线状态；
4. 自适应性的损坏从属于一个小的延迟，安全参数呈线性。或者，参与者可以访问一个发件人匿名的广播频道。

第四，我们将注意力转向该议定书的激励架构。我们提出了一个新的奖励机制，激励参与者加入到被我们证明为大概是一个纳什均衡的系统中。通过这种方式，我们的设计减轻了例如区块扣押和私自挖矿这样的攻击。奖励机制背后的核心思想是为那些与协议行为一致的参与方提供积极的回报。通过这种方式，我们可以证明，在合理的假设下，某些协议执行成本是很小的，当所有参与者都是理性的时候，忠实地遵循协议达成了一种平衡。

第五，我们引入了一个股份委托机制，可以无缝地添加到我们的区块链协议中。股份委托在我们的语境下特别有用，因为我们希望我们的协议能够在一群利权者高度分散的环境中扩大规模。在这种情况下，委托机制可以让利权人委派他们的"表决权"，即参与每个纪元的首项选举协议的委员会的权利。

4.3 钛链的技术方案

4.3.1 总体架构



钛链的技术总体框架

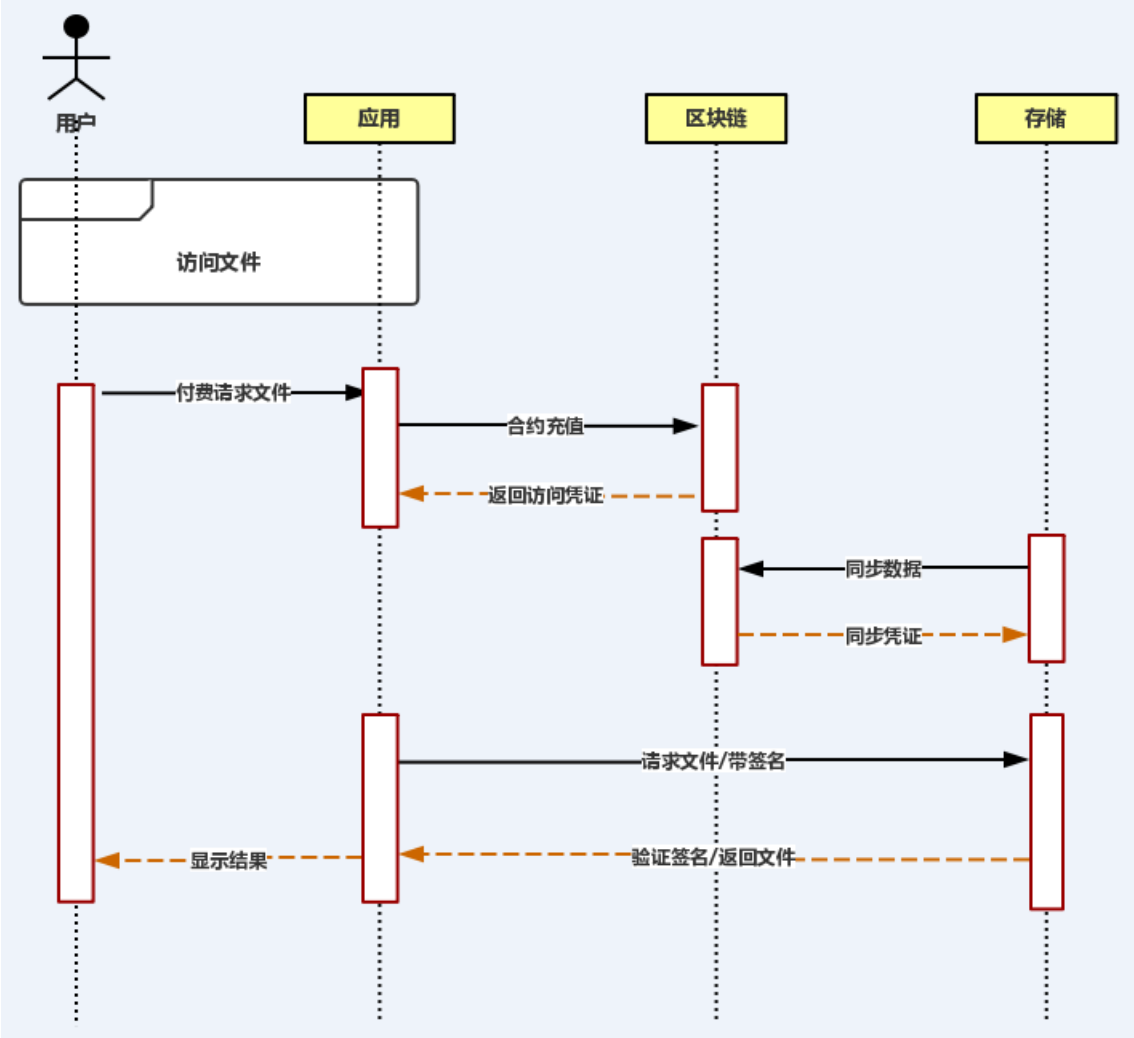
首先有两个独立的分布式网络：

区块链构成一个控制和业务网络，主要负责账本数据的维护，包括出块，转账和合约功能。

分布式存储的各个节点构成一个存储网络，主要负责存放实际数据，以及做权限控制，同时能同步区块数据。

4.3.2 主要流程

分布式存储的节点之间有简单的共识，就是接收区块链数据，根据链上数据来执行权限控制。因为数据是分块存储的，因此即使少部分节点不遵循共识，也无法访问到完整的数据。用户所有对文件的访问都需要在区块链上发起请求（具体就是调用合约，比如给合约充钱）。然后区块链会给用户的请求生成访问凭证，并记录在链上。用户拿到这个凭证之后，可以用自己的私钥进行签名，并带着这个凭证向数据节点发起请求。数据节点通过同步链上数据，可以验证这个凭证，同时通过前面可以验证这个请求属于对应的用户。然后会把数据发送给对应的用户。



钛链的主要技术流程

4.3.3 智能合约

智能合约是链提供的扩展性功能，但是为了安全起见，并不会任意的注册合约。链上会提供一些合约模板，对于文件的上传，下载提供基本的管理功能。客户端必须通过合约来对文件进行访问。

整个生态完善之后，会有更多的需求，链上也可以提供更多的合约模板，这些功能都不需要改动底层的链，只需要注册新的合约。

虚拟机

链上智能合约使用图灵完备的语言开发。语法可以通过适配支持 Lua，C#语言等。虚拟机执行的结果在链上记录，无需所有节点都运行虚拟机，减少了整个区块链网络的负载。

