星图 XT

全球社区用户共建自治的去中心化金融综合生态系统

XT DAO • 2022

前言

新一轮科技革命带来了人工智能、大数据等创新技术广泛应用，催生了一大批金融科技新业态。其中，以区块链技术为代表的新型互联网底层技术，则为行业带来了颠覆式影响。

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。具体而言，区块链技术利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

以比特币为代表的区块链 1.0 和以以太坊为代表的区块链 2.0 技术的成熟，使得区块链已经走出了概念性阶段，接下来将会跨入区块链 3.0 时代，区块链 3.0 是超越货币、金融范围的区块链应用，它将会和各个行业的实际应用契合起来，让用户能切身感受到区块链的真正价值。

我们认为，与传统技术相比，区块链技术有着去中心化分布式存储、不可篡改、点对点传输、共识机制、智能合约等特点，这些特点与多元金融应用具有较高的契合度。不仅如此，随着以太坊智能合约的推出，2018 出现了 DeFi（去中心化金融）的概念，即分布式金融的概念。DeFi 的意义在于它有通过合约构建金融场景的能力，通过智能合约人们可以完成无须中间人参与的金融服务，比如借贷、稳定币、代币交易、衍生品交易、保险、预测等。它呈现出跟之前完成不同的金融服务特征。比如它有不可篡改和透明账本，非人为控制的合约，即使是合约的开发者，协议的开发者，也无法控制合约的运行，这是一个全新的金融生态，有很多可能性。

区块链发展到今天，各类应用都在探索中，但现有区块链基础设施普遍存在的实用化程度较低，尤其是交易拥堵、交易费高、交易确认时间长、抗量子攻击能力较弱、通信层节点匿名性不高、交易匿名保护、跨链通信和多链融合能力较弱、存储空间较大等问题。

因此，我们在此提出一种解决方案——XT 基于区块链 3.0 架构而研发的去中心化区块链基础设施，全球社区用户共建自治的去中心化金融综合生态系统。旨在为 DeFi 生态提供基础底层支撑，为广大用户提供更高效的创新型数字金融应用。通过 XT 的底层支持，优化提升区块链技术在各个层面的协议和机制，实现价值传输网络各层次的支撑协议。进而使应用生态和数字资产在公平、公正、公开、安全、高效、稳定的交易环境下交易，防止交易平台依靠有利优势篡改伪造数据、不执行交易结果等行为。

未来，随着 XT 在多元场景的应用，如：跨链桥、swap、稳定币、NFT、金融衍生品等，将为行业带来更多积极影响。为让更多人了解项目的价值，本白皮书将详细介绍 XT 的

诞生背景、区块链解决方案、产品架构、技术特色与优势、应用生态、XT 代币的发行以及顶级团队实力、未来发展规划等。XT 致力于打造价值互联网时代的顶级区块链解决方案，开发高性能、高可扩展的 DeFi 区块链基础服务平台，快速构建上层应用业务，满足大规模用户数量的应用场景。并以去中心化信任为核心，构建新一代价值通证流通网络，让数字资产价值与实体经济价值相结合，驱动价值的全球自由流动。

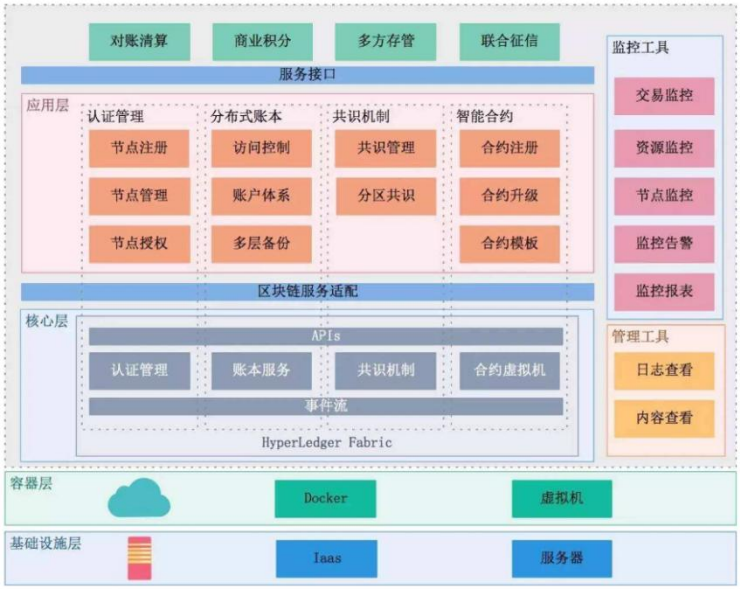
目录

第一章 区块链技术的发展

随着数字货币的流行，作为背后基础技术的区块链逐渐走入大众视野。区块链技术也已经经历过多个发展阶段。本章我们将从区块链基础理论、发展历程和发展趋势进行分析，让用户真正了解到 XT 诞生的背景，从而对其价值有更深入的理解。

1.1 区块链技术概述

区块链（Block chain）是一个分布式账本，一种通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案，是最具体革命性的新兴技术之一。区块链本质上是一个去中心化的分布式账本数据库，其价值在于通过构建自组织网络，使用密码学相关联算法所产生的一串数据块，时间有序不可篡改，每一个数据块中包含了多次交易有效确认的信息，由此建立分布式共识机制，从而实现去中心化信任体系。作为底层构架技术的区块链，利用去中心化、不可伪造、公开透明、分布式记账、不可篡改、智能合约等特点，向世人展示了一种不需要中介却可以实现价值传递的可能。



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。

因此，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（或去中心化）”，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。

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。

1.2 区块链的设计思想

价值交互的基础是双方信任的建立。区块链技术的革命性在于它实现了一种全新的信任方式，通过在技术层面的设计创新，使得价值交互过程中人与人的信任关系能够转换为人与技术的信任，甚至于由程序自动化执行某些环节，商业活动得以更低成本的实现。

1）经济层面的设计思想

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“弱中心化或去中心化”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。

2）技术层面的设计思想

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。

1.3 区块链发展历程

2009 年，第一枚比特币面世至今，区块链技术历经十余年的发展，从基于程序算法的 1.0 数字现金时代（或称数字货币时代）、基于智能合约的 2.0 数字代币时代、基于区块链的 3.0 应用时代。

1）数字货币时代

区块链 1.0 时代，是以比特币为代表的“数字现金”时代。其可编程的数字货币的应用场景包括支付、流通等货币职能。

中本聪于 2008 年 11 月发表了名为《比特币：点对点的电子现金系统》的著名论文，正式提出一种完全通过点对点技术实现的电子现金系统。其核心内容是基于密码学原理而不基于第三方信用，使得在线支付能够直接由一方发起并支付给另外一方，中间免去中介/第三方金融机构。次年一月，中本聪又通过使用自己写的第一版软件挖掘出了创始区块， 其包含了一句不可修改的语句，“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks (2009 年 1 月 3 日，财政大臣正站在第二轮救助银行业的边缘）”。这正式启动了比特币为代表的区块链 1.0 时代，即数字现金时代。

区块链 1.0 时代首次通过区块链技术，利用时间戳、公开透明和不可篡改等特点解决了电子现金的点对点支付问题，但其基于 POW 共识机制，需要进行大量低价值的挖矿软件运算，消耗巨大的能源，且存在无法处理大量交易和扩展性差的瓶颈。

2）数字代币时代

区块链 2.0 时代，是以“以太坊”为代表的基于智能合约的“可编程金融”时代。

2014 年 1 月 23 日 Vitalik Buterin 发表了《以太坊：下一代加密货币和去中心化应用平台》的白皮书，并一直致力于将以太坊打造成最佳智能合约平台。通过其专用加密货币合约（Ether，又称“以太币”）提供去中心化的虚拟机（称为“以太虚拟机”Ethereum Virtual Machine）来处理点对点的合约。

区块链 2.0 以太坊 ETH 为代表的公共区块链平台解决了比特币的扩展性不足的问题，同时基于智能合约，大量的数字代币（token） 基于以太坊发行。但区块链 2.0 公链技术吞吐量只能达到每秒千次量级，无法支持大规模实时交易应用，极易拥堵，并推高手续费，这成为制约区块链在产业中大规模商用的主要原因。

3）区块链生态应用时代

区块链 3.0 是指区块链在金融行业之外的各行业的应用场景。能够满足更加复杂的商业逻辑。区块链 3.0 被称为互联网技术之后的新一代技术创新，足以推动更大的产业改革。

区块链 3.0 涉及生活的方方面面，所以区块链 3.0 将更加的具有实用性,赋能各行业。不再依赖于第三方或某机构获取信任与建立信用，能够通过实现信任的方式提高整体系统的工作效率。

也可以说,区块链 1.0 是区块链技术的萌芽,区块链 2.0 是区块链在金融,智能合约方向的技术落地，而区块链 3.0 是为了解决各行各业的互信问题与数据传递安全性的技术落地与实现。

基于 Hashgraph 数据结构的区块链 3.0 技术逐步受到业界的关注，基于该数据结构实

现的 POC 共识算法可在交易吞吐量、可扩展性上实现质的飞跃，POC 及其变种算法可以解决 PoW 算法一直被诟病的浪费算力问题，从而进一步支撑区块链作为某个行业的基础设施，并形成基于区块链的完善生态体系，将广泛而深刻地改变人们的生活方式。

进入区块链 3.0 时代，区块链技术正在促进行业大发展。行业市场对区块链底层技术平台的技术需求和区块链应用场景实现的服务需求，我们有巨大的信心。

总结而言：

• 区块链技术解决的核心问题是信任成本与数据安全，区块链具有不可篡改的特性，而认证和知识产权领域的核心需求完全符合这些特性，因此具有巨大的市场。

• 目前纵观全球范围，基于区块链的底层应用技术平台并可提供低门槛上链及定制化区块链服务的混合型产品寥寥无几。真正实现规模化商业落地的更是一片空白。市场定位仍处于高技术门槛的卖家市场。

• 很多服务商和政府部门都看到了区块链背后的强大潜力，认识到区块链的技术以及落地后的商业性可以帮助企业理清思绪、开发潜能。但由于拥有的资源和技术有限，区块链企业化应用和开发周期长。市场有对区块链快速上链和应用，并在不断变化的规范和持续涌现的机遇中实现最大获利的显性需求。

• 区块链底层技术相对于应用开发层更被资本看好。现在区块链 3.0 发展还处于初始期，整个标准和协议架构还处于开发完善阶段，此刻技术周期和发展阶段决定了创投资本和金融资源将更倾向于底层技术并自然流入。

1.4 区块链应用发展趋势

进入 2020 年之后，疫情倒逼全球各国和各行业的数字化进程加速，进而推动互联网服

务也进一步升级：不仅要满足个人用户的日常生活需求，更要逐渐满足包括企业在内的商业机构和大量公共部门的工作需要，即需从消费互联网发展到产业互联网。而产业互联网的发展，对相关信息基础设施的可信、开放、敏捷、协作等能力的要求随之提高，并要求数据等生产要素能更合理地流动和配置。由于区块链恰好具备解决以上一系列难题的架构和方案，因此被寄予厚望，产业区块链的时代也渐渐拉开序幕。2020 年以来，基于疫情带来的数字化发展思考、以及全球央行数字货币探索的推进，各国政府纷纷加强了对区块链技术的战略部署。

今年，尽管在疫情导致企业整体 IT 支出削减和全球经济趋缓的不利前提下，区块链市场支出的幅度仍然较高。根据 IDC 发布的《全球区块链支出指南 2020》（Worldwide Blockchain SpendingGuide, 2020V1）报告指出：2020 年全球区块链市场整体支出（仅统计联盟链或分布式账本技术支出，已剔除虚拟货币相关支出）达到 42.8 亿美元，亚太地区的五年复合年增长率（CAGR）为 55.3%，全球为 57.1%，到 2023 年，全球支出将达到 144 亿美元；分行业支出来看，金融行业在区块链解决方案上的投入是最大的，但制造业和资源行业在 2018-23 年期间的增长速度将最快，五年复合年增长率为 60.5%；具体的应用方场景向则集中在跨境支付和清结算、贸易融资、交易后结算和监管合规等方面。

