TITAN中文白皮书

社区志愿者翻译版

目录


1
TITAN创世
源于海洋，归于海洋

人类文明从古到今发展了几千年，源远流长，奔腾不息。

纵观全球生命的起源、繁衍与流传，无不和一个字紧密相关，那就是“水”。窥历史以得真理，古代文明的崛起基本以河流及流域为发源地，如两河文明、尼罗河文明以及中国的长江、黄河，奔涌的河水中蕴藏着人类对这个世界孜孜不倦地追求。

而所有的河流，终将汇入海洋。如果说河流代表着人类永恒的探索，那么海洋则充当着人类探索之后智慧的容器。

生命的起源、文明的交流、文化的兴起，无一不与海洋密切相关，人类“乘船走向海洋”的冲动开启了大航海时代，破除了大陆之间闭塞，物种、经济、文化之间的碰撞造就了近五六百年的人类文明快速发展。

依赖于海洋进行商品生产和交换所形成的海洋文明，在更深层次上代表着人类崇尚自由的天性、竞争冒险的精神以及平等民主的主张。

人类的发展史与商业史，归根到底其实是一部海洋史

TITAN，中文名为泰坦，名字源自古希腊神话中曾经主宰世界的古老海神Titan，寓意着巨人与守护。中文名“泰坦”，既有泰山压顶之势，也有一马平川之平坦，预示着未来的“泰坦”必将势如破竹，引领新一轮区块链通证经济的大航海时代。

TITAN的诞生，从一开始就遵循以海洋思想为向导哲学内核，那就是自由、平等与希望。坚持以移山填海的态度不断创新的技术探索全新的商业模式，海纳百川，以开放、包容、共赢的心态创造极致的价值。水利万物而不争，TITAN致力于让每个人都有机会充分享受到人类科技文明发展的红利。

打破财富分配不均，颠覆传统经济的固化模型。就像人类目前只探索了5%的海洋一样，TITAN的使命是冲向深邃而无际的经济文明之海，将人类积累了几千年的商业文明成果以更普世、平等、多元的方式展现给大众，与大家共同探索科技与商业结合之美。

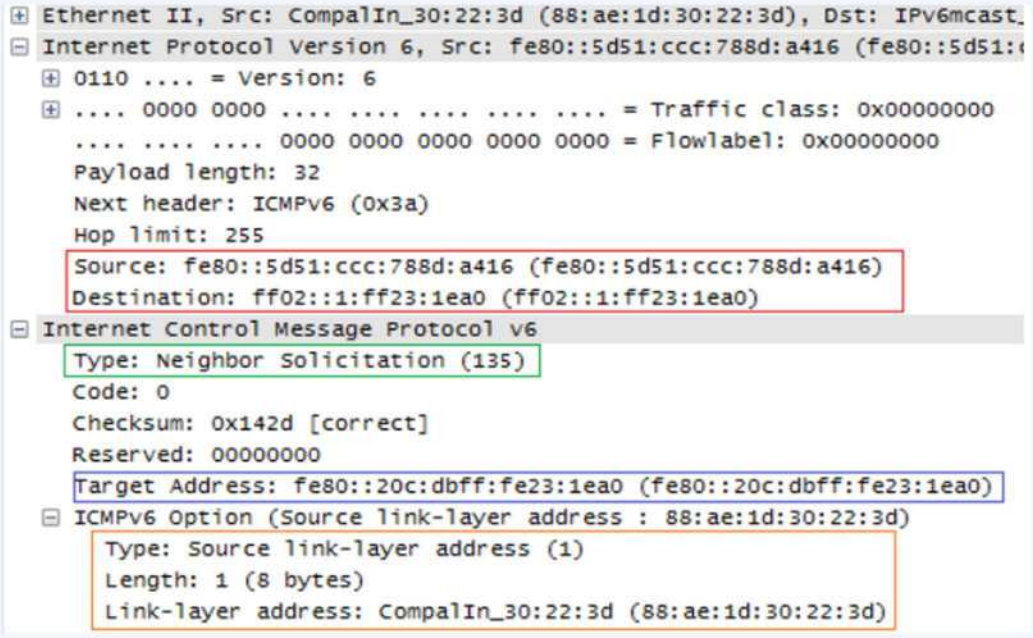
TITAN，作为全球通证经济5.0、产业区块链的领航者，将在区块链大航海时代建立一个无边界链上生态帝国，开启全球数字经济新浪潮。


2
TITAN共识机制
背负使命，破除陈规

2.1、目前行业存在的问题

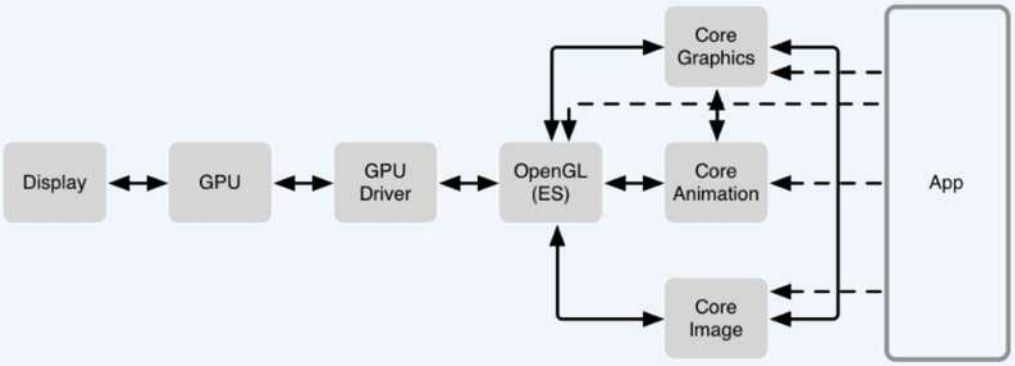
可以将TITAN区块链技术理解为一种互联网协议，即在网络中传递和管理信息的一些格式和规则。正如人与人之间的语言交流，因为我们学习了相同的词汇和语法，这才使交流沟通成为可能。在互联网的世界里同样需要这样的规范，在这种规范之下的信息才能在互联网中自由传递，信息接收方才能确保收到正确的信息内容。

目前的互联网协议中最基础的协议就是TCP/IP协议，又名网络通信协议，是国际互联网络的基础，由网络层的IP协议和传输层的TCP协议组成。TCP/IP定义了电子设备如何连入因特网，以及数据如何在它们之间传输的标准。互联网上的每个节点都执行这个协议，赋予信息相同的格式，使信息能自由地在互联网上点对点的传输。基础协议好比是互联网的地基，而应用程序是盖在上面的房子。2020年中国提出“新基建”政策，区块链位列其中。TITAN区块链既是一种互联网的“地基”，同时也是“新基建”中的重要组成部分，所有基于大数据、人工智能以及去中心化的应用都可以构建在其中，组成完整的闭合循环且可持续的通证经济生态。



IPv6协议代码

看似简单的理念，构筑了互联网的世界的基石，使信息全球化变成了现实。随着IP协议已深深进入网络领域中（设备，软件堆栈，应用程序，服务，工程知识，业务模型，甚至是国家政策），考虑使用非IP协议似乎令人生畏。但是，尽管IP协议在过去40年来，一直是非常成功的互联网协议。但随着技术和时间的不断演进，我们有理由相信不会一直使用。尽管用另一种协议替换IP协议随之带来实施方面的挑战，但并不一定意味着改变应用程序和用户使用网络的方式。换句话说，网络的外观和使用功能上和现在相差无几，但是它将变得更加精简和高效。



软件堆栈

众所周知目前全球IPv4协议地址已经枯竭，而其接任者也就是IPv6协议发展较为缓慢并且已经影响到互联网发展。没有足够的地址池让许多家庭用户和企业只能共用地址，而企业如果要申请地址的话有时候可能需要斥巨资购买。

我们处在一个IoT物联网、AI人工智能、5G通讯的时代背景下，这些新兴技术的背后都是以大数据为基础，以互联网为驱动力，构建一个快速发展的社会。这是一个数据大爆发的时代，数据就是财富。中心化的数据存储已经被当今的巨头垄断，分布式存储才是下一个万亿级蓝海市场。

在这样的背景下，备受瞩目的IPFS项目横空出世。以分布式账本、去中心化信任、时间戳、非对称加密和智能化合约五大技术为特征的区块链，和以区块链技术为基础的IPFS协议被寄予厚望，试图改变互联网的底层技术，解决互联网

所面临的发展困境。但遗憾的是，IPFS项目由于各种原因，主网上线一再推迟，测试网络也是漏洞百出，严重影响了前期投资IPFS矿机的机构和矿工的投资收益，变现难成为不争的事实。随着时间的推迟，越是早期进入的投资人，就越有可能蒙受了巨大的经济损失。

TITAN的出现，将在底层构建一个全新的互联网协议，解决现有IP协议固有的许多缺点，升级互联网及区块链底层协议。TITAN将全新的理念和技术传播给全球区块链支持者和信仰者，通过TITAN的价值，联合全球互联网及区块链开发者、商业应用者以及普通区块链用户，形成庞大的联盟平台，抱团发展。

TITAN链万物互联

2.2、现有区块链系统的六大问题

2.2.1、串行处理的局限

随着区块链技术更广泛地被应用，其线性处理压力日趋面临超过其设计容量的风险，进而导致了现在的网络性能瓶颈。目前的区块链系统面临着亟须提高吞吐能力的多重考验，有时甚至必须付出牺牲交易效率的代价。例如，比特币手续费随着交易量的增加正在急剧升高，并且有大量的交易需要等待很久才能被确认；以太坊在代币发售时也时常经历大面积的拥堵。在传统的IT架构里，现代优化技术例如分库、分表或改用分布式架构等策略都被证明可以极大提高系统性能。

另一方面，并行任务处理的概念还没有被应用于提高区块链效率。当一个区块包含大量交易数据和复杂智能合约的时候，串行处理压力已逼近区块铸造和验证的效率极限。

2.2.2、数据复杂度和冗余

目前的状况是一个通用区块链系统需要被用来处理不同

的业务情景。通用区块链系统的缺点在于过度复杂的智能合约和共识机制、缺少对于特定业务情景的定制解决方案，以及数据冗余。

2.2.3、协议升级困难

尽管区块链技术发展十分迅速，但它目前还是处于初级阶段。重大的改进和更新还会在未来陆续出现。这些更新对于区块链的进化和保持与时俱进是至关重要的。区块链生态系统里利益相关方的多样性导致在缺乏有效治理机制的情况下通常很难达成一致，这也造成了现在许多协议升级被搁置的情况。以比特币系统为例，近几年许多新特性的引入都经历了社区中长期的争执。

2.2.4、区块膨胀

一个区块链系统越成功，其维护成本也就越高。现在运行一个比特币全节点需要超过130G的硬盘空间，以太坊更是超过了180G，且这种情况远期也不会得到改善。随着更多的人接纳了区块链并且开始进行更多的交易，区块的存储空间会加速膨胀，维护成本也会日渐高昂。对此，我们必须采取行动来缓解这个恶性循环。

2.2.5、低效的点对点通信

现有的区块链主要是通过广播网络来进行通信的，且对于P2P网络的支持既低效又不安全。举例来说，如果某种数据只针对一个用户群，那么这些数据就应该只在有限的节点里传播，而不是被广播到所有节点。

2.2.6、亟须突破的跨链通信

现有区块链技术领域内已有一些在区块链系统间处理相关业务逻辑的尝试，然而数据的跨链交互一直是业界棘手的技术难题。现有的跨链通信包括中心化的实现方案和基于HTLC的方案。中心化的方案背离区块链的本质，而且面临授信困难、单点故障、单点性能瓶颈等问题，应用场景较为局限。基于HTLC的方案则只能在处理资产交换等一些特定应用模式时发挥作用，同时，该方案对参与通信的两条链的协议和共识机制有严格的要求，实现方案复杂。无论哪一种实现方案，在区块链系统间协议的差异适配及数据标准交互格式定义这两个核心议题上都有待突破性的技术进展。

2.3、PoST超时空证明与PoS股权证明

区块链的核心技术是共识机制。目前比较常用的共识机制有PoW（Proof-of-Work，工作量证明）、PoS（Proof-of-Stake，权益证明）、DPoS（Delegated-Proof-of-Stake，委托权益证明）、PoC（Proof-of-Contribution，贡献证明）。

基于GPU和FPGA挖矿的众多数字货币例如ETH、GRIN等，由于GPU昂贵的价格，始终难以成为主流大众的选择，而PoS方式的数字货币，并不能承担锚定现实世界资产的重任，也难以将更多的资金引入数字货币领域。因此区块链5.0希望，让矿工和新入场者通过硬盘挖矿的方式获得数字货币，其目的是让更多新的用户通过更低的门槛参与挖矿获得数字货币，并由此进入数字货币市场。PoW的最主要问题就是耗电量十分巨大。