合约

在类似以太坊这样的系统内，合约是可以任意注册并调用的。这对于扩展性

和试验有很大的好处。但是在我们的存储系统内，我们支持任意的合约，但需要有一定的权限才能注册上链。一定程度上限制了合约的种类，但是对于整个网络的稳定，以及未来的发展方向上，是受控的。同时，对于未来发展需要新增的合约来说，它的扩展性和灵活性没有受到任何影响。

第五章 钛链的应用

5.1 私有股权等级转让

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。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，易于符合监管合法合规性要求。

钛链可应用于众筹平台、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。

5.2 资产的自由流通

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：

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；

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。

5.3 区块链云存储

云存储依赖于第三方大型存储商来传输和存储设备，如 360 云盘，百度云盘等。但是受限于非标准的客户端加密系统，非常容易受到各种安全威胁。基于数据中心的分散式存储可以有效改善这种状况，有效抵制审查，篡改和未经授权的访问。文件应该在客户端加密前进行分段，这样可以保护数据的内容，数据所有者保留对加密秘钥的完全控制，从而可以限制其他人对数据的访问。

数据所有者可以单独确定文件如何分片以及碎片在网络中的位置。如果没有事先了解碎片的位置，随着网络的扩散，找到任何给定的分片的难度是指数级增长的。这意味着该文件的安全性与网络大小的平方成比例。碎片尺寸作为可协商的合同参数。标准化大小劝阻侧线试图确定给定分片的内容，并且可以屏蔽通过网络的分片流。分割大型文件，如视频内容，系统会分发碎片节点以减少内容传递对所有节点产生的影响。云状存储系统中的所有设备对使用者而言都是完全透明的，任何地方的任何一个经过授权的使用者都可以通过一根接入线缆与云存储连接，对云存储进行数据访问。通过各种数据备份和容灾技术和措施可以保证云存储中的数据不会丢失，保证云存储自身的安全和稳定。