区块链作为通用型的信息技术，是多类细分技术的组合，因此涉及到的生态体系较为庞大，上游包括芯片、一体机、基础设施网络等，中游则是创新的核心，主要包括的区块链平台、中间件、安全配套服务；下游的应用行业与场景更是普适，基本覆盖国计民生的所有行业。

从各大区块链云服务平台下一步的技术攻关方向来看，共识机制以及区块链单链性能方面的优化已接近完善，未来预计将在隐私保护算法、跨链技术、多链并行计算技术、分布式存储、分布式数字身份等更广泛的细分技术方面继续突破。

进入 2021 年，区块链发展迎来新趋势与新机遇。当前，传统商业模式如果要解放数据要素的生产力，就需要解决三个非常核心的问题：一是需要提供安全存储的解决方案，二是要提供可信传输的一些手段，三是需要提供一个协同生产的机制。因此，2021 年区块链的重要趋势和使命之一，就是如何通过对自身技术能力的挖掘发挥，以及如何与其他前沿科技进行深度融合，以便够有效攻克以上三个数据要素需要突破的问题，实现数据要素的产权可以被界定，价值可以被存储，同时这些价值也能够被评估，以及可以有效地流通，最终真正能够实现数据生产力的全面解放。

第二章 DeFi 去中心化金融市场

2.1 区块链与 DeFi 模式的融合

在区块链技术的支撑下，金融产业形态有了更多的创新可能性。其中，DeFi 就是较为典型的模式。DeFi 的全称是 Decentralized Finance—去中心化金融。DeFi 是指基于数字货币或者 Token 进行的金融行为和服务。例如基于 token 的借贷服务、交易所、支付、保险、投资甚至理财等服务。其中，基于以太坊的 DeFi 服务和产品在当前阶段最为繁荣。广义的 DeFi，是指围绕去中心化技术为基础来构建的金融业务和服务。广义的 DeFi 它包括两层含义：业务和服务完全基于去中心化技术进行构建。例如基于区块链去中心化技术和智能合约的抵押、交易、贷款等。服务本身不是去中心化的技术的，但是服务的对象，是基于去中心化技术的数字资产等对象。例如数字货币交易所等。

这些金融业务和服务，可以是已有的传统金融业务的升级，采用去中心化技术进行了重构；也可以是全新的金融服务，例如基于数字货币的交易和其他金融行为等。

对于金融行业来说，DeFi 是一个非常重要的方向。因为去中心化的运作模式能够极大降低金融运作的成本。而且在运作的过程中能够消除行业中存在的信息不对称，让整个金融行业变得公开透明。例如，传统的借贷领域有着这样那样的缺陷，比如抵押纯在欺诈现象，或者抵押出现多重抵押的现象。又比如催贷、断贷。事实上在传统的借贷领域有着许许多多不透明环节。去中心化金融的意义在于，透明并且不可逆。当贷款者发起一笔贷款的时候，只要抵押物价值符合要求，便不会遭受来自传统机构的贷款崔收压力，也不会受到断贷的威胁，因为去中心化金融是合约自动执行，从而杜绝了人性方面的干扰，可以很好的保护贷款者的权益。

虽然一开始 DeFi 领域的借贷资产标的仅仅是数字货币、稳定币，但随着技术的发展，其正在向更多可能的价值空间延伸。

2020 年和 2021 年，是去中心化金融（DeFi）的大热之年，各类项目纷纷上线。DeFi 的应用方向众多，包括去中心化交易所、借贷平台、稳定币等等，目前市场上已经围绕这些应用方向出现了上百个 DeFi 项目。DeFi 借贷龙头 Compound 通过用 COMP 代币来吸引用户参与存贷，一个月内资金沉淀量飞增 10 倍，COMP 估值高企，拉开 DeFi 的狂欢序幕。在这之后，DeFi 新概念层出不穷，借贷平台、去中心化交易所、去中心化自治组织、稳定币、预言机不断涌现，优秀的 DeFi 项目纷纷利用 token 流动性挖矿实现用户冷启动。

这让 DeFi 成为区块链生态系统中发展最快的领域之一，目前总体锁仓量超过 50 亿美元。在 DeFi 众多业务领域中，最引人注目的三大方向为稳定币、去中心化交易所和借贷业务。其中，DeFi 借贷业务的发展尤为迅速。

2.2 DeFi 的价值核心

DeFi 利用智能合约让数字资产在区块链网络中重建传统金融秩序，并且互相产生协同效应。与 CeFi（Centralized Finance）中心化金融对应，DeFi 去中心化金融具有代码中立开源，去中心化运行，无中心化监管，去中心化自治等特质：

• 代码中立开源：指区块链上运行的 DeFi 项目在区块链网络中公开运行，且代码开源。每一笔智能合约交互和开源的代码随时可以在区块浏览。

• 器上公开查阅：链上的主流项目代码经过代码审计公司审计，避免出现后门，bug 等恶性事件影响系统健康运行。大部分的传统互联网应用的代码不是全面开源的。

• 去中心化运行：指 DeFi 项目可以在区块链主网分布在全球的矿工节点中运行，而不像传统的互联网应用，需要在公司拥有的中心化服务器中运行。去中心化的区块链节点抗风险能力更强，只要全球还有矿机在为这条公链进行挖矿记账，区块网络就能够正常运行。

• 无中心化监管：区块链网络应用运行在无数个区块链节点上，项目上线主网不用经过中心化机构审查，使得创新更加自由，发展速度更快。无监管使得 DeFi 网络在短短半年间完成传统金融系统的链上重构，并且在原有基础上尝试各式各样的创新。另一方面，无中心化监管也使得投资者受到的保护更少，DeFi 网络在一次次黑客，漏洞等意外事件中以去中心化的组织形态逐渐成长。

• 去中心化自治（DAO，Decentralized Autonomous Organization）：大部分头部区块链网络应用都采用去中心化自治来进行项目的重大事项 和发展路径管理。任何社区成员都可以发起提案，持有数字资产的所有用户可以根据持仓量投票决定项目的发展方向。DAO 类似于 24 小时 365 天不间断，随时发起的股东大会。

DeFi 概念于 2014-2017 年开始兴起，2018-2019 年各种去中心化借贷等 DeFi 项目逐渐上线，2021 年 1 月随着比特币牛市吸引市场注意力后开始广泛流行。DeFi 锁仓量在 2021 年 04 月突破 800 亿美元。在 DeFi 网络中的数字资产存量在 4 月初期也突破 1010 亿美元，约占数字货币整体体量的 5%，且有进一步加速的趋势。

2.3 DeFi 主流应用场景

DeFi 利用智能合约让数字资产在区块链网络中重建传统金融秩序，并且互相产生协同效应。典型应用有利用数字资产进行的量化、做市、借贷、保险、swap、流动性挖矿、衍生品、机枪池、清算结算等等。

1）借贷

借贷平台的盈利模式为赚取借方与贷方的利息差，并且在项目初期通过项目方数字资产作为营销推广成本对存款方和借款方都进行数字资产补贴，培养用户使用习惯。DeFi 平台数字资产普遍具有分红平台利润+去中心化治理的功能。

• 双方利率由预言机（去中心化报价器）综合市场信息做出实时动态变化，通过调节利率达到供需平衡。利率收益以平台数字资产形式发放。

• 在由于数字资产价格波动，或拖欠利息导致质押率超过 60%时，贷方需要补充抵押物或归还部分贷出数字资产来把质押率降低到 60%以下。否则超出 60%的部分的对应抵押物会被清算智能合约清算。清算存在 5%的清算罚金。

在每一笔借贷成交时，平台抽走的手续费中一部分用于支付存款方利息，一部分留存成平台的盈余公积。平台的盈余公积一部分用于风险赔付准备金，在极端行情或黑客攻击下提供赔付；一部分用于激励团队；一部分用于回购平台币并销毁，造成平台币通缩，为价格提高产生基础。

2）Dex 去中心化交易所

Dex（Decentralized Exchange）去中心化交易所，与 Cex（Centralized Exchange）中心化交易所对应，去中心化交易所采用智能合约在公链上自动运行。用户可以在 Dex 中用进行数字资产兑换。以 cake 为例，每笔交易收取千 2 手续费，其中千 1.7 发放给做市商，万 3 作为平台盈余公积。

• Dex 作为中立平台，自身不提供做市所需数字资产，只提供做市的智能合约算法。

• 用户在平台存入等额的两种数字资产作为 LP（Liquidity Provider）做市商交易对，为平台提供做市所需的数字资产。作为回报，用户采取 LP 做市可以得到平台数字资产作为收益。LP 同时还作为能够兑换回存入数字资产的凭证。LP 在借贷平台还可以作为抵押物使用。

• 平台发放数字资产激励做市商来做市→交易盘口深度变好→交易滑点磨损降低→交易效率提高→更多人前来平台交易→平台手续费收入增加→用部分交易手续费回购平台数字资产→造成平台数字资产通缩→价格提高→激励做市商的奖励升值→循环。

3）聚合器

聚合器通过分析每个 Dex 的容量，把大单通过智能算法拆成多个小单，走多个平台，寻找最佳汇率，来降低交易中的磨损与滑点。不管是流动性挖矿、staking、借贷，还是 DEX 的 AMM，其本质上都是将代币存入存储池，然后赚取收益。这意味着，谁的收益更高，谁就有可能虹吸更多的代币。

现在吸引代币的有借贷、DEX、衍生品协议以及聚合器，最后还有各种代币自身的staking。这些协议之间看似所处领域不同，但本质上，它们存在一定程度的竞争关系。底层协议是产生收益的基础，聚合器则负责收益的优化，最终会达成均衡。从用户操作的角度，聚合器更符合其利益，更灵活，收益更优。

4）资产映射

资产映射，即将区块链外的资产通过预言机映射进区块链内，在数字资产市场中追踪股票、期货、交易所交易基金和其他传统金融资产价格。

例如：通过超额抵押美元稳定币 UST 来发行 m 合成资产。质押率最低为 150%，且与借贷智能合约类似，质押率低于 150%会被清算机器人清算。UST 美元稳定币通过销毁数字资产 Luna 发行。UST 美元稳定币通过套利行为锚定 1 美元价值。

在资产映射可以让普通用户绕过 KYC、AML、换汇、开户等流程，无需整股持有，无休市无涨跌幅熔断等限制，随时用数字资产双向兑换美股及传 统金融衍生品的映射数字资产。

5）机枪池

采用智能合约在不同的 Dex、借贷平台和其他能够生息的平台中不断帮助用户选择收益最高的投资方案，并自动帮助用户复投，取得最高收益。不同的 Dex 和借贷平台对于相同资产的利率是根据供需动态调节的，普通用户难以随时关注各个平台的各种数字资产的利率变化并频繁切换，机枪池提供了全自动托管资产的解决方案。

2.4 XT 的诞生

随着 DeFi 生态的日益发展，又出现了更多创新性加密货币资产，带动了 DeFi 2.0 的发展，优质项目也从提高资金利用效率角度提升了整个 DeFi 生态的脚步。

当下，对于市场而言，数字化转型已经成为必然，然而在转型之路上，受限于技术门槛、差异化需求等多重因素，仅凭一己之力显然无法推动整个数字化转型走向成功，必须通过结合实体产业链各方乃至跨行业伙伴之间的开放合作才可能实现共赢。如何在各方合作的基础上实施有效的管理，把资源的分工协作和统筹分配等内容做好合理的预案，构建一个成成本最低、效率最高、价值最大的发展模式，仍面临着诸多问题：

