

Tachyon field Chain

区块链技术白皮书

Version 1.0.0

<https://www.tafchain.com/>

■ 序言

以比特币、以太坊代表的区块链和数字货币正以燎原之势震动着传统的货币体系和金融体系，区块链技术虽然还处于发展的初期，但更加透明、开放的理念和机制已经展现出无与伦比的生命力，在最近几年中，区块链和数字货币领域经历了从追捧到泡沫，从泡沫到低谷的阶段，这同时也是大浪淘沙去真伪的过程。

区块链和数字货币领域经过一轮又一轮的风暴和泡沫，有人避之不及，有人坚定拥抱。资本驱动是区块链上半场发展的关键要素，同时他也将区块链的发展带入弯道，带入了虚假泡沫。当我们回归技术、回归理性，一个真正属于区块链的时代也许才能真正降临。

根据国际数据公司（IDC）研究报告显示，2018 年中国区块链的市场支出规模达到 1.6 亿美元，预计这一强劲增长态势将在未来三年延续至 2022 年，预计该市场的支出规模将达到 16.7 亿美元，2017-2022 年复合增长率将超过 80%。在区块链的支持下到 2021 年，分布式架构将成为数据市场的核心基础，区块链技术的核心价值--塑造数字信任，也将对现有的商业社会产生深远的影响。随着技术的不断发展，区块链技术将会“多点开花、加速推进”，在各行各业中实现突破。

当下大多数企业期望利用区块链的特性来优化自身的产业结构，而目前市面上的各类公链系统，其低下的性能无法能够支撑商用，那么公链的技术突破也愈发迫在眉睫。而 TAF Chain 凭借自身对区块链技术创新，解决业内不可能三角问题，从而将区块链技术融入现有的商业模式，降低区块链技术的使用门槛，解决实际问题，从而让区块链在各行各业中发挥出最大的价值。

目录

第一章	区块链简介	5
1.1.	区块链概念	5
1.2.	区块链价值	6
1.3.	区块链技术	7
1.4.	区块链环境	8
第二章	发展现状与未来趋势	9
2.1.	区块链现状	9
2.1.1.	区块链分类	9
2.1.2.	区块链演进	10
2.2.	未来趋势	11
2.2.1.	高吞吐、高并发	11
2.2.2.	低延迟	12
2.2.3.	分布式高效存储	12
2.2.4.	隐私保护	12
第三章	区块链整体架构	13
3.1.	什么是 TAF Chain	13
3.2.	核心	13
3.2.1.	共识机制	13
3.2.2.	智能合约及虚拟机	15
3.2.3.	高效储能技术	15
3.2.4.	跨链与侧链	17
3.3.	区块链浏览器	17
3.4.	钱包	17
3.5.	API 及 SDK	18
3.6.	特色	19
3.6.1.	高性能、高并发、低延时	19
3.6.2.	安全保护机制	19
3.6.3.	支持动态参数	19
3.6.4.	开发者友好	20
3.6.5.	交易免手续费	20
3.6.6.	便捷数字资产发行	20
第四章	商业场景	21
4.1.	普惠金融	21
4.2.	游戏市场	21

4.3.	社交平台	22
4.4.	数据权益	23
4.5.	更多场景	24
第五章	经济模型	25
5.1.	Token 经济	25
5.1.1.	首次发行	25
5.1.2.	出块奖励	26
5.1.3.	社区贡献	26
5.1.4.	活动奖励	27
5.1.5.	开发者扶持计划	27
5.2.	权益价值	27
5.2.1.	治理委员会	27
5.2.2.	节点投票	28
5.2.3.	重要参数修改	28
5.3.	生态价值	28
5.2.4.	开发资源使用	28
5.2.5.	应用内结算	29
5.2.6.	流通交易	29
第六章	研发线路图	30

第一章 区块链简介

1.1. 区块链概念

谈到区块链，大家往往会想到比特币，比特币只是基于区块链的一个应用，区块链是多种现有成熟技术的组合，这其中包括密码学、共识机制、分布式账本、智能合约、P2 网络等。区块链是一种以密码学方式保证不可篡改和伪造的分布式账本，其特性是账本中的数据按照时间序列顺序叠加形成一种链式存储结构。作为一种全新的分布式基础架构与计算范式，区块链利用链式数据结构来验证和存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的技术保证安全的传输数据和控制访问、利用自动化脚本代码组成的智能合约来编程和操作数据。

区块链的核心技术在于以下几点：

一、 共识机制

共识可简单理解为，不同群体所寻求的共同的认知、价值、想法等，在某方面达成的一致性意见。共识机制就是确定达成某种共识和维护共识的方式。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。拥有共识机制作为区块链网络的核心模块，去中心化功能才有可能实现。由于场景的不同，采用不同的共识机制。常用的共识机制主要有 PoW、PoS、DPoS、BFT 等，共识机制既是数据写入的方式，也是防止篡改的手段。

