



# XZ WHITE PAPER 2.0

打造DeFi+NFT数字医药智慧生态



# 目 录

## 1 前 言

### 项目理念

- 3 XZ 打造DeFi+NFT数字医药智慧生态
- 4 NFT造就XZ高价值捕获
- 5 DeFi铸造XZ高流通性价值
- 6 销毁+融化缔造NFTXZ高稀缺性价值

### XZ应用场景

- 7 以XZ实体智能药柜为枢纽的智慧医药生态
- 8 XZ大健康公链生态
- 9 NFTXZ DeFi
- 10 XZ创新优势

### 技术 支持

- 11 NFT+
- 13 创新的智能药柜挖矿机制
- 15 多重激励体系
- 16 共识机制
- 17 授权节点共识制度
- 24 数据存储共识
- 27 安全性与数据合法性
- 28 数据与预言机



# 目 录

## 通证经济

29 代币价值

30 挖矿机制

31 释放机制

## 发展规划

33 社区治理

34 发展路线图

38 核心团队

39 结论



# 前言

COVID-19的意外到来，加速了整个世界数字化进程，2020堪称“奇点之年”，疫情的扩散彻底改变了人们的社交、工作与生活，与此同时医疗与大健康产业再次被推上了全球经济的风口浪尖。

区块链作为一种多方维护、全量备份、信息安全的分布式记账技术，为医疗、医药数据共享带来了很多突破点。能够有效解决医疗健康领域中的数据存储、共享、溯源防伪等一系列现实问题。

NFTXZ正是在这一特殊历史背景下诞生的加密数字智慧医药生态体系。NFTXZ结合区块链与医疗行业领域知识，以“大健康产业”为核心，构建基于区块链医疗健康数据共享平台、无人智能零售平台，创新性实现了医疗健康产业各方在不影响数据所有权的情况下实现数据的可信交换和验证。

该体系由NFT与DeFi两个部分组成，平台代币XZ是该生态体系中的激励轴心，堪比比特币网络中的BTC，承担着维系整个NFTXZ智慧医药生态长久且自主持续循环的重任，XZ也是联通平台NFT与DeFi系统的重要纽带，每一枚XZ的铸造都离不开实体智能医药矿柜和NFTXZ，XZ在生态体系中的流通又激活DeFi体系，以此形成一个高效价值循环体系。

NFTXZ这种DeFi（高流动性）+NFT（高价值捕获）的独特创新模式也给实体产业数字化升级和数字经济领域带来了全新的想象空间，完美的展现了数字化的一体两面：即“生产力x生产关系”的融合，基于物联网的无人智能零售药柜、医药健康大数据是先进生产力的呈现，基于区块链技术之上的XZ+DAO架构则构建无国界、人人可参与加密经济生态，是对未来分布式商业的探索和实践。



随着XZ在“区块链+医疗”领域的不断深究，大健康数据公链的数字医药智慧生态逐步落实。未来，XZ大健康数据网络将会在监管合规性和医疗、健康监控记录领域发挥出巨大的价值，以及在健康管理、医疗设备数据记录、不良事件安全性、医疗资产管理、医疗合同管理等方面发挥出强大的作用。



# 项目理念

## XZ 打造DeFi+NFT数字医药智慧生态

医疗行业是社会刚需，从需求层面说，人口数量不断增加和老龄化严重，加之我国城镇化率稳步提升人们的就医能力和就医意愿显著提高，尤其是在COVID-19肆虐之后，人们的健康意识更强烈，对医疗的需求不断扩大。然而在供给层面医疗行业规模虽然在逐年增加但人均资源仍不足。除此之外，医疗资源配置、利用率等方面也有待提升。

区块链作为颠覆性的前沿技术，在市场的热捧下，与许多传统行业碰撞，创造出区块链赋能的应用案例，对人类社会生活的方方面面都产生了深远影响。XZ借助区块链去中心化、有序加密的安全性、智能化信任的私密性、可无限扩展的分布式网络、以及NFT的独一无二性，建立独特的DeFi+NFT数字医药智慧生态。打破医疗体系数据孤岛，将个人大健康数据电子化并上链存储，实现分布式数据共享，打破不同系统或机构间的壁垒，减少医疗资源浪费，提高老百姓看病就医的效率；一定程度上遏制假药伪药，在为老百姓提供药品保证的同时，重塑人们对医疗体系的信心。

NFTXZ是基于HECO（火币生态链）开发的流动性矿池，突破性地引入非同质化（NFT）代币NFTXZ锚定数字医药产品XZ实体智能药柜，基于数字资产属性转移、高稀缺性、强流动性等特点，打造DeFi（高流动性）+NFT（高价值捕获）的创新模式，帮助XZ捕获更高的生态价值。



## NFT造就XZ高价值捕获

NFT（Non-Fungible Token）非同质化代币，拥有不可分割、不可替代、独一无二等特性。诚如，莱布尼茨所言说“世界上没有两片相同的树叶”。NFT这种特点意味着NFT可以提供对实物的安全所有权证明以保护商品的价值。

NFTXZ就是利用NFT这一重要属性对标物理世界中的实体“数字医药矿机终端”即XZ实体智能药柜，每一台XZ实体智能药柜都是独一无二的，我们会记录其GPS地理位置，与其在运行过程中的独特数据。XZ实体智能药柜融合了智能零售+医药健康大数据+区块链等技术，对数字医药的所有权等权益进行溯源和保护。XZ实体智能药柜除了承担在物理世界中输送医药用品与服务的重任外，还将成为一台可以远程链接全球数万医生的智能无人远程问诊终端。