- 数据所有权的归属
- 信任缺失

- 链条复杂，资源、信息配置不对称

基于以上问题，XT 项目诞生，XT 通过创新的共识算法、主链——子链多链结构、主链——主链跨链结构、开发者友好的智能合约等核心技术，构建泛在价值流通的互联网基础设施和 DeFi 金融投资体系。

XT 通过打造创新型 DeFi 协议（XT 协议），综合运用密码学和区块链技术，在技术层面上支持去中心化的协会制治理能力，实现了区块链 Token 资产的可信、高效托管清算，进而解决了交易平台面临的核心问题，这种创新型的资产托管和清算技术，为加密货币市场带来了颠覆性创新，能够让用户的资产得到强于银行级的安全保障。

借助于协议的技术优势，XT 在打造相关平台时可以实现去中心化的安全可信，还能保持百万级交易并发的高性能。同时，采用超级节点与全球化托管和清算的底层区块链模型，具备传统金融级别的业务、技术和监管能力。用户的资产完全通过去中心化区块链技术实现托管和清算，提供个人、机构的加密数字货币资产透明化服务。而 XT 代币作为 XT 的生态激励侧链，在 DeFi 应用方面也具备更多价值依托，XT 将获得更具竞争优势和核心技术的基础支撑，为 DeFi 体系构建和商业百业支付的落地等应用奠定坚实基础。

第三章 XT 项目概述

3.1 XT 项目简介

星图 XT,简称 XT,XT 由全球顶尖的区块链、金融等领域人才打造,并以完全自治 XT DAO 社区为纽带，为全球社区用户共建自治的去中心化金融综合生态系统。一个基于区块链技术的全生态平台，依托强大的区块链底层应用技术和社区丰富的产品功能，XT 联合 FAR NFT 生态和 HALO Network 快速完成跨链桥、SWAP、稳定币、NFT、金融衍生品相关智能合约，让 XT 真正实现去中心化金融综合生态系统的应用价值。

XT 通过 DeFi 模式和 DAPP 应用等，解决传统金融领域和现有 DeFi 模式存在的诸多问题。同时，作为强大的开放金融协议构建的应用程序，XT 也会使金融企业能够在平台上得到最灵活的部署。

在技术方面，XT 依托 Halo network、FAR NFT ecosystem 的技术融合发展和支持，自主研发的底层公链技术架构，实现分布式账本结构、海量数据的差异化存储和 DeFi 分布式金融体系的构建。在底层技术的支持下，XT 将颠覆传统的金融运行架构，构建开放、创新的全球分布式商业与金融体系，建设完善的分布式金融基础设施，接入海量分布式金融应用，迅速链接广大用户群体，以流量赋能产品与生态，打破传统平台壁垒，降低经济损耗，优化利益链条，为智能金融的发展指明方向！

通过 XT 的应用实践，XT 的通证经济模型、主链 XT Chain、XT DeFi 生态、XT DAO 等将逐步在全球落地。此外，自治社区还将开发 XT DAPP 应用程序，为全球用户提供一个快捷、安全、可信任的 DeFi 和实体商业支付架构搭建的基础工具。通过建立不同区块链账本之间的连接，实现数字资产的跨账本转移、质押借贷等，为基于数字通证和数字资产的金融应用提供一个基础设施。将区块链承载价值和传递价值的功能发挥到极致，将区块链的平等、开放的理念发挥到极致，XT 将让亿万用户的资产更自由。

3.2 愿景与使命

XT 认为真正的资产自由是来自信息的隐私与安全，只有让资产以自己的意愿流动，并且永远处在安全的地方，才是真正的资产自由。区块链并不意味着标新立异，除了让资产更自由，同时要做到让体验更人性。

XT 愿景是：将把匿名的 DeFi 服务提供给所有人，让现代金融不再只是富人敛财的工具，而是成为平民通向财富自由的钥匙。

为了实现数字资产的最终自由，打造真正去中心化的分布式未来“数字金融服务生态

圈”，让区块链技术和数字资产应用能够更大范围的普及，根据对已有技术的调研，结合区块链去中心的特点和其应用场景考虑，XT 的使命如下：

1）跨链资产转移

能够连接现存的主要数字通证网络（如比特币、以太坊等），完成资产兑换的同时不改变原有链机制。新产生的数字通证网络也能以极低的成本接入到 XT 协议中。

联盟链性质的区块链网络能够接入 XT 的主链 XT chain 体系，实现资产由原有链转入 XT chain、由 XT chain 转回原有链、多种资产在 XT chain 上进行交易等功能。保证跨链交易资产的安全性以及跨链交易服务的稳定性。

2）提供交易的隐私保护

- 交易双方可以选择带隐私保护的交易。
- 能够为数字资产转移、交易提供隐私性保护。
- 能够为数字资产持有者提供匿名性保护。

3）具有场景的延展性

- 能够成为多种数字通证兑换的分布式平台。
- 能够开展不同数字货币的质押借贷业务。
- 能够以数字通证为媒介完成数字资产的交易。
- 能够发行和交易全新的数字金融资产。

3.3 XT Chain

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，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，都面临着很多挑战。

• 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 POW；

• POW 的共识机制很难被行业应用和大规模部署；

• 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；

• 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；

• 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；

• 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，很少有来自外界的触发条件，即缺乏与现实世界的交互。

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底层生态系统，作为未来世界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。因此，XT Chain 首先以公链的基础设施建设为目标，在解决现有区块链基础痛点的基础上，构建一个支撑多元应用生态的综合性平台，不断拓展区块链技术的应用边界和技术边界，并为全球用户提供全新的基于区块链技术的开发者和用户生态系统。

XT Chain 在共识算法进行了创新，建立在验证节点的网络上，极速出块时间能够为 DeFi 协议建立高速的基础设施。XT Chain 中的智能（smart）一词则体现在智能合约相关的功能上：XT Chain 支持智能合约编写功能，兼容现有的以太坊虚拟机 EVM（Ethereum Virtual Machine）以及其生态系统下的所有应用和工具，开发人员可以轻松实现以太坊 DApp 的迁移和部署，节省开发精力。最后，作为可以与其他链进行交互的并行链，XT Chain 原生支持跨链通讯和交易。

XT Chain 对现实的意义和必要性体现在如下几个方面：

1）智能合约

在上段中关于 XT Chain 的简单介绍中，借由 Smart 一词引出了 XT Chain 的智能合约的编写功能。功能各异的 DApp 是构成 DeFi 的生态的基本元素，而智能合约则代表了 DApp 的底层规则和运行逻辑。于此同时，可编程性也极大地增加了 XT Chain 的拓展性，实现 DApp 功能的多样化。因此，智能合约是建立 XT 生态“大厦”的基石。

2）兼容 EVM

XT Chain 兼容现有的以太坊虚拟机 EVM（Ethereum Virtual Machine）以及其生态系统下的所有应用和工具，极大地降低了开发人员 DApp 开发的门槛。开发人员可以轻松实现以太坊 DApp 的迁移和部署，节省开发精力。兼容 EVM 的意义在于可以最大程度上兼容目前最火的以太坊生态，吸引开发人员和以太坊上的溢出资金，对于新生的 DeFi 生态起步有明显的助力作用。

3）跨链功能

跨链的意义在于丰富 DeFi 生态的币种和增加流动性。XT Chain 将在 DeFi 应用场竞争实现流动性挖矿以及各类高算力挖矿，将实现 BTC、以太坊上的 ERC20（ETH、LINK、USDT、DAI 等）、XRP、BCH、LTC、DOT、EOS 等资产的跨链互通。这也就意味着这些资产都能迁移到 XT Chain 上，成为 DEFI 运行的流动性。

3.4 XT 的技术特点

为了实现对 DeFi 应用生态场景的更好的支持，XT 对区块链基础设施的各个层面均作了很大改进，在部分层面提出了突破性的创新。XT 主要技术创新包括：

• 在底层 P2P 网络节点通信层面，结合现有基于 Tor 的匿名通信网络、基于区块链的分布式 VPN 的优点实现了独创的匿 P2P 通信网络，设计实现了节点匿名接入的方法，并实现了私有加密的通信协议，极大地增强了底层通信网络中节点的匿名性，确保节点间通信难以被追踪和破解。

• 在底层数据结构层面，采用了新型数据结构，增强式的有向无环图（DAG）——哈希网（HashNet，HN），从而实现异步并行的事件共识验证，提升了系统的可扩展性。

• 在抗量子攻击层面，采用新型抗量子攻击密码算法，通过将 ECASDT 签名算法替换为基于整数格的 NTRUsign 签名算法，同时用 Keccak-512 哈希算法替换现有的 SHA 系列算法，降低了量子计算飞速发展和量子计算机逐步普及带来的威胁。

• 在匿名交易层面，结合现有加密虚拟货币的特性，通过一次密钥和环签名技术，设计了效费比极高和安全性极好的交易匿名和隐私保护方法，并支持零知识证明作为选择功能，满足不同应用场景隐私保护需求。

• 在智能合约层面，通过实现 EVM 的兼容，支持声明式非图灵完备智能合约和面向摩西（Moses）语言的高级图灵完备智能合约，优势在于较好的支持链下数据访问，支持第三方资产发行，能以更多形式落地到实际应用场景。

• 在跨链通信和多链融合层面，采用中继链技术将跨链通信和多链融合功能模块作为单独一层 Overlay 来实现，既能够保持跨链操作的独立性，又能够复用 XT 础链的各种功能。

• 在生态激励层面，综合使用 XT Token 激励模型和创新型挖矿机制，并支持挖矿用于生态激励。

• 在行业应用层面，通过流通支付、数据传输、数据搜索、合约调用等 JSON-RPC 行业通用接口的开发，支撑上层的各类应用。

第四章 XT 的应用生态示例

4.1 XT SWAP

XT SWAP 将在为全球用户搭建最安全、稳定、高效的数字货币价值网络，提供最优质的数字货币 AMM 服务。自主研发的撮合系统，能够每秒处理数百万笔交易。此外，为了满足用户多元化的需求，XT SWAP 不仅研发了先进的撮合系统，用于币币交易，同时也开放了安全、高效的 C2C 交易服务，为用户用区块链技术和通证经济模型，构建一个连续的、透明的、低摩擦的、无歧视的交易环境。

XT SWAP 在注重提高用户体验度的同时，还将不断升级平台技术、完善生态体系，以科学而高效的管理运营方式，积累分布式的生态资源及能量并将此能量向整个行业输出，最后通过被赋能的应用反哺整个生态，最终形成循环赋能、持续壮大的发展态势，以此为全球用户建立一个无需信任及高度去中心化的金融基础设施。

在功能设计方面，XT SWAP 协议的基本功能将实现以下设计：

- 以“应用+协议”的模式构建去中心化交易和清结算网络；
- 强化应用层壁垒，降低分叉风险；
- 连接与融合中心化交易所和去中心化交易所的交易市场与交易深度；
- 突破目前去中心化交易所的可扩展性瓶颈；
- 具备跨链互操作性，可兼容多种底层公链的原生通证；
- 内置暗池交易特性，可支持大额交易订单的拆单、独立成交。

4.2 XT 机枪池

Valut 英文直译应是叫保险库，不过，圈内更倾向于把它称作机枪池。XT Valut 是一个智能化的收益聚合器(Earn Collection)，基于自动实现最佳收益策略配置的 DeFi 协议。它能够帮助投资人一键获取市场最优收益，从而在大大降低普通投资者进入门槛的同时，能减少因信息不对称而导致的收益损失。

XT Valut 优势明显，能免去流动性挖矿复杂的合约操作环节，节省用户高昂 Gas 费用，只需充值资产给 XT Vault 智能合约作为代理，一键充值/提现，就能获得市场上最佳收益。

• 资金权重线性释放：为防止大户通过快速存入并提取资金的方式来稀释其他人的收入，所有收益将在每次存入资金后的 24 小时内被均匀释放，而 T+1 更符合监管和反洗钱要求。