CDN 的基本原理是广泛采用各种缓存服务器，将这些缓存服务器分布到用户访问相对集中的地区或网络中，在用户访问网站时，利用全局负载技术将用户的访问指向距离最近的工作正常的缓存服务器上，由缓存服务器直接响应用户请求。CDN 内容分发系统、数据加密技术保证云存储中的数据不会被未授权的用户所访问，同时，通过各种数据备份和容灾技术保证云存储中的数据不会丢失，保证云存储自身的安全和稳定。钛链建立在一个分布式哈希表，这个分布式哈希表可以用来存储数据位置信息或其他信息。

5.4 智能存储

前面提到过，结合智能合约和分布式存储，我们可以做的事情很多很多。

首先是基本的分布式文件存储功能，传统的分布式存储要么需要中心化的公司来提供服务，要么就是像 p2p 网络那样免费使用。前者是一个强控制的系统，一旦中心化服务因故不再提供服务，那么所有的用户都会蒙受巨大的损失。后者则由于免费，很难激励参与者持续共享他的存储或文件。通过智能合约，可以给存储提供者/文件提供者代币的奖励。无论是提供存储，还是分享文件，都可以获得一定的收益，以此鼓励大家分享（包括存储空间和数据资源）。

有了基础的文件存储的保障，再利用智能合约，可以实现复杂的商业逻辑。比如用户可以把自己的遗嘱上链，定期向合约支付一定的费用，以保证合约内容

不公开。一旦用户确实过世，则由于发起人无法再继续支付费用，合约内容可以被任何人访问。

用户可以把一些需要存证的文档上传到钛链，定期支付费用以保证内容一直有效。在需要的时候随时取出作为证据使用。

用户可以通过合约，指定一些文档在少部分用户之间分享。或者在一定的时间之后才能分享给其他用户。

用户可以发布一些求购合约，付费的方式购买一些自己需要的资料。而持有这些重要资料的人则可以选择自由交易。这也是一个简单的价值交易市场。

其他还有更多的想象空间。目前的区块链都是基于账本的分布式数据库，很难存放大量的数据。如某些做公证业务的链，也只是把源文件的 hash 存放在一个比较小的字段内，无法复原源文件。而区块链加上无限的存储空间，带来的组合效应，足以大大提升区块链的应用场景，加速区块链应用在各个行业的落地。

第六章 团队成员

6.1 技术顾问

徐伟　区块链技术专家与创业者、数字货币早期参与者与布道者

曾任香港联交所上市公司神州数字董事长特别助理、信和云创始人。

2007 年徐先生作为美资创业公司核心成员，参与研发全球首款多媒体智能卡。

2009 年加入神州数字集团，负责神州数字新技术和新模式的研发，尤其致力于电子货币的模式探索。于 2014 年底创建电子货币领域首家网络商城，实现数字货币和虚拟货币的直接兑换，2015 年创办信和云。

申屠青春 银链科技创始人

银链科技 CEO，金链盟常务副秘书长，深圳市金标委委员，深圳大学博士，2013 年开始区块链研究，发表 20 多篇区块链相关技术文章。

赵微 OracleChain CEO

2011 年开始接触比特币，参与多项区块链社区项目(Peercoin、Factom、BitShares)，作为 BitShares 中国社区核心人员维护全球 1/23 出块节点 。在新加坡留学工作 8 年后，于 2016 年回国创业，当年获“上海万向德勤区块链编程马拉松”第二名和“梅赛德斯-奔驰科技马拉松”第二名。