## DeFi铸造XZ高流通性价值

每一枚NFTXZ锚定一台XZ实体智能药柜，基于DeFi流动性挖矿机制，质押NFTXZ可产出XZ，打破了NFT流通性差的瓶颈。每台XZ实体智能药柜会7x24小时持续采集该区域的数字医药健康大数据信息，这些大数据在采集、上传、分析、运营的过程中会通过其独特的算法产出XZ。XZ作为加密数字医药生态中的激励凭证，将整合上下游数字医药产业链，以形成强大的“加密数字医药生态”，成为推动人类科技+健康可持续发展的重要力量。



# 销毁+融化缔造NFTXZ高稀缺性价值

NFTXZ在线下能够赋能实体，在线上能够基于NFT特性打造高稀缺性的加密实体资产。为进一步提高NFTXZ价值，在产出XZ的同时，也将激活NFTXZ的自动销毁机制及融化机制。

## 销毁逻辑

NFTXZ前期会基于HECO（火币生态链）进行智能合约部署，代币初始总量为1万枚，铸币开始后便开启自动销毁。

NFTXZ为平台原生数字资产，1枚NFTXZ价值锚定一台XZ实体智能药柜，对标151110枚XZ。每枚NFTXZ对标的151110枚XZ逐步线性释放，每日解锁138枚XZ，并扣除5%的节点托管费用。

## 融化机制

NFTXZ代表的是未来的算力收益权，所以每质押一天，就会减少一天的预期收益，即区块链智能合约中的融化机制。

首先，区块链上的时间序列是用秒去计算，所以算力磨损也是基于秒进行。其次，我们设定了一个标准单位（24小时）=86400秒，当用户质押时间低于86400秒时，那么用户将无法获得收益，并且NFTXZ无损耗；当用户超过n个单位时间，低于n+1个单位时间时，用户将获得n份奖励，同时融化 $n * 1/1095$ 个NFTXZ，即结算时是基于单位时间进行的（unit time）。这意味着用户每质押一天并获得一天的收益时，就会磨损掉相应的NFTXZ，即代表剩余的产币量减少。

在销毁机制和融化机制的双重作用下，NFTXZ总量日益减少，NFTXZ由此成为高稀缺性的加密实体资产。未来我们将上线NFT专用资产转换平台的NFTSwap，成为真正稀缺的DeFi+NFT双轨资产。



# XZ应用场景

## 以XZ实体智能药柜为枢纽的智慧医药生态

NFTXZ锚定的XZ实体智能药柜，是全球首个实体药店+权益通证链接的数字金融智能药柜，每一台药柜背后都有一个药店作为盈利支撑。XZ实体智能药柜是由中国领先的医药企业发起打造的基于“云计算+物联网+权益通证化”的智能医药新零售平台，拥有国家颁发的售药资格证和众多专利技术保障，由中国领先的医药企业直供药品，能够有效解决夜间购药、偏远地区购药、隐私购药、急需购药等现实问题，同时提供远程医疗、家庭药箱等专业的医药服务。

专业的硬件设备技术企业为XZ实体智能药柜提供硬件技术支持和完备的运行基础保障。通过科技芯片植入GPS定位系统和矿机商城使XZ权益通证流通，实现医药产业链的产融一体化闭环，将消费者、权益经销商、药店药企、医药流通公司有效串联，让大众用药放心，让权益收益合理分配。用户还可通过XZ实体智能药柜享受线上医疗问诊平台、医药互联网公司的全国专家资源和远程诊疗服务。计划将在全国大规模布点24小时智能售药柜，让更多用户受益于去中心化医疗服务，真正做到医药配送最后一公里。



## XZ大健康公链生态

“区块链+医疗”拥有多样的应用场景及生态模式，如医疗健康、基因组数据、医疗保险、医务人员身份认证、药品防伪、医疗供应链金融、临床试验、手术记录等等。XZ希望打造一条能够承载更多元数据、更广泛应用的大健康公链。

目前，NFTXZ主要以XZ实体智能药柜作为大健康数据公链生态的重要载体，将药柜的线上医疗系统数据、购药数据、环境情况等数据自动采集并上链至大健康数据公链，为日后公链再开发提供广泛的数据支撑。

未来，XZ构建的大健康数据系统将打破医疗信息领域边界，通过区块链让数据在医院与医院间、医院与保险公司之间流动起来，化解数据孤岛导致低效问题，并且通过人工智能技术提供智能化的服务。在智能化的信任机制下，不需要医患之间的相互信任，就可以建立互信共享机制，规范医疗行为，提升健康医疗服务效率和质量，推动健康医疗大数据应用新发展。

XZ实体智能药柜提供药柜权益通证化系统性方案以及大健康数据公链的底层技术架构搭建由星河共创科技有限公司提供，通过区块链技术优势和通证经济的权益化内核动力，赋能XZ实体智能药柜以及医药产业的提速增效，带来广阔的发展空间和市场影响力。



## NFTXZ DeFi

NFTXZ通过XZ权益通证的有效激励和区块链公开透明、可信任的分布式技术让医疗数据上链，能够有效帮助药品流通过程中的成本测算、渠道监控、药品溯源、收益分配，让追踪溯源践行药品从制作到出售在每一个环节之中。

一方面，用户可通过NFTXZ DeFi流动性挖矿获得XZ；另一方面，XZ可用于XZ实体智能药柜出纳，XZ权益通证的流通，将为XZ实体智能药柜更快、更高效率的搭建自我可循环的用户池。当积累大数据和流量后，项目可以借助专利池进行授权，也可以推动XZ实体智能药柜从药品向医疗服务的延伸，由此形成一个更加完整的DeFi医疗体系。