• 收益策略自动再平衡：根据当前市场情况，XT 机枪池会自动切换策略。对于某个币种来说，用户无需提币再充值到新池子，即可获得当前市场最高收益。每个币种的唯一池子就是当前市面上最高收益的 Vault。

• 支持币种：XT Vault 将支持 ETH、DAI、BUSD、 USDT、 WETH、 USDC、 HBTC、OKT 等，合计 APR 超过 70%。

XT 机枪池，本质上是一个包含实现资产收益最大化策略的资金池。机枪池策略比起只能借出币的 XT 标准协议活跃度高很多。事实上，大多数机枪池策略可以做多件事来实现收益最大化。这可能涉及提供抵押品和借入其他资产（如稳定币）、提供流动性并收取交易费用，或挖其他代币并出售它们以获得利润。每个机枪池都遵循由 XT 社区投票通过的策略。

4.3 XT 质押借贷

XT 质押借贷协议中，用户通过质押标的风险分级，实现持续融资。做市商在平台在提供初始流动性之后，将 LP Token 作为质押物锁定在 XT 协议中，从而持续获得流动性买盘。当用户在 XT 中提供流动性，并设定较大的区间时，流动性标的的基于本位币计价的价值波动幅度较小。

如果供应商质押 XT 中的 LP Token，则质押物在极端行情下，抗风险能力将显著提升，这也将使得助推池系统更加稳健：在项目代币在大幅上涨时，做好合理的风险预警；在代币大幅下挫时，做好风险缓冲。而 XT 最终能够让优质资产能够长期上涨，不良资产逐渐衰亡并被清退。

在平台中，为了实现更精准的风险定价，需要对风险进行分级，从而形成固定收益分级基金。除了项目的发起方（IP）外，还需要两类主要角色参与，分为重要参与者（GP）和固定收益者（LP）。这两类角色都会为项目提供持续的资金输入，GP 作为项目的直接投资方，将会将本金全部兑换成项目代币，而 LP 的资金将被用以作为 GP 的杠杆，帮助项目实现更大的价值增长。

XT 允许 IP 质押高质量资产，这对于 GP 而言增加了一层保障，鼓励大量的 GP 资金流入。每一次 GP 资金的流入都会往 Vault 注资，用以存放 LP 的风险准备金及利润。随着 Vault 资金体量的增加，LP 的投资意愿也被逐步放大。

如下：

$$LPw \propto Vault \propto IPcol * GPturnover * IPltv$$

$$GPturnover \propto GPw$$

其中：

- IPcol 为 IP 的质押物
- IPltv 为 IP 当前质押率
- GPturnover 为 GP 的换手率
- GPw 为 GP 的投资意愿
- LPw 为 LP 的投资意愿
- Vault 为准备金

由此可见，通过有效信号传导，IP 质押波动率更小的标的资产有效驱动 LP 的资金容量，LP 资金作为市场反馈循环中最重要的一环，将发挥积极的乘数效应。如果项目为不良资产，GP 参与者由于将本位币都换成了项目代币，GP 的杠杆标的的波动率将远高于 IP 质押物的波动率，此时 GP 可能因为项目资产价格的下挫，而被率先清退。剩下的 GP 更愿意享受 IP 被清仓之后的质押物，从而减少换手率。这回直接导致 Vault 增量的萎缩，从而大幅降低 LP 的投资意愿，进而使得劣质项目被逐步清退。

$$LPw \propto IPcol * GPturnover$$

$$GPturnover \downarrow \Rightarrow LPw \downarrow$$

此类传导机制不仅能使 XT 良性运转，成为不良资产的清道夫，还能传递大量有效市场信息，作为 XT 风险定价的外部喂养数据，给投资者和流动性提供者提供决策反馈。

4.4 XT 跨链桥

跨链桥是将代币或数据在区块链之间转移的连接方式，两条链可以具有不同的协议、规则和治理模型，跨链桥提供了一种兼容的方式在两者之间安全地进行互操作。

跨链桥负责在 layer1 上保管资产，同时把这笔资产在另一个（和外部）服务上释放。它定义了谁来托管资金，以及资产被解锁必须满足的条件。简而言之，只要像以太坊这样的 layer1 区块链要连接到任何其他系统，就需要使用桥。所有桥接都有类似的操作：

• 存款，用户可以将资金存入桥，代表该资产（的代币）就会在其他系统上发行；

• 更新账户余额，桥被通知新的账户余额信息，这可以用来帮助提款；

• 提款，用户可以根据他们在另一个系统上的余额从桥上提取资产，在这个系统上所发行的代币将被烧毁。

此外，Layer2 可扩展性的承诺是将交易吞吐量从一层转移到另一个链下系统。需要一个桥接器来保管在另一个系统上发行的资金。Layer2 桥是所有跨链桥中最强大的。而 XT 跨链桥即是专注于 layer2 的协议，它不依靠托管者来保护资金。相反，在资金被释放之前，桥必须确保链外系统一切正常。如果处于某种原因，桥确信链外系统被破坏，那么桥可以简单地完全绕过其他网络。

4.5 XT NFT

XT 以 NFT 价值模型，并以此为切入点，形成一个 XTChain 和其支持下的 NFT 系统的应用。因此，XT 拥有对整个行业更广域的价值解决方案，以此推动行业痛点的解决。当前，行业存在着一些潜在的问题，而这些问题若不能得到妥善解决，很容易导致这一市场的非良性发展及运行。简要而言，这些问题主要表现在以下几点：

• 数字化藏品和艺术品存在赝品、仿品层出不穷，鉴真防伪难度大；实物产品创作中的抄袭问题也非常严重，这对利用主体的权益造成重大挑战；

• 游戏领域，存在资产无法确权；激励机制不完善；个人隐私容易泄露；平台中心化；

• 传统经营模式中，产品（无论艺术品，还是数字化藏品、游戏产品）均由中介机构来运作市场，创作者难有直接的话语权。

NFT 为价值流转创造了更好的条件。NFT 资产作为区块链系统中的交易媒介，可以实现无障碍的跨境支付结算，同时也作为一种价值承载，能够有效地联动生态中的各个参与者，以共同协作创造更大的价值。因此，XT 利用 NFT 模式，构建产业的分布式治理和产业发展模式，最终实现价值互联网与全球艺术品、游戏产业相连接。XT NFT 的产业各个成员一包括艺术家、创作者、收藏者、游戏玩家、交易者等，更参与主体均可以在应用中公开透明的获得产品的信息，实现经济生态中的高质量鉴赏、资产确权、交易和募集资金等。

立足于建立全方位的数字产业，面对市场的困境，XT 立志成为市场的革新者，以实现净化生态，促进产业长远健康良性的发展。具体而言，XT 实现如下：

• 产品数字身份的确权，为鉴定提供新路径；

- 去中心化的区块链社区共识，实现共识化的价值认可；
- 链上记录，高价值资产、数字化藏品、游戏道具、艺术品、IP 版权等。
- 智能合约创造便捷且智能的交易；
- 在区块链上用 Token 证明，驱动 NFT 作品所有权的透明性。

4.6 XT AMM

近几年，区块链行业基于自动做市商(AMM)的去中心化交易(DEX)已被证明是最有影响力的创新之一，可以为一系列不同的代币创造和运行公开可用的链条流动性。AMM 从根本上改变了用户交易加密货币的方式。与传统的订单簿交易模式不同，AMM 双方都在与供应链中的流动性资产池进行互动。流动性池允许用户以完全分散和不受管理的方式在链中的令牌之间无缝切换。流动性提供者通过交易成本获得被动收入，交易成本基于他们对资产池的贡献百分比。

XT 认为 AMM 最基本的曲线形态已经定型，后续的创新应该会在 AMM 基本曲线形态的基础上实现“策略化”，于是我们在 AMM 上实现集中的自定义流动性。为了解决传统 AMM 模式中存在的限制，XT 推出了 virtual reserves（虚拟储备金）概念，以下我们将通过举例对 XT 的自动定义流动性进行解析。在传统 AMM 模式中，Alice 一次性将 500,000 DAI 和 333.33 ETH 注入储备池，总价值$1m，提供全区间(0,\infty)的流动性，但实际上 ETH 的价格波动范围在很长一段时间内是有局部范围的，这种为全区间无私提供流动性的行为大大浪费了资本利用效率。

所谓的集中流动性便是让 LP 自主选择波动范围，只为该范围提供局部流动性，例如 Bob 认为未来一段时间内 ETH 的价格区间在(1000,2250)，并且如果未来真的是在这个区间波动，Bob 希望自己获得的收益能够跟百万富豪 Alice 一样多，于是 Bob 一开始只需要投入 91,751 DAI 和 61.17ETH，总价值$183,500，远远小于 Alice 实际投入的资金。我们对照下图来解释其中的道理。

$$x_c y_c = (x_b + 61.17)(y_a + 91751) = x_b y_b$$

$$y_b = 2250 x_b$$

则

$$D = x_b y_b = 166678636.343 \asymp 166665000 = 500000 \times 333.33$$

即 Bob 所获得的虚拟曲线（D 值）几乎跟 Alice 一样。

上述计算过程是一种反证法，实际上用户 Bob 会向系统算法提出自己的需求输入，包括预测价格区间范围、当前价格点、最终想要获得的一个 virtual reserves 规模（即虚拟曲线 D 值）。有了虚拟曲线表达式的确定，可以轻松算出 a、b、c 三个确定的点坐标，进而便算出 x_{real}=61.17 以及 y_{real}=91751。

同时，也可以看到，一旦未来价格越出了区间，Bob 其中一种资产将彻底消失。

$$i_c = \left\lfloor \log_{\sqrt{1.0001}} \sqrt{P} \right\rfloor$$

全局状态中有 feeGrowthGlobal0(f_{g},0) 和 feeGrowthGlobal1 (f_{g},1)—f_{g}，用来从全局角度统计总的手续费收益。例如，当在一个 tick 内发生了一笔交易，系统会计算出该笔交易产生的手续费：

$$f_a(i) = \begin{cases} f_g - f_o(i) & i_c \geq i \\ f_o(i) & i_c < i \end{cases}$$
$$f_b(i) = \begin{cases} f_o(i) & i_c \geq i \\ f_g - f_o(i) & i_c < i \end{cases}$$

f_{a}变量是对所有高于 i tick 的区间的 fee 统计，f_{b}是对所有低于 i tick 的区间的 fee 统计，因此在上述总公式中，我们从全局总累计手续费 f_{g}中减去所有低于下界 i_{l} 的累计手续费，再减去所有高于上界 i_{u}的累计手续费，便是(i_{l},i_{u}) 之间的累计手续费。f_{o}可以理解为一个计算单元，用于累积截止到 i tick 的手续费，在它的初始化过程中，我们约定如下：

<img src="https://img.XT.com/4923026_image3.png" auto";'>

再来看 f_{a}的计算，分成了两段，可以理解为——

• 如果当前 tick 等于 i 或者高于 i，此时从全局总手续费 f_{g}中减去“累积到 i tick”的手续费 f_{o}(i)，剩下的便是对所有高于 i tick 的区间的 fee 统计；

• 但如果当前 tick 还未抵达 i，此时根据对 f_{o}的初始化定义为 0，则所有高于 i tick 的区间的 fee 统计尚未产生，为 0。

同样对于 f_{b}——

• 如果当前 tick 抵达或者超过了 i，f_{o}(i)表示累计到 i 的手续费，也即对所有低于 i tick 的区间的 fee 统计；

• 如果当前 tick 还未抵达 i，对所有低于 i tick 的区间的 fee 统计值即为当前的全局变量 f_{g}（当前总手续费）。

通俗来概括，系统算法要统计某一个 range 内累计的手续费，

• 如果当前 tick 已经处于 range 内部，即 i_{l}\leq i_{c} < i_{u}，只需要从全局手续费 f_{g}减去所有低于 i_{l}组成的 range 累计的手续费；

• 如果当前 tick 不处于 range 内部，且低于下界 i_{l}，说明尚未在(i_{l},i_{u})区间内产生交易，也就未产生手续费，因此该 range 内累计量为 0；

• 如果当前 tick 不处于 range 内部，且高于上界 i_{u}，需要从全局总量中分别去除“两头”各自的累计量，即从全局 f_{g}中减去所有低于 i_{l}区间累计量，再减去“从 i_{u}到当前 tick 区间累计量”。

XT 计算手续费的过程是一种从微观走向宏观的思想，它将空间划分成离散的，每一个时间刻度只会在一个离散空间上产生交易，从而产生手续费，每一个微观 tick 都在各自记录着自己从最低 tick 到自身这段区间内的累计手续费总和，然后供上述公式不断调用，以计算各种宏观结果。

XT 已经改变了传统 AMM 对 LP 行为的设定，也不再基于全局流动性（Global Liquidity）和份额（Share）来为每一个 LP 计算手续费收益。对 XT 来讲，只关注在每一个 tick 里存在多少“虚拟”流动性，以及这些虚拟流动性产生了多少手续费，算得单位虚拟流动性对应的手续费值；在这个时空之下，我们再把视角切到具体每一个 LP 上，对于任何 LP，都会存在一个“开仓”（Position）的区间设定，他在自己设定的区间提供了虚拟流动性，可能是一个 tick，也可能是连续多个 tick，从最简单的“一个 tick”角度解释，系统会记得同一时空下每一个 LP 在此 tick 注入的虚拟流动性值，并为他们确定出一个比例，以此分得该 tick 内所有手续费累计。

<img src="https://img.XT.com/4923027_image3.png" auto";'>

在实际情况中，LP 们还会存在复杂的行为，比如注入/退出的时间纷杂、选择的 range/tick 纷杂。但 XT 的优势之处正是利用全局计算来屏蔽掉单个 LP 视角，只关心 ticks 视角和 Position 视角。在确定好上述所述的一系列全局状态变量的定义后，认真记录好每一笔 swap 交易在 ticks 中发生的情况，同时只记录每个 tick 内虚拟流动性的大小，以此为根本去提供 swap 交易公式以及 swap 后手续费如何分配给参与该 tick 的所有 LP 们。LP

的复杂行为体现在空间的不连续性和时间的不统一性两方面，对于时间不统一性，XT 还会引入 Position 这一级别的全局变量为每一个身份（address）记录下其对 range/tick 加入/退出（“setPosition”）时手续费的统计（uncollected fee/feeGrowthInside），确保后来的 LP 不会参与到前序 LP 们已经累计的收益分配。

4.7 XT 支付清算

虽然在当前的互联网时代，已经使得支付结算效率在很大程度上有所提升，但是在跨币种、跨国界、多种经济合约下，依然在多中心、多环节方面受到了限制，从而使得支付结算的效率往往显得力不从心。

要实现 XT 应用生态的良性发展，则必须具备强大的支付清算系统，XT 将在跨链技术的基础上，打通聚合支付跨链壁垒。去中心化和点对点特征，能够减少中间环节、降低交易成本，在很大程度上提升交易效率。在全球支付结算方面的应用，使得应用方能形成一种全新的支付结算方式。

基于 XT 的支付清算系统用多重签名的组合来控制钱包的支付权限，多重签名的一个私钥可由托管机构掌握，不同权限(大额或小额)的钱包地址都需要进行不同程度的身份认证，通过大数据或投诉举报系统可以建立黑名单或可疑名单，对可信白名单无需多重签名也可进行支付。

依据申请钱包的使用额度可以要求不同程度的身份验证，银行、非银行金融机构可面对面的对用户 进行强身份验证，而通过视频语音则可以作为弱身份验证，公交、高铁、地铁、机场、高速公路收费站、商场收银台的付款时视频记录都可以作为连续身份验证。

在传统的供应链运作，我们为了解决信任问题，往往会引入第三方平台。但是同样我们需要向平台支付相应的费用，这就是所谓的信任成本。但区块链不需要中介参与，通过分布式账本，来解决信任的问题，也大大降低了企业因为信任所投入的成本。

XT 支付清算系统将成为全新的数字经济价值载体，促进和发展全球的贸易经济。构建一个数据无边界流通、价值开放共享、产业协同创新的数字经济联盟。利用区块链、大数据、物联网、AI 等尖端科技，实现全球各产业数据、资产安全上链，推进产业数据融合，通过海量数据连接实现价值，打造全球价值共同体，从而让联盟内各主体创造更大的价值，沟通构建开放共享、创新协同、持续循环的数字经济生态联盟。

第五章 XT 的技术体系

5.1 技术架构概述

XT 的技术架构体系基于 XT Chain 主链协议展开，全景架构由基础网络层、中间协议层及应用服务层三部分组成，通过高效的多链——跨链体系，实现端到端的数据透明度，同时有效降低成本和风险，实现数据价值的全球流通。

5.2 共识机制

XT 的共识机制为 HashNet 的 DAG 共识和 BA-VRF 共识机制相结合的双层共识机制。

目前已有的区块链技术多数无法进入到实际的大规模商用阶段，其主要原因在于共识机制难以在去中心化和可扩展性之间取得较好的权衡考虑，例如比特币、以太坊具有较好的去中心化程度，但 TPS 较低；EOS 具有较高的 TPS，但中心化程度较高。双层共识机制的主要创新点在于将分片与共识分离。具体来说，XT 的顶层全节点负责对参与共识的下层局部全节点周期性地动态分片，局部全节点在片内对交易达成共识，片间通过 gossip 协议同步全局账本。这样设计的主要优点在于顶层全节点之间采用 DAG 和 BA-VRF 协议保证分片的公平性和去中心化程度；底层局部全节点采用 DAG 共识实现高交易吞吐率，且分片数量不受限制。

1）HashNet 共识机制

已有的 Hashgraph 共识算法通过 gossip 网络和虚拟投票策略达成交易顺序的共识，该共识的前提是要求网络节点超过 2n/3 的投票能力具有对 famous witness 事件的一致投票结果，其中 n 是全网的当前投票能力总和，该投票能力通常为节点的持股数量。由于采用了本地投票策略，Hashgraph 可以实现较快的交易确认速度。然而该方法存在以下问题：

• 在广域网环境中，节点波动性较强，全网的投票能力 n 的波动也随之增强，这可能导致系统长时间无法找到满足 2n/3 投票一致的事件，从而无法达成共识。

• 受节点稳定性、处理能力、带宽等因素影响，不同节点处理事件的能力差别较大。若系统中存在大量能力较弱的节点参与投票，同样会造成系统长时间无法达成共识。

• 广域网环境下，节点频繁波动可能导致节点被分割成多个子网。根据 gossip 邻居交换协议，节点会周期性剔除长时间未更新的邻居。当邻居稳定后，节点可在子网内达成共识。此时若子网规模较小，很容易使恶意节点在同一轮产生两个 famous witness 事件，从而产生双花交易。

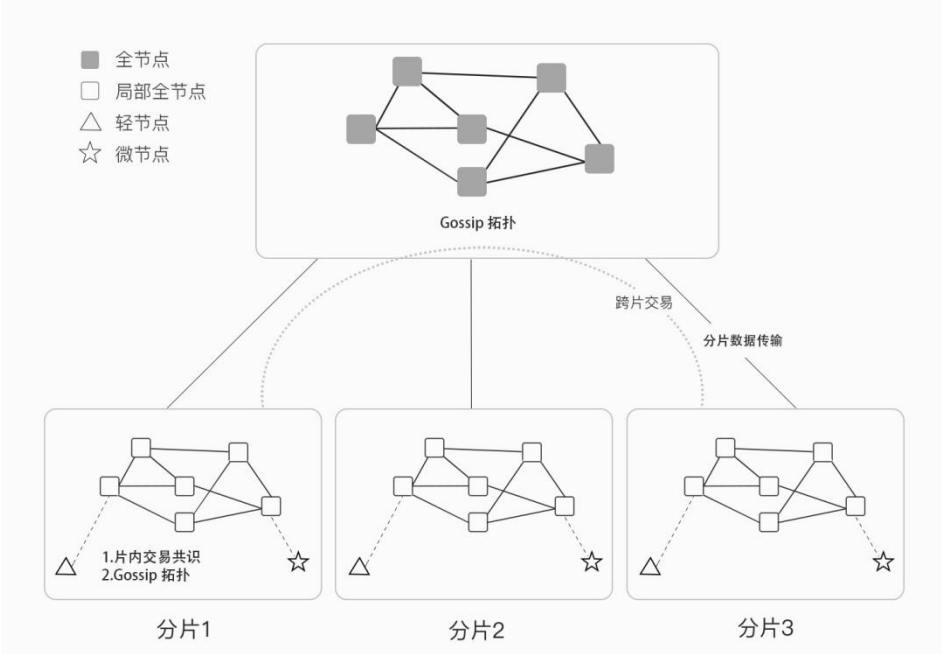
• 随着系统规模增大，节点收到的同步信息越来越多，可以预见系统的吞吐率会随节点数目的增加而降低。

基于以上挑战性问题，我们提出 HashNet 共识机制。如下图所示，HashNet 采用基于双层 gossip 拓扑框架，通过"片内自治，片间协作"的方式形成一个分而治之的分布式账本系统。在 HashNet 中，顶层 gossip 网络中的节点称为全节点（full node），负责节点拓扑和分片的维护;下层 gossip 网络的节点称为局部全节点（local full node），负责交易共识、交易验证、交易存储以及账本一致性。

HashNet 共识机制的主要优势在于：

• 全节点和局部全节点具有较强的稳定性和处理能力，能够有效避免 Hashgraph 长时间无法达成共识的问题，也能够避免因网络被分割造成的恶意节点攻击问题。

• 采用双层 gossip 拓扑对节点分片，顶层节点不参与交易共识和交易验证过程，分片可并行工作，保证了系统具有较好的可扩展性。



HashNet 中节点共分为四类：全节点、局部全节点、轻节点和微节点。

• 全节点：负责维护节点拓扑，包括全节点的周期性加入退出过程、局部全节点的周期性加入退出过程；负责更新分片，包括确定每个周期的分片数量、将哪些局部全节点划分到同一个分片。

• 局部全节点：作为代理节点，向轻节点和微节点提供交易代理服务;在分片内，局部全节点作为交易共识的主体，实现交易在片内的验证、共识和记账；在分片间，局部全节点

采用 gossip 协议传播各自片内账本信息至其他分片，从而实现账本数据一致性。

- 轻节点：通常为轻量级客户端钱包，该节点可通过局部全节点做代理完成数据请求和发送。

- 微节点：通常为智能物联网设备，该节点可通过局部全节点做代理完成数据请求和发送。

全节点在审核通过所有下一轮局部全节点申请人后，需要对这些申请人分片以保证系统的可扩展性。

2）BA-VRF 共识机制

基于可验证随机函数的拜占庭协商共识（BA-VRF）共识主要用于选举责任全节点，他是一种基于可验证随机函数（Verifable Random Function，VRF）和 BA 算法构建的共识机制，该共识机制能够随机选出少量全节点作为公证节点，并确定公证节点的优先级。

BA-VRF 每一分钟执行一次，每次达成共识将随机选出若干全节点作为公证节点，公证节点有权发送公证单元，公证单元须满足 DAG 共识中的父子引用规则。公证节点发送的公证单元成为稳定主链的单元后，该公证节点可以获得公证奖励。当交易活跃时，新单元不断产生，则公证节点会及时获得公证奖励;当交易不活跃时，极端情况下一分钟内没有新单元产生，已经发送公证单元的节点在发送的公证单元成为稳定主链单元时获得公证奖励，没有发送公证单元的节点不获得公证奖励。

- 共识状态

BA-VRF 有最终共识和临时共识两种状态。如果一个全节点达到最终共识，意味着任何其它全节点也达到了最终共识或者在同一轮中的临时共识必须同意这一共识结果，而无论强同步假设是否成立。而临时共识意味着其它全节点可能在其它公证单元上达到了临时共识，没有全节点已经达到了最终共识。

所有公证单元都必须直接或间接引用之前生成的公证单元，这可以确保 BA- VRF 的安全性。BA-VRF 产生临时共识有两种情况。首先，如果网络是强同步的，一个攻击者可以以一个很小的概率让 BA-VRF 达到临时共识。此情况下，BA-VRF 不会达成最终共识，也不能确认网络是强同步的。但经过几轮后，很大概率上会达到最终共识。第二种情况是，网络是弱同步的，整个网络都被攻击者控制。此情况下，BA-VRF 将达到临时共识，选举出不同的公证节点集合，形成多分叉共识。这能够避免 BA-VRF 达到最终共识，因为全节点被分成了不同的组，各组之间并不同意对方。为了恢复活性，BA-VRF 将被周期性地执行，直到消除意见分歧。一旦网络恢复到强同步状态，将会在短时间内达成共识。

- 全节点选择

抽签算法是基于可验证随机函数（VRF）构造而成的，可根据每个参与 BA-VRF 共识的全节点的权重选出这些节点的随机子集。某全节点被选中的概率约等于自身权重与总权重的比值。抽签的随机性源于 VRF 函数和一个可公开验证的随机种子，每个全节点可根据随机种子验证自己是否被选中。

VRF 函数定义：给定任意字符串，VRF 函数输出哈希值和证明结果。

$$(\text{hash}, \pi) \leftarrow \text{VRF}_{S_k}(\text{seed}||\text{role})$$

- 拜占庭协商

拜占庭协商（BA）能为每一个被选中的全节点确定公证优先级并提供公证优先级的证明。达成拜占庭共识需要执行多个步骤，BA 算法会被执行多次。

每次协商都从抽签开始，所有全节点都去查看它们是否被选中成为当前 BA 的参与者。参与者广播一个包含选择公证优先级的消息。每一个全节点用它们收到的公证优先级消息去初始化 BA 算法。上述过程将被不断重复执行，直到某轮协商有足够多的全节点达成共识。在不同全节点之间，BA 算法并不是同步的，每个全节点发现之前的步骤结束后应立即查看新的参与者选举结果。只有全节点在某轮协商中投票并最终达成共识，它才可以参与下一轮协商。

BA 算法的一个重要特征是，参与者不需要维护私有状态，仅存私钥，所以参与者每个步骤之后都可以被更换，以减少对参与者的攻击。当网络是强同步的，BA 算法保证如果所有的诚实全节点以相同内容进行初始化，那么可以在很少的交互步骤之内达到最终共识。此情况下，即使存在少量攻击者，所有的诚实全节点也将在有限交互步骤步下在达到最终共识。

5.3 智能合约

区块链技术为智能合约提供了安全可信的执行环境，促成了智能合约概念的实现。智能合约是由事件驱动的、具有状态且运行在一个可复制、可分享的账本之上并能够保管账本上资产的程序，其目的是让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行。智能合约不仅可以接收和储存价值，也可以向外发送信息和价值，整个过程可以在无中心，无信任的前提下，自动化、智能化的执行。智能合约在设计上需要在安全性和功能性之间寻求平衡。

现有区块链项目主要聚焦单一种类智能合约的设计，在智能合约种类限定的条件下谋求安全性和功能性之间的平衡，往往达不到满足多样化用户群体使用体验和用户多样化交易需

求的理想效果。比特币区块链的交易脚本是智能合约的雏形，属于非图灵完备智能合约，具有复杂度低和轻量化优势，并且在比特币区块链网络运行将近十年时间内没有出现过安全性问题，但是比特币交易验证脚本支持的功能非常有限，仅用于支付验证。

以太坊区块链支持采用 Solidity 高级语言编写的图灵完备智能合约，极大地丰富了智能合约的功能，扩展了区块链技术的应用领域，但是编写以太坊智能合约容易出现安全漏洞，The DAO 事件正是因为编写的以太坊智能合约出现安全漏洞导致以太坊社区分裂。

XT 在智能合约功能实现上采用类似计算机存储体系结构的层次化思想，摩西虚拟机（Moses Vitual Machine，MMM），支持声明式非图灵完备智能合约和高级图灵完备智能合约。用户根据使用体验和交易需求选择使用这两类合约，平衡计算安全和计算功能以及计算费用和计算复杂性，以满足交易多样化需求。声明式智能合约部署简单，安全性高，更加接近法律合同语言;高级图灵完备智能合约部署难度相对较高，主要用于开发程序逻辑更加复杂的 DApp。

两类智能合约部署的手续费机制不同，声明式智能合约的手续费根据合约所占字节计算，而高级图灵完备智能合约则以程序运行时消耗的 XT Token 作为手续费。

类似以太坊账户概念，在 XT 中也存在外部账户和合约账户两类账户。外部账户是用户控制的账户，用于发起转账交易。合约账户由外部账户控制，通过接收外部账户和其他合约账户消息调用启动智能合约的执行。

声明式非图灵完备智能合约嵌入在外部账户发起的交易数据中，用于为交易提供条件约束，没有账户概念。智能合约账户专指部署高级图灵完备智能合约后返回的账户信息。外部账户和合约账户具有状态的概念，如账户中余额信息和交易发起数等信息。为了消除外部账户和合约账户的差异，账户状态有 MVM 代码哈希值信息，该信息在高级图灵完备智能合约部署后是无法修改的。此外，为了访问用户存储在链下的数据，账户状态还包含链下数据访问目录信息。

在 XT 中有两种交易手续费计算规则，外部账户发起的普通交易采用按交易数据字节数进行计费，调用智能合约则按程序指令执行数进行计费。为了消除这两部分计费规则的差异，在交易数据结构中包含类似以太坊的 Gas 上限和 Gas 价格两个域进行统一计费。对于按交易数据字节数计费的规则，交易数据字节数是已知的（也就是交易手续费是事先知道的），通过固定 Gas 上限也就得到了 Gas 价格。在用户发送部署高级图灵完备智能合约的交易时，交易数据结构中有指定 MVM 代码的域。

5.4 分布式账本结构

账本结构是区块链的数据储存的重要表现形式，随着区块链应用场景变得越来越复杂，账本结构的设计也越来越显得至关重要。XT 的分布式账本结构，主要考虑以下几个因素：

• 可扩展性：在 XT 的支持下，分布式账本的层次化结构提高了架构的可扩展和可插拔性，方便开发者以模块为单位进行开发，为应用提供更多的数据支持能力。

• 稳定、易用性：便捷高效的的账本操作，在一定程度上降低了门槛；在账本层面内置许多关键操作功能， 并融合诸多业务模型，为多行业用户提供便捷。

• 安全、兼容性：数字资产及其操作是区块链账本的最典型应用方式，通过对多资产的兼容，支持市面上多种主流数字资产，同时确保对于账户资产操作的原子性，增强账本的实际应用及操控功能。

1）广泛兼容的账户结构

• 账户地址：区块链账户的唯一标识，当查询某个账户的信息或想某个账户转账时，需要使用账户地址定位到该账户；账户余额：该账户内的原生 Token 数量；

• 智能合约代码：如该字段不为空，则账户为智能合约账户，用于存储相应的智能合约代码；交易序号：为避免账户下的交易乱序，每次处理一个交易时，账户的交易序号递增，以此记录当前最大序号，每个账户都有自己的交易序号，账户间互不影响；

• 资产列表：资产列表用户记录该账户下的各种数字资产的资产代码、发行方和余额等信息。在符合系统安全性和可靠性要求的前提下，最大程度实现资产发行、流通的可扩展性和便利性。

• 元数据：元数据字段为每个账户提供一个 Key-Value 结构的私有数据存储，用户扩展业务的自定义数据处理，同时，元数据的设计提供智能合约代码执行状态数据存取；

• 权重及门限：在账户操作中，权限控制是一项很重要的需求，因为显示业务中往往不同主体具有不同的角色和权限。XT 在协议的支持下，提出一种多权重的操作门限控制方法，能够为不同的成员账户设置不同的操作权重，并未操作执行设置一定的门限值。

区块包括区块头和区块体两大部分，其中区块头主要包含以下数据字段：

• 区块号：区块在整个账本中的序号，序号按区块生成的先后顺序递增；

• 区块的哈希值：对区块序列化后的文本做哈希运算的到的哈希值；前一区块的哈希值：区块的前一区块的哈希值；

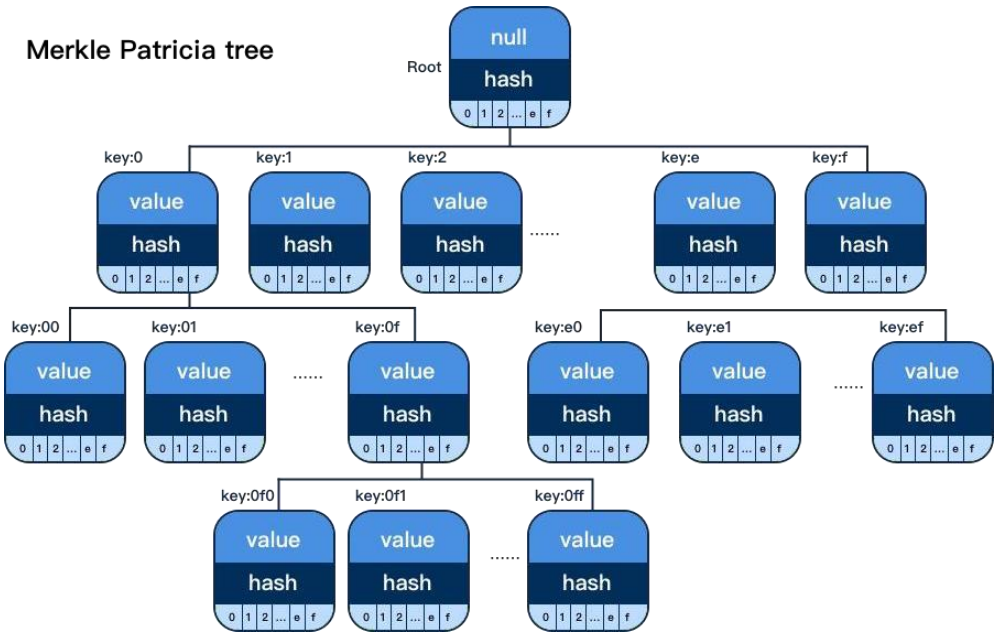
• 账户树的哈希：用 MPT 构建的账户树的根哈希，MPT 上每个节点任何比特级的数据更改，都能反馈到根哈希上吗如果在区块对比时，发现账户树哈希不一致，可以从根节点开始对子节点层层对比，快速找到不一致的账户；

• 共识信息的哈希：在区块生成之前，验证节点集合需要对交易进行打包生成提案，然后对提案进行共识并达成一致，共识信息哈希即对共识的提案做哈希运算后得到的值；验证节点机的哈希：对所有参与共识的验证节点的地址做哈希运算得到的值；