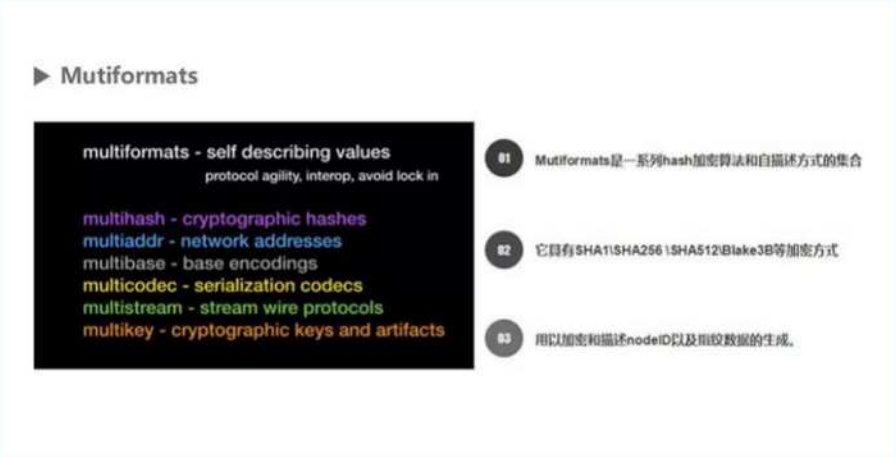
这意味着比特币每年相当于排放了2000吨的二氧化碳，这对于地球的环境、气候以及人类文明未来的可持续发展都是不可逆及不可忽视的破坏。我们从另一种隐喻的角度来看，比特币P2P网络基本上就是一个分布式的超级人工智能，它正在把宇宙所有的能量（也就是物质）都变成比特币。比特币的PoW共识机制没有窍门。SHA-256算法除了暴

力破解以外别无他法。这意味着CPU要不停地运算，冷却风扇需要不停运转来冷却超热、超载的处理器。

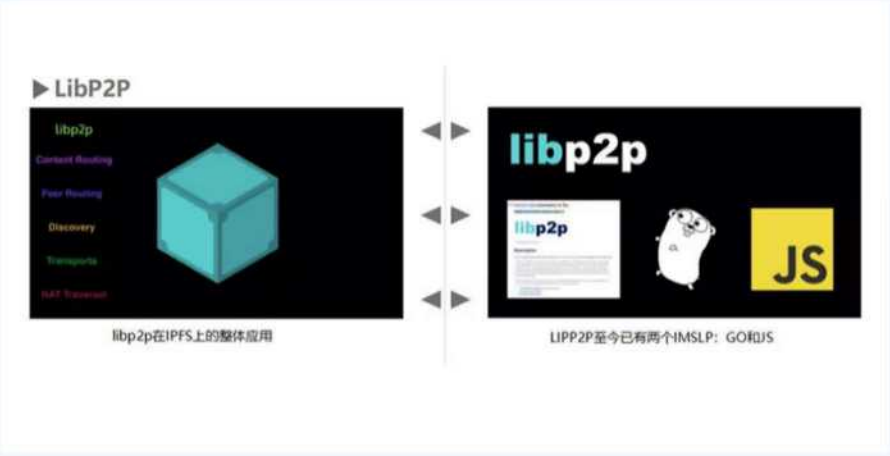
区块链5.0时代，共识机制朝着不浪费资源、适当考虑安全性、提高吞吐量和并发数方向发展。

在TITAN中有两种证明，PoST超时空证明（IPFS的升级）+PoS股权证明，用以反映矿工的即时状态及其已创造的价值。

PoST超时空证明，是Filecoin项目采用的共识机制的升级版，使用该数据量作为算力大小的证明。IPFS的团队在开发时，采用高度模块集成化的方式，像搭积木一样去开发整个项目。协议实验室团队2015年创立，到17年的时间里都在做IPLD、LibP2P、Multiformats这三个模块的开发，它们服务于IPFS底层。



Mutiformats是一系列hash加密算法和自描述方式（从值上就可以知道值是如何生成）的集合，它具有SHA1\SHA256\SHA512\Blake3B等6种主流的加密方式，用以加密和描述nodeID以及指纹数据的生成。



libp2p是一个模块化的、点对点网络的库。它具有强大的浏览器支持，能够完全在浏览器上，或通过WebSOCkets和WebRTC等协议工作，被认为是IPFS核心中的核心。它面对Quic和Tor传输协议、GO、JavaScript和Rust语言、Polkadot

等各式各样的传输层协议以及复杂的网络设备，都可以帮助开发者迅速建立一个可用P2P网络层，快速且节约成本，这也是为什么IPFS技术被众多区块链项目青睐的缘由。

PoS（Proof of Stake），在PoW机制中，由于想要找到符合条件的nonce往往需要花费大量的电力和时间成本，因此，为了使每个Block更快被生成，PoS机制去掉了寻找nonce这一过程，继而采用以下更快速的算法：

$$H(H(Bprev),A,t) \leq balance(A)m$$

H依然为某个哈希函数；t为UTC时间戳；Bprev指的是上一个区块；balance(A)代表账户A的账户的余额；m依然代表某个定义的数。等式左边，唯一可以不断调整的参数是t，等式右边m是某个固定的实数，因此，当balance(A)越大，找到合理t的概率越大。网络中，普遍对于t的范围有所限制，如可以尝试的时间戳不能超过标准时间戳1小时，也就说，一个节点可以尝试7200次，来找到一个符合条件的t，如果找不到即可放弃。因此，在PoS中，一个账户的余额越多，在同等算力下，就越容易发现下一个区块。

基于PoS机制的检索分发证明在PoST共识的前提下，采用了PoS机制作为分发的共识机制，完美避开了设备效率与资源配置的直接矛盾，极大改善了区块链5.0时代的挖矿模式。PoS算法具体运作过程是由利益相关者（stakeholders），即由通证的持有者、矿工进行投票，通过选举程序选出TITAN超级节点（TITAN Super Node），然后区块的超级节点们会被确定性随机打散（pseudo-randomly），在规定的时间内TITAN超级节点可以选择是否出块。TITAN依据PoS最长链原则（longest-chain rule），也就是说在相同时间内，拥有最多矿工拥护的那条链会比其他链生长得更快，也就是说如果存在两条链，则生长速度快的这条链，最后一定会成长为最长链。传统的PoS算法和PoW一样都是依循最长链原则，在这种原则下，只要在一个时刻任何人生产出了一个合理的最长链，那么剩余的所有节点都会切换到这条链上。PoS相对于PoC的优点，好处就是其达成共识的效率被大大提升了，同时所能提供的不可逆保证也是相似的。因为不再是由全网达成共识，而是由被选举出来的生产者之间达成共识，所以效率得到了极大地提升，这对于应用而言是比较重要的，因为对于类似高频的场景和小额的情况，用户难以忍受长时间的等待。TITAN选择了PoS，倾向于选择了速度和效率。分发

证明PoDT(Proof-of-Distribution)是一种新型的证明方式。这是一种适当减少了实现难度的方案，无须构建复杂机制防止攻击难题，只需证明数据分发的频次和使用度，即可与挖矿系统结合，形成完整方案。

同样作为储存共识的cPoC来说，cPoC条件容量证明有它自身的优势，即体现在挖矿更节能，更经济、更环保。基于PoC共识机制采用硬盘挖矿，与传统ASIC化矿机相比，具有硬盘设备保值高、可回收，对电力资源能耗需求低，噪声小的特点，从而降低矿工挖矿成本，能耗可控，收益可观；降低挖矿参与门槛。由于硬盘设备天生具备抗ASIC化特点，对传统因PoW共识机制，所造算力集中化、垄断化的痛点形成冲击，并以更轻、更经济、更环保的区块链精神优化去中心化与可信化的价值回归，为“全民挖矿”的愿景提供了更多的可能性与可行性。但是从另外一个点来说，PoC生态所存储的宝藏，即挖矿出来的哈希值，并不能够被任何实体用在任何实际的地方。也就是说，在IPFS侧，矿工存储数据，通过发起挑战，来让矿工证明对数据的真实存储的过程，就是PoST存储证明机制。用户们在挖矿时存储的是有价值的数据，而不是像PoC一样，存储无意义随机数据。

这样我们能够利用全球庞大的空闲的硬盘存储空间，建立起基于区块链的数据存储、检索、交换、分享环境，进而为大数据、AI、隐私计算、多方计算等提供数据源。

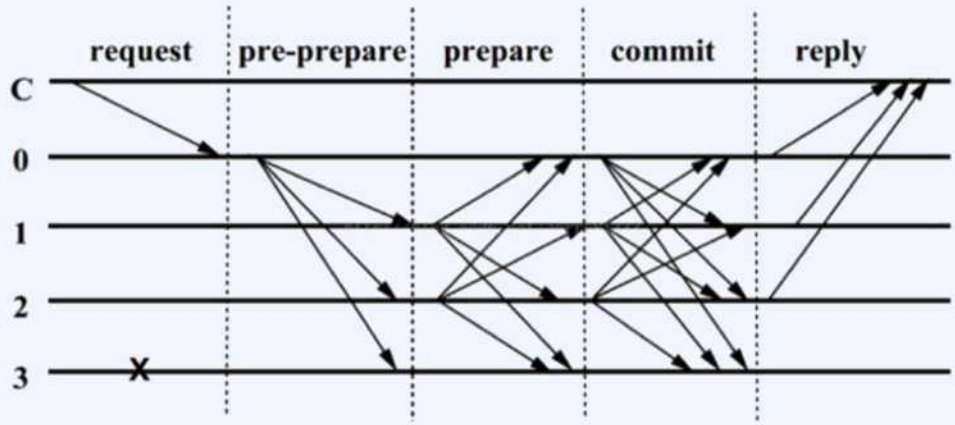
一方面，当存储市场发展有了良好的激励循环体系，比如我将一份有价值的File交给矿工存储，矿工不仅可以获取经济激励，还可以在我交换、分享数据的过程中获取授权下载的佣金。另一方面，为整个数据存储市场提供了高效率的数据存储、检索、交换、分享的解决方案。

TITAN相信未来的区块链一定是以落地应用为主，为价值服务，如果只创新不做应用也只是过眼云烟，PoST存储证明机制下的挖矿红利这些都将得到验证。

2.4、容错机制的优化选择

1、拜占庭容错算法

基于拜占庭将军问题，PBFT算法一致性的确保主要分为这三个阶段：预准备（pre-prepare）、准备(prepare)和确认(commit)。流程如下图所示：

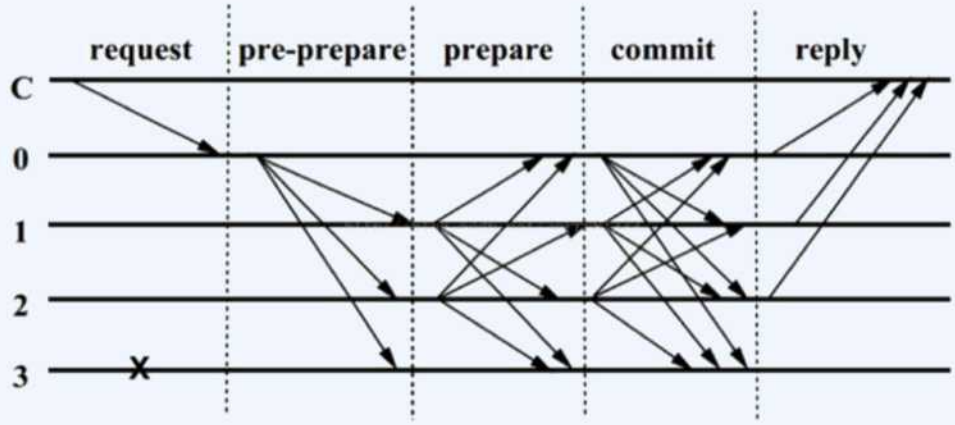


我们首先解释一下上面各个符号表达的意思：

C表示客户端；

0，1，2，3表示4个节点；

0在这里为主节点，1，2，3为从节点；（注意，这里其他节点也可以作为主节点，若0发生错误只能由服务器监测。如果服务器在一段时间内不能完成客户端的请求，则会触发视图更换协议，将其他节点换为主节点）3为故障节点；



下面我们结合上图，详细说一下PBFT的步骤：

Request：请求端C发送请求到主节点，这里是0节点；

Pre-Prepare：节点0收到C的请求后进行广播，扩散至123；

Prepare：123节点收到后记录并再次广播，1->023，2->013，3因为宕机无法广播；（这一步是为了防止主节点给不同从节点发送不同的请求）；

Commit：0123节点在Prepare阶段，若收到超过一定数量（2F，实际使用中，F为可以容忍的拜占庭节点个数）的相同请求，则进入Commit阶段，广播Commit请求；

Reply：0123节点在Commit阶段，若其中有一个收到超过一定数量（2F+1）的相同请求，则对C进行反馈；

根据上述流程，在N ≥ 3F + 1的情况下一致性是可能解决，N为总计算技术，F为有问题的计算机总数。

下面我们来举一个PBFT（实用拜占庭容错算法）的例子来进行说明。

我们假设N=4，F=1，即有四个节点，其中有一个节点是坏的，我们还使用上面的图，即节点3为故障节点。

1.请求端C发送请求到0节点，假设这里请求内容为“1”；

2.节点0收到C的请求后进行广播，将请求内容“1”扩散至节点123；

3.节点1、2、3收到后内容“1”后，再次广播，节点1->023，节点2->013，节点3因为宕机无法广播；

4.节点0，1，2会在上一阶段分别收到三个请求内容“1”，均超过了2个，于是节点0、1、2会分别广播请求内容“1”；

5.此时如果一个节点（0，1，2中任意一个）收到3即（2+1）条commit消息，即对C进行反馈。

2、PoS股权算法

PoS算法类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。

简单来说，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。你每被清空365币龄，你将会从区块中获得0.05个币的利息(假定利息可理解为年利率5%)，那么在这个案例中，利息 = 3000 * 5% / 365 = 0.41个币，这个对于用户是个利好：持币有利息。