## XZ创新优势

### 1) 开拓数字化医疗蓝海，打造24小时未来药房

XZ实体智能药柜是首个行业内具备完整产业生态和实体应用场景的智慧医药服务平台，实现实体资产与数字化服务相链接，能够有效解决医院处方外流、就诊程序繁琐、效率低下等问题同时实现互联网线上医生就诊和线下24小时无人未来药房的全生态闭环。作为政策红利下的首个智慧医药新零售项目，XZ实体智能药柜率先开拓创新数字化医疗的蓝海市场。

### 2) 全国布点为用户提供全覆盖式的智慧医药服务

XZ智能药柜真正地开创跨终端无缝协同的智慧医药模式，GPS数字身份识别系统联接。全国布点，7X24小时为用户提供覆盖端、边、云的全栈式场景应用和跨终端无缝协同的健康医疗服务体验，打造从药企到终端、从线下到线上的新零售闭环。

### 3) 自上而下多方合作，发挥产业链优势

医疗行业体系复杂，为了真正找到医药行业的痛点，提供行之有效的区块链解决方案。XZ项目的合作伙伴均在医药行业、区块链技术应用上颇有建树。目前XZ已与中国领先的医药企业、线上医疗问诊平台、医药互联网公司、硬件设备技术企业、星河共创科技有限公司达成战略合作关系，共创XZ智慧医药生态。

XZ真正秉承以人为本理念的创新科技投资项目，经营权和收益权分离，有效构建厂家、权益经销商和消费者新价值互联网，实现多方协同共赢。



# 技术支持

## NFT+

NFT“唯一性”的特点让数字资产扩展到了更高的维度。如游戏中的身份、珍稀道具、极品装备等数字资产完美符合成为NFT的条件。NFT是XZ的核心数字资产体系。它提供了比传统NFT更加强大的数据储存与验证接口，因而更加适合于数字资产认证及管理。与传统的通证不同，每一个NFT具有一个唯一可以识别的ID，且不可细分。比如著名的加密猫（CryptoKitties）游戏，每一只猫即是一个不可细分的NFT。由于生活中的每一个物品都可以看成是非同质的（即唯一的），每一台XZ实体智能药柜都是唯一的，所以NFT具有广泛的应用场景。

NFTXZ认为，无论是药品的追踪溯源，还是个体的健康数据也具备这种特性。因此，NFTXZ将NFT概念引入到实体智能药柜，一方面XZ实体智能药柜能够对售卖出去的每一份药品实现全程跟踪溯源；另一方面，XZ实体智能药柜将会为每一个用户及案例个人医疗档案，也就是个人的健康大数据，随着NFTXZ健康医疗体系落地，无论您在哪一家医院、诊所、药店看病就医，您所有的健康大数据将在您允许的情况下被问诊医生查看。这将是区块链推进医疗发展极其重要的一步。



XZ的核心数字资产是新一代的非同质化通证NFT+。NFT+将在原有的NFT基础上提供一个强大的大数据录入与管理接口。NFT+是NFT的改进版本，旨在解决数据储存与验证及实物链接问题。NFT+的解决方案是在NFT中引入一个私钥的概念。每一个NFT+通证除了对应着一个唯一的ID外，还对应了一个公钥私钥对。NFT+在交易或转移时需要有私钥的签名才能完成交易。每一个NFT+的数据，在储存之前需要使用其私钥进行签名。

如此操作，其作用有以下三方面：

- 1、NFT+的公钥可以用来验证其附属数据的合法性，从而可以防止数据篡改。
- 2、NFT+的私钥可视为另一层的拥有权证明。此私钥与拥有者的钱包合并作用可以产生更为丰富的应用场景。比如，NFTXZ的拥有者可以将NFTXZ质押。在质押期，NFTXZ通证将表现为数字资产XZ。私钥拥有者可以随时赎回资产。
- 3、NFT+的私钥可以是由实物确定的。比如未来电子产品或者实际许可证等物件会植入了一个可产生签名但不泄露私钥的集成电路。交易时需要实物的参与才可发生交易。这解决了NFT与实物脱节的问题。

为了给XZ智能药柜提供一个完整的生态保证，XZ将提供一个去中心化的NFT日志系统，用户都可以获取其完整的不可篡改的行为数据。



## 创新的智能药柜挖矿机制

用户通过获得代表药柜算力的NFTXZ，即用以获得挖矿资格以及未来的产币收益权。XZ目前智能合约基于HECO主网，实现完全的去中心化激励机制。

在1.0版本的合约中，用户使用NFTXZ挖矿获得XZ奖励，对应于药柜矿机的三年有效期，当用户使用NFTXZ挖矿时，会产生磨损，磨损期限为1095天，每天铸币138枚XZ，相对应的磨损为1/1095。

磨损机制令NFTXZ可以用以反映时间线问题，即已经使用过的矿机与未使用过的矿机的潜在收益是不同的，这一特性能极大地扩展未来的适配性。

在2.0版本中，NFTXZ的挖矿经济模型进行了迭代更新，在新版的挖矿激励机制中，除NFTXZ外，需要质押XZ以及提供用于作为能量消耗的XZ。

XZ质押数量：

质押的XZ数量=质押的NFTXZ数量\*4140

XZ手续费池存入数量：

存入的手续费=质押的NFTXZ数量 X 1500

XZ产出公式：

XZ日产量=138\*质押的XZ数量/4140\*对数函数

(1 NFTXZ的满算力是铸币138 XZ/日，其中5%为节点)