二、 分布式账本

分布式账本是一种在网络成员之间共享、复制、同步的数据库，它记录网络参与者之间的交易。区块链网络中交易在多个节点共同存储，每一个节点都记录完整的交易记录，因此它们都可以参与监督交易合法性并验证交易的有效性。在区块链系统中没有任何一个节点有权限单独记录交易，从而避免了数据被主动或被动更改而造假的可能性；另一方面，由于全网节点参与记录，理论上讲，除非所有的节点都被破坏，否则交易记录就不会丢失，从而保证了数据的安全性。

三、 安全及隐私保护

区块链技术很好地集成了当前对称加密、非对称加密和哈希算法的诸多优点。通过引入加解密技术,降低密钥被泄露和破解的可能性;通过非对称加解密算法确保整个网络的交易安全;通过各种签名策略,如群签名、环签名等保护用户身份的隐私。其中最具代表性的是使用椭圆曲线加密算法生成用户的公私钥对,和使用椭圆曲线数字签名算法保证交易安全。另外国密算法也在越来越多的应用于区块链网络中。

四、 智能合约

智能合约是一种特殊的协议,是可以自动化执行预先定义规则的一段计算机程序代码。它自己就是一个系统参与者,旨在提供、验证及执行合约。它能够实现价值的存储、传递、控制和管理,在不需要第三方的情况下,执行可信、可追溯、不可逆转、安全的价值传递。为基于区块链的应用提供了创新性的解决方案。

1.2. 区块链价值

近年来,随着区块链技术的蓬勃发展,各企业和研究机构对区块链系统的深入分析及大力推广,人们逐渐认识到区块链技术本身所带来的巨大价值。

相对于传统数据库,区块链技术具有以下几个显著特征:

一、 可靠存储

基于去中心化 P2P 网络技术,分布式一致性算法。区块链网络为人们提供真实可靠的数据来源,每一条数据都有严格的签名及验证签名机制,并确保数据一旦上链即不可篡改。即使网络内的部分节点出现故障或者被恶意攻击,仍然无法改变数据的真实性。

二、可信网络

区块链是可信网络，它结合了密码学，数字签名，以链式结构将数据的变更按照时间序列依次叠加，不可篡改和不可伪造。人与人之间无需建立任何信任关系，即可完成数据之间的可信交换。

三、安全和隐私保护

区块链采用国际通用的加密算法，如 ecc，国密算法等，以及各种分层加密技术，从技术上避免数据泄露及破解的可能性。它采用高度的散列及摘要算法来保证用户地址的合法，并通过复杂的签名技术，如环签名，群签名等对用户身份进行隐私保护。

四、变更历史可追溯

区块链技术固化了数据变更历史，并提供数据变更历史的可追溯。通过加密技术手段，保证链上数据信息的不可篡改和不可抵赖。数据一经上链，即可通过区块链网络确定与用户间的锚定关系，且后续的每一次数据操作都会被准确记录，不可篡改。

五、价值共享

区块链实现了节点之间的去中心化连接。各参与方均有一份完整数据的拷贝，参与节点之间共享数据价值。交易双方避免了中介的接入，在数据流通方面大幅降低了时间成本，增加信任，避免了数据被篡改、造假的风险。

1.3. 区块链技术

区块链技术并非单一技术，从科技层面来看，区块链涉及分布式数据存储、加密算法、P2P 传输以及共识机制等计算机技术的新型应用模式。每项单一技术都有着十几年乃至几十年的发展历史，具备较高的成熟度。当这些相对成熟的技术经过整合设计，成为具有创造性的区块链系

统之后，其作为新兴技术的特点开始显现，有了全新的发展路径。

但是，现存的区块链技术本身的成熟度有待有进一步提升，主流公链仍然面对一些技术挑战，如系统吞吐量、跨链系统、节点规模及容错性、共识机制效率、合约的安全性都需要提升。因为每一项核心技术的突破都需要耗费巨大的人力和物力，高昂的创新成本成为区块链技术发展的重要阻碍。

1.4. 区块链环境

为什么会出现区块链，我们真的需要吗？TAF Chain 团队创始人作为区块链早期的参与者和见证者，认为这一创新不可逆转更不会昙花一现，原因有两个：

一、降低信任成本

人们需要真实、有价值的信息、够降低信任成本。计算机和互联网让信息分享更加便宜、更加便捷，利用信息透明，优化价值链，提升协作效率。但是，无法杜绝的虚假信息、违约行为也让人头疼不已，基于互联网的传播和复制也极为容易，人们为信任所投入的成本已经越来越大，必然阻碍效率的进一步提升。

二、客观公正的生产关系

人们需要一个将共识、行为和价值激励相互连接的生产关系网。相比工业革命带来生产力巨大飞跃，生产关系的改变就不那么巨大。人类的生产活动以组织为中心开展，依旧是自上而下、金字塔层级的中心化结构。组织业务越复杂，层级越多，要实现客观公正的利益分配就越难，因此，效率提升也就难上加难。区块链将分布式存储、加密技术、P2P 网络等技术融为一体，有去中心化、去信任化的技术优势，被人们称之为价值互联网。