然而，一旦币的权益被用于签名一个区块，则币龄将清为零，这样必须等待至少30日才能签署另一区块。同时，为防止非常老或非常大的节点控制区块链，寻找下一区块的最大概率在90天后达到最大值，这一过程保护了网络，并随着时间逐渐生成新的代币而无需消耗大量的计算能力。

单纯的PoS或拜占庭容错都有它自身需要满足的条件

证据算法允许验证者通过发送一种或多种类型的签名消息对块进行“投票”，并指定两种规则：

最终条件 - 确定给定哈希何时可以被认定为最终的规则。

削减条件 - 决定何时可以认为某个验证者无可置疑的行为不当（例如同时投票多个冲突块）的规则。 如果验证者触发这些规则之一，则其整个存款将被删除。

为了说明削减条件可以采取的不同形式，我们将给出两个削减条件的例子（下文中，“2/3的所有确认者”是“存入硬

币加权的所有确认者的2/3”的简写，对于其他分数和百分比依此类推）。在这些例子中，“PREPARE”和“COMMIT”应该被理解为简单地指代验证者可以发送的两种类型的消息。

1、如果MESSAGES包含相同view的形式为["COMMIT", HASH1, view]和["COMMIT", HASH2, view]形式的消息，但由同一个验证器签名的HASH1和HASH2不同，则验证器被削减。

2、如果MESSAGES包含形式为["COMMIT", HASH, view1]，则除非view1 = -1，或者对于某些特定view2还存在形式为["PREPARE", HASH, view1, view2]的消息，其中view2 < view1，由所有验证器的2/3签名，然后使提交的验证器被削减。

对于一组合适的削减条件，有两个重要的要求：

负责任的安全 - 如果相冲突的HASH1和HASH2（即HASH1和HASH2不同，并且两者都不是另一方的后代）最终确定，那么至少有1/3的验证者违反了相应的削减条件。

似是而非的不确定性 - 除非所有验证人中至少有1/3违反了一些相应条件，否则存在一组验证人可以产生的一组消息，最终确定一些价值。

如果我们有一套满足这两个属性的削减条件，那么我们可以激励参与者发送消息，并开始从经济终结中受益。

2.5、TITAN激励机制

区块链行业目前仍处于相当早期的阶段，现有的落地应用主要分为以下两种方向：与区块链技术非常匹配的新商业模式，以及对已有的中心化业务进行改造，实现区块链赋能。

市场对于区块链应用的落地太过急切，并且希望一步到位实现区块链的所有技术特性，现状是底层去中心化的公有链对于各行业不能通用，智能合约太过简单不能支撑复杂的商业场景，现在已有很多联盟链形式的底层平台致力于解决效率、扩展性、智能合约复杂度等问题，但应用的落地应当是和底层技术不断磨合互相促进成长的过程。

底层平台欠缺、性能不完善、兼容性不足导致区块链应用层发展仍然属于早期。绝大部分与区块链结合的商业场景仍然处于探索期，金融领域天然适配区块链的特性使得支付清算已经率先进入高速发展期，而社交、溯源等还处于市场启动期，伴随底层平台的快速发展，大量的垂直行业应用将会快速度过低谷，迎来高速发展。

1、去中心化构建信任的解决手段

区块链提供了在很多没有强中心价值交换网络里面的一

种基于去中心化构建的信任解决手段，并由此衍生出区别于经典互联网的诸多新商业模式，例如跨境支付、供应链金融、存证、溯源等所有场景其实是基于它们的业务场景和业务逻辑跟区块链技术有天然高度的匹配性，需要自信任、高效的去中心化的跨主体协作、数据的可追溯和不可篡改。

$$\int \frac{dx}{\cos^2 x} = \int \sec^2 x dx = tgx + C$$

$$\int \frac{dx}{\sin^2 x} = \int \csc^2 x dx = -ctgx + C$$

在探索激励机制的过程中，我们分析了PoW，DPoS等多种模型，在结合拉格朗日中值定理时，发现了TTC闭环生态激励模型的预演前提。

$$f(b) - f(a) = f'(\xi)(b - a)$$

2、对中心化业务改造

现有的一些商业场景中，中心化业务运行良好，使用区

块链不是在改造以前一些比较糟糕的基础设施，它提供了另外一种赋能，即通证的经济激励机制。

在TITAN的网络中，TTC作为TITAN区块链系统中的通证，可作为经济激励机制来衡量原来场景中的行为、信息、价值、数据等，TTC可迅速流通、有明确的价格，并且还会有升值的潜力，这就会对用户形成一个强大的激励。

目前，能够落地的应用多为基于区块链的不可篡改、智能合约、激励、工作量证明其中一个或者多个技术特性去解决业务的具体痛点，能够做到多个技术叠加的更是其中的佼佼者，但如何深刻理解这些技术特性并可以很好地与业务进行融合也是目前很多项目遇到的最大困难。

2.6、实现TITAN系统的主要途径

2.6.1、性能提升

TITAN的核心原则是使用成熟高效的技术来解决实际的技术问题。我们更关注如何提供一个可以稳定运行商业应用的可靠配置，而不是“优化”区块链的概念。

以下是一些如今已经被探索过的想法：

大部分的区块链分片（sharding）方案都是通过把一个单独的共识划分成许多子共识。基本上来说，就是作为整体的共识被分开，变成一些更容易被攻击的子共识群。人们也可以通过增加随机性来复杂化路由路径，但是这也限制了挖矿节点的专门化。

随着更多的矿池使用专门的记账系统取代PoW的挖矿节点，这些节点的数量急剧减少。这些矿池能保证挖矿效率和交易的即时广播、减缓区块链的分叉，也同时保证系统的稳定。借鉴IT行业的经验，矿池已经抛弃了官方的软件，转而通过负载均衡和并行运行智能合约来聚集算力，并且在全球部署节点来提高广播的效率。但是，矿池的效率还是受到矿池里用到的技术差别的限制，也受到每个节点等同的设计以

及协议本身的限制。所以升级一个节点并不能带来整个网络的提升。

TITAN的逻辑是这样的：

TITAN里的节点根据不同的职能分类，使运行在集群上提供标准服务的节点开源，并通过PoS来达成主链上的共识。被委托的挖矿节点能够在最大限度上保护侧链，并且还能分享主链的强共识。这个方法增加了每个节点的压力，但是效率会随着更多的侧链的加入而得到提高，因为被委托的挖矿节点能够在集群上运行。侧链之间是相互独立的，所以每多一条侧链都会增加整个系统的效率，每一条侧链的效率也因为并行处理而得到提高。

2.6.2、资源隔离

为保护智能合约免受不必要的干扰，维持其在区块链上的稳定运行，TITAN抛弃了“一链治所有”的方案，自己设计了一个可以保证每个合约都正常运行的公链。

由于历史原因，现有的区块链治理结构通常在初始时都没有被很好地定义，导致当有重大功能更新或者Bug导致系统错误时问题更加突出。例如，比特币在扩展性问题上停滞

了两年，最终还是选择了分叉；以太坊社区和基金会之间关于Dao事故的分歧，导致了ETC的诞生。

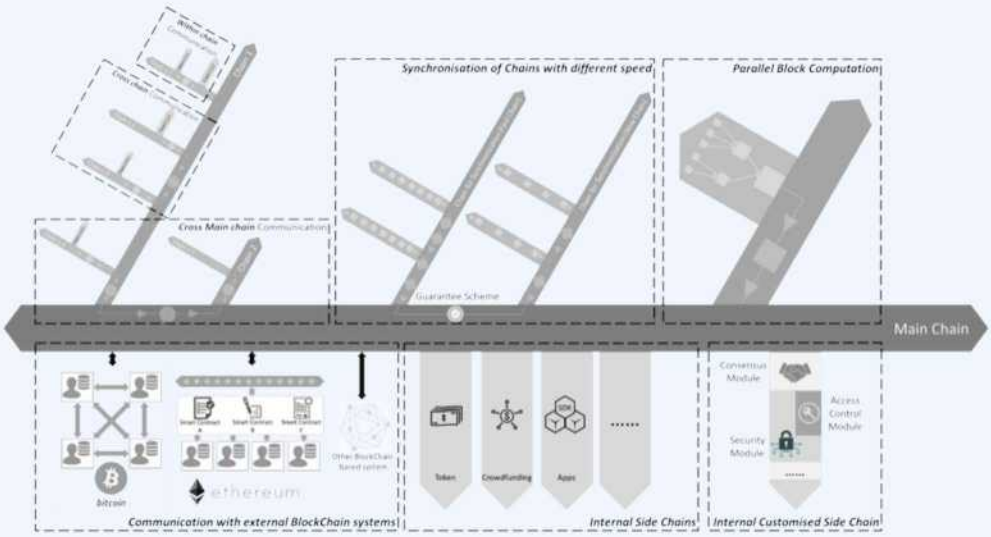
TITAN的愿景是实现像AWS一样的计算平台，任何业务都不会被其他业务干扰，如期货市场的交易不会被黑色星期五的流量所干扰。然而，这种看起来不可能的干扰在区块链世界里却很常见。因此我们认为，正是区块链的初始设计妨碍了区块链技术在现实场景中的运用。


3
TITAN技术架构

TITAN的主链是一个采取TITAS架构的分布式账本。TITAN通过对数据的协调使系统中的信息和信任更好的在利益相关者之间分发和分配。加密经济内部激励层，以便不同的利益相关者和用户基于经济激励来确保生态的有效运行。通过数字资产整合，使生态融入数字商品经济。同时采取由TITAN改进的智能合约编程语言，和数据库虚拟机。TITAN公链凭借优化全网最优算力获得了极高的可扩展性与极快的处理速度，目前在测试环境下真实可用的TPS为20万＋。在TITAN的区块链生态当中，gas消耗极低，底层架构优越于行业所有公链，更适用于商业应用。

一个新型的可跨生态的智能合约架构

在进行数据的价值管理存储发现的过程中，TITAN使用一个TTC架构的分布式账本和一个具有数据库功能的虚拟机，任何人都可以编写数据库以及发布智能合约和DApp，由此他们可以制定自己项目中的数据所有权、数据交易格式和数据价值转换等规则。



TITAN系统整体架构

例如，在一个实验项目中可能需要多个实验室共同完成，每个实验室都可以把有用的实验数据共享在同一个数据库中，并制定贡献数据者可获得的通证数量，而数据使用者需支付通证，数据使用者所得的分析结果又可以重新被共享

以获得通证。当协作者们为通证的经济价值作出了相互认同的协议，通证则可作为数据价值的承载体，只有当合适的人真正使用了数据本身，并且定义了存储载体和转移的规则，数据价值才能真正体现。

一个点对点的网络拓扑

相当于颠覆HTTP所代表的分布关系，TITAN所升级的网络拓扑具有内容可寻址的特点，通过文件内容生成唯一的哈希标识，一定程度上节约了空间开销的成本。

核心网络层

基于libp2p优化而来的LibT2T可以支持任意传输层协议。NAT技术能让TITAN网络层中的设备共用同一个外网IP，这样可以使整个网络内部的设备及固件达到更高的信息交互速率及可信度。

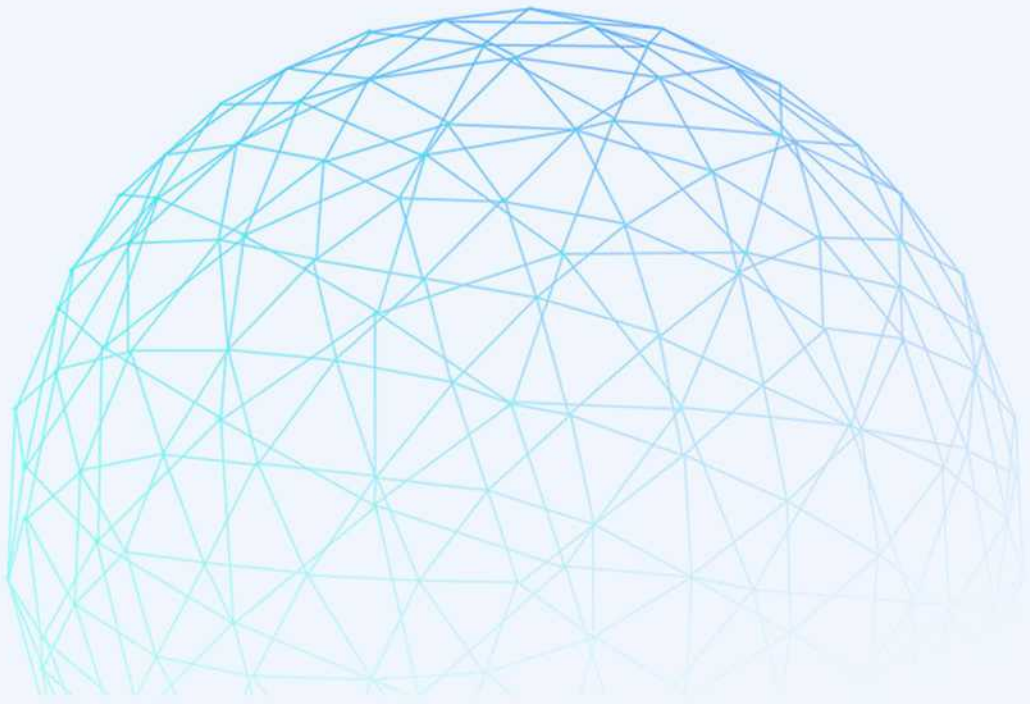
对等节点身份信息的生成以及路由规则是通过协议生成制定，其实质是构建了一个分布式松散Hash表，简称THT，每个加入这个THT网络的人都要生成自己的身份信息，然后才能通过这个身份信息去负责存储这个网络里的资源信息和其他成员的联系信息。

TITAN底层架构的关键逻辑通过智能合约实现，核心数据也使用智能合约写入区块链，内容数据存储在内部节点当中。

区块链的上层是TITAN Node节点，用于运行去中心化爬虫、调用外部服务、进行复杂的运算等功能。TITAN Node直接和区块链连接，调用智能合约完成关键操作和数据写入及验证。比如，TITAN Node可以和“原本”服务进行连接，完成高精度的存在证明以及电子取证等功能并保证其在法律上的有效性。TITAN Node还会提供Restful API供所有客户端调

用，并提供分布式数据缓存、索引等功能以加速客户端访问。

在 TITAN Node的上层是用户直接使用的客户端，包括TITAN的Android和iOS手机客户端、PC浏览器插件等。除了TITAN的客户端以外，任何机构或者个人（三方App、公众号、平台网站和企业内部系统等）都可以通过与TITAN Node的连接，加入TITAN生态圈中。



3.1、TITAN共识机制

3.1.1、独创PoST超时空证明+PoS股权证明

泰坦链TITAN采用PoST超时空证明+PoS股权证明共识机制，创新性地将这两者结合，同时兼顾整体性能和共识效率。TITAN链固定每0.5秒产生一个新的区块，每个区块中产生0.3个TITAN通证积分TTC。经过TITAN链主网最新版本的运行测压证明，TITAN链交易能力达到均值1,000,000+TPS和同步运行侧链时的峰值7,500,000+TPS。

TITAN的PoST超时空证明，是Filecoin项目采用的共识机制的升级版，使用该数据量作为算力大小的证明。TITAN通过引入一个非线性证明函数，在给定块上定义了一小部分活动时间和空闲时间，从而解决了当前模型中存在的一些主要缺陷。空闲时间被定义为不再支持共识分布而开始降低共识分布的年龄比例。这种量化的闲置时间对于每个股权来说都是独一无二的，因为它降低了满足证明的概率，并通过共识影响到可获得的到期权益的比例。

基于PoS股权证明机制的检索分发证明TTC在PoST共识的前提下，采用了PoS机制作为分发的共识机制。在这套体系

中，所有参与者都成为TITAN链的管理员和参与着，完美避开了设备效率与资源配置的直接矛盾，极大改善了区块链5.0时代的挖矿模式。TITAN的PoS股权证明机制不需要消耗电力来进行运算，而是通过抵押TTC来获得打包区块的权利，当一笔交易发生时，系统会对打包区块和验证区块的节点来进行奖励，奖励来源是增发或者解锁的TTC。

PoST超时空证明机制+PoS股权证明机制，解决了目前区块链行业存在的交易效率低下、安全性不高等问题，同时结合零知识证明技术，TITAN尽可能解决行业中亟待解决的区块链“不可能三角”难题。

3.1.2、共识机制选取方式

权益证明必须采用某种方法定义任意区块链中的下一合法区块，依据账户Staking来选择将导致中心化，例如单个首富成员可能会拥有长久的优势。为此，TITAN设计了独创的PoST+PoS方法来选择下一合法区块。

在PoST中，我们考虑两种不同的“可花费”资源：一种是CPU工作（即，如先前的工作量证明中所述），另一种是“时空”：在指定的时间段内填充指定数量的存储（在此期间不能

用于其他任何用途）；我们认为时空是工作的“正确”基于空间的模拟（它是随时间推移CPU功率的度量），像工作一样，时空可直接转换为成本。我们基于不可压缩的工作量证明（PoW）构建PoST；工作量证明的一种变体，我们可以降低工作量证明本身所需的存储空间。我们基于标准的“哈希原像”PoW和存储单个哈希输出的一部分，给出了两种简单的候选构造。我们的协议和证明与现有的空间证明使用的技术非常不同，并且易于实现。（我们注意到，尽管结构极其简单，但证明其安全性并非易事。）

不同的参数制度。与现有的PoS构造相比，我们认为初始化和证明阶段之间的时间为数周而不是数分钟（例如，这可以启用一种加密货币，其中“矿工”可以在数周内完全关闭电源），可以认为我们的构造是针对不同参数体制的现有PoS机制的补充一。一方面，我们的PoST协议的证明阶段效率较低（它需要访问整个存储，所以证明可能要花几分钟而不是秒，这与基于搅动的构造的情况一样。这意味着它不太适合两次验证之间时间空隙太短的情况。另一方面，与现有的PoS结构不同，我们初始化阶段的计算难度可以独立于空间量进行调整，因此可以使用它来证明长期（例如几周或几个月）的合理存储大小。在此参数范围内，花费几分钟的证明是合理的。

单位和符号

我们的基本度量单位是CPU吞吐量，空间和时间。这些可以对应于任意现实世界的单位（例如，每分钟230次哈希计算，分别为1GB和1分钟）。我们根据基本概念定义其余的单元：

• **工作：CPUxtime**；消耗的CPU工作量单位（例如230个哈希计算）。

• **Spacetime：spacextime**；在一个时间单位内“保留”的空间单位（并且在该时间段内无法用于其他任何空间）。

在我们的定义中，尤其是在谈论理性对手的行为时，我们希望衡量证明者所花费的总成本，而与所耗费的资源类型无关。为此，我们需要指定工作时间与时空之间的转换率：

实际成本我们将y定义为按实际价格计算的每时空成本比率。也就是说，在现实世界中，一个时空单位的成本高达y个工作单位（y的值可能会随时间变化，并且取决于存储空间和处理能力的相对实际成本）。

我们定义相应的成本函数，即PoST的实际成本为工作单位中的标准化成本：使用\a\时空单位和x个工作单位的PoST的实际成本为c = y\a\ + x。

PoST方案包含两个阶段，每个阶段都是证明方P=（Pinit，Pexec）与证明方之间的交互协议。验证者V=（Vinit，Vexec）.（为简便起见，当从上下文中清除init和exec下标时，我们将其删除。）双方都可以访问随机预言机H（工作）。

初始化阶段双方都收到一个id字符串id∈{0，1} *作为输入。在此阶段结束时，证明者和验证者输出状态字符串（σP∈{0，1} *和σV∈{0，1}）

$$(\sigma P, \sigma V) \leftarrow DPH\ (work)\ init\ (id), VH\ (work)\ init\ (id)E$$

执行阶段双方都从初始化阶段接收ID及其对应的状态。在最后阶段，验证者接受或拒绝（outV∈{0，1}，其中1解释为“接受”）。证明者没有输出：

$$(\cdot, outV) \leftarrow DPH\ (work)\ exec\ (id, \sigma P), VH\ (work)\ exec(id, \sigma V)E$$

执行阶段可以重复多次，而无需重新运行初始化阶段。这很关键因为初始化阶段需要工作，而执行阶段却非常节能。因此，尽管单PoST的执行与工作量证明相比没有任何优势，每次执行的摊销工作可以被任意降低。

系统初始化工作（w）在初始化中执行的预期工作相同。这应该是“可调和的”，以确保存储输出仍然是合理的选择，而不是重新计算时空工作成本比率的变化会导致初始化。

如果初始化阶段的成本太低，则违规者可以比守规者更低成本地生成区块，方法是在初始化之后删除所有数据，然后在证明阶段之前重新运行初始化。在这种情况下，对手不会在阶段之间存储任何数据，因此不会支付任何时空成本。我们对此进行形式化并将其作为理性攻击。请注意，这是一种通用攻击，也适用于PoS方案一因此它们还必须对初始化所需的工作有一个下限。

$$\Pr\Big[out_V = 1 : (\sigma_P, \sigma_V) \leftarrow \big\langle P_{\text{init}}^{H^{(\text{work})}}(id), V_{\text{init}}^{H^{(\text{work})}}(id)\big\rangle, \\ (\cdot, out_V) \leftarrow \big\langle P_{\text{exec}}^{H^{(\text{work})}}(id, \sigma_P), V_{\text{exec}}^{H^{(\text{work})}}(id, \sigma_V)\big\rangle\Big] \geq \eta$$

从量化的结果来看，PoST与PoS的结合将会为TITAN链带来更高的加密性质、全链检索效率以及出块方式播报等优势。

3.1.3、PoST+PoS机制相对于单纯的PoW及PoS的优势

相比于传统老一代公链单纯的PoW或者单纯的PoS机制，TITAN混合式PoST超时空证明机制+PoS股权证明机制存在不可比拟的优势。

首先，在能源消耗层面，PoS股权证明机制不需要消耗电力来进行运算，相比老一代PoW，可以大大节约能源消耗。

PoS为使用博弈论机制的技术打开了全新的一扇大门，以便有效地阻止中心化垄断的形成，且如果这些技术成型，也能够阻止对网络造成损害的行为(比如PoW中的自私挖矿)。在基于PoS的公链（例如以太坊即将推出的Casper实现）中，一组验证者轮流对下一个区块进行提议和投票，而且每个验证者投票权重取决于其押金(即权益)大小。

相比于PoW机制，TITAN的PoS股权证明机制的显著优势包括更高的安全性，更快的交易处理速度，减少的中心化风险以及更加节能。

而另一方面，PoST超时空证明又可以弥补单纯PoS机制的不足。首先PoST同样不消耗能源，其次PoST与PoS的区别主要在于：PoS是通过币龄数挖矿的方式来达成共识，PoST改良了这一点，PoST将有效存储在全网中的占比作为获得出块权的依据，抵押的代币仅是为了避免存储矿工作恶，对于通证的流动性损伤不大。

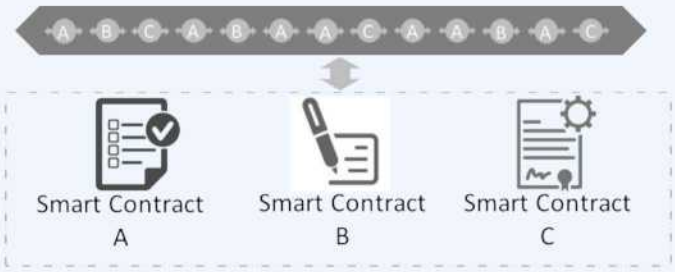
3.2、TITAN侧链技术

侧链协议本质上是一种跨区块链解决方案，能够最大化地对公链进行扩容，使得链上生态在蓬勃发展的道路上越走越强。通过这种解决方案，可以实现数字资产从第一个区块链到第二个区块链的转移，又可以在稍后的时间点从第二个区块链安全返回到第一个区块链。其中第一个区块链通常被称为主区块链或者主链，每二个区块链则被称为侧链。TITAN侧链实现的技术基础是双向锚定，通过双向锚定技术，可以实现暂时的将数字资产在主链中锁定，同时将等价的数字资产在侧链中释放，同样当等价的数字资产在侧链中被锁定的时候，主链的数字资产也可以被释放。

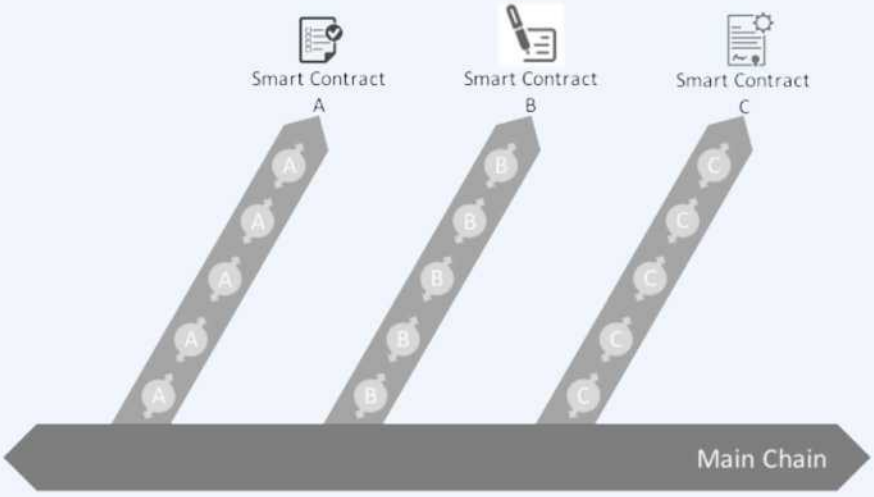
通过TITAN侧链，矿工及各节点转账用户可以在TITAN主链的基础上，进行交易隐私保护技术、智能合约等新功能的添加，同时可以让用户访问大量的新型服务，并且对现有主链的工作并不造成影响。另外，侧链也提供了一种更安全的协议升级方式，使得TITAN生态中的应用，例如链上交易系统、TITAN商城、TITAN泛文娱板块能够更高效的独立运作，同时通过TITAN通证TTC的价值承载贯穿于主链与各个侧链当中。