NFTXZ的融化公式：

NFTXZ每日融化数量=XZ日产出量\*1.05/15000

手续费消耗公式：

XZ每日消耗=XZ日产量\*1%



新版的NFTXZ挖矿合约，在原有NFTXZ的基础上，创造了XZ质押和XZ消耗两个需求，这一改变存在两方面考虑。

一是出于经济模型的优化，通过增加这两方面，在系统层面增加了XZ的需求，而在一定程度上降低了供给，同时由于手续费消耗池的存在，XZ的通缩途径被增加了。

二是出于技术层面要求，随着主网上线（这将在后面进行描述），主网将在数据存储，智能合约的执行方面进行优化，而为了确保数据存储的有效性，类似于IPFS的质押规则是一个很好的解决方案，这也是本次升级增加XZ质押的一个技术考量。

在主网上线前，XZ合约可能将会同样部署在币安的BSC链上，这主要取决于未来的应用场景。



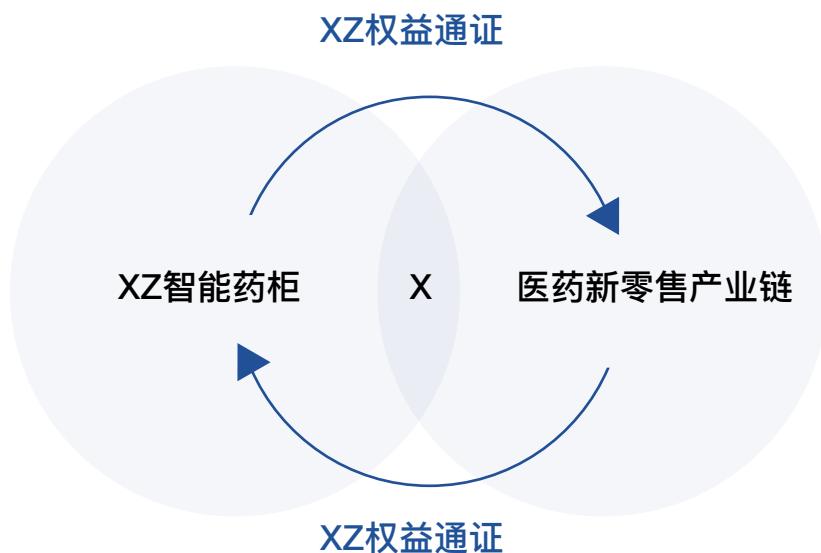
## 多重激励体系

用户购买XZ实体智能药柜后，可以通过账号注册登陆XZ实体智能药柜的APP。在完成注册的同时，APP会自动为用户分配区块链数字地址，XZ实体智能药柜的药品销售收益、广告收益、外送收益以及XZ实体智能药柜授权合作的药房内药品的销售收益，均会通过后台云计算智能系统和矿机商城的算力机制产出，以XZ权益通证的方式回馈给用户。

用户持有XZ权益通证，还可以在XZ实体智能药柜的APP内：

- 1) 通过XZ权益通证兑换产品；
- 2) 通过XZ权益通证兑换专业的远程诊疗服务；
- 3) 持有XZ权益通证享受其权益增值服务；

随着未来XZ权益通证经济应用场景的不断拓展，用户还将参与到更多的体验场景中，享受更多的权益收益。





# 主网机制

## 共识机制

前测试主网采用POZ共识，POZ共识是基于数据存储和授权式节点共识制度。



## 授权式节点共识制度

### 1 为何不采用传统的POW共识?

首先，POW存在51%攻击问题，恶意挖矿者超过全网算力的51%后基本上就能完全控制整个网络。由于链无法被更改，已上链的数据也无法更改，但恶意挖矿者也可以做一些DOS攻击阻止合法交易上链。考虑到具有相同创世块的矿工都能加入你的网络，潜在的安全隐患会长期存在。

其次，POW大量的电力资源消耗也是需要作为后续成本考虑。POS可以解决部分POW问题，比如节约电力，在一定程度上保护了51%的攻击(恶意矿工会被惩罚)，但从控制权和安全考虑还有欠缺，因为POS还是允许任何符合条件的矿工加入。

在已经运行的测试网络Ropsten中，由于POW设定的难度较低，恶意矿工滥用较低的POW难度并将gaslimit扩大到90亿（正常是470万），发送大量的交易瘫痪了整个网络。而在此之前，攻击者也尝试了多次非常长的重组(reorgs)，导致不同客户端之间的分叉，甚至不同的版本。

这些攻击的根本原因是POW网络的安全性依赖于背后的算力。而从零开始重新启动一个新的testnet将不会解决任何问题，因为攻击者可以一次又一次地进行相同的攻击。Parity团队决定采取紧急解决方案，回滚大量的块，并设置不允许gaslimit超过某一阈值的软分叉规则。



虽然Parity的解决方案可能在短期内有效，但是这不是优雅的：Ethereum本身应该具有动态gaslimit限制；也不可移植：其他客户端需要自己实现新的软分叉逻辑；并与同步模式不兼容，也不支持轻客户端；尽管并不完美，但是Parity的解决方案仍然可行。一个更长期的替代解决方案是使用授权共识共识，相对简单并容易实现。

## 2. 授权共识的特点

授权共识是依靠预设好的授权节点(signers)，负责产生block。

可以由已授权的signer选举(投票超过50%)加入新的signer。

即使存在恶意signer，他最多只能攻击连续块(数量是  $(\text{SIGNER\_COUNT} / 2) + 1$ ) 中的1个，期间可以由其他signer投票踢出该恶意signer。可指定产生block的时间。

## 3. 授权共识需要解决的问题

如何控制挖矿频率，即出块时间？

如何验证某个块的有效性？

如何动态调整授权签名者(signers)列表，并全网动态同步？

如何在signers之间分配挖矿的负载或者叫做挖矿的机会？

对应的解决办法如下：

协议规定采用固定的block出块时间，区块头中的时间戳间隔为3s，先看看block同步的方法，从中来分析授权共识中验证block的解决办法。

有两种同步blockchain的方法：

经典方法是从创世块开始挨个执行所有交易。这是经过验证的，但是在Ethereum的复杂网络中，计算量非常大。

另一个是仅下载区块头并验证其有效性，之后可以从网络下载任意的近期状态对最近的区块头进行检查。



显然第二种方法更好。由于授权共识方案的块可以仅由可信任的签名者来创建，因此，客户端看到的每个块（或块头）可以与可信任签名者列表进行匹配。要验证该块的有效性就必须得到该块对应的签名者列表，如果签名者在该列表中带包该块有效。这里的挑战是如何维护并及时更改的授权签名者列表？存储在智能合约中？不可行，因为在快速轻量级同步期间无法访问状态。

因此，授权签名者列表必须完全包含在块头中。那么需要改变块头的结构，引入新的字段来满足投票机制吗？这也不可行：改变这样的核心数据结构将是开发者的噩梦。

所以授权签名者名单必须完全符合当前的数据模型，不能改变区块头中的字段，而是 \*\*复用当前可用的字段: **Extra**字段.\*\*

**Extra**是可变长数组，对它的修改是非侵入操作，比如RLP、hash操作都支持可变长数据。**Extra**中包含所有签名者列表和当前节点的签名者对该区块头的签名数据(可以恢复出来签名者的地址)。

更新一个动态的签名者列表的方法是复用区块头中的 **Coinbase**和**Nonce**字段，以创建投票方案：

常规的块中这两个字段置为0

如果签名者希望对授权签名者列表进行更改，则将：

**Coinbase** 设置为被投票的签名者

将 **Nonce** 设置为 0 或 0xff ... f 投票，代表添加或移除

任何同步的客户端都可以在块处理过程中“统计”投票，并通过投票结果来维护授权签名者列表。



为了避免一个无限的时间来统计投票，我们设置一个投票窗口，为一个epoch，长度是30000个block。每个epoch的起始清空所有历史的投票，并作为签名者列表的检查点。这允许客户端仅基于检查点哈希进行同步，而不必重播在链路上完成的所有投票。

目前的方案是在所有signer之间轮询出块，并通过算法保证同一个signer只能签名 ( $\text{SIGNER\_COUNT} / 2 + 1$ ) 个block中第一个。

综上，授权共识的工作流程如下：

在创世块中指定一组初始授权的signers，所有地址保存在创世块Extra字段中。启动挖矿后，该组signers开始对生成的block进行签名并广播，签名结果保存在区块头的Extra字段中。

Extra中更新当前高度已授权的所有signers的地址，因为有新加入或踢出的signer每一高度都有一个signer处于IN-TURN状态，其他signer处于OUT-OF-TURN状态，IN-TURN的signer签名的block会立即广播，OUT-OF-TURN的signer签名的block会延时一点随机时间后再广播，保证IN-TURN的签名block有更高的优先级上链。如果需要加入一个新的signer，signer通过API接口发起一个proposal，该proposal通过复用区块头Coinbase(新signer地址)和Nonce("0xffffffffffffffffffff")字段广播给其他节点。所有已授权的signers对该新的signer进行“加入”投票，如果赞成票超过signers总数的50%，表示同意加入。

如果需要踢出一个旧的signer，所有已授权的signers对该旧的signer进行“踢出”投票，如果赞成票超过signers总数的50%，表示同意踢出。



signer对区块头进行签名

Extra的长度至少65字节以上(签名结果是65字节，即R、S、V、V是0或1)。

对blockHeader中所有字段除了Extra的后65字节外进行RLP编码。

对编码后的数据进行 Keccak256 hash。

签名后的数据(65字节)保存到Extra的后65字节中。

### 授权策略

以下建议的策略将减少网络流量和分叉

如果签名者被允许签署一个块（在授权列表中，但最近没有签名）。

计算下一个块的最优签名时间（父块时间+ BLOCK\_PERIOD）。

如果签名人是in-turn，立即进行签名和广播block。

如果签名者是out-of-turn，延迟 `rand(SIGNER_COUNT * 500ms)` 后再签名并广播  
级联投票。

当移除一个授权的签名者时，可能会导致其他移除前的投票成立。例：ABCD4个  
signer，AB加入E，此时不成立(没有超过50%)，如果ABC移除D，会自动导致加入  
E的投票成立(2/3的投票比例)。

### 投票策略

因为blockchain可能会小范围重组(small reorgs)，常规的投票机制(cast-and-forget，投票和忘记)可能不是最佳的，因为包含单个投票的block可能不会在最终的  
链上，会因为已有最新的block而被抛弃。

一个简单但有效的办法是对signers配置“提议(proposal)”，例如“`add 0x...`”，  
“`drop 0x...`”，有多个并发的提议时，签名代码“随机”选择一个提议注入到该签  
名者签名的block中，这样多个并发的提议和重组(reorgs)都可以保存在链上。



该列表可能在一定数量的block/epoch之后过期，提案通过并不意味着它不会被重新调用，因此在提议通过时不应立即丢弃。

加入和踢除新的signer的投票都是立即生效的，参与下一次投票计数。

加入和踢除都需要超过当前signer总数的50% 的signer进行投票。

可以踢除自己(也需要超过50%投票)。

可以并行投票(A, B交叉对C,D进行投票)，只要最终投票数操作50%。

进入一个新的epoch，所有之前的pending投票都作废，重新开始统计投票。

投票场景举例

ABCD，AB先分别踢除CD，C踢除D，结果是剩下ABC

ABCD，AB先分别踢除CD，C踢除D，B又投给C留下的票，结果是剩下ABC

ABCD，AB先分别踢除CD，C踢除D，即使C投给自己留下的票，结果是剩下AB

ABCDE，ABC先分别加入F(成功,ABCDEF)，BCDE踢除F(成功，ABCDE)，DE加入F(失败，ABCDE)，BCD踢除A(成功，BCDE)，B加入F(此时BDE加入F满足超过50%投票)，结果是剩下BCDEF。

#### 4. 授权共识中的攻击及防御

恶意签名者(Malicious signer)。恶意用户被添加到签名者列表中，或签名者密钥/机器遭到入侵。解决方案是，N个授权签名人的列表，任一签名者只能对每K个block签名其中的1个。这样尽量减少损害，其余的矿工可以投票踢出恶意用户。

审查签名者(Censoring signer)。如果一个签名者（或一组签名者）试图检查block中其他signer的提议(特别是投票踢出他们)，为了解决这个问题，我们将签名者的允许的挖矿频率限制在 $1/(N/2)$ 。如果他不想被踢出去，就必须控制超过50%的signers。

“垃圾邮件”签名者(Spamming signer)。这些signer在每个他们签名的block中都注入一个新的投票提议.由于节点需要统计所有投票以创建授权签名者列表，久而



久之之后会产生大量的垃圾的无用的投票，导致系统运行变慢。通过epoch的机制，每次进入新的epoch都会丢弃旧的投票。

并发块(Concurrent blocks)。如果授权签名者的数量为N，我们允许每个签名者签名是 $1/K$ ，那么在任何时候，至少 $N-K$ 个签名者都可以成功签名一个block。为了避免这些block竞争(分叉)，每个签名者生成一个新block时都会加一点随机延时。这确保了很难发生分叉。



## 数据存储共识

作为矿机的药柜终端，是目前的主要物理节点，药柜终端需要负责记录相关的数据，包括消费、医疗等，这些数据与收益高度相关，未来具有极高的延展性。为了确保数据的完整性以及准确性，主网将数据存储的共识作为一个基本共识进行验证。

### 1. 复制证明 (PoRep)

复制证明是一种过程，存储节点可以通过该过程向XZ网络证明他们已代表网络创建了某些数据的唯一副本。

### 2. 时空证明 (PoSt)

时空证明是一种过程，存储矿工可以通过该过程向XZ网络证明他们已存储的文件，并在一段时间内代表该网络继续存储某些数据的唯一副本。

### 3. 窗口时空证明 (WindowPoSt)

窗口时空证明 (WindowPoSt) 是一种机制，可用来审核存储矿工的承诺。它看到每个24小时周期分解为一系列窗口。相应地，每个存储矿工的保证扇区集都被划分为子集，每个窗口一个子集。在给定的窗口内，每个存储矿工必须为其各自子集中的每个扇区提交时空证明。这要求可以立即访问每个面临挑战的部门，并且将导致zk-SNARK压缩的证明作为块中的消息发布到XZ区块链。这样，在每个24小时内至少对每个保证的存储部门进行一次审计，并保存永久，可验证的公共记录，以证明每个存储矿工的持续承诺。



XZ网络期望存储数据的持续可用性。未能为某个扇区提交WindowPoSt将导致故障，并且将削减提供该扇区的存储矿工（惩罚）。

#### 4.赢得时空证明（WinningPoSt）

赢得时空证明（WinningPoSt）是一种机制，通过这种机制，存储矿工可以为他们对XZ网络的贡献而获得奖励。在每个时期的开始，都会选举少量的存储矿工来为每个矿开采一个新的区块。为此，每个矿工的任务是为指定部门提交压缩的时空证明。每个当选矿工谁成功地创建了一个块被授予FIL，以及收取其他XZ参与者的费用包括在块消息的机会。

未能在必要的窗口中执行此操作的存储矿工将丧失其开采区块的机会，但不会因此而受到惩罚。

附录：zk-SNARK代表零知识的简洁非交互式知识论证：

知识论证是一种结构，通过这种结构，称为证明方的一方可以说服另一方（验证方）证明方可以访问某些信息。这种构造有几种可能的限制：

非交互性知识论点要求从证明者发送给验证者的单个消息应作为充分论据。

知识的零知识论点要求验证者不必为了证明证明者的主张而需要访问证明者可以访问的知识。

对于这两个术语的适当定义来说，简洁的知识论点可以被“迅速”验证，并且是“小的”论据。



零知识的简洁非交互式知识论证（zk-SNARK）体现了所有这些属性。XZ利用这些构造来使其分布式网络能够有效地验证存储矿工是否正在存储他们承诺存储的文件，而无需验证者自己维护这些文件的副本。

总之，XZ使用zk-SNARKs生成一个“证明”，使“验证者”确信存储文件上的某些计算已正确完成，而验证者无需访问存储文件本身。



## 安全性与数据合法性

我们需要面对的安全性问题包括：

**51%攻击：**51%攻击通常存在于POW共识当中，这也是XZ主网并未采用POW共识的主要原因之一，为了在降低成本，提高效能的情况下，规避掉51%攻击，采用授权节点，能够尽量高的提高可信节点的占比，以规避51%攻击。

**女巫攻击：**女巫攻击指的是某些节点模拟多个节点身份以骗取奖励，相对于51%攻击而言，因为授权节点的数量相对而言更加有限，因此女巫攻击的风险更高，普通节点仅同步来自挖矿节点发来的新区块，并不参与共识，而觉得其共识算法的安全性仅依赖于验证节点的数量，因此普通节点的数量增加并不能提升拜占庭容错的安全性。为了规避女巫攻击，XZ主网拥有另一套新的验证机制以验证身份，包括验证抵押以及使用更多非挖矿节点进行验证等方式。

### 双挖以及跳块等共识攻击

当节点开放后，矿工可以在忽略共识机制的条件下采取在同一高度下同时打包两个区块，或跳块等方式骗取主网奖励，在这种情况下，将直接没收所有抵押的XZ通证以作惩罚。

### 数据合法性：

与其他的以存储为主要目标的主网（如IPFS）不同，XZ主网目前的数据拥有自己的来源以及验证方式。如此前所说，现实世界中的药柜，目前充当XZ主网主要的数据采集节点，以及验证节点。药柜本身具有数据采集以及录入功能，采集以及录入的数据包括价格，用户数据以及用户的行为数据。



## 数据与预言机

由于拥有数据的采集以及存储功能，XZ智能药柜天然具有预言机属性。

在经过数据采集后，XZ智能药柜节点能够为主网提供数据喂价。随着药柜节点的不断部署，这将形成一个可信的数据网络，主网上的智能合约能够调用获得相关的数据喂价。

预言机的存在使XZ的主网存在极大的扩展性和想象空间，当智能合约能够直接调用链上的医疗以及用户数据，那么其他数据在提高合约可用性方面也是可行的。



# 通证经济

## 代币价值

XZ作为大健康数据公链的主网通证，拥有链与现实交互、实体矿机挖矿、算力释放等全新颠覆性概念，以及基于“云计算+物联网+权益通证化”的去中心化解决方案，具有抗垄断化、公平透明等特质，通过实体与通证链接实现全链路生态闭环，切实高效地解决传统实体经济的问题。

基于NFTXZ的稀缺性映射和XZ本身的销毁、通缩双涡轮驱动机制，内循环挖矿、外循环流通实现内外一体化，XZ由此具备科学、自带造血能力的增值逻辑，并塑造长期主义生态价值。



# 挖矿机制

## 节点头矿阶段

XZ总量的1%（1511万枚）用于节点初期挖矿，主要用于机构节点以及爆石基金会挖矿，挖矿机制为POZ算法，无私募、无质押、无GAS燃烧费。1T算力每天产出138枚，并扣除5%节点托管费用。

## 正式挖矿阶段

节点头矿阶段完成后，XZ将自动进入正式挖矿阶段。

### 1) 质押挖矿-第一阶段

XZ总量的2%（3022万枚）用于质押挖矿第一阶段，每T算力挖矿需要质押4140枚XZ作为保证金，取消NFTXZ质押挖矿后，质押的XZ锁仓180天解锁后方可提取。赎回的NFTXZ可再次用于质押，当用户再次质押NFTXZ进行挖矿时，仍需质押相应的XZ作为保证金。同时，每T算力铸币时需要燃烧对应产出XZ的1%作为GAS费。

### 2) 质押挖矿-第二阶段

XZ总量的17%（2.5687亿枚）用于质押挖矿第二阶段，每T算力挖矿需要质押8280枚XZ作为保证金，取消NFTXZ质押挖矿后，质押的XZ锁仓180天解锁后方可提取。赎回的NFTXZ可再次用于质押，当用户再次质押NFTXZ进行挖矿时，仍需质押相应的XZ作为保证金。同时，每T算力铸币时需要燃烧对应产出XZ的1%作为GAS费。

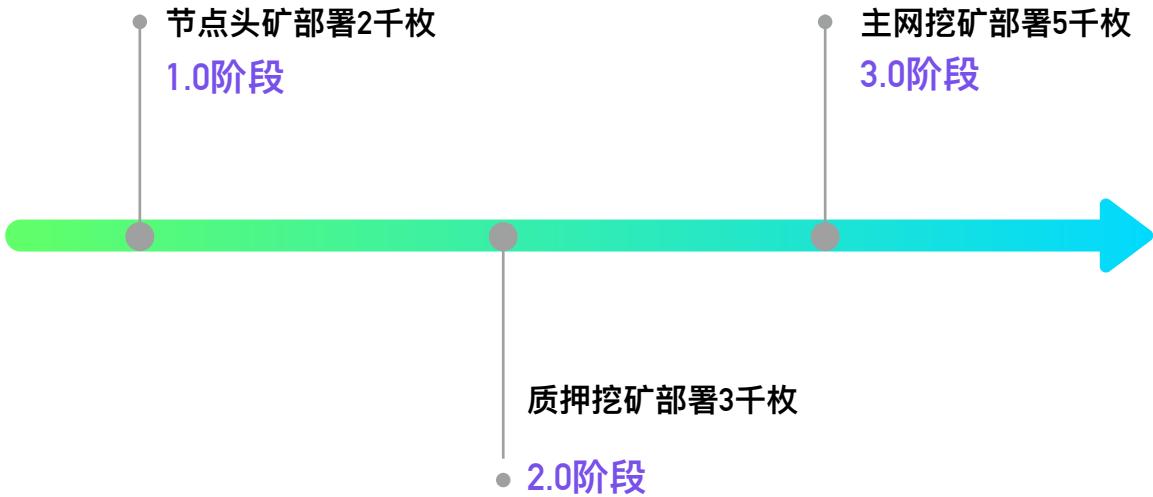


### 3) 主网挖矿阶段

大健康数据公链主网上线后，XZ总量的80%（12.088亿枚）用于POZ算力挖矿，每T算力挖矿需要质押12420枚XZ作为保证金，取消NFTXZ质押挖矿后，质押的XZ锁仓180天解锁后方可提取。赎回的NFTXZ可再次用于质押，当用户再次质押NFTXZ进行挖矿时，仍需质押相应的XZ作为保证金。每T算力铸币时需要燃烧对应产出XZ的1.5%作为GAS费，拥有更多算力可以提高工作量证明机制下获得爆块奖励的概率。