• 费用的哈希：对当前区块的费用配置，包括 Gas 价格和最小预留费用等，做哈希运算后得到的值；

• 区块版本：区块结构的版本号，用于实现向下兼容性；交易数量：区块所包含的交易总数。区块主体主要包含交易的信息和签名。

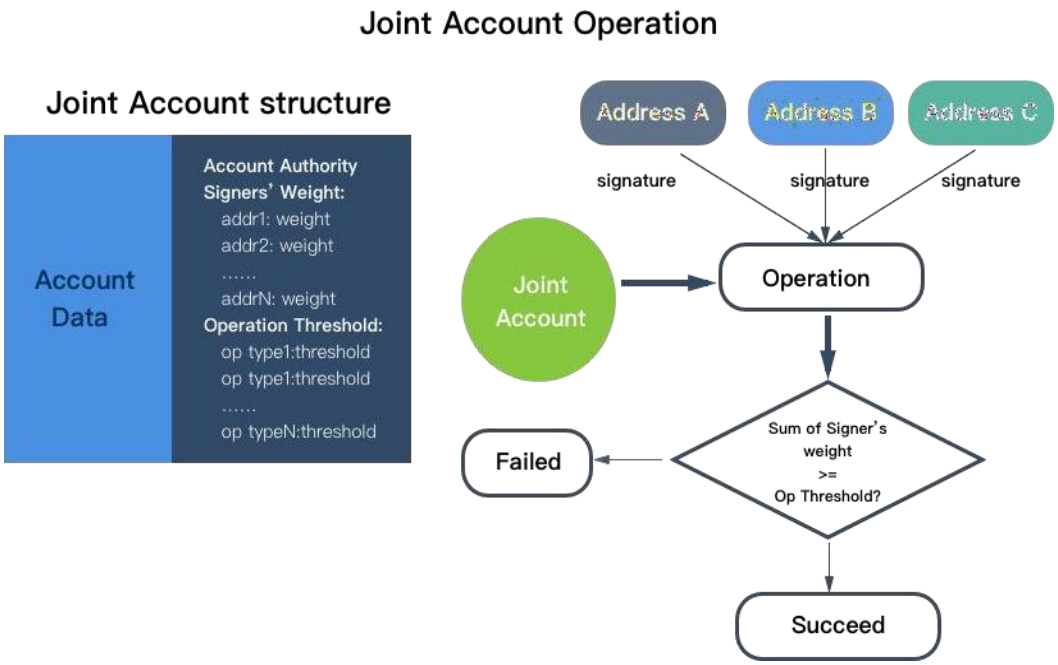
通过哈希索引将各类关键信息都引用至区块的各个字段中，使得整个账本中，任何部分的数据变动，都能反映、表现到区块字段值中，提高信息验证比较的便利性。同时一旦出现不一致的情况，能够根据区字段的索引，有针对性的快速定位问题所在，提高问题解决效率。



采用 MPT(Merkle Patricia Tree)树进行账本数据储存，MPT 树是 Trie 树和 Merkle 树优点融合的产物，可以有效减少账本树的深度、增加树的平衡性、提高树的安全性和可验证性。基于 MPT 树的账本数据结构，使得 XT 在数据对比查询、插入修改等操作方面，均可以做到高效而低耗。

2）安全稳定的联名账户控制

在账户设计中，考虑了多权重的操作门限控制属性，能够为不同成员账户设置不同的操作权重，并未操作执行设置门限值。通过上述方式，可以实现多方用户联合控制账户，并按照操作门限进行精准操作的目标，满足协作多样化、操作模式精细化、业务模式丰富化的需要。



如图所示，用户 A\B\C 想要对联名账户进行操作，首先需要计算用户的权重之和，然后将权重之后和与操作门限进行对比，如果不小于操作门限，则具备操作权限，否则操作被拒绝。

XT 通过体系化设计、模块协作和丰富的操作类型，构建了多资产原子操作的可扩展账本结构，为多种类型的业务操作提供强大数据支持，满足用户复杂应用场景下的需求，同时也尽可能兼顾用户对高性能和低消耗的需求。

随着技术的发展和完善，区块链应用场景已经不仅仅局限于支付转账、信息追溯等领域，各类新的应用场景不断涌现，视频、图片、医疗信息等大体量数据也越来越多地需要存储于区块链中。大规模分布式数据的存储和管理需求， 使得区块链数据处理的时间和空间消耗问题越来越突出。XT 在数据存储设计中充分考虑到上述挑战，提出了海量数据的差异化分布式存储体系。

通过对数据进行差异化分类处理，根据数据特点将其分为链上数据和链下数据。链上数据指实时存储于区块链节点的数据，比如账户、交易、区块头等基础链数据等。但是链下数据需要进行链上数据锚定，即将数据哈希值作为链上数据存储。其次，在针对链上数据和链

下数据的不同特点，选择不同的存储引擎，并进行接口封装和成本计算，满足大规模数据差异化存储需求的同时，具有较高的用户友好性。

5.5 差异化海量数据存储

1）数据差异化定义

链上数据指实时存储于区块链节点的数据，区块链节点具备对链上数据的全拷贝能力，是能形成区块有效性证明的最小单元数据集合，典型数据如下：

• 链基础数据：比如账户、交易、区块头等直接数据，账户树、交易树及区块生成证明等区块有效性证明数据，以及供用户数据查询必要的索引数据等；

• 智能合约及合约操作数据：智能合约的图灵完备脚本及其依赖数据均需要在链上存储， 以保证其可执行和去中心化特性，随时提供智能合约访问能力；

• 资产类数据：这类数据存储需求量小，但对安全性要求极高，链上存储可以在提供充分冗余存储的同时提供安全的计算环境；

• 简短静态数据：比如交易备注等通常数据量很小的数据。

链下数据指无需实时存储于区块链节点的数据，通常是使用频率较低、存储体量相对较大的数据集合，比如存在性证明所需的历史视频数据等。链下数据通常需要进行链上数据锚定，即将数据哈希值、数据索引等作为链上数据存储。典型数据如下：

• 大体量数据：该类数据特点是所需的存储空间大，比如视频、图片、日志、地理位置等数据；

• 区块历史数据：使用频率低，用户无需实时查询，链下数据可作为备份手段；

• 保密性要求较高的数据：比如个人身份信息，医疗数据等，链下数据脱敏存储，只在验证请求或授权请求时提供原始数据证明。

2）数据分类筛选

存储适配器模块负责筛选、甄别链上数据和链下数据，并分别进行存储操作。一般而言，区块链网络中的参与节点均会选择使用链上存储、而链下存储的选择则与用户应用方式紧密相关。链下存储按照数据存储的开放程度，可分为私有存储和共享存储两类。

链下私有存储指用户搭建并进行运维的存储系统，具有前期投入打、运维成本高的特点；

链下共享存储指无需用户自身投入建设，通过付费等方式获取的共享存储系统。存储适配器模块的主要作用如下：

• 接口封装：将复杂的内部存储功能封装为少量简单易用的用户服务接口；

• 数据分类：对链上数据及链下数据进行分类，如需进行链下数据存储，需进一步选择链下共享存储或者链下私有存储。在链下数据存储前，需先将待存储数据进行哈希运算，进而将哈希值作为链上数据进行存储操作；

• 成本计算：支持对链上数据存储所需的成本（比如 Gas 值），以及共享存储需支付的费用等进行综合计算，提供给用户作为成本参考。

3）链上数据存储

针对链上数据存储需求，XT 基于 TiDB 技术构建了专用的分布式存储引擎数据库。TiDB 是受 Google Spanner / F1 论文启发而设计的开源分布式 HATP (Hybrid Transactional and Analytical Processing) 数据库。

XT 专用分布式存储引擎数据库具备如下能力：

• 水平弹性扩展：通过简单配置即可实现新节点添加并且能在不停止终端业务的前提下，动态添加存储节点，提高整体的数据存储能力；

• 高可用性：数据存储引擎可在保证大多数副本不丢失的前提下实现故障的自动恢复；

• 分布式任务：采用优化后的模型支持分布式任务，同时使用乐观锁技术，在任务执行过程中不会检测写冲突，只在提交过程中进行冲突检测，冲突双方中较早完成提交的一方会率先写入成功，另一方会尝试重新执行整个任务，具备高效的任务处理能力。

4）链下数据存储

结合 IPFS 等现有分布式存储技术，XT 将有效满足链下存储需求。不同于链上数据的相对传统数据存储方案，IPFS 等存储体系是永久、去中心化保存和共享文件的技术，是内容可寻址、版本化、点对点超媒体的分布式存储协议，基于该类技术构建的链下数据存储引擎具备如下能力：

• 降低存储空间：通过对文件生成唯一哈希值的方式标识文件，取代传统的通过文件位置标识文件的方式，有效降低存储空间；

• 提高存储多样性：支持更多业务数据类型及大量数据的存储（视频、照片、日志、地

理位置）；

- 降低硬件成本：支持水平扩展，对存储节点的硬件要求降低；
- 多种部署形成：在提供共享服务能力的同时，也可以利用该技术进行私有化部署。

5.6 技术优势

XT 始终都围绕着为用户交付真实的、实时的、可持续的数据价值来展开，为解决数字经济发展痛点，扩大可信共享的数字经济联盟生态边界。区块链使用的非对称加密算法是天然的用户认证系统，可构建去中心化的数字身份系统，XT-ID 是系统命名空间中唯一的、永久的身份标识。通过 XT- Key，用户可以方便便管理自己的数字资产，比如：通证、数据、信用等，以及对其进行访问控制;比如：授权第三方访问自己的数字资产，获得收益等。由于区块链的不可篡改等特性，也自然形成了信用体系。

1）信息访问

用户可以随时维护自己的数字资产，针对不不同类型数字资产设置相应的模式，分为私密、公开、收费等，以及为收费模式的数字资产定价。

2）信息访问控制

第三方通过访问控制协议申请访问用户数字资产，用户可以选择授权通过、拒绝等。信息访问审计：查看自己的访问控制记录，交易记录等。

3）提升交易速度

通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，XT 将以实现秒级的快速交易验证。满足绝大部分区块链应用场景的用户体验。

3）增加数据存储

区块链复式的记账模式，在系统不断的运用，积累了大量的数据，造成运行速度下降，XT 将会实现分离存储、分表存储机制，实现数据海量存储。

4）高吞吐量

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，XT 的处理性会进一步大幅提高交易吞吐量。

5）节点数据快速同步

XT 将会研发镜像机制，可以定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚；同时，缩短新加节点加入运转的周期，仅需同步最新镜像及少量近期交易集合，即可融入网络并参与共识验证。

6）权限控制

提供数据信息写入与读取两类权限控制策略。数据信息写入权限，同一账户下设置多个使用用户，并针对不同的操作设置相应的权限，满足多方签名控制的 使用场景。数据信息读取权限，用户可以授予和撤回单用户或用户组对数据的操 作权限，用户组可以由用户灵活配置。数据包括用户账户信息，交易信息等，粒度可以细化到交易或账户的各属性字段。

6）高扩展性

XT 的区块链结构，能够满足不同业务领域的需求，提高系统的可扩展能力和维护效率。即可用于标记资产和资产转移，也可提供不可篡改的多维事件记录，还可以用于供应链金融溯源以跟踪资金的流通过程。

7）高安全性

• 私钥存取：为了方便用户使用 XT 产品服务，除了传统的客户端生成和保存的机制，还提供网络托管存取和私钥硬件存取(U-key)两种方案。网络托管存取，即把用户名和密码通过特定算法映射成私钥并在服务端进行存储。服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；硬件私钥是为了满足金融行业及物联网行业的使用需求。

• 多重隐私保护方案：提供多重隐私保护功能。首先，底层提供同态加密方式，用户所有数据均加密存储，仅用户本身可见。其次，Adaptors 提供加密中间件服务，用户可根据业务需要进行选择。最后，上层应用可以在录入时对数据进行加密处理，平台负责对用户生成的加密数据进行写入和读取。

8）可视化运维

提供运维管理所需的可视化工具。XT 节点上部署的系统监控服务（MonitorAgent)：支持业务(区块、交易、合约、共识等)、网络(组网、时延、吞吐量等)、系统层面(CPU、内存、磁盘等)的数据信息监控;同时提供完备的日志、告警与通知机制，便于商用系统的维护。

第六章 全球技术团队

XT DAO 核心团队成员由来自计算机、信息安全、通讯、数学、金融、DeFi、web 开发和高频算法交易等各个领域的行业最优秀的专家组成，在区块链底层、分布式数据库、密码算法、运用层建设、跨链技术等方面具有丰富的经验。XT DAO 不仅具备强大的技术能力，还拥有优秀的科研能力，在分布式账本和密码学等多个领域取得了重大研究突破。