刘帅成

新加坡国立大学电子与计算机工程博士，现任职于电子科技大学，主要研究方向为计算机视觉和算法理论，有多篇研究文章在国际知名期刊及会议发表。

6.2 技术团队

唐辉辉

资深软件工程师，丰富的软件开发及项目管理经验。曾主导开发多款用户百万量级产品。

董天圣

资深 C++开发工程师，曾就职于多家软件与互联网公司，精通 C/C++，熟练

使用多种语言，具有多年的软件开发和系统架构经验，善于分析和解决软件复杂环境下的各种疑难问题。

李洋渝

毕业于西南民族大学计算机专业，前诺基亚资深工程师，曾参与信息安全，云计算等多个创新项目，区块链技术爱好者。

廖韩

电信资深软件工程师，曾参与客服系统设计与研发，开源社区贡献者，区块链技术爱好者。

陈思齐

国内某知名数据恢复公司前高级算法工程师，对数据加解密、数据恢复及共识算法有深入研究，开源社区贡献者，区块链技术爱好者。

NICKO

Universitas Surabaya 信息技术管理博士；印度尼西亚籍企业家,区块链资深爱好者，PT EMRIC ASIA（亚洲教育多媒体信息研究中心）协会理事长。

Haykel（德国籍）

软件架构师专家，在德国，埃及，突尼斯多家互联网巨头企业担任技术开发专家，对以太坊、比特币等开源系统软件有深入研究，擅长多语言计算机编程有丰富的系统设计经验，负责钛链项目整体技术工作。

6.3 营销团队

尚币哥

大连理工大学工学博士，著名天使投资人，区块链行业资深专家，具有多年的营销和管理经验。

张淞皓

清华大学五道口金融学院进修，90 后创业黑马 8 年互联网从业经验 5 年数字货币和区块链的深度耕耘。

享乐才子

比特币行业多年工作经验，研究并扎根于数字货币和区块链市场，有着丰富的行业经验和敏锐的市场判断。

雷晶喜

13 年涉足比特币行业，引进区块链技术应用理念并在全国高校进行布道，14 年加入创立中币交易所，对区块链项目技术应用落地有敏锐的洞察力.15-17 年任房司令副总裁,有丰富项目实战经验和团队管理能力.在美国、澳大利亚、日本等 10 多个国家 20 多个高校范围内进行宣传与布道,推动了区块链技术应用在全球高校这个年轻群体快速发展。

叶向阳

曾就职国内顶级域名服务商新网，8 年互联网从业经验，数字货币资深爱好者。

蔡鑫

多年市场营销工作经验，具有较强的市场感知能力，能敏锐的把握市场动态及其发展方向。

张薇

澳大利亚留学归来曾任省级新闻机构记者、编辑，后转型新媒体编辑。

张帅

西南交通大学文学硕士。曾供职大学、培训机构，任日语、对外汉语教师，以及日企编辑。

参考文献

《数据结构与算法分析》:严蔚敏，清华大学出版社, 2011

《区块链:如何重新定义世界》:唐建文，吕雯，机械工业出版社

《区块链革命》, [加]唐塔普斯科特（Don Tapscott）/[加]亚力克斯·塔普斯科特(Alex Tapscott)，中信出版集团, 2016 年 9 月

《中国区块链技术和应用发展白皮书 2016》

《Qtum 白皮书》

https://en.bitcoin.it/wiki/Category: History

https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle.pdf/

https://github.com/bitcoinbook/bitcoinbook/

https://github.com/ethereum/wiki/wiki/White-Paper/

S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, https://www.bitcoin.org/ bit-coin.pdf/

N. Szabo, Smart contracts, 1994, http://szabo.best.vwh.net/smart.contracts.html/

N. Szabo, The idea of smart contracts, 1997, http://szabo.best.vwh.net/idea.html/

Bruce Schneier, Applied Cryptography (digital cash objectives are on pg. 123) Crypto and Eurocrypt conference proceedings, 1982-1994

David Johnston et al, The General Theory of Decentralized Applications, Dapps, 2015, http://github.com/DavidJonstonCEO/DecentralizedApplications/

Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, http://ethereum.org/ethreum.html

Paul Sztorc, Peer-to-Peer Oracle System and Prediction Marketplace, 2015, http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf/