

ChainX | 白皮书



2020.12.31

 ChainX

打造比特币的 layer2 平台

背景	3
概述	4
系统架构	5
经济系统	7
共识算法	10
账户系统	11
社区自治	12
比特币金融平台	17
数字资产网关	26
波卡二级中继链	27
路线图	28

比特币是一种以区块链技术为基础且总量恒定在 2100 万枚的数字货币。其诞生至今，已经走过 11 个年头，期间价格几乎从零增长至 20000 美元，这让比特币的商品属性尤为突出。2017 年比特币被冠以“数字黄金”的称号，其抗通胀、去中心化、全球化、匿名性等特性，决定它的不可替代性。

近期，围绕比特币产生了很多有影响力的事情和现象，DEFI 的兴起、PayPal 支持比特币等主流加密货币的购买和出售、新加坡新展银行开设数字货币交易所、灰度基金大举买入比特币等，这些事件的意义和价值远远超过比特币从 4000 美金上涨到 20000 美金所带来的市值增长，这预示着比特币正在从支付媒介的角度重新被认识，然而这些都还可能只是比特币价值体现的冰山一角。金融市场宏观实践还包括：比特币的外溢效应（DEFI）、比特币衍生品市场、灰度基金等。

与此同时，比特币作为通往数字货币世界的钥匙，逐步开启区块链深层技术的大门，其潜在价值也在被快速挖掘释放，近年来，比特币背后代表的区块链技术已经开始引领继互联网之后的又一次重大的技术变革。目前最为受关注的是针对比特币 Layer2 领域的研究和探索，其旨在解决以比特币为首的区块链性能拓展问题。

ChainX 定位于比特币 Layer2 扩展和资产网关研究，实现高性能的比特币交易托管和资产跨链互通。

其中，Layer 2 技术通常被称为“链下”解决方案，其主要目的是扩展区块链的性能，同时保留分布式协议的去中心化优势。为了构建一个好的区块链生态系统，需要在架构中做一些事情来平衡安全性、去中心化和可扩展性的需求。Layer 2 平台和协议以减少基础层（根链）负担的方式来处理数据，通过将主链的部分数据处理转移到 Layer 2 上，从而增强整个区块链网络的可扩展性。区块链正演变成为多层的系统，比特币 Layer2 的扩展可以帮助我们创建“可用”的区块链系统，并扩展到其他行业中去，在不破坏 Layer1 的基础上，让更多的区块链应用场景、支付场景在 Layer2 层遍地开花。

ChainX 资产网关是全球首个基于 Substrate 框架开发的项目，作为 Polkadot 生态的资产中转枢纽，利用跨链消息传递协议接通 Polkadot 生态以外的资产流通，在解决单链间资产互通的基础上，打通多链信息传输，逐步演化为 Polkadot 的二级中继链，将主流的比特币等外部资产路由进 Polkadot 生态，并孵化后续的衍生金融服务。

在数字经济蓬勃发展的当下，已进入了万物皆资产、资产即价值、价值即可交易的时代，以比特币为代表的加密数字资产在新一轮的国际金融、货币秩序博弈中充当重要的角色，其背后的区块链技术也在突飞猛进的拓展而来。然而，链与链之间无法突破隔离，无法建立有序连接、无法进行资产跨链、自由流动、低摩擦互换，则无法实现区块链价值互通的愿景。为了打破其价值孤岛，ChainX 通过对比特币 Layer2 的拓展、数字资产网关及波卡2级中继链的运行，旨在打造安全稳定、价值互通的全生态资产跨链流转体系。

ChainX 是波卡生态基于 Substrate 框架开发且最早上线的项目，其中，Substrate 是由以太坊前 CTO Gavin Wood 主导的 Parity 团队进行设计和开发的区块链架构开发平台，具有完全通用的状态转换功能 (State Transition Function, STF) 和模块化组件，实现了共识，网络和配置。此外，还具有底层数据结构的标准和约定，特别是 Runtime 模块库 (Substrate Runtime Module Library, SRML)，从而可实现快速开发一条区块链。ChainX 的快速发展迭代与 Substrate 框架的通用便捷性有着密不可分的关系。

ChainX 致力于比特币 Layer2 拓展、数字资产网关及波卡 2 级中继链的研究与应用。在治理运行层面，ChainX 采用动态资产挖矿模式，实现安全高效的链上治理和共识；在技术实现层面，ChainX 通过“轻节点+托管方案”实现主流加密货币在异构多链的资产跨链，并通过去中心化比特币资产托管和镜像资产跨链形成数字资产网关，实现所有加密货币同链交易；同时，作为 Polkadot 的第二层网络，承担拆分多链架构，搭建平行转接桥，撮合多方交易的角色。

ChainX 上线之初基于 Substrate 1.0 稳定运行一年半的时间，在波卡 2.0 正式发布后，ChainX 已于 2020 年 11 月底正式上线 2.0 主网。ChainX2.0 建立在通用的基础链框架 Substrate2.0 之上，实现了混合 PoS 共识、链上理事会治理、Wasm 虚拟机、智能合约原生执行、高效轻客户端协议、Off-chain worker、多重签名等功能，同时与 Polkadot 网络具有高度兼容性。

其中，PoS 共识首创了 One Asset One Vote 的资产挖矿模式，不存在 ICO 阶段，根据用户跨链充值进来的 BTC、ETH、EOS 等多种资产的市值衡量权重与原生代币共同参与挖矿，沿用比特币从零开始逐步减半的模式发行新币，公平分配系统发行的 PCX，避免了预挖发行及算力垄断。用户将自己持有的各类数字资产跨链接入 ChainX 后，既可在系统集成的交易所 DApp 上完成币币资产交易，参与比特币金融衍生运作，同时也将产生公允价格进行资产市值权重挖矿。

ChainX 现阶段采用去中心化的轻节点方式，跨链整合主流数字资产，现已实现比特币跨链。后续将结合独立信托人、MPC、同态加密等手段升级跨链流程，陆续开展比特币金融衍生，加速 ETH、ERC20、EOS、ADA、ZEC 等主流币种的接入。同时培养社区进行跨链资产转账的习惯和开发者生态，促进比特币价值的流动，孵化采用最新智能合约技术的 DApp。





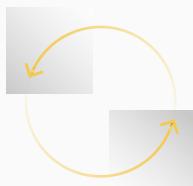
PCX 模块

基于原生资产 PCX 的运作程序。主要包含了 PCX 质押挖矿，支付手续费，参与链上治理，发放跨链资产挖矿奖励，用于比特币金融衍生抵押等。



DEX 模块

ChainX 链上发生的不同资产之间的跨资产交易模块。这样可以促进异链资产形成快速流通且能最大化的节省交易费用。



跨链模块

异链资产及 X-Token 在进入或者转出 ChainX 网络时用到的模块。主要包括了跨链交易验证系统，链上铸币程序，信托程序以及 X-Token 充提程序等。

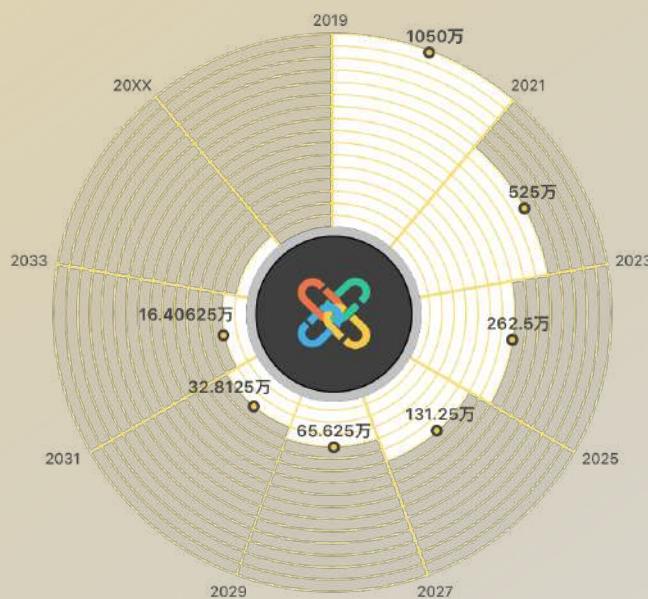


中继模块

ChainX 网络与外界各原链传递信息及辅助验证的主要窗口。主要包含了更新原链信息程序，原链监听程序及 ChainX 跨链信息收集传递程序等。

发行模式

ChainX 发行的加密货币 PCX (P 代表 Polkadot) , 总量 2100 万枚, 前 21 万个分红周期, 即初始轮分红周期, 每个分红周期奖励为 50 个 PCX。次轮分红周期奖励为 25 个 PCX, 依次类推。初始轮分红周期发行量的 20% 归创始团队所有, 用于持续性的开发经费。之后的发行量将全部归社区所有, 创始团队将只占总量的 10%。



挖矿分类

ChainX 采用 One Asset One Voted 的资产挖矿模式, 主要由跨链资产挖矿和投票挖矿两种形式构成。所有参与方以 PCX 为算力单位进行竞争。

跨链挖矿 指用户持有通过充值, 映射等方式进入 ChainX 的各类链外资产, 如 BTC、ETH 等, 通过形成虚拟算力的方式参与挖矿。每个跨链资产有独立虚拟算力计算方式, 如资产固定算力、市价折扣计算等, 下文将做详细解释。跨链资产的虚拟算力计算方式主要由社区投票决定。之所以会有跨链资产折扣, 是因为 PCX 作为系统原生货币, 理应比跨链资产获得更大的挖矿权重, 鼓励用户更多地持有 PCX 。

投票挖矿 指用户持有的真实 PCX , 通过将 PCX 投票抵押给某些节点参与挖矿。

算力计算

当前跨链资产与 PCX 投票挖矿算力上限比例为 1:9，该比例可由社区投票调整，即所有跨链资产的挖矿算力上限设定为 10%，保证 PCX 投票挖矿的算力占比大于等于 90%。

ChainX 作为一个 PoS 系统，总算力由 PCX 投票挖矿算力及跨链资产虚拟算力组成，其安全性依托于用户抵押的 PCX，抵押的 PCX 越多，系统越安全。同时由于 ChainX 致力于成为跨链资产网关的特性，其另一个价值支撑点在于所连接的跨链资产，接入的跨链资产越多，价值越大。此外，由于原生资产与跨链资产竞争性地共同参与资产挖矿，因此两者是一个相互依存又相互竞争的关系。为了避免在系统初期跨链资产短时间内大量涌入对系统造成冲击，原生资产与跨链资产挖矿采用动态挖矿模型，当跨链资产增速太快时，采用固定分红比例对跨链资产和原生资产进行分配。挖矿模型的变动由链上治理全民公投决定。

计算公式

$$\text{Power total} = \text{Power real} + \text{Power virtual}$$

$$\text{Power real} = \text{Staked}$$

$$\text{Power virtual} = \sum (\text{Power}_c), c \in \{X-BTC, X-ETH, S-DOT, \dots\}$$

$$\text{Power}_c = \text{Amount}_c \cdot \text{Fixed}_c \cdot \text{UbiquitousDiscount}$$

**当前所有跨链资产挖矿算力比上限为 10%，
即 Power virtual : Power real = 1:9。**

当 Power virtual : Power real > 1:9 时，

则上限挖矿算力规则生效。

$$\text{UbiquitousDiscount} = \frac{\text{Power real}}{9 \cdot \text{Power virtual}}$$

当 Power virtual : Power real <= 1:9 时，

则上限挖矿算力规则失效。

$$\text{UbiquitousDiscount} = 1$$

Power total：全网总算力

Power real：PCX 质押投票形成的总真实算力

Power virtual：跨链资产形成的总虚拟算力

Power c：跨链资产 C 的总虚拟算力

Fixed c：单位跨链资产 C 对应的固定算力乘数，当前 Fixed BTC = 400 · PCX

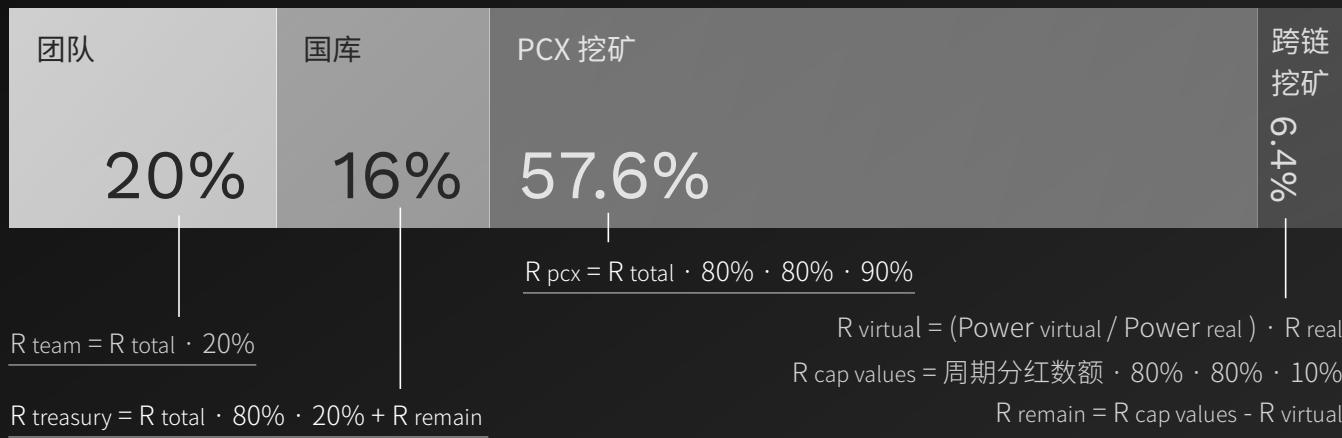
Amount c：跨链资产 C 的总量

UbiquitousDiscount：跨链资产动态竞争折扣

收益分配

ChainX 的挖矿收益被分发给 4 个部分，分别是创始团队、国库、PCX 挖矿用户及跨链资产挖矿用户，在后续的社区治理中，可经由全民公投更改收益的分配。

下图收益数据以硬顶收益计算



团队收益 主要作为持续性开发经费归创始团队；

国库收益 主要用作促进社区发展及插槽竞拍归国库资金；

PCX 挖矿收益 是作为 PCX 投票挖矿用户的奖励；

跨链资产挖矿收益 是作为跨链挖矿用户的奖励，其具体收益根据跨链资产的虚拟算力和 PCX 真实算力的比值计算得出。跨链资产收益存在如上计算的硬顶收益，若未达到此硬顶时，剩余的奖励划归国库。

按照跨链资产与 PCX 投票资产动态算出两类资产总奖励以后，根据各真实和虚拟节点在所在类别的比例得出单个节点的奖励，进而根据票龄算出单用户收益。当所有跨链资产总数激增达到上限后，相当于每个跨链资产始终有一个单资产折扣的情况下，再施加一个所有跨链资产总折扣。

Power_{real} : PCX 质押投票形成的总真实算力

$\text{Power}_{virtual}$: 跨链资产形成的总虚拟算力

R_{total} : 每个分红周期中产生 PCX 的总数

R_{team} : 初始分红周期中的团队收益

$R_{treasury}$: 国库收益

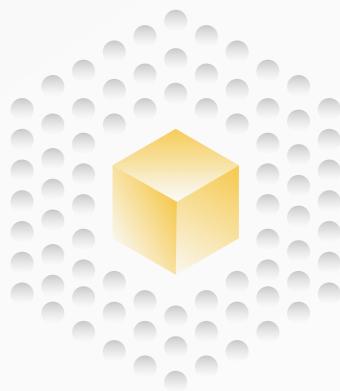
R_{real} : PCX 抵押投票真实算力挖矿收益，即 $R_{real} = \text{周期分红数额} \cdot 80\% \cdot 80\% \cdot 90\%$

$R_{cap\ values}$: 跨链资产分红的硬顶收益

$R_{virtual}$: 跨链资产挖矿实际收益，归参与跨链资产挖矿的用户

R_{remain} : 跨链资产挖矿剩余收益，划归国库

ChainX 采用波卡全新的共识机制即“Babe+Grandpa”混合共识机制。该共识机制最显著的特点就是将确定最终性的任务从区块生产的流程中分离出来，BABE 模块 6 秒稳定出块，Grandpa 进行最终确认。



传统的 PoW 算法，单个矿机的算力很弱，无法独立出块，只能选择加入矿池或自建矿池，造成每条链只有数 10 个矿池节点。初代 PoS 链一般是 7 个节点左右，后来的 PoS 链也最多只有几十个节点。区块链网络的去中心化特性一直没有发挥出来，普通用户无法直接成为共识节点，只能依附于大机构，掌握不了系统记账权。

ChainX 的共识节点的数目限制将从几十个起步，待社区培养成熟后逐步放大限制。起始阶段需要使用云服务器搭建共识节点，后期普通用户只需下载桌面钱包就可以出块，但需要保持持续良好的网络接入环境和计算能力，否则出块如果延迟将受到惩罚，一般情况下的良好的家用网络和高性能台式机就可以满足基本需求。惩罚资金会转入国库，供后续的全民公投决定如何处理。

节点的盈利模式是获得用户投票挖矿所得的 10%，具体比例可以通过后续的全民公投形式修改。节点的掉线或其他恶意行为将受到惩罚，将同时扣减节点自抵押和用户待领奖励。每届验证节点的选举周期为 1 小时，将根据总得票数排序。未能选上验证节点的成为同步节点，也同样需要搭建真实的节点发送心跳交易，不能注册空节点。由于共识节点和同步节点的得票都会同等地参与到挖矿奖励中，用户将获得同样的收益，这样就不会影响到同步节点的进阶。

ChainX 目前发起一笔普通转账交易的手续费仅 0.0001PCX，随着 ChainX 的性能和吞吐量逐步提高，用户发起每笔操作的手续费将逐渐忽略不计。在网络发展后期，链的增发将逐步减慢，用户挖矿收益的主要来源是手续费收集和各类惩罚得来的资金。

为了防止 DDOS，用户在链上发送交易需要支付矿工手续费，系统会根据不同操作的复杂度扣除相应的手续费。用户还可以根据网络拥堵情况，选择不同的加速倍数，实现灵活控制。表面上用户需要支付手续费，但只要用户参与投票或拥有适量资产，在网络发展前期可以获得大量的挖矿收益，足以满足非高频用户在链上的交易需求。并且共识节点打包时会将手续费再收集进去节点奖池，回补给投票用户。所以投票用户仍然能够在这个闭环系统内“免费”使用区块链，并且大部分挖矿用户会处于盈利状态，只有某些高频交易用户需要额外支付手续费。而传统矿工费往往因为吞吐量低，导致单笔交易手续费过于昂贵。

PCX 主要有以下几种用途



矿工费用

用于支付矿工费用，类似于比特币



市值单位

作为资产挖矿时的市值单位，所有资产根据兑 PCX 价格折合成投票，类似于 ETH / ERC20



抵押品

链上比特币金融衍生运作及资产跨链信托的核心抵押品，是比特币金融衍生的风控衡量标准和提高信托信誉的主要工具



兑换媒介

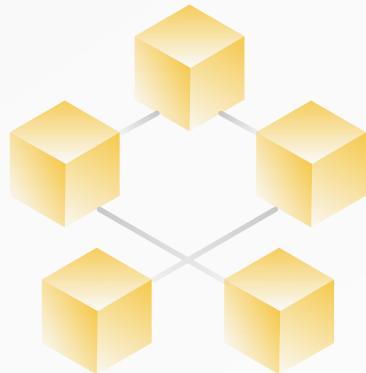
在系统集成的交易所 Dapp 中，作为交易某些小众资产的基础货币和兑换媒介



衡量标准

链 POS 共识选举的衡量标准，总得票数越高肩负的出块和共识责任越大，也是链上治理的抵押和投票工具

为推动社区的去中心化治理，ChainX 依波卡采用三院制（Tricameral）的治理结构，包括公投议院，理事会和技术委员会。除了链上三院制外，通过引入了 X - Association 和国库的概念完善社区自治的框架。



公投议院（Referendum chamber）

公投议院拥有最广泛的成员（即所有的 token 持有人）和最高的权利，所有的“立法”（即区块链 runtime 逻辑的修改）必须经过民主公投。由于 ChainX 是构建在 Substrate 2.0 上，社区或理事会可通过提交议案进行公投，一旦公投通过，在等待一段时间的等候期后，系统将对 ChainX 网络上 runtime 逻辑进行自动修改，实现无分叉升级。

理事会（Council）

ChainX 网络若仅仅依赖公投，治理效率将会很低，于是引入了理事会来处理网络中一些常规事务。理事会成员由持有 token 的用户投票选举产生。目前 ChainX 网络的理事会正式成员有 11 个，候补成员 7 个。选举方式采用的是 Phragmén method 选举算法，每届任期 1 天，即每 24 小时重新选举，不过正常情况下成员构成的变化很小。

理事会选举流程

参选

有意参选的人员，可通过理事会页面提交候选人申请，质押 10 PCX，若当选理事会成员或候补人员，押金将退回，否则将划归国库过所有。这里的质押机制主要是避免恶意参选行为占用链上资源。

投票

拥有 PCX 资产的人员，可通过理事会页面进行投票，每次投票最多可选择 16 个候选人进行投票，并给出参与投票的资产数量，同时需要抵押 0.01 PCX，投票可以随时撤回，并取回押金；

公布结果

每个选举周期为 1 天，周期结束统计投票并更新组织成员。

理 事 会 主 要 职 责

取消惩罚

理事会有权取消由于网络异常引发的 staking 惩罚，需要至少
1/2 的理事会成员同意

提交理事会公投议案

在理事会内部达到一定程度共识后，理事会可以提交议案参与
全民公投以对链上核心 RUNTIME 逻辑做迭代

紧急取消公投

在发现有恶意或错误的公投提案即将施行时，理事会在 2/3 的
成员同意的情况下可以取消公投，并罚没提案质押资金归国库
保管

国库议案审批

理事会需要对的国库提案及 Tips 奖励进行处理，当大于等于
3/5 的成员同意提案视为提案通过，当大于等于 1/2 的成员否
决提案即视为提案未通过

技术委员会 (Technical Committee)

技术委员会的成员由开发 ChainX 网络的技术团队组成，目前由 PolkaX 开发团队担任，技术委员会将作为理事会的补充和制衡，同时受理事会钳制。

技术委员会的职责

提交紧急议案

技术委员会可以在发现紧急的 bug 或迭代需求时，经过理事会批准后发布紧急议案，直接参与全民公投，不需要等待现存公投提案结束

否决理事会公投提案

若技术委员会一致同意，或者根源（例如 sudo 或 Council）触发了此功能，则可以取消公投提案，提案押金将划归国库

X - Association

X - Association 是一个非营利性的组织。其目的是为了更好的支持 ChainX 链的发展以及相关生态的建设。X - Association 由熟悉 ChainX 链，熟悉区块链社区管理和运营，熟悉区块链技术和发展，有时间长期为 ChainX 发展而贡献力量的专家、爱好者组成。

X - Association 成员构成

X - Association 初始成员由 ChainX 议会选出，初期包括秘书长 1 名和干事 4 名。X - Association 成立后，为了保证运营效率和连续性，由 X - Association 自行决定人员的更替，并报理事会备案，但 ChainX 理事会有权对 X - Association 的某个或某些成员发起撤换提案，并在获得理事会三分之二成员的同意下，通过撤换提案。X - Association 下设动态的多个工作组，这些工作组因某个具体的任务而创建，由秘书长或干事领导。

X - Association 在 ChainX 理事会的批准下
履行以下职责

为 ChainX 链的发展和规划提供建议或咨询服务

培育、管理和支持 ChainX 社区(包括爱好者社区和开发者社区)的发展

为 ChainX 链的用户和开发者提供直接的技术支持

协调和管理 ChainX 链的各个开发团队

定期向理事会和社区发布工作报告和资金使用报告

X - Association 资金来源和管理

X - Association 有独立的 PCX 账户，其资金来自理事会的定期拨款，资金位于一个 PCX 链上的 3/5 多签账户，由秘书长和 4 名干事分别持有私钥。当秘书长或干事发生人事变动时，该多签账户相应进行换届。

国库 (Treasury)

国库是一个 PCX 资金池，其中的资金来自 ChainX 网络的 Staking 罚没的金额，跨链挖矿剩余收益、理事会候选人落选后的押金，国库提案罚没押金等。国库的作用是给那些促进 ChainX 网络发展的项目提供资金支持，从而促进生态的繁荣。随着 ChainX 网络的成长，任何对 ChainX 生态做出有益贡献的个人、组织或公司都可以提交国库议案申请国库资金作为激励。

包括但不限于下面这些领域的贡献

基础设施的部署和运维

网络安全，如监控服务、审计等

生态支持，比如和第三方区块链的合作

市场活动，包括广告、合作等

社区活动和外联，如见面会，ChainX
parties 等

软件开发类，比如钱包，客户端的开发等

比特币 Layer2 平台

比特币作为通往数字货币世界的钥匙，市值已经突破 4700 亿美元，逐步开启区块链深层技术的大门，也预示着比特币正在从支付媒介的角度重新被认识，这些都可能只是比特币价值体现的冰山一角。

ChainX 将基于比特币网络开展 Layer2 金融平台的研究和拓展，旨在促进比特币价值流动、丰富比特币金融衍生及完善比特币投资对冲工具。

比特币托管路线

比特币网络无法集成其他链的轻节点形成智能合约，所以 ChainX 通过“轻节点+托管方案”的方式进行资产跨链，目前我们已完成比特币轻节点桥及 X-BTC 1.0 托管方案的开发，可以完全去中心化映射比特币进入 ChainX。同时 X-BTC 最新托管方案逻辑框架也初步成型，届时将依次或同步上线。

X-BTC 1.0 —— 信托节点托管方案

在 X-BTC 1.0 中，信托由参与 ChainX 测试网的优秀节点担任，之后的每届信托采用禅让制度，由议会和上一届信托共同决定并执行。信托节点须生成冷热两个多签地址或合约，每次换届后，老地址的资金会转入新地址。用户可以实时查看系统的跨链资产发行和储备量，没有任何信托节点可以单方挪用。

X-BTC 1.0 托管方案中，用户在用比特币账户向信托多签地址发起普通转账交易时，通过备注中填写 ChainX 的账户地址来完成跨链绑定。ChainX 根据用户比特币绑定地址的交易情况发行 X-BTC。跨链绑定只需进行一次，在后续的转账中，ChainX 网络自动识别该比特币地址最近一次备注过的 ChainX 地址为跨链绑定地址。

X-BTC 1.0 托管方案流程

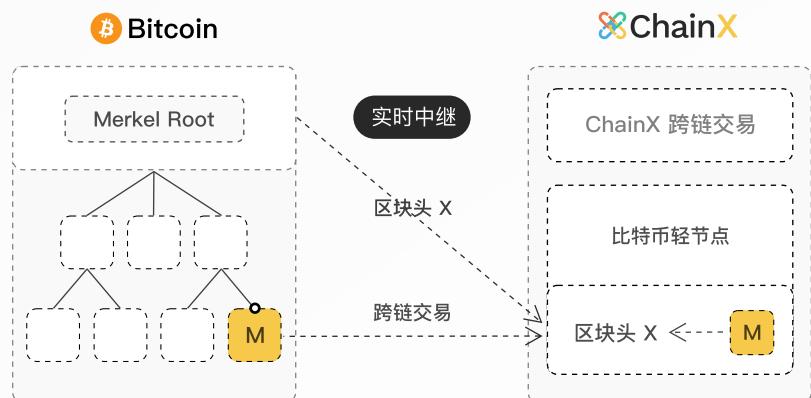
跨链充值

链上运行比特币轻节点，并由 Relay 实时传递 Header，保持最长链更新；

用户转账到信托的热地址，并在交易中的 OP_RETURN 中携带用户十六进制格式的 ChainX 地址及其他信息，携带了 OP_RETURN 转接桥才可识别出这笔充值转账交易是与哪个 ChainX 用户相关；

Relay 监听比特币网络，并在发现这笔交易所在的块经过原链确认后，将这笔交易 Tx、Proof 证明路径及 OP_RETURN 相关信息提交到转接桥中；

转接桥验证 Tx 有效和 OP_RETURN 备注有效后，从 OP_RETURN 中解析出 ChainX 地址，发放对应的 X-BTC 金额至该 ChainX 账户。



跨链提现

用户在 ChainX 网络中发起比特币提现申请；

ChainX 转接桥/网关模块中的记录模块会锁定对应的 X-BTC 并记录用户申请信息，该信息有唯一 ID 与其关联；

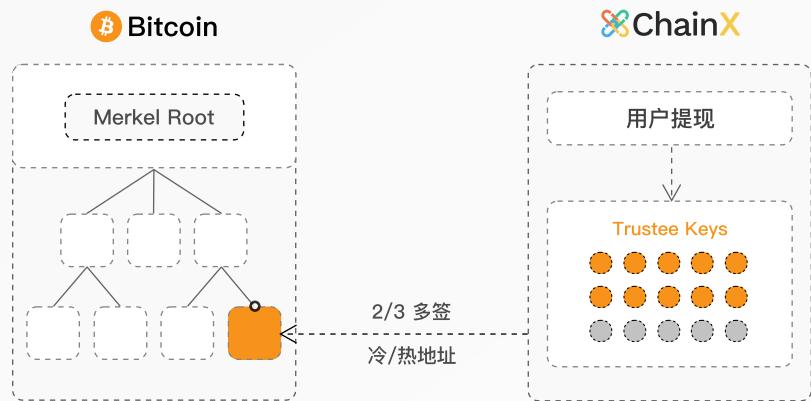
信托周期性获取当前申请中的提现，并根据提现信息组件形成比特币提现交易原文；

提现交易原文发送到 ChainX 比特币转接桥中后会锁定对应提现记录，之后其他的信托基于这个比特币原文进行比特币多签签名；

Relay 在监听到签名完成后的比特币交易，便会将其提交至比特币网络；

提交的比特币交易经过确认后，relay 会提交该提现交易及证明路径至转接；

转接桥验证比特币交易 Tx 有效后，将会关闭对应提现记录及销毁锁定的 X-BTC。



X-BTC 2.0——资产保管人托管方案

X-BTC 2.0 是基于 XCLAIM 框架实现一个去信任和高效率的资产跨链系统，通过 XCLAIM 引入了两种协议来实现分散的、透明的、一致的、原子性的和抗审查的跨链交易。与 X-BTC 1.0 最大的不同在于引入 Vault (资产保管人) 机制，让更多人参与到资产跨链的流程中。

X-BTC 2.0 托管方案优势

XCLAIM 通过以下方式克服了集中式方法的局限性

安全审计日志

构建日志来记录所有用户在 Bitcoin 和 ChainX 上的行为

交易包容证明

链中继用于向 ChainX 证明 Bitcoin 上的正确行为

证明或惩罚

XCLAIM 不依赖及时的欺诈证明(被动)，而是要求积极主动地证明正确的行为

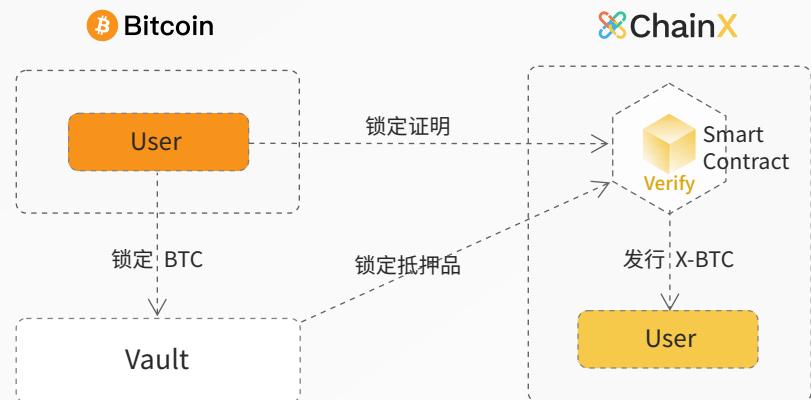
过度担保

不受信任的 Vault (资产保管人)，受到抵押品 (PCX) 的约束，并建立了缓解汇率波动的机制

X-BTC 2.0 托管方案流程

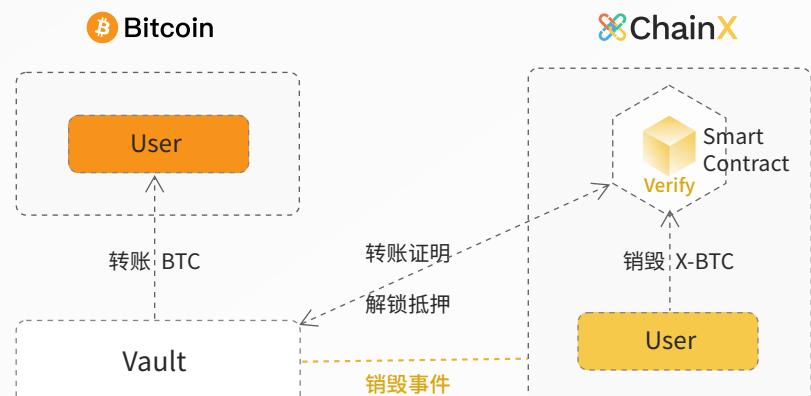
跨链充值

- Vault 在 ChainX 链上锁定抵押品;
- 用户将比特币资产转账至 Vault 处锁定;
- 提交资产锁定证明至 ChainX 链上;
- ChainX 智能合约锁定 Vault 额度并发行 X-BTC 至用户账户;



跨链提现

- 用户通过 ChainX 链上智能合约销毁 X-BTC;
- Vault 在读取到相关的销毁事件后转账比特币给用户;
- Vault 提交转账证明至 ChainX 解锁抵押资产。

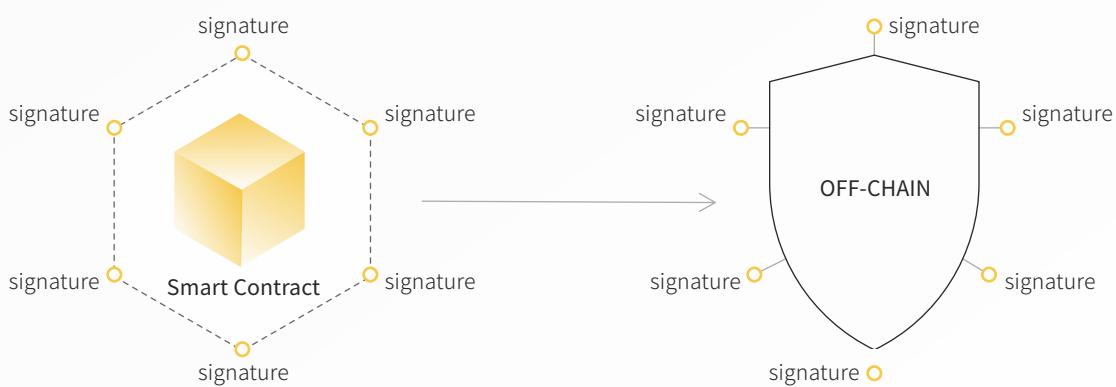


X-BTC 3.0——基于 MPC 的门限签名托管方案

X-BTC 3.0 主要是加入 MPC 门限签名的方式来完成资产跨链，由交易员节点 (Tradernode) 组成计算网络，为系统提供算力，维护系统正常运行。通常人们提到的 MPC (Multi-party Computation) 中有两个主要分支，分别是“基于混淆电路的安全多方计算”和“基于秘密分享的安全多方计算”，而 X-BTC 3.0 则使用的是后者，基于 Shamir's Secret Sharing 完成数据的加密和分发。

ChainX 计划前期开放 100 个席位，28 天为一个选期。每 48 小时所有交易员节点会被随机分组一次，并且保证每个节点彼此绝缘，此时每个节点持有被分解的私钥碎片也会刷新。每组会有 n 个节点，每笔交易需要至少 m 个节点共同合作才可以成功签名 ($m < n$)。且链上还存在一个惩罚制度，该制度会惩罚那些违反协议的交易员节点，惩罚力度超过与他人合谋得到的预期回报。

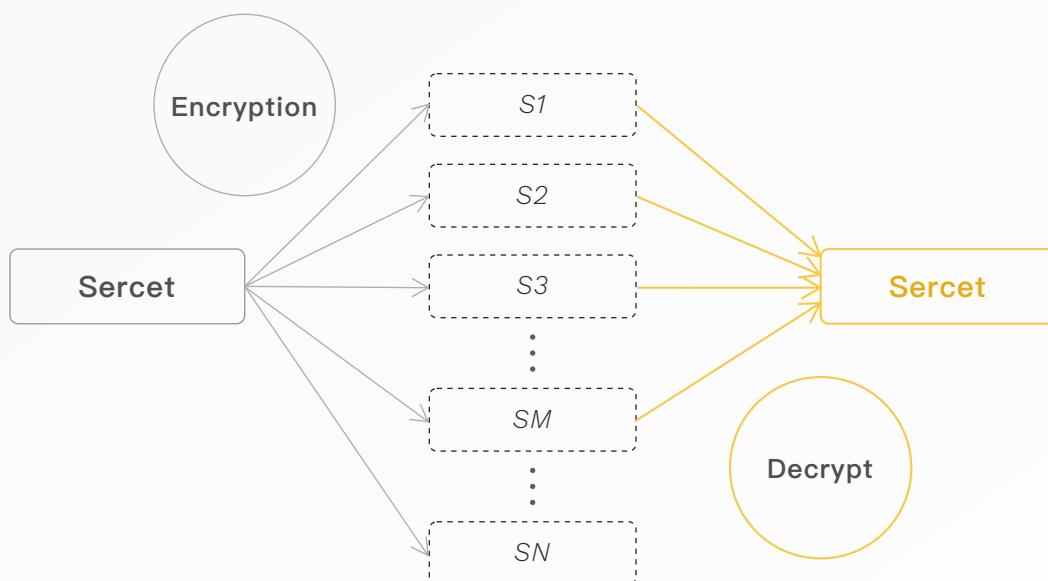
X-BTC 3.0 的优点 主要体现为基于 MPC 的门限签名与合约模块是完全解耦的，它只要区别签名算法，只要签名算法是链系统支持的，它就能很好地衔接，所以兼容算法就能兼容很多链。基于 MPC 的密钥管理能做到对多链友好，这是一个大的优势，而且它是链下的，它避免了合约被黑客攻击的风险。



MPC 的工作方式

如现有 N 个参与者，其中一个参与者将一段私钥、密码或者敏感信息分为 N 个加密碎片，设置的恢复阈值是 M ($M < N$)，将每个唯一的片段分给每个参与者，各自妥善保管。要恢复原始私钥、密码或者敏感信息，需要至少 M 个加密的片段。通常我们将此类加密解密的方式称为多签，比如设置了 3 / 5 多签，需要至少 3 个人签名 (Shamir's Secret Sharing Scheme 中叫做提供加密的片段) 才能发送交易 (Shamir's Secret Sharing Scheme 中叫做解密原始私钥、密码或者敏感信息)。

其中被分解的私钥加密碎片由交易员节点储存，发生交易时各个节点相互合作完成签名。所有想要参与的用户都可以通过抵押资产来成为交易员节点，然后贡献自己的计算资源来赚取经济回报，并且在 ChainX 网络中不会公开其节点身份。而被分解的私钥加密碎片由交易员节点储存，发生交易时各个节点相互合作完成签名。所有想要参与的用户都可以通过抵押资产来成为交易员节点，然后贡献自己的计算资源来赚取经济回报，并且在 ChainX 网络中不会公开其节点身份。



X-BTC 4.0——去中心化自主控制资产托管方案

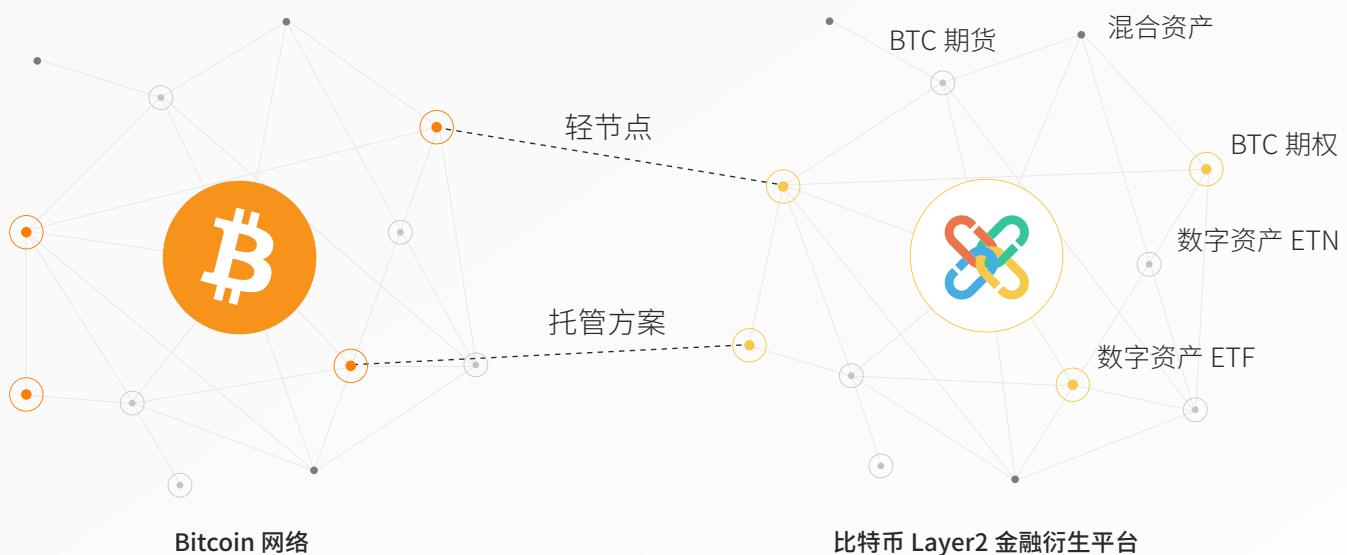
X-BTC 4.0 在通过修改 MPC 算法及阈值，让用户自己也成为私钥加密碎片的拥有者，且用户自持的碎片具有一票否决权，也就是说在用户本身没有参与解密的情况下，资产是不可能被移动的，从而提高了 BTC 托管资产的安全，也大幅度降低了对托管者的抵押数量要求，甚至可以低于跨链资产的价值，是最理想化的解决方案。

例如用户发起了一次 X-BTC 赎回请求，他的步骤将会是：

- 用户使用自身掌握的密钥份额计算消息签名份额发送给所有相关交易员节点；
- n 个交易员节点使用自身掌握的密钥份额计算消息签名份额；
- 交易员节点将产生的签名份额发送给同一组其他所有交易员节点；
- 某一节点收到大于 m 个签名份额之后重构出 `Signature_share_nodes`，加上 `Signature_share_user` 即可计算出完成签名私钥并完成交易签名。

比特币衍生平台

随着比特币受到越来越多主流机构的认可，市值不断创出新高，价格呈现波动趋窄稳步提升的趋势，且已逐渐成为主流价值储存手段之一。在这样的背景下，市场对数字资产投资对冲工具及资金杠杆工具的需求也在不断攀升。ChainX 也将逐步上线比特币期货、期权、合成资产及互换协议等衍生品，逐步成为比特币最大的 Layer2 金融衍生平台。

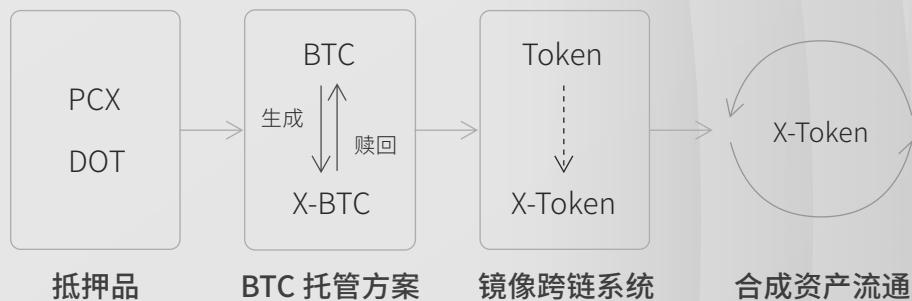


数字资产网关

ChainX 加密资产网关主要由去中心化比特币资产托管方案和镜像资产跨链两部分组成。用户通过充值抵押比特币来获得 X-BTC，再使用 X-BTC 来交易其他加密货币的合成资产，实现所有加密货币同链交易的场景。

加密货币合成资产，就是对目标资产的镜像模拟。如同传统金融市场上的衍生品，可以锚定这些加密货币交易对象，创建一类虚拟资产，可以直接在区块链上表示这些传统的交易市场，通过预言机去复制他们的价格，从而实现链上交易。合成资产所做到的只是复制了锚定物的价格，让人们可以直接在链上进行这些虚拟资产的交易。

其中 ChainX 镜像资产跨链系统的功能是使用 X-BTC 作为担保物生成各类映射或合成资产，只要将 X-BTC 在 ChainX 智能合约中锁定，即可发行合成资产。用户可以直接使用智能合约在合成资产之间执行转换，且不需要有交易对象。系统根据用户的贡献，奖励发行合成资产的 X-BTC 持有者，从而鼓励用户持有锁定 X-BTC，X-BTC 的价值来源于比特币。



波卡二级中继链

平行链可以使用不同类型的区块链底层技术进行开发，中继链负责全网的共享安全共识和平行链的跨链交易转发。中继链本身不包含任何应用，应用均在平行链上进行开发和部署。Polkadot 将整个区块链世界的开发层次推进了一个维度，加速了区块链世界向 3.0 时代的跨越。Polkadot 专注于 Polkadot 生态内的新型链间的通信，其他链则交给社区进行接。ChainX 将在 Polkadot v2 版本发布以后，拆分为多链架构，作为 Polkadot 的第二层网络运行。

ChainX 中继链

全系统的最高安全性保障，负责第二层网络的整体安全共识。

交易平行链

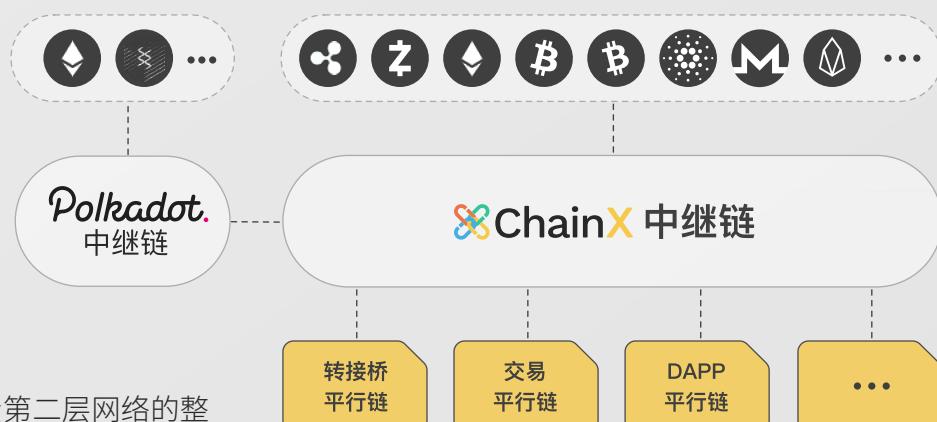
为全系统的资产提供免费撮合服务，提升交易吞吐