3.2.1、一链一合约

不同于传统的“所有合约一条链”，TITAN提出“一链一合约”架构。如下图所示，每条链都专门处理一种类型的交易，解决一种类型的业务问题。这就让整个架构和数据变得更简单，更加契合业务需求。通过向TITAN增加侧链，TITAN拓展了更多的功能，同时还能保持易于维护的架构。



多个合约一条链



一链一合约

区块链的复杂数据结构

3.2.2、侧链动态索引

TITAN是一个动态的系统，所有的侧链都依附于主链。主链包含了系统边界的索引（记录挂载的侧链）。链与链之间通过主链的Merkle Tree以及外部消息的输入验证来交互，而不是直接交互，这样就可以很容易的在TITAN系统里添加或者删除侧链。

3.2.3、树形侧链延展

TITAN定义了一个“主侧链架构”。理论上来说，任何侧链都可以与其下的一些子链连接，成为那个部分的“主链”。这造就了系统里的分级结构，使得TITAN同时具有了横向与纵向延展的能力。这个想法和数据库架构里的分库和分表类似。每个分表能执行专门的功能，并且当单表太大到难以管理时，它就会被进一步被分成多个表。在TITAN里，这对应的是侧链。

3.2.4、侧链索引系统

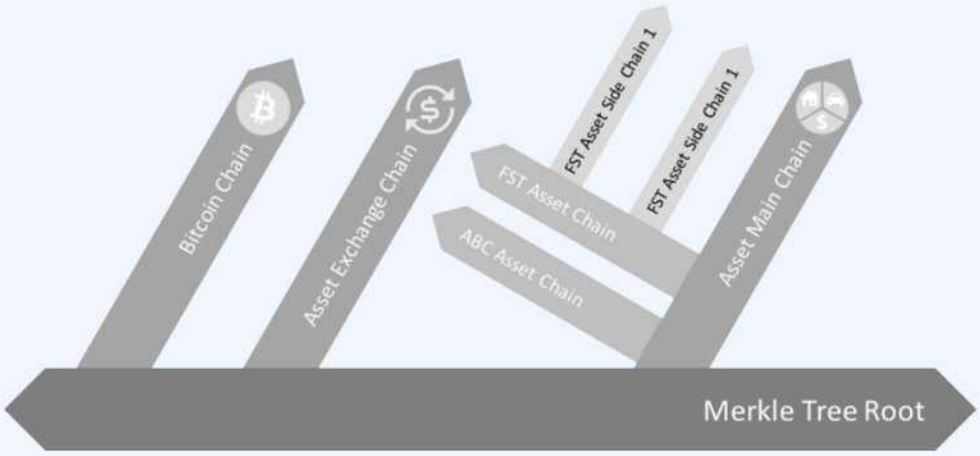
侧链索引系统连接TITAN生态系统里所有的链。TITAN索引两类链：

重要的外部链，用来扩充TITAN的边界，如比特币、以太坊；

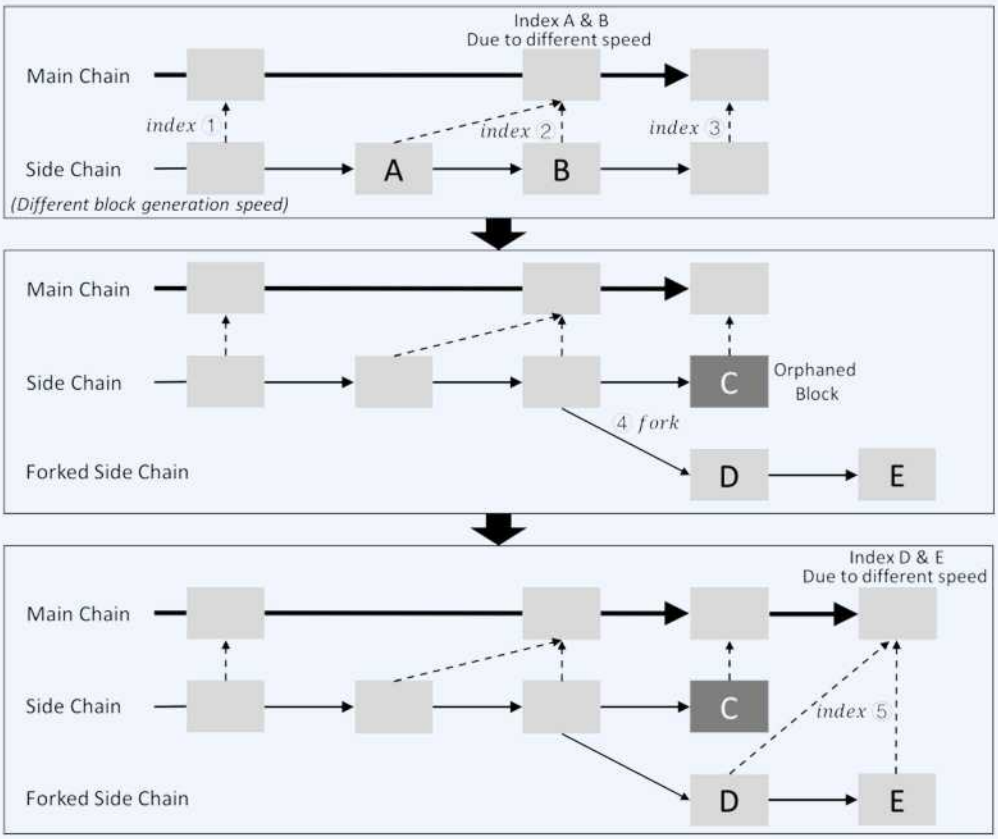
在TITANOS下运行的内部侧链，使用TITAN代币为整个TITAN系统做出贡献。

主链节点从侧链读取信息并生成一个Merkle Tree；

新区块的区块头记录Merkle Tree Root，如果我们想要验证BTC第1000个区块的交易TX1，我们只需要通过主链的Merkle Tree Root，证明BTC第1000个块的Merkle Tree Root的存在，并基于这个（BTC第1000个块的）Merkle Tree Root和附加的消息证明TX1的存在。这个方法也同样被用于其他的链比如以太坊，只要区块是基于Merkle Tree的形式组织的。



还有一个关键的问题是侧链被主链索引的时机。如果主链频繁地索引一条很可能分叉的侧链，就是在索引孤块上白费力气。所以我们为每一条链基于它自己的特点提出不同的索引策略，并且这些可以在系统里预先定义好。对类似比特币的系统进行索引可以在区块形成一分钟之后进行。因为数据证明区块形成一分钟之后基本可以被确认不是孤块。在TITAN里，如果一条侧链选择与主链一起联合挖矿，则该侧链可被实时索引，因为主侧链被同样一群矿工维护。



索引时机

3.3、TITAN链跨链技术

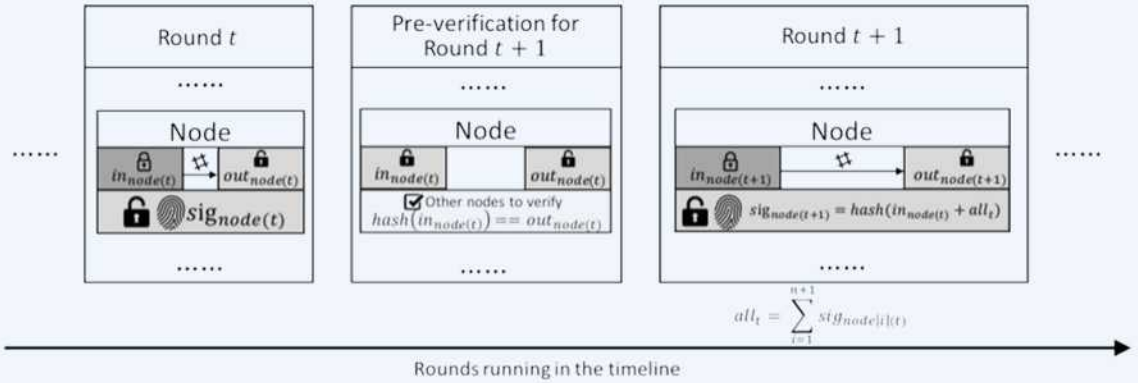
基于TITAN模块仓库实现的区块链（生态内的区块链），可以通过模块选择的方式，添加跨链模块，实现底层上和TITAN的互通。相对于以太坊和比特币等老一代公链，遵循协议跟TITAN不同的公有链，需要通过特殊的机制实现协议的转换，将其他公有链的协议和TITAN跨链协议做适配，达到统一协议通讯的目的。

所有区块链都只和TITAN主网通信，交易的验证由TITAN主网负责，各平行链信任TITAN主网的验证结果。各区块链上的资产，可以通过跨链的方式，流通到TITAN生态中任意一条接受外链资产转入的链上，且仅需花费很小的代价。

预验证：（t+1）轮里一个节点开始产生区块之前，它在t轮里的状态需要先被验证。在t+1轮里，innode(t)已经被公布了，outnode(t)也能被随时查询。所以要验证节点在t轮的状态，其他节点可以验证--outnode(t), hash(innode(t)

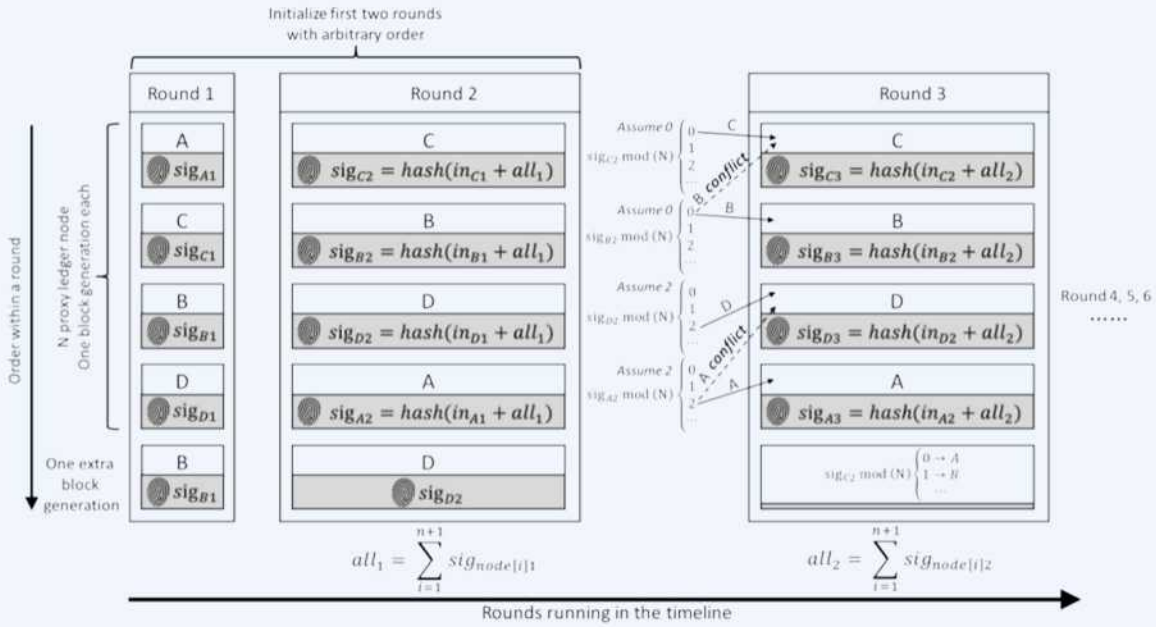
signode(t+1) = hash(innode(t) + allt 其中n+1，allt =Signode[i](t)计算的。这里， node[i](t) 代表这个节点处理t轮里的第i个交易。

考虑冲突的情况，即结果指向非空缺的位置，我们就把节点指向下一个空缺的位置。如果该节点和第n个位置冲突了，我们就从头开始寻找可用的地址。



预验证

signode[0](t) 是由以下决定的：(1)前一个(t-1)轮的所有签名；(2)它自己在(t-1)轮的in值；(3)哪一个节点生成多余的区块。所以它只能在(t-1)轮结束后才能得到。另外，因为它需要前一轮所有的签名，而且in值也是有每个节点单独输入的，所以不可能控制这个顺序。总的来说，我们创造了一个依靠外界输入的随机系统。基于每一轮里任何一个节点都不知道其他所有节点的输入的假设，可以认定没有人能控制排序。



前3轮计算顺序细节

如果一个节点在t轮不能产生区块，它也不能在这轮输入in值。这种情况下，前一轮的in值将会被使用。还有一种不太会常发生的情况，那就是所有的挖矿节点是被选举出来的可靠节点。即使这种情况发生了，上面提到的策略也足够很好地应付这种情况。

每一个节点只有特定的T秒来处理交易。在当前网络环境下，T=4是合理的值，意味着每个节点只有4秒来处理交易以及将结果提交到网络上。任何没能在4秒内提交结果的委托节点，都被认为放弃了这个区块。如果一个节点连续两次失败，就会给这个节点一个W小时的窗口期（W=2N ,N是失败的次数）。

3.4、TITAN链分片技术

TITAN在以太坊分片技术上作出了较大的改良，主要的不同点在于TITAN链上的区块垂直堆叠，因此能够运行不同的应用。TITAN技术的第一个落地的应用会是一个兼容各条区块链的去中心化交易所。TITAN与以太坊的分片相比，一个显著的优势在于，在每出一个块之前，全网的状态被创建一个副本。分片技术导致，分片与分片之间的交易会出现问题，而TITAN链上的所有交易都共享同一个全球状态，从而杜绝了这一问题的发生。由于每个区块都由不同的验证人进行验证，因此每层区块都会产生共识，TITAN公链的扩展性的唯一限制只是当前可工作的已质押代币的验证人的数量。

TITAN采用分片技术作为公链底层可拓展性和易用程度的解决方案。TITAN的设计原则主要是围绕易用性、高拓展、稳定性而展开的。

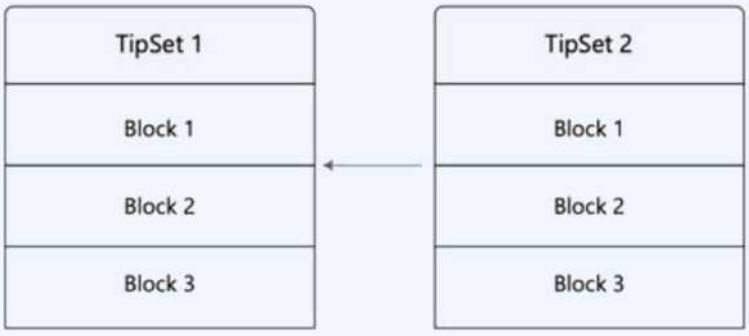
易用性是让每个系统的组件设计都尽可能简单，对实用性和易于理解性方面进行优化，不在基础协议里添加多余的负担；可扩展性只要有经济上的合理性，TITAN就没有上限的限制，以支持全球通用型的Web应用程序运行；稳定性是

提供一个稳定的基础层，并且能尽可能地隐蔽底层技术的实现细节，让开发人员在开发过程中能使用自己熟悉的语言和模式，且在运行过程中平台能保证其安全性。

实现一个基于分片技术的区块链就像在原本只有一个收费站的高速公路上增加N多个个收费口。它会极大地提高车辆通行速度，分片技术带来巨大的差异，并能显著提高区块链的交易速度。

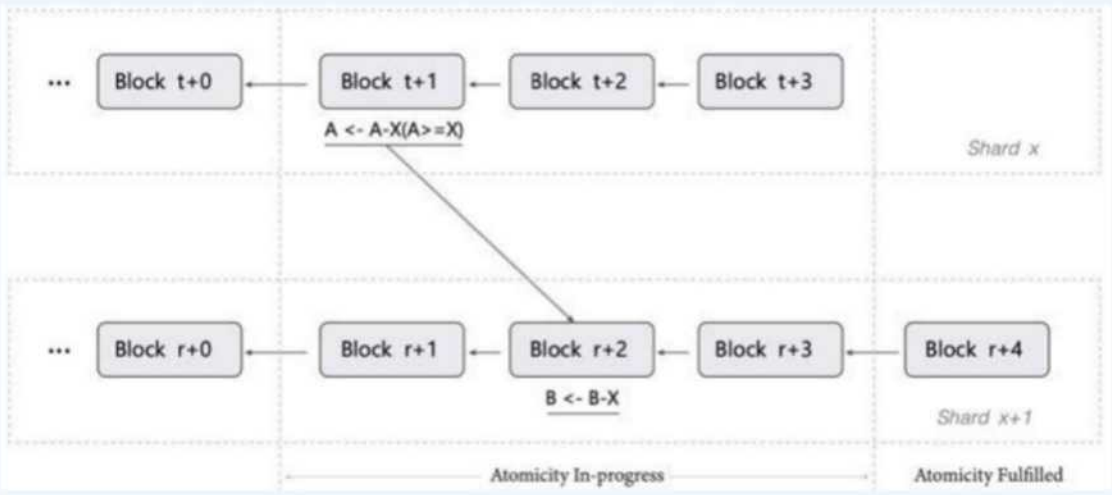
与目前大多数主流的采用信标链加分片链的结构不同，TITAN采用单一链式结构。整条链由TipSet依照顺序排列组成一个链式结构。TipSet由Block组成，一条分片对应一个Block。每个TipSet将会包含多个Block信息。TipSet不包含交易信息，交易存储在Block中，网络中所有的交易都被划分到各个分片当中并被出块人打包进Block。

在PBFT的协议中，由于考虑到TITAN的验证者最多可以达到10万+，让这么多验证者每个块都参与验证，显然是不现实的。为此，我们和以太坊2.0一样，使用了一个确定性小工



具，利用证明确定区块。为了降低系统复杂度，我们使用的确定性工具在任何情况下都将不影响分叉选择规则，而只是引入额外的惩罚条件。这样一来，一旦一个区块被确定性工具确定下来，就不可能出现分叉，除非占总权益极大百分比的权益都被罚没了。TITAN Protocol的确定性小工具参考了Solana的PoH设计。

TITAN采用的是PoS共识机制，意味着出块人和验证人把一定数量的代币锁定一段时间。在TITAN中并不强制每个收集人和验证人都是独立的实体，但每个收集人和验证人都需要单独质押。所有的收集人和验证人共同构建单一的区块链，我们称之为Mstternode Chain，即主链。主链的账户被分到各个分片中。每个收集人和验证人在任何时候都只在本地下载对应某个分片的状态子集，且只处理和验证影响这部分状态的交易。



3.5、TITAN链存储技术

3.5.1、TITAN在数据存储价值中发现的设计目标

一个实现数据价值管理存储的去中心化系统。TITAN通过对IPFS的升级改造，实现对文件的加密机制和授权机制，利用独有的“加密后去重”技术保证加密后不增加系统存储成本，并增加了算力加成机制，这样不仅可以用于保存个人或者企业非公开的文件，从而真正的取代http协议，而且从IPFS的“存储+网络”升级成了“存储+加密+计算+网络”，从而具备了完整的基础架构能力，不管是应用场景还是商业模式上都具备了无限的发展空间。

3.5.2、TITAN提出的技术解决方案

TITAN经过多方分析后提出的以下几个技术和创新的解决方案，来实现TITAN的设计目标。

在进行数据的价值管理存储发现的过程中，TITAN使用一个TTC架构的分布式账本和一个具有数据库功能的虚拟机，任何人都可以编写数据库以及发布智能合约和DApp，由

此他们可以制定自己项目中的数据所有权、数据交易格式和数据价值转换等规则。

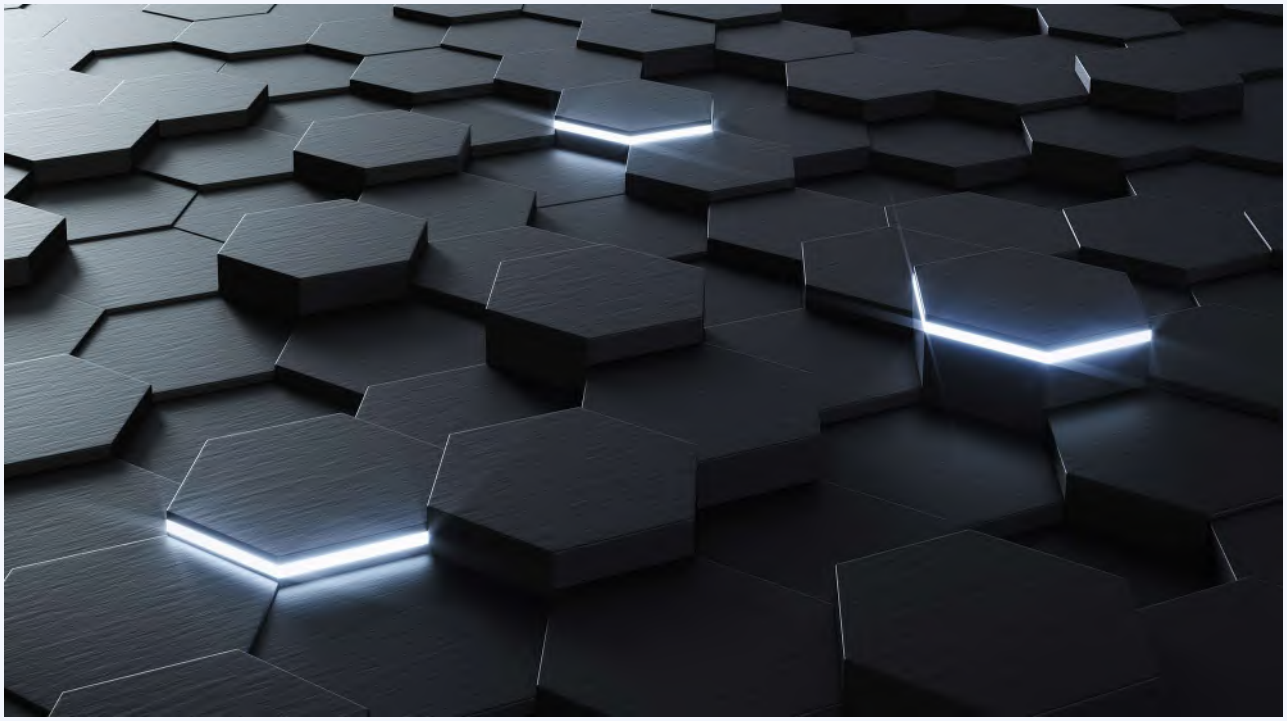
例如，在一个实验项目中可能需要多个实验室共同完成，每个实验室都可以把有用的实验数据共享在同一个数据库中，并制定贡献数据者可获得的通证数量，而数据使用者需支付通证，数据使用者所得的分析结果又可以重新被共享以获得通证。当协作者们为通证的经济价值作出了相互认同的协议，通证则可作为数据价值的承载体，只有当合适的人真正使用了数据本身，并且定义了存储载体和转移的规则，数据价值才能真正体现。

3.5.3、跨分片交易

TITAN网络允许将交易从一个分片发送到另一个分片。由于网络使用异步模型,验证和处理首先在发送方分片中进行,然后在接收方分片中进行。当交易被调度时,TITAN链通过创建和提出新的区块(TITAN链上创建的区块),并公证从发送分片中来的区块确保它的安全。

区块包含有关每个分片区快的以下信息:发送方分片ID、接收方分片ID和分片区块哈希。

在跨分片交易中,接收分片从区块中获取交易的相关分片区块的哈希(在分片中创建的区块,而不是TITAN链中创建的区块哈希），请求发送分片中的分片区块，分析交易列表，请求缺少交易（如果有),然后最终在本地分片中执行相同的分片区块,并将此分片区块发送到元链中成为区块。一旦这一点被TITAN链公证,交易就最终完成。



3.6、TITAN链上信息及资产加密

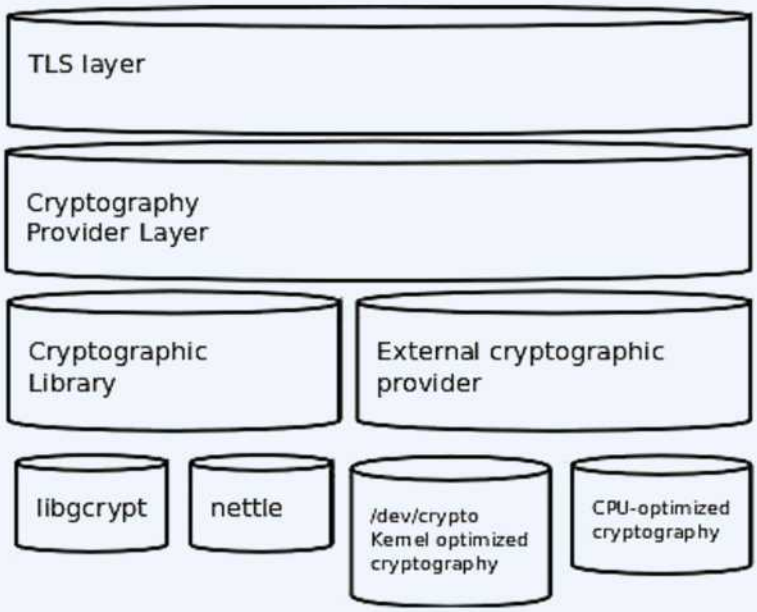
TITAN致力于向区块链的发展贡献自己的力量，保障用户在TITAN主网链上的资产及信息安全，为此TITAN独创TISS解决方案，该方案安全性高，可快速安装和签署，并且在特殊情况下方便找回，对很多公司的机密文件来讲，起着重要的作用。

TITAN为了实现TISS投入了许多开发资源。TISS作为一种用于分布式密钥生成和签名的加密协议，它可在基于ECDSA的区块链兼容并重用，包括TITAN链，比特币和以太坊网络等。

任何区块链的最底层基础都是加密层。这本质上是区块链的DNA,因为这一层是交易和区块验证条件的设计层。

该网络利用Schnorr方案进行交易签名和验证；使用Schnorr签名占用的数据空间更小。Schnorr方案不仅简单高效,还采用了经过充分研究和久经实战的算法。这种创建数字签名的方法已经存在于各种加密货币中,也有人建议将其集成到比特币网络中。