区块链最有可能解决人与人之间的信任问题，并缔造出新的生产关系网络——点对点价值交换，从而改变效率低下的生产分配关系。

第二章 发展现状与未来趋势

2.1. 区块链现状

2.1.1. 区块链分类

目前，按照区块链去中心化程度，准入机制，应用情况可以分为：公有链、私有链以及联盟链三种类型。一般来说，公有链适用于对可信度、安全性有很高要求，而对交易速度要求不高的场景。私有链或联盟链更适合对隐私保护、交易速度和内部监管等具有很高要求的应用。在实际中，私链通常在企业内部署，与传统数据库差异较小，而公链和联盟链的地更为广泛。

公有链

顾名思义是全公开，所有人都可以作为网络中的一个节点，不需要任何人给予权限或授权，每个节点都可以自由加入或退出网络，任何人都可以读取数据、发送交易，且交易能够获得有效确认的共识区块。目前，基于公链的区块链项目以面向消费者的应用(DApp)为主，生态刚刚起步，整体发展并不成熟。根据 DAppRadar 的统计，截至 2020 年 4 月 3 日，主流公链平台上的 DApp 仅有 3076 余款，且集中在竞猜、游戏和加密收藏品等少数领域，在应用数量、类别、用户数以及用户活跃度等方面与互联网应用相比都存在数量级上的差距。

私有链

私有链也属于一种许可链，整个区块链网络的节点加入、数据的读写权限仅仅掌握在某一家组织或机构中。它的应用场景一般是单一企业内部或者针对分公司管理方面，在有些场景中私有链还被称为专有链，其价值体现在它提供了一个可靠的、可追溯的不可篡改的平台，并且可以防止来自外部及内部的攻击。

联盟链

联盟链只针对某个特定群体的成员和有限的第三方，内部指定多个预选的节点为记账人，多个

记账人共同完成区块的生成及账本的记录。联盟链属于一种许可链，这就意味着并不是任何节点均能自由加入，作为一个新的节点加入该网络，需要特定权限的许可。与公链不同，联盟链的落地更多地以企业级市场为主。行业用户通常面临一定的行业痛点，试图将区块链技术特性与业务场景相结合，在信任、效率和成本等方面发挥区块链的价值。目前，中国市场上常见的企业级区块链应用包括金融源类、存证类等，在整体上处于积极探索期。

2.1.2. 区块链演进

自从区块链诞生至今，技术上经历了三次重大的技术变革，其典型代表项目为 2009 年由中本聪发布的 Bitcoin、2015 年的 Ethereum 和 2016 年 Linux 基金会所主导推出的 Hyperledger Fabric，其组织形态从资源消耗严重、交易性能低下、缺乏灵活控制机制的公有链，向高效共识、智能可编程、可保护隐私的联盟链转变。

技术创新推动性能安全不断完善，当前区块链技术尚不成熟，仍处于发展早期。对于区块链性能、隐私保护、可扩展能力以及安全问题等方面的技术创新正在不断涌现，针对区块链性能问题出现如下几类创新解决方案：

一、 并行的方式

例如 Ethereum 分片技术、MOAC 子链技术、 Hyperledger Fabric 多通道技术。

二、 DAG（有向无环图）技术

例如区块链与物联网创新项目 IOTA 采用 DAG 技术使得区块链系统的可扩展性不再受到区块大小限制，仅取决于网络带宽、CPU 处理速度和存储容量等限制。

三、 优化共识算法

例如 PoS 共识算法通过保持多中心情况下减少参与共识的节点的方式以获取性能的提升。

四、 链下扩容

例如闪电网络、雷电网络等创新技术提高区块链处理交易能力，实现即时确认、低费用、高吞吐量的支付。

针对区块链技术中隐私保护问题，业界提出了混币、环签名、同态加密、零知识证明多方安全计算等创新技术方案；针对区块链可扩展和互联互通问题，业界提出了跨链的解决方案。主流的跨链技术有侧链/中继、公证人机制和哈希锁定三种方式，代表项目分别有 COSMOS, Ripple, Lightning network。

针对区块链安全问题，尤其是区块链的智能合约安全问题、公私钥存储安全问题以及底层平台攻击问题，业界提出了代码审计、形式化验证、智能硬件钱包、混合共识机制等解决方案。

随着学界和业界对区块链研究不断深入区块链技术创新成果将不断落地，随着区块链技术不断发展、产业链不断完善、社会认知逐步提高、场景日益丰富，区块链应用效果逐步显现。

2.2. 未来趋势

2.2.1. 高吞吐、高并发

针对大型应用，如 Facebook、淘宝网等需要能够处理数亿级日交易量，如部署区块链技术则要求区块链系统的性能、吞吐量至关重要。而主流公链项目的交易处理都是串行执行的，无法充分利用多核心处理器资源，另外也无法像传统的互联网高并发服务器一样，通过简单的堆机器的方式进行性能方面的扩展。为了有效实现区块链系统高并发，高吞吐量的问题，未来的研

究方向应该是朝着单节点跑得快，并可通过堆机器的方式平滑扩容的方向进行。

2.2.2. 低延迟

Bitcoin 交易确认时间约为 1 小时，EOS 也是在大部分生产节点确认后才能完成交易确认。毫秒级的确认时间是未来区块链项目的重要研究方向，及时的反馈是良好用户体验的基础。延迟时间如果超过了秒级，会大大影响用户体验，如果到分钟级别甚至压根无法胜任商业需求，严重降低应用的竞争力。

2.2.3. 分布式高效存储

目前的区块链在物理存储方面通常是单盘甚至是串行存储的，IO 性能低下。另外由于区块链的链式结构特性，数据量的不断增大导致存储空间的需求线性增长。高效的分布式并行存储模型，将成为一个重要的发展方向。

2.2.4. 隐私保护

随着物联网设备的连接越来越紧密，更多的数据将在人与人、公司、政府和生态系统之间共享。在数字世界中，用户的数据大多放在巨头服务器中，存在被黑客攻击、丢失、非法交易等风险。数据资产的开发与利用固然是大势所趋，但数据的权益认定和信息的隐私保护尤为重要。

第三章 区块链整体架构

3.1. 什么是 TAF Chain

TAF Chain，是一条为全球商业服务的公有链，旨在打造高效底层系统。

TAF Chain 基于 DPoS 共识机制的自研创新底层架构的分布式系统，同时具备链上配套功能，方便各类应用便捷开发。

TAF Chain 拥有一支全球化的技术团队，整个公链完全自主研发，团队成员在区块链，信息管理和大数据领域具有独特的见解与经历，他们利用多年的开发经验和工程经验，进行技术革新，创造大量专利技术如自主设计的集群方案、自研的高效存储技术等，完成业界的吞吐能力的突破，理论完全优化后最高可达百万 TPS 每秒，在未来完全能够支撑整个社会的各类商业应用。

3.2. 核心

3.2.1. 共识机制

TAF Chain 中采用目前 DPoS 共识机制，用来实现区块链记账和数据交换。

DPoS (Delegated Proof of Stake) 机制源自于 Graphene，中文名叫做股份授权证明机制 (又称受托人机制)，它的原理是让全网持有代币的人可以通过链上的投票系统来选择区块生产者，一旦当选任何人或者组织都可以参与区块的生产，当然区块生产者也会获得系统的 Token 激励。

在 TAF Chain 的网络中，全网代币持有者都可以进行投票产生 21 位代表作为系统的区块生产者，这 21 个超级节点彼此的权利是完全相等的，每个出块周期中，由 21 个超级节点轮流进

行出块，直至下一周期投票选举新的超级节点。

TAF Chain 超级节点由全体持币者投票选出，每 2 个小时举行一次，投票率排列的前 21 位自动成为超级节点，如果在出块周期中某个超级节点存在作恶情况，则会被投票出局，网络会选出新的节点（第 22 位开始）来取代他们。

投票用户需要质押相应的代币才可以进行投票，实行 1 币 1 票制，质押代币一个月后自动解锁，在质押期间投票用户可以设置投票固定的节点选举者。

现有区块链项目的主要共识机制为 PoW (Proof Of Work, 工作量证明机制) 和 PoS (Proof of Stake, 股份证明机制)，少部分项目采用修改后的 BFT(拜占庭容错) 的共识机制。比特币就是 PoW 机制下最成功的加密货币，PoW 机制虽然已经成功证明了其长期稳定和相对公平，但效率相对低下，以比特币为例，每秒只能处理约 6 笔交易而且还需要消耗大量的能源，不太满足成为基础链的高性能要求；而 PoS 机制下较为成熟的数字货币是 Peercoin(点点币)，相对于 PoW，引入了“币天”这个概念来参与随机运算，由于可能会存在少量大户持有整个网络中大多数代币的情况，整个网络有可能会随着运行时间的增长而越来越趋向于中心化，PoS 机制虽然节省了能源，却也没有很好提升性能和安全性。

为了在保障安全性、去中心化的基础上实现性能的提升，DPoS 机制应声而出。这些值得信任的节点来代替全网持币人行使权力，出块节点要求长期在线，从而解决了因为 PoS 签署区块人不是经常在线而可能导致的产块延误等一系列问题。

DPoS 机制通常能达到万次每秒的交易速度，在网络延迟低的情况下可以达到十万次每秒级别，TAF Chain 在使用 DPoS 共识机制后，同时通过对技术底层的革新，每秒交易速度预估可以达到十万 TPS，这将完全支撑起现代社会的各类应用以及企业应用。