## 释放机制

1万枚NFTXZ通过以下三个阶段逐步线性释放，无私募，并基于DAO机制进行全球去中心化节点建设和社区自治治理。





## 通缩效应

XZ Token上线数字资产交易所之后，其市场价格拥有实体资产的稳定支撑，XZ 智能药柜实体销售收益的 45% 将进行市值管理回购 XZ Token，回购即销毁，有效通缩助推价值增值，将数字资产的价值真正回归于XZ Token的全球共识者。由此，质押产出→通缩→回购→销毁的闭环路径，形成了一个完整的通证经济生态圈。

XZ Token发行总量恒定为15.11亿枚，无预挖无增发，随着DeFi 流动性挖矿和NFTXZ的自动销毁，XZ Token 将呈现高稀缺性、强流动性、资产价值稳步提升的趋势。



# 发展规划

## 社区治理

NFTXZ采用区块链自然分散的操作和管理方法，创建了一个基于用户协作努力的合作系统——XZ DAO，利用区块链中每个节点的权利和义务的等效性，以确保我们的用户社区能够获得平等的权利与义务。

在XZ DAO，参与者既是投资人，是员工，也是这个组织的管理者所有参与者都遵循同一共识，不受任何人干预，自由地交换、记载、更新数据。由于信仰相同，每个参与者又有大批拥护者，他们以共识缔结联盟，相互自觉的协作，在帮助其他参与者实现理想的同时，共同治理，推动组织前进。

自治社区本质上讲也不是完全去中心化的，而是有中心加上自治。当新的中心，也践行不断输送财政政策的话，领土就会不断的扩张，就会反映在我们的商业应用，反映在我们的资产升值上。最终，人人都能实现自己的商业抱负。



# 发展路线图

## 2021年Q1

- NFTXZ的分散应用DeFi流动性矿池在Heco部署智能合约；
- XZ Token的POZ算法在Heco主网部署完成；
- NFTXZ节点矿池进行中，Dapp1.0（xzcloudpool.net）版本上线；
- XZ Token开启创世头矿，参与者主要包括DAO基金节点、媒体机构；
- NFTXZ白皮书V1.0发布；
- NFTXZ官方网站V1.0（域名：xzpool.com）上线；
- NFTXZ完成2000T算力部署，并释放相应算力；
- XZ智能药柜1.0进行工厂标准化生产；
- NFTXZ启动基金节点；
- XZ Token创世头矿产出达到7556694.39枚。



# 发展路线图

## 2021年Q2

- XZ Token正式进入POW挖矿阶段；
- XZ钱包1.0开发完成并上线；
- XZ 开始机构轮；
- XZ 进行IDO；
- NFTXZ完成4000T算力部署；
- XZ智能药柜2.0持续布局，构建完善药品供应链及新零售系统。



# 发展路线图

## 2021年Q3

- 大健康数据公链主网测试；
- XZ智能药柜线上问诊系统上线，数据储存及处理系统开始研发；
- XZ钱包2.0版本上线，支持DeFi借贷功能；



# 发展路线图

## 2021年Q4-2022年Q2

- 大健康数据公链主网公测并正式上线；
- XZ智能药柜3.0支持数据采集，并上链至公链主网；
- XZ钱包3.0版本上线，实现多链资产互通；
- 大健康数据公链主网实现跨链交易；
- 完成全国一万台XZ实体智能药柜点落地。



# 核心团队

**王宝征**

修正清修新零售事业部副总裁 深圳卓联控股联合创始人  
区块链金融科技领域投资者。2015年开始涉足通证研究，拥有多年创业和运营管理经验，在房地产、医药、电商、供应链管理等实体领域拥有丰富经验。

**袁广恒**

星河共创创始人 新加坡XZ基金会会长  
数字金融服务及策略领导者。2017年开始进入加密货币领域，参与了多个项目的早期投资。近年来，主要专注于数字金融及通证经济体系研究，协助许多巨头企业解决关键的数字化升级和战略扩张问题。

**赵小悦**

星河共创COO 新加坡XZ基金会运营官  
曾任OFbank市场运营负责人，CoinMex交易所市场运营&上市负责人，负责过多个海外项目的落地方案，对项目全周期运营部署有一定经验。

**王文鑫 Steven**

XZChain CTO XZ技术总监  
香港中文大学数学与信息工程双学士学位，加州大学伯克利分校数学系Master。  
量化交易平台iaitrade的发起人，曾任职于美银美林(香港) 固定收益部门，负责  
算法以及套利投研，目前专注于DeFi、NFT领域的精研加密算法。



## 结论

虽然NFTXZ目前仍不完美，但XZ关于NFT领域的愿景正在实现，和DeFi一样，NFT拥有光明的未来。越来越多像NFTXZ这类的代币尝试和DeFi结合，并逐渐拼凑起NFT生态领域具有可组合性的NFT乐高。

人类所珍视的资产，可以由我们的价值观决定，金融市场中标的资产的价值来源于我们所遵循的道德观念所创造的价值，集体信仰或许也有胜过基本面的可能性，变化正在发生。

对于全球的数字原住民和加密货币爱好者而言，Crypto文化提供了一个经济产出和文化表达的新景观，真正的数字所有权时代已然到来！