由于区块验证需要来自多个验证者的聚合签名,因此需要多重签名方案。这样，网络将使用Boneh-lynn-shacham(BLS)多重签名方案进行区块签名和验证。



TISS的主要步骤：

1、Vault初始化：该步骤将建立一个端到端加密的通信渠道，对参与各方进行初始化。例如需要三方参与。

2、密钥生成：在本步骤中，我们需要确定签名人数的阈值策略并共享私钥。例如，若采用2/3政策，这意味着私钥将被分割成3个私钥碎片，并且3个参与者中的任何2个都可以签署交易。

3、签名：从各自的私钥份额中生成数字签名，且私钥不会泄露

4、Vault重组：如果有人丢失了他保管部分的私钥，则有必要重新分享私钥。重组会生成新的密钥碎片，同时之前的碎片将失效。

TITAN生态

五位一体，生生不息

TITAN生态：五位一体，生生不息

2008年，一位叫作中本聪的匿名极客发布比特币白皮书，自从以比特币为代表的区块链技术横空出世。比特币自诞生至今，短短十余年时间，其价值最高暴涨将近2000万倍，由此可见区块链技术在未来巨大的发展潜力。

区块链技术具有去中心化、公开透明、全民参与、生态激励、可溯源等优势，这些特点无论是对于目前传统金融行业还是传统互联网行业，都能带来颠覆式的改变和提升。

正如比特币一样，TITAN也是由全球一批精通区块链技术的数字极客MCobian、Sadlife等发起，他们对区块链与传统互联网和商业结合有着狂热的追求和信仰，深信技术的价值在于探索、储存并赋能人类所有的文明活动，便利化人们生活。

基于此，通过融合区块链技术，TITAN独创了新通证文娱、全行业直播、普惠新金融、全新消费挖矿商城及一键发币五位一体生态体系，打造全球通证经济5.0帝国版图。

4.1、新通证文娱

社群经济网络

信息质量评价维度复杂，在信息质量的概念的量化和评估方法上仍然存在非常多的困难。从实践角度，社会化推荐是比算法推荐更加高效的方式。除了引入多维度的Metadata提升信息质量之外，TITAN将通过建立信息社群的方式将拥有共同利益、共同价值观和共同期望的人聚集起来，在系统内部对信息的可信度做进一步的评价。

TITAN生态中，社群是主要的信息组织形式，无论是新的内容还是外部引入的内容都通过社群发布后，经过社群用户的评估做进一步的传播。社群的质量由社群中所有个体的内容贡献决定，同时社群评分也会反向影响社群中内容的质量评价。为了避免社群的水化降质，任何加入社群的用户必须先存储少量的TTC，储存数量的下限在社群建立时确定，或由社群成员投票决定。

社群还是一个自组织的生态，每个社群的成员都是社群的利益共享者，社群的成长和质量的提升，系统都会给社群成员中分配TTC激励。激励会根据社群内成员的人均贡献进行分配，任何对社群的破坏或者灌水行为都可能招致社群成员的一致抵触甚至被逐出社群。

传统社群一方面具体有天然的信任基础，另一方也是非常脆弱的，传统社群往往容易被个别人利用传播虚假信息。区块链的信任机制恰好弥补社群信任中的短板，避免出现对社群的恶意信息攻击，TITAN在社群中引入经济学中的激励也让社群的自我成长具备了更多的潜能。

用户自治内容社群

4.1.1、短视频

在移动互联网行业整体增速放缓的大背景下，短视频行业异军突起。据统计，中国某头部短视频平台平均日活用户6亿人。如此庞大的用户聚集领域，自然会吸引众多品牌广告主的青睐。目前，各行业品牌都把短视频作为自媒体营销的

主战场。在这样的背景下，短视频营销市场也呈现出了获取流量曝光成本高、数据可更改不真实等问题，而TITAN短视频的诞生就是为了打破这一僵局。

TITAN短视频旨在打造一款全民共治、全民分红的区块链技术支持的国际化短视频社区，利用区块链不可篡改的技术有效打击短视频盗版现象，将作品的授权掌握在原作者手中，完成版权追踪和权益的保护。同时，通过平台通证TTC实现创作及互动激励，使平台更加开放、包容以及充满活力。

在TITAN短视频生态侧链上，无论是短视频创作者还是短视频观看者，都能获取相应的通证收益，娱乐挣钱两不误，真正实现“以时间换金钱”。

对于创作者而言，上传短视频作品可以获取TTC激励，激励多少会根据上传作品的优质程度进行划分，越优质受到用户欢迎点赞越多的作品能够获得更多的TTC激励。同时，如果有其他创作者想模仿原作者的作品，可以商讨后用通证TTC来进行交易购买版权，从而保护原创，为作品内容进行版权声明。

其次，对于用户而言，无论是观看短视频，还是参与互动，进行举报（需要审核通过，恶意举报将获得相应惩罚）、点赞、转发、评论等的过程中也会根据时长、频率及

优质程度激发通证奖励。TITAN通过这种“互动挖矿”的方式激励用户共同维护生态，保持生态平衡。

传统互联网是提供产品与服务，而TITAN平台创造一个规则和生态。在TITAN生态里，大家都是价值创造者和价值持有者。相较于现有的短视频产品，TITAN生态圈中的内容生产者、内容受众、内容传播者和广告主不再受制于平台，生态角色不再有高低贵贱之分，MCN业态的混乱现状将不复存在，实现了在去中心化体系下优质内容点对点的自由交易与传播，实现生态的良性可持续循环。

4.1.2、去中心化游戏

TITAN还将构建一个去中心化游戏侧链，即一个去中心化的分布式智能合约游戏有机生态世界，提供一个基于区块链技术的集多类型游戏为一体的新生代游戏生态平台。

在TITAN平台，游戏各方通过开源合约快速建立信任，使用过程完全透明，信息完全对称，游戏数据无法篡改，游戏规则的改变也要经过社区投票决定。同时，能做到切实保护用户的资产，以不至于因为游戏的衰落或者游戏厂家的不合理回收而流失。

TITAN除了自己开发的游戏之外，也会接入大量优质的第三方游戏。因此，交易数据既要流动，又要保持对交易用户的透明性与私密性。这对于TITAN游戏链的交易数据透明性以及安全性都提出了很高的要求。TITAN也在这两个方面采用了最先进的技术以保证用户的使用体验感，保障去中心化的完全实施。

4.2、全行业直播

在通证经济的模型下，区块链当中的点对点交易、公正透明、行为即奖励等优点，使得TITAN网络直播更符合用户的需求，更具吸引力。

基于另一个TITAN全行业直播的侧链，参与TITAN网络直播的主播可以直接收到用户的通证打赏，收益全部归主播所有，不需要经过某中心平台参与分成。其次，用户也可通过观看直播、打赏主播、参与讨论等行为，获得通证回馈。主播和用户所拥有的通证也可直接用于商城购物、平台交易。这就相当于用户在“消费”的同时也在“盈利”，提高用户的参与度，革新当下直播行业的生态现状与消费模式。另外，人人参与的社区模式，也让TITAN网络直播平台持续产生经济效益，让整个生态更有凝聚力。

在TITAN打造的直播世界中，一个真正的直播互动系统得以构建，消费者直接与内容生产者连接，消费者直接付费和打赏给内容生产者，“中心”在这个世界里消解了。基于去中心化的设计，TITAN为内容生产者和消费者搭建了一个公开公平民主的互联网乐园。在TITAN直播生态中，同时可以实现交互式跨平台匿名聊天，无需注册账户钱包地址及账户

保护用户聊天内容的隐私性，且无需第三方监管。直播主可一键发行代币作为激励，也可以和其它有粉丝的社区团队合作运营，为平台引流打造平台产业化。

TITAN使用了全新设计的开放式内容价值评价体系。在这个体系下，对单个内容的价值评分不再单纯使用点击量等指标进行计算，而是综合考虑了社会化推荐、内容传播和作者信用等因素，从深度和广度两个方面全面衡量内容的价值。

受众和内容进行交互的方式，按照受众付出的操作成本从低到高可以排序为点击、点赞、评论、转发、转载。对读者来说越是高成本的操作，对于衡量内容的价值来说贡献越大。受众进行一次转发，比几次点赞更能表现出内容的价值，而进行一次转载则比转发更能表现出内容的价值。要对内容价值做出准确的评价必须能够综合评估全部的因素。TITAN的评价体系内采用的用户交互指标包括了点赞、评论、转发和转载：

$$V_c^t = \sum_{i=1}^{3}\sum_{j=1}^{c_i^t} \alpha_i HP_j \Gamma_j + \beta \sum_{j=1}^{d^t} HP_j \Gamma_j S_j$$

其中/span>"#是在/span>时刻内容/span>的价值评分，/span>/,/span>8,/span>0和/span>分别对应点赞、评论、转发、转载的权重。/span>'# 是在/span>时刻一个给定的时间窗口内的第i种交互操作的次数。

进行第/span>次交互操作的用户的信用评分。和Voting Power思想类似，*是用户在进行交互操作时的能量值：

其中/span>*是第j次交互操作时用户账户中非锁定状态，/span>*是用户在第j次交互操作时刻一个给定的时间窗口内的用户交互操作总数。θ是阈值。当用户在一段时间内进行了频繁的交互操作时，HP会不断减小，导致该用户的操作对内容价值评价的影响不断减小。当用户停止频繁操作后，HP则会随着时间恢复。对于内容转载来说，还需要额外考虑转载来源方的质量因子C>'：

$$S_i = \frac{s_i}{\sum_j s_j}$$

$$s_i = \sum_{i=1}^{C_a} \left[\frac{1}{C_i} \sum_{C_i} V_{C_i} \right] \cdot C_a C_p^2$$

Si由该转载来源方的质量评分Si进行归一化后得到。Si由该转载方的全部转载的价值评分、作者人数以及爬虫总数进行计算得到。其中Ca是作者总数，Cs是爬虫总数。Si同时用于防止单个作者或者单个爬虫通过自行生成转载的方式骗取奖励。注意到/span>'的定义中包括内容价值评分/span>"#，因此对/span>'的计算是一个迭代的过程。对于一个新的转载来源来说，初始时刻其质量评分被设置为一个较小的固定值。随着该来源的转载数不断增多，其质量评分也会不断更新，最终作用于对一篇新内容的价值评价中。

4.3、普惠新金融

金融的核心是信用的建立和传递，区块链以其不可篡改、安全透明、去中心化或多中心化的特点，天然适用于多种金融场景。TITAN将会以金融全业务场景落地的模式，拥抱区块链技术，布局多产品以及多服务金融场景，为全球用户提供全方位一体化的高水准、智能化、全体系的智能金融服务。

在公平公正公开的在区块链的世界中，TITAN将构建一个人人当家做主的去中心化金融服务体系，以卓越的技术体验为投资者赋能，在区块链的世界实现和谐大同的金融社会。

4.3.1、去中心化借贷

在现有的金融系统中，金融服务主要由中心化机构（如传统银行）进行控制和调节，所以无论是基本的存取转账，还是贷款或者衍生品交易，用户都绕不开银行。

这种过度中心化的金融服务，容易带来很多问题，比如效率低下、中间成本高昂、准入门槛高等痛点。在这些痛点背后，是数十亿无法享受到正常金融服务的用户群体。

据世界银行数据显示，各国未享受银行服务的人群比例相差悬殊，一些发达国家只有1%不到，而一些发展中国家则超过98%。另一方面，截至2016年，手机在全球人口中的平均使用比例已达62.9%，然而手机支付的全球平均使用比例仅为2%。这数据背后的原因，除了传统金融服务的高壁垒以外，还有人们对传统金融机构缺乏足够的信任。

TITAN网络，将为解决这一困境带来全新视角。TITAN怀着“将区块链价值带给全球数十亿人”的愿景，利用区块链技术打造一个更为去中心化和包容的金融体系，通过通证机制降低金融服务门槛，提供基于数字资产的去中心化借贷、挖矿、存储、量化交易等服务，让所有人都能参与金融生态建设并获取相应激励。

“金融无界限，人人能发达”，TITAN将逐步推动全球普惠金融的实现，在金融领域民主自治，均衡获益，打破中心化银行与投资者的不平等关系结构。

4.3.2、去中心化钱包与跨境支付

TITAN多链的钱包（和im通证钱包类似）。凭借TISS加密技术，确保钱包内资产安全性高，并可用于主流数字资产

的储存，以及通证在DApp的运用。在未来，TITAN钱包系统将是区块链时代粉丝及流量入口，当钱包的流量够大未来的应用就会更丰富，好比微信提供的小程序和公众号。在目前的跨境支付中，主要由银行电汇、第三方支付和提现等三种方式，跨境金融机构间的对账、清算、结算流程纷繁复杂，涉及诸多手工流程，存在着成本较高、结算周期长、占用资金大等问题，且因为成本高导致小额跨境支付不能实现。

在跨境支付和结算中，TITAN可以摒弃中转银行的角色，实现点到点快速且低成本的跨境支付。未来银行与银行之间将不再通过第三方，而是通过TITAN实现点对点的支付，不但省去了第三方金融机构环节，还可以实现全天候支付、实时到账、便捷提现和低成本。当拥有低成本和高效率的优势时，金融机构便能处理原来因为成本因素而被视为不现实的小额跨境支付。