3.2.2. 智能合约及虚拟机

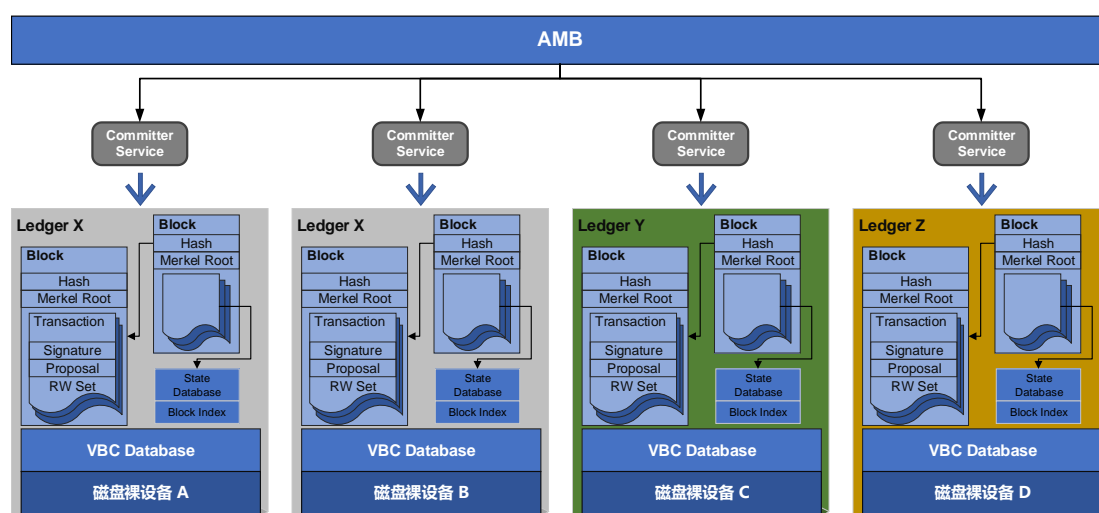
作为区块链的重要模块，智能合约在生态中扮演重要的角色。用户通过智能合约可以发行各种数字资产，也可以实现复杂的业务逻辑。

我们的 1.0 版本预计将协议层和通用性较多的数百种种合约都写成了内置合约。这些合约都是 HardCode(硬编码) 在链上的，开发者可以按照合约的接口参数进行调用。

主链将采用自研的高效合约机，开发者可以运用自己熟悉的编程语言编写智能合约，为了降低开发者编写智能合约的门槛，借助 TAF Chain 内置的编译工具，目前支持 C++、JAVA、Python、GO、JS 等主流编程开发语言。

3.2.3. 高效储能技术

TAF Chain 链存储系统，默认支持微服务化，可通过简单的配置后，添加机器的方式实现扩容，如下图分布式存储所示。



分布式存储体系结构，带来的好处在于其可以通过多台服务器分摊存储负荷，利用位置服务器定位存储信息。

它不但提高了系统的可靠性、可用性和存储效率，还易于扩展，将通用硬件引入的不稳定性因素降低到最低。主要有以下几个优点：

一、 高性能

分布式存储系统，具有高性能的读缓存和写缓存，并且支持自动的分级存储。它通过将热点区域内数据映射到高速存储中，来提高系统响应的速度。一旦这些区域不再是热点，那么存储系统会将他们从高速存储中移出。另外，写缓存技术则可以配合高速存储来明显改变整体的存储性能。按照事先约定的策略，先将数据写入到高速存储，再在适当的时间把数据同步存盘。

二、支持分级存储

由于采用的是微服务化，松耦合方式链接，分布式存储系统允许高速存储和低速存储分开部署，或者采用混搭的方式部署。在不可预测的业务环境或敏捷应用情况下，分层存储的巨大优势可以发挥到最佳。有效解决了当性能池读不命中后，从冷池提取数据的粒度太大，导致延迟高的问题。解决了目前区块链存储性能低下的瓶颈。

三、多副本一致性

与传统的存储架构使用 RAID 模式来保证数据的可靠性不同，分布式存储系统采用了多副本备份机制。在数据存储之前，系统先对数据进行了分片，分片后的数据按照一定的规则存储在了集群的节点上。为了保证多个数据副本之间的一致性，这里采用的是一个副本写入，多个副本读取的强一致性技术，使用镜像、条带、分布式校验等方式满足租户对于可靠性不同的需求。而多个副本之间的交叉保护也尤为重要，在一个副本出错的时候，系统可以通过从其他副本读取数据，重新写入该副本进行恢复。这样可以有效保护业务系统数据的可靠性。

3.2.4. 跨链与侧链

为应对未来的庞大业务量对底层区块链系统的性能挑战，TAF Chain 将采用侧链协同技术，将各类业务的核心功能放置于专用的侧链，保持主链作为基础数据、智能合约和基础 Token 交易的承载，将复杂的应用处理分布到各条侧链，从而提升系统的整体性能。

同时，TAF Chain 将采用适当的跨链协同机制有效保证内部各条并行链之间，以及与其他公链之间的共识和价值的有效和可靠传递。

3.3. 区块链浏览器

TAF Chain 将搭建与主链配合工作的区块链浏览器，以提供各类区块链信息的检索和使用，主要功能包括：

- (1) 交易总量、交易总额以及总手续费等信息；
- (2) 提供区块信息的展示，包括块、交易概要和详细信息；
- (3) 提供基于区块高度、区块 hash、交易 hash、地址的查询功能；
- (4) 支持新货币的快速接入；

3.4. 钱包

我们将配套与主链配合工作的钱包软件，用于链上账户及资产管理，并向第三方开放 API 及文

档，功能特性包括：

- (1) 提供多系统电脑客户端、Web、移动版图形化钱包程序。
- (2) 支持多账户。
- (3) 支持 TAF Chain 上所有应用独立资产，并支持多种链上资产。
- (4) 具备转账，收款，导入导出等基本功能。
- (5) 易于使用的 API 及文档，方便应用层开发。
- (6) 提供密码保护钱包的私钥。
- (7) 交易历史查询和账户管理功能。
- (8) 提供文本地址及二维码地址，快速复制粘或到处。

后期也将规划行情功能、实时查询全球的数字交易行情和相关资讯，同时也可以作为一个去中心化的交易所，实现币币交易。

3.5. API 及 SDK

系统将提供一整套完善的 API 及 SDK，用于身份创建、Token 创建、智能合约、跨链交互、可信数据、可信存储等场景进行调用。

SDK 可支持主流编程开发语言，如 Golang，C++，js，Python 等主流开发编程语言。

3.6. 特色

3.6.1. 高性能、高并发、低延时

基于DPOS共识算法进行深度优化，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，实现了毫秒级确认交易，完全优化后理论达到十万TPS/秒。

3.6.2. 安全保护机制

支持多种主流的隐私保护及安全机制，多方位多渠道构建安全体系，让企业及个人用户在实际应用中兼顾安全和隐私，包含但不限于以下：

- (1) 支持 ECC 公私钥对及国密算法。
- (2) 引入分层加解密技术，降低密钥被泄露和破解的可能性。
- (3) 采用高度的散列和摘要算法来保证用户地址的合法性。
- (4) 采用安全多方计算、零知识证明保证数据的机密性。
- (5) 运用环签名、群签名机制保证身份隐私。

3.6.3. 支持动态参数

TAF Chain 不需要分叉就可以动态调整系统全局参数，治理理事会可以发起提案投票决定来升级共识算法，及相关的参数。通过提案及投票机制，用户也是可以升级或修改区块链运行参数的，如块大小、交易大小、出块时间等参数。

3.6.4. 开发者友好

我们会建设一整套的辅助工具，用于服务用户、社区和团队，保证整个生态的健康持续发展。

同时有丰富的 API 和内置开发运行环境及完善的多语言开发文档，欲将打造资源齐备的开发者平台，实现对开发者从入门、发布、商用的全流程支持。

3.6.5. 交易免手续费

在 TAF Chain 上进行转账本身是完全免费的，所有的手续费均由每年增发的代币支付，仅开发者在调用合约等需要占用系统资源时需要持有代币冻结。

3.6.6. 便捷数字资产发行

TAF Chain 上有极简的数字资产发行流程和标准，允许开发者自由发行和流通基于 TAF Chain 的数字资产。

第四章 商业场景

4.1. 普惠金融

金融领域是区块链技术最早落地的领域，最早比特币的出现就是期望解决传统货币体系的一些顽疾。

在传统金融领域中，以资产证券化、产业链金融、国内信用证、福费廷等，区块链探索应用已处于核心环节。从多家银行披露的 2019 年年报来看，“区块链”技术这个数年前被众多银行等金融机构竞相布局的金融新科技，正逐步从 POC 验证性测试阶段走向应用阶段。区块链技术同时服务着越来越广泛的金融领域，如互联网借贷、稳定币、去中心化交易协议、金融衍生市场/预测市场、资产组合协议、KYC/反洗钱/身份协议等。

TAF Chain 分布式数据存储、TPS 吞吐能力等技术突破，解决当下金融中的基础问题。数据是金融应用的核心，大部分的金融产品都是围绕数据进行的，链上数据的不可篡改、公开透明、高效传输更好的保证了金融模型中输入数据。智能合约的完备、数据传输的安全性保证了金融场景的开放应用，提供了信任基础。

4.2. 游戏市场

游戏行业市场规模巨大并且与区块链以及 Token 经济有着天然的结合。

游戏行业过去 20 年作为一个朝阳行业保持了高速增长，《2019 年中国游戏产业报告》中显示，2019 年中国游戏市场实际销售收入 2308.8 亿元，同比增长 7.7%；中国游戏用户规模达到 6.4 亿人，同比增长 2.5%。其中，2019 年国内移动游戏市场的实际销售收入达到了 1513.7 亿元，

比 2018 年同比增长了 13.0%。但是目前的游戏行业从业者也面对了重重的困境。游戏用户红利衰减，大部分游戏生命周期短，除少数头部游戏外，付费率和 ARPU 的提升空间很小。此外，寡头集中度持续提高，中小游戏厂商生存困难。

而区块链的发展，则给了游戏行业从业者一个机会去突破困境，如区块链游戏云撸猫 CryptoKitties (CK) 在 17 年 11 月底横空出世，短短几周的时间，吸引了全球的关注。一方面，区块链形成了全球分布的高净值用户群体，为游戏 ARPU 提供了更多的挖掘空间；另一方面，区块链行业发展尚处于初期，对于新进入者是一个机会更加公平的市场。同时，Token 经济能给游戏参与者更强的激励和项目参与感。区块链游戏将是一个全球化的新市场，有着优质的用户群，给新进入的游戏厂商一个公平的起点。

截止目前，具 Dappradar 上显示已有的区块链游戏 DAPP 已到达 628 个，但大部分游戏玩法单一，场景简单。经常相信 TAF Chain 极度便捷的 Token 系统，完备的智能合约，突破业界水平的交易吞吐能力，综合性能等都是区块链游戏及娱乐最好的催化剂，能够让当前的区块链游戏有条件去创造更多的可能性。

4.3. 社交平台

我们生存的时代是一个以信息和数据为中心的时代，大众对社交媒体的依赖渐进增强，同时，社交带给大众信息安全的威胁也在日益上升。社交对用户有着强大的吸引力，也是绝大部分用户的刚需，这促使社交网络成为了互联网时代最基础和最重要的应用之一。

在传统互联网社交领域中存在哪些弊端呢？总结一下主要存在这 3 个方面：

一、 知识产权无法保证

用户在社交平台上发布的文章、图片等原创内容被免费转载，其所有的行为都无法得到相应的利益回报，长此以往，社交平台上内容的质量其实是会逐步下降的。

二、 被剥削的言论自由

用户在社交平台上发布的東西其实是收到平台的监管的，当发布内容损害到某方的利益或者影响到某方的形象时，哪怕内容时真实可信的，也会当即被“公关”。

三、 信息造假

在互联网上，因为信息的不对称，伪造成本太低，所以在如社交平台、婚恋网站中诈骗案件层出不穷。同时因为隐私无法保护顾虑也导致大多数用户需要上传真实数据时止步，这也陷入一个恶性循环。

而在 TAF Chain 能较好的解决现有基于互联网的社交网络的一些痛点。TAF Chain 改善了社交平台盘剥内容创作者收益的问题，通过 Token 的激励机制，创作内容和贡献算力的用户都可以获得奖励。用户也可以自行创建频道，获得内容创作的收益；用户可以言论自由，不受到平台的影响。

其实，在互联网社交平台，用户发布的言论是受到平台的监管的，网络匿名的形式反而催生网络暴力和虚假的东西，用户失去了信任，也就无所谓社交了，在 TAF Chain 中基于点对点的沟通方式，去中心化的网络结构存在不可篡改的特性，同时加密去中心化保护用户隐私数据，能够确保建立这种信任，当运用到社交平台后能够重新建立人与人之间的信用体系。

4.4. 数据权益

现有的互联网世界中，个人数据得不到很好的保护，如数据被盗、黑市泛滥、数据所有权错误归属等，个人数据安全问题频发，50% 以上的世界 500 强公司都出过数据泄露、黑客攻击等数

据安全问题。各大互联网巨头以及数据黑市商通过数据的加工和交易将数据产生的价值占为己有,我们在各类平台的信息往往会被卖给其它公司,例如当年的facebook事件, Facebook “泄露”几千万用户的信息事件后,市值已跌去 20%多,这不论是对用户还是对企业都是一个惨痛的教训。

未来,各类企业都可以通过 TAF Chain 利用分布式网络来取代集中式的数据服务器群,将用户的关键隐私数据进行加密,并以公开的形式在区块链上进行保护,也无法让黑客通过后门进行获取,这无疑将革新现有的数据权益机制。

4.5. 更多场景

基于 TAF Chain 的特性可以在更多商业领域提供支持,如在医疗健康领域、电子合同领域、广告领域等,我们也期待那一天的到来。

第五章 经济模型

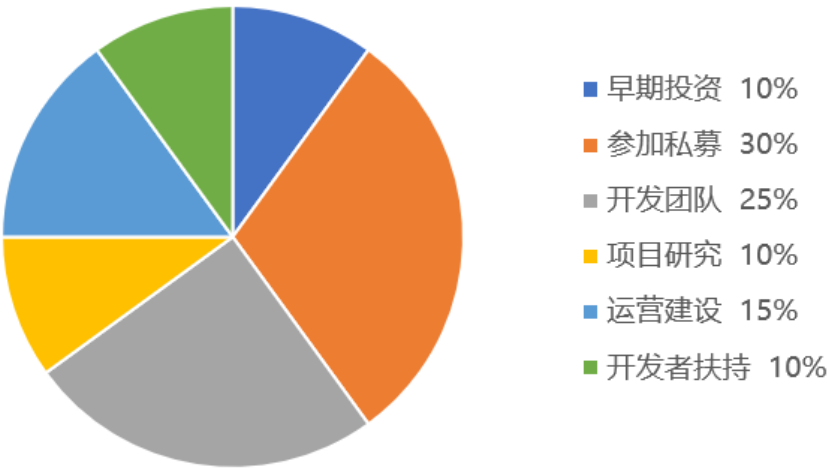
TAF Token 是 TAF Chain 上的核心资产，是生态内构建的基础虚拟流通加密通证权益证明，具体的Token 经济模型如下：



5.1. Token 经济

5.1.1. 首次发行

根据公链项目在产品开发，技术人才引进，社区建设多个方面的实际进展需求，为了更好的建设社区生态基础的目标，发行总量 60-100 亿个 TAF Token，分配如下，具体以全球发售的白皮书规定的为准。



- (1) 早期投资 10%，早期投资者，可以在初始发售时获得一定数额的回报；
- (2) 参加私募 30%，首次发行代币时申购的投资人按照投资额进行奖励；
- (3) 开发团队 25%，用以回报 TAF Chain 的创始团队，支付他们前期的巨大投入以及未来的工资；
- (4) 项目研究 10%，未来对一些更加先进的技术研究及引入，都需要巨大的投入；
- (5) 运营建设 15%，社区建设做出贡献者奖励；日常进行宣传、品牌营销经费；举办比赛奖励；公众号等社交活动奖励；
- (6) 开发者扶持计划 10%，鼓励及支持参与 TAF Chain 生态建设的开发者进行一定的 Token 支持，定期对有出彩表现的应用进行大额的奖励；

5.1.2. 出块奖励

在 TAF Chain 中，每生产一个区块，那么系统都会奖励区块生产者一定数额的 Token，这部分的 Token 由系统每年增发补充。

5.1.3. 社区贡献

TAF Chain 将会上线自己的官方社区，并会开通多类社交渠道，如 FB、TW、Wechat、Telegram、公众号、微博等。

在社区活跃并作出贡献的用户，如踊跃进行社区内交流、发现 bug 并提交管理者、积极参加官方活动等用户，都将受到高额的 Token 奖励。

5.1.4. 活动奖励

为了保持前期生态的活跃性及提高各类群体的积极参度，TAF Chain 不定期举办各类线上线下活动，用户可以通过活动获取丰厚的 Token 奖励。

5.1.5. 开发者扶持计划

凡是在 TAF Chain 中进行建设，应用搭建，丰富公链内应用生态的开发者，都将会得到一定的开发扶持基金。扶持积极额度不固定，由治理委员会成员共同决议。

对于那些优秀应用，将在社区投票，每年选出前三名，将获得 TAF Chain 给予的专项奖励。

5.2. 权益价值

5.2.1. 治理委员会

治理委员会是 TAF Chain 的决策机构，负责整个生态的健康运转。

委员会名单不固定，每年选举一次。

治理委员会的主要职责包括：

- (1) 各类重大事件及临时事件投票；
- (2) 年度运营建设预算方案及审定；
- (3) 年度项目研究预算方案及审定；
- (4) 开发者扶持计划变更提议及审定；

5.2.2. 节点投票

TAF Token 在生态中最终要的作用就是用作超级节点的投票，机制采用一币一票制，全体的持币用户都可以成为投票人，用户投票时需要将自己的 TAF Token 进行质押，如果资产转出，则视为撤票。

5.2.3. 重要参数修改

在公链系统中，存在一些影响生态运行的重要参数，这些参数的修改权交给全体持币用户进行投票确定，通过合约自动执行。

5.3. 生态价值

5.2.4. 开发资源使用

在 TAF Chain 中进行开发资源调用需要依托 TAF Chain 进行，其中资源调用包含以下几个方面：

- (1) 创建开发者账户，创建 Dapp；
- (2) 升级账号；
- (3) 部署智能合约，调用智能合约；
- (4) 调用底层服务；
- (5) 发行自有的数字资产；
- (6) 发起转账交易
- (7) 使用生态内的各类基础设施

5.2.5. 应用内结算

基于 TAF Chain 的 DApps, 都支持 TAF Token 作为底层的支付与结算

5.2.6. 流通交易

TAF Token 本身的稀缺性以及强应用需求支撑了巨大的生态内流通价值, 在未来将释放巨大的能量, 对于 TAF Chain 生态看好的长期持有者, 将能够得到丰厚的价值回报。

第六章 研发线路图

截至当前已有包括创始团队在内的一批核心研发力量，并在持续地扩充。考虑到初期的研发力量尚显薄弱，生态内商家和用户数量也是个逐步放大的过程，为了尽早建成 MVP（Minimum Viable Product，最小化可行产品），以快速推进和迭代优化 TAF Chain 基础设施和应用生态，持续做大做强社区，研发团队将采取分阶段逐步建设的研发方式。

在初期团队的主要研发精力将聚焦在 TAF Chain 公链底层设施的研发上，上层应用生态初期将在区块链核心技术基础上以半去中心化方式构建和运营，并随着社区生态力量的发展和增强，逐步地自我迭代演进为完全去中心化的形态。为了做到研发过程的公开、透明，研发团队将在项目代码托管 Github 上以周报的方式持续地更新研发工作相关的各项进展情况，让社区成员能够及时地获取信息。





后记与声明



本白皮书基于技术、权益、激励打造了完整的高效信任生态。

但信任生态的建立，尤其在现有的公链市场中，也是一项庞大而艰巨的任务。所以，我们希望各类伙伴的加入，我们欢迎开发者、社区志愿者、商业伙伴能够为了这份伟大的事业贡献自己的力量。

同时，TAF Chain 也希望通过生态合作伙伴的共同努力，把信任带到所有人的身边，让信任能够赋能新的区块链改革，造福人类。



TAF Token 是平台生态内重要流通的数字价值，并不是一种投资品。拥有 TAF Token 不代表授予其拥有者对公链平台的所有权、控制权、决策权。

TAF Token 作为一种数字加密货币不属于以下类别：

- (1) 任何种类的货币；
- (2) 证券；
- (3) 法律实体的股权；
- (4) 股票、债券、票据、认股权证、证书或其他授与任何权利的文书。

TAF Token 的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何价值，团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。