Kennedy——国际知名数据工程师，曾在多家全球知名互联网大数据研究中心就任过关键职位，负责互联网基础技术应用研发，参与众多国际知名项目，是区块链技术领域先驱。

Theodore——毕业于耶鲁大学计算机系，并取得计算机与大数据博士学位，架构师、数据库专家，交易所构建的首席技术专家，长期从事交易行业的数据库应用、数据仓库、大数据和区块链开发，拥有丰富的区块链项目开发经验。

August——全球知名的区块链应用专家，全球区块链技术商业应用领袖级人物。曾任美国商业理事会理事，哥伦比亚大学社会学博士、金融研究中心研究员，是全球智慧金融技术应用领域权威。

Jason——拥有 15 年技术开发经验，并在区块链底层技术开发方面拥有权威影响力，职业生涯中覆盖了学术界和企业界两个领域，是一名研究学者、工程师及领导者。曾在谷歌和亚马逊历任多个工程管理职位。

Donahue——区块链和 5G 技术专家，长期从事大型系统工程开发，层就职于高通等国际顶级公司。哥伦比亚大学数据工程学客座教授，区块链知名学者。

Wesley——精通比特币、以太坊、HyperLedger 等主流区块链技术原理及实现，对区块链共识机制、智能合约、跨链技术、侧链技术、隐私保护等有深刻理解和丰富实践。

Montague——哈佛大学计算机系硕士，著名区块链软件开发工程师，层负责比特币、ETH 等虚拟货币的挖矿算法跨平台移植和矿机软件开发管理工作。在虚拟数字货币钱包和虚拟数字交易所技术架构方面，拥有丰富的经验。

第七章 XT 社区自治（DAO）模式

7.1 DAO 的基本定义

DAO（DAO，Decentralized Autonomous Organization）意为去中心化的自治组织，最早由以太坊创始人 Vitalik Buterin 提出相关的概念，第一个 DAO 项目就是 The DAO（去中心化的基金会，给有潜力的以太坊项目进行投资）。

简单来理解，DAO 需要满足三个特点：去中心化、自治、组织。

去中心化是指 DAO 需要构架在公有区块链上，从技术层面来避免中心化权力集中，所带来的垄断和绝对话语权。自治的意思是，项目的发展和规则制定，完全由社区成员来进行把控。社区成员可针对某些事情发起提案，一旦投票通过提案将自动强制执行，所有成员均享有权力来治理项目。组织是指 DAO 不需要由公司或者机构来进行运作，人们通过社区共识聚集在一起，大家朝着一个共同目标工作的社会群体。

DAO 最大的价值之一，在于去中心化治理。DAO 和 DeFi 概念相结合，可以创造出更有价值的项目。DeFi 和 DAO 一样，都具有去中心化的特质，同时 DeFi 中的许多流动性挖矿决策和手续费等问题，需要经常征求社区成员的意见，这时候就会使用到 DAO 来作为治理手段。

在 DeFi+DAO 的融合之路上，XT 的设计充满了创新和看点，从单个资金池的治理，到 Swap 子协议的治理，再到整个项目生态的治理，XT 将 DAO 元素融合进了生态内的每个角落。

DAO 是一个为组织机构服务的工具，目前可以分为三种类型：

- 通用型 DAO：为项目提供创建 DAO 组织机构提供成套组建，类似于阿里云，比如 Aragon。
- 专用型 DAO：因项目而生，主要为该项目服务，类似私有服务器，比如 Yearn.finance。
- 特殊型 DAO：主要为实现某些功能，类似特殊功能服务器，比如 MolochDao。

7.2 XT DAO

XT 是一个完全有自治社区主导的项目，在 DAO 的主导下，实现了完全的去中心化和社区高度共识。XT 发起的全新去中心化自治组织属于专用型 DAO 范畴，社区有强烈的共识，100% 社区自行管理。项目上线后，社区将投票开发自己的去中心化应用和 DAPP。

XT DAO 的全球社区建设遵循高度的去中心化，通过链上和链下相结合的模式进行。XT DAO 所有的程序设定成功后，它就能根据原有的规则开始运转。它在运作的过程中，还能根据实际情况不断的自我维护和升级，通过不断的自我完善机制，不但消除了信任问题，更实现了前所未有的集体协调水平，从而形成 XT DAO 的技术基础。

- 智能合约让 XT DAO 的规则有了技术实现；

- XT 通证经济模型，让 XT DAO 的利益分配有了现实的激励基础；

- 区块链本身就是连接世界各地的个人或组织，让 XT DAO 的拓展突破地域限制。

以 XT 作为价值流通证明和激励手段，然后用智能合约确定成员协作关系和利益分配模式。成员之间并没有明确的身份划分，例如投资者、开发者、合作者、运营者、消费者等等，都会因持有代币而成为社区的一份子。成员之间可自行通过合约结构的持续优化，不断寻求最短路径，保持高效的协同能力和更好的发展方向。

7.3 XT DAO 的价值

XT DAO 作为一个去中心化的自治组织，是用代码编写、运行在区块链上的技术工具，同时也是一种新型的治理机构，能够实现公开公正、无人干预和自主运行，且没有法律实体。

1）最大化利用资源

XT DAO 把一切内容都存放在去中心化存储网络中，公开透明、不可篡改。任何人都可以审查项目的规则变更等，及时调度资源，无须因审查消耗时间。

2）实现创新发展

在 XT DAO 的人可以随时在区块链上提出自己的意见并被他人看到，用户可以更便捷、更及时深度参与到 XT DAO 发展事项中，推动项目创新发展。

3）提高结果可信度

XT DAO 分布式账本的使用，会使得投票人的每一票都真实公开地记录在区块链上，无需人工计票来产生选举结果，及时可信。

XT DAO 将是 XT 生态治理和发展的核心驱动力。XT 希望以民主、协作、透明的方式激发社区主观能动性、调动社区优质资源，推动构建一个去中心化、正向驱动的 XT 自治体系。同时成立了 XT DAO 管理委员会，负责 XT DAO 各项事务的推进。

XT DAO 管理委员会成员不仅可以为 XT 的发展做出贡献，而且可以通过提案的落地获得额外盈利收益。XT DAO 管理委员会没有层级结构，所有成员都是平等的，且利益目标是一致的，只有共同推进 XT 生态的价值增长，才符合所有成员的利益，形成一个良性循环发展的 XT 治理生态。

第八章 免责声明

本白皮书内任何内容均不构成法律、财务、商业或税务建议，您应在参与任何与此有关的活动之前咨询自己的法律、财务、商业或其他专业顾问。平台的工作人员、项目研发团队成员、第三方研发组织以及服务商都无需对因使用本白皮书所可能导致的直接或者间接的损害和损失承担责任。

本白皮书仅供一般信息参考之用，并不构成招股说明书、要约文件、证券要约、招揽投资或出售任何产品、物品或资产（不论是数字资产还是其他资产）的任何要约。以下信息可能并非详尽无遗，也不意味着具有合约相关的任何要素。

白皮书无法保证信息的准确性或完整性，不保证也不承诺提供信息的准确性和完整性说明。在本白皮书包含从第三方获得的信息的情况下，平台和团队尚未独立验证此类信息的准确性和完整性。此外，您需要了解的是，周围环境和情况可能会随时发生变化，因此本白皮书可能因此而过时，平台没有义务更新或更正与此相关的内容和文件。

本白皮书的任何部分不构成也将不会构成平台、分销商以及任何销售团队（如本协议中所定义的）的任何要约，也不可以将白皮书所陈述的内容作为任何合同和投资决策所依赖的基础。

本白皮书中所包含的任何内容都不能作为对未来业绩的陈述、承诺或保证。

通过访问和使用该白皮书或其中任何内容时，您将向本平台、其附属机构和您的团队提供如下保证：

1)在任何购买 Token 的决定中，您并未依赖本白皮书中的任何声明内容;

2)您将自愿承担费用并确保遵守适用于您的所有法律、监管要求和限制（视情况而定）;

3)您承认、理解并同意 Token 可能没有任何价值，不保证也不代表有任何价值和流通属性，并不可以用来做投机相关的投资;

4)平台及其附属机构以及团队成员均不对 Token 的价值、可转让性、流通性以及通过第三方或其他方式提供 XT 项目的任何市场负责或承担责任;

5)您承认、理解并同意，如果您是满足以下条件的某个地理区域或国家的公民、国民、居民（税务或其他相关的）、居住地或国家的绿卡持有人，您将不具备购买任何 Token 的资格：

i.出售 Token 可能会被定义或解释成为出售证券（无论如何命名）或投资产品；

ii.法律禁止接触和参与 Token 的销售或者 Token 被法律、政策、条例、条约或行政法规所禁止的国家和地区。

平台和团队不会也不打算向任何实体或个人作出任何陈述、保证和承诺，并在此声明不承担任何责任（包括但不限于本白皮书的内容以及任何平台发布的其他材料内容的准确性、完整性、及时性和可靠性）。在法律允许的最大范围内，平台、相关实体和服务提供商不承担任何因使用了白皮书内容、平台发布的相关材料以及通过其它形式展现的相关内容（包括但不限于任何错误或遗漏的内容）所产生的侵权、合同纠纷或其他形式导致的非直接的、特殊的、偶然的、间接的或其它形式的损失的责任（包括但不限于任何由此产生的违约或疏忽引起的责任、任何收入和利润的损失以及使用方面和数据的损失）。潜在购买者应仔细考虑、评估与销售，平台、分销商和团队相关的所有风险和不确定性（包括财务、法律和不确定性的风险）。

本白皮书中提供的信息仅供社区讨论，并不具有法律约束力。任何人均无义务就收购 XT 项目订立任何合约和具约束力的法律承诺，除此之外，本白皮书不会接纳任何虚拟货币或其他形式的付款。Token 的买卖协议和长期持续持有 Token 须遵守一套独立条款或一个包含有相关条款和条件的购买协议（视情况而定），这些条款和条件会单独提供给您或可以从网站上获取。如果本条款与条件与本白皮书之间有任何不一致之处，请以本条款与条件为准。

监管机构并没有审查或批准本白皮书中列出的任何信息，而且在任何司法管辖区的法律、法规要求和规则中，都没有规定需要或将要求这样做。本白皮书的发布，分发或传播并不意味着适用的法律、法规的要求或规则已得到履行和遵守。

这只是一个概念白皮书，用来描述将要研发的 XT 项目的远景发展目标。本白皮书可能会不时修改或更换。这里并没有更新白皮书和向受众提供超出本白皮书内容范围之外的其它信息的义务。

本白皮书中包含的所有声明、新闻稿和公众可访问的声明以及平台和 XT 项目团队可能做出的口头声明均可构成前瞻性声明（包括相关的意向声明以及对当前市场状况、经营战略和计划、财务状况、具体规定和风险管理决策的信心和预期等方面）。请注意，不要过分依赖这些前瞻性声明，因为这些声明涉及已知和未知的风险、不确定性风险以及其他多方因素，这可能会导致未来实际结果与这些前瞻性声明所描述的内容大不相同，同时，需要说明的是，并没有独立的第三方审查和判断这些陈述和假设的合理性。这些前瞻性陈述仅适用于本白皮书所示的日期，平台和 XT 项目团队明确表示对该日期之后因对这些前瞻性声明进行修订所引起和产生的后果或事件不承担任何责任（无论明示还是默示）。

在此使用的任何公司或平台的名称或商标（除了与平台或其关联公司相关的内容）并不意味着与这些第三方平台和公司有任何关联或得到了其背书。本白皮书中提及的特定公司和平台仅供参考和说明之用。

本白皮书可能会翻译成中文以外的语言，如果本白皮书的中文版本和翻译版本之间存在冲突或含糊不清之处，应以中文版本为准。您承认您已阅读并理解了本白皮书的中文版本。