TITAN Chain在很好地完成主链职能之外，可以配合其他币种的主链，作为侧链来增强交易速度，安全，和隐私保护。TITAN Chain的改进对等钱包侧链技术特性如下：

1、双向锚定（ two-way peg ）映射主链资产到侧链上交易；

2、智能合约（EVM）兼容以太坊智能合约；

3、支持现实/虚拟世界资产数字化；

4、安全与隐私增强。主链只负责资产的转移确权，侧链完成快速交易，交易信息保护，账号安全保护和用户隐私保护。

基础原理：

使用2to2多重签名（multi sig）钱包预充值的方式，构建双向微支付通道。通过构建更多双向微支付通道，达到全网节点可达的闪电网络的方式，使得在主链上的资产转移达到即时和非常低的手续费。

基于技术：

1、序列到期可撤销合约RSMC（Recoverable Sequence Maturity Contract）

2、哈希时间合约HTLC（Hashed Time Lock Contract）

3、多级跳节点构成闪电网络（Lightning Network）

4、未来实现跨链原子交易（atomic cross-chain swaps）

4.3.3、供应链金融

在传统的供应链金融中，处于风控的考虑，银行仅对供应链上核心企业的上下游大型供应商提供保理和融资服务，

这使得供应链上的中小企业融资难、成本高、征信周期长；另一方面，商业汇票、银行汇票使用场景受限，转让难度大，转让审核流程相当复杂。

在TITAN上可以发行、运行一种数字票据，可以在公开透明、多方见证的情况下进行随意的拆分和转移。这种模式相当于把整个商业体系中的信用将变得可传导、可追溯，为大量原本无法融资的中小企业提供了融资机会，极大地提高票据的流转效率和灵活性，降低中小企业的资金成本。银行与核心企业之间利用区块链多方签名、不可篡改的特点，使得债权转让得到多方共识，降低操作难度。

4.3.4、资产证券化ABS

传统的资产证券化需要结算机构、交易所和证券公司等的多重协调。而在区块链技术的支撑下，通过搭载智能合约的联盟链，可以自动实现跨多主体间的证券产品交易，显著提高资产的流动性和安全性。

基于TITAN区块链技术的资产证券化管理系统，能够确保消费金融服务公司底层资产数据的真实性，且不可篡改、可追溯，提高机构投资者信心，从而降低消费金融服务公司

发行ABS的门槛和发行成本，同时还可以进行ABS全生命周期管理，及时识别和管控风险。

4.3.5、无国界货币

在TITAN的金融体系中，将打造一种可以让全球人民共同使用的开放、包容且技术上可行的无国界货币，同时构建一种易于访问的支付系统。无国界数字货币可以让全球最贫穷、最弱势的群体享受金融普惠，使其参与本地、本国乃至全球经济。

在未来，TITAN的用户将能够像发送照片和邮件一样，快速安全地跨境汇款和转账，推动全球价值无障碍进行流通。

4.4、消费挖矿商城

TITAN将打造全球首个去中心化消费流量聚合社区。基于TITAN生态通证TTC，通过使用区块链技术，TITAN将打造全球首个去中心化消费挖矿创新商城。TITAN商城通过利用流量漏斗将精准的流量注入实体经济，同时将实体企业生态红利以交易通证TTC的形式反哺流量池，使消费共识不断壮大。TITAN新通证经济以区块链为信任基础，为实体企业带来了新的活力，为客户忠诚度计划提供了新的解决方案。TITAN将致力于实现证股同权，将实体企业的增长价值回馈给社区，每一位贡献者都可以共享实体经济消费生态增长的价值红利。

4.4.1 去中心化商城

相对于传统中心化电商而言，通过交易通证TTC，TITAN去中心化电商可以有效让买家、卖家、平台充分参与生态运作并获取相应奖励。TITAN创新商城内种类丰富，涵盖食品生鲜、酒水、大健康、美妆日化、数码电子、家纺家饰、母婴用品、旅游、教育和家居百货等类目，未来将进一

步涵盖房车旅游、游艇会务、奢侈品等商品和服务，商品品类超过20万+。TITAN商城只接受经区块链确权的TTC数字资产支付进行商品消费，目的在于确定一个商业平台与一个流量型数字资产合作后的长期确权，帮助消费者少花钱，多挣钱。

TTC通证作为去中心化电商TITAN平台的灵魂所在，承担着激活整个社区生态的重任。TITAN鼓励普通用户分享商品，平台上的消费者可通过个性化地推送，将好货推荐给针对性人群，好物不独享的同时让流量转化率更高，也为自己带通证奖励收益。

4.4.2、线下消费场景

TTC可用于线下消费场景。消费者可以选择在线上咨询，然后通过线下买单，推广分享并获得通证奖励。TITAN依托溯源联盟链，并结合智能合约发行专属积分，消费者可以在平台DApp上速览美容商品、即时咨询客服、快速预约课程，再服务结束后进行线下支付。除此之外，消费者还可以在线下进行推广分享，获得通证奖励。TITAN通过线上线下结合，致力于成为区块链分享经济的先行者。

4.5、一键发币（黑色以太坊）

以太坊提供了一个简单的发币系统，打造了ICO的区块链巅峰时代，但以太坊之下的发币也需要程序员通过写代码完成，这对传统用户而言依然是一个很高的门槛。

在TITAN生态中的一键发币，只需要填写代币英文全称、简称、发行数量，上传LOGO后1分钟发币完成。让数字资产的便捷性能够为全球每个潜在用户都能够使用。

基于以上几个大的生态板块，将形成完整的生态闭环，凭借着TTC生态通证的价值承载，差异化的、拥有强竞争力生态平台将成为全行业流量入口，从而打造真正能落地，高实用的TITAN全闭环生态。


5
TITAN生态通证

5.1、TITAN新加坡基金会

TITAN社区通过设立TITAN新加坡基金会来保证社区项目的可持续性、精细化治理的有效性以及募集资金的安全性。

TITAN新加坡基金会负责托管TITAN项目募集取得的资金与发展储备代币。同时TITAN新加坡基金会承担将资金合理使用与分配的义务。节点竞选完成之后，适当的环境下，基金会将逐步公开资金使用情况。

5.2、TITAN的经济模型

泰坦（TITAN）网络中内置一种主网通证代币，全称为TITAN Coin，简称是TTC。TTC是整个TITAN生态系统中的驱动剂，将用于支持社区建设、社区治理、应用发展、支付消耗、参与共识奖励、支付交易手续费、支付造链消耗和资产跨链流通的手续费等。

5.2.1、TTC分配方式

代币名称：TITAN（泰坦）TTC

发行总量：1.8亿

代币分配：

A、160万用于母币聚变，20万用于前期流通，共180万--约占1%

B、1.782亿用于挖矿--占99%

日产币量：0.3TTC/0.5s x 10x12 x 60 x 24 =51840

年产币：1892.16万，产量低需求大，增值空间高

减产机制：

$$Y_{(\text{总量为 1.8 亿})}=X_{(\text{减半周期：天})} * \left(51840+\frac{51840}{2}+\frac{51840}{4}+\frac{51840}{8}+\frac{51840}{16}+\cdots+\frac{51840}{2n}\right)$$

根据公式得出X约为1750天（约等于4.79年），即减半周期为1750天。

-1750天：9072万

-3500天：4536万

-5250天：2268万

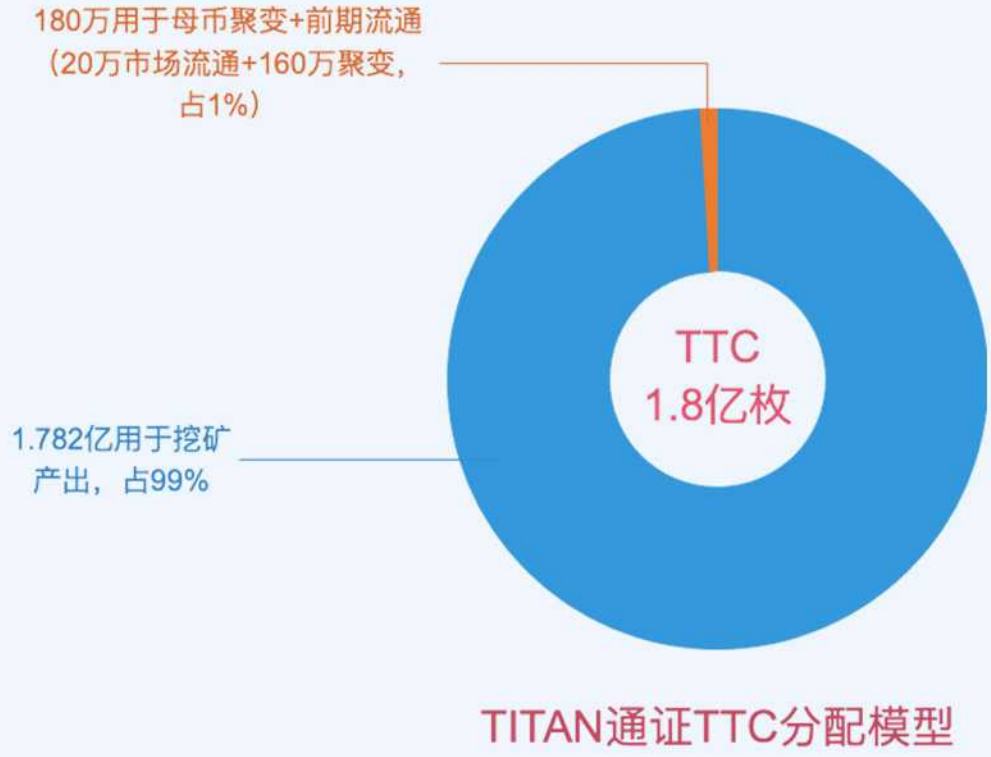
-7000天：1134万

-8750天：567万

-10500天：283.5万

…

总量1.8亿枚，共30年挖完。



TITAN通证TTC分配模型

5.2.2、销毁机制

经济学中最基本的思想：在市场需求高的情况下，资产的相对稀缺性能够更好地提现货物的价值。TITAN生态代币TTC将长期处于“通缩”的状态，流通中的TTC会以不同的机制来磨损销毁，从而保证TTC单价的无限上升。正所谓“一币永流传，价值涨无限”。

TTC通证将采取以下机制来销毁流通中的TTC，为生态价值提升保驾护航：

1、当全网算力不足以满额分享当日总产币的情况下，未能够全额分配的代币将被销毁；

2、TTC交易所80%的手续费将定期进行销毁；

3、TITAN新加坡基金会从二级市场回购TTC并进行销毁；

4、TTC公链的转账手续费为每笔0.01TTC，TTC全网转账手续费的将100%销毁。


6
TITAN里程碑

TITAN里程碑

2018年9月TITAN新加坡基金会发起TITAN链，致力于探索新兴区块链与传统互联网和商业有机结合，赋能并颠覆传统商业模式，引领通证5.0经济。

2018年11月面向全球进行市场调研，确定平台发展方向。

2019年2月招揽贤士，最终确定核心团队，完成整体方案设计。

2019年12月首次内测公链。

2020年3月公链内测成功。

2020年8月主网上线，交易所开启交易。

2020年开启商城生态同时启动娱乐直播板块。

2022年完成TITAN生态基础搭建，完善生态闭环，生态构建形成规模。

2023年公链共识升级，品牌升级，在全球范围内开展合作，拓展全球生态。

2024年TITAN全球链景蓝图构建基本完成，全球生态呈规模化、系统化纵深发展。TTC通证实现全球商业化、商品化，成为全球90%主要货币价值标的，实现全球资产的高效无国界流通。

7

免责条款

免责条款及风险提示

风险声明

1、购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制享有者的TTC，为了最小化该项风险，购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

2、司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则TTC应用和代币可能受到其影响，例如法令限制使用，销售，电子代币诸如TTC有可能受到限制，阻碍甚至直接终止TTC应用的发展。

3、TTC应用缺少关注度的风险

TTC应用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对TTC和TTC应用造成负面影响。

4、TTC相关应用或产品达不到TTC自身或购买者的预期的风险

TTC应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何TTC自身或购买者对TTC应用或TTC的功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，一个设计的改变等均有可能导致这种情况的发生。

5、 黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断TTC应用或代币功能的可能性，包括服务攻击，Sybil攻击，游袭，恶意软件攻击或一致性攻击等。

6、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量子计算机的发展，或将破解的风险带给加密代币和TTC平台，这可能导致TTC的丢失。

7、缺少维护或使用的风险

首先 TTC不应该被当作一种投资，虽然TTC在一定的时间后可能会有一定的价值，但如果TTC缺少维护或使用的话，这种价值可能非常小。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对TTC是非常不利的。

8、未保险损失的风险

不像银行账户或其它金融机构的账户，存储在TTC账户或以太坊网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保，但诸如FDIC或私人保险公司将会为购买者提供保障。

9、应用存在的故障风险

TTC平台可能因各方面的原因故障，无法正常提供服务，严重时可能导致用户TTC的丢失。

10、无法预料的其它风险

密码学代币是一种全新且未经测试的技术，除了本白皮书内提及的风险外，此外还存在着一些TTC团队尚未提及或尚未预料到的风险，此外，其它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。

11、 特别风险提示

TTC作为一种虚拟货币，不是真正意义上的货币，不能在市场上流通使用，属于一种虚拟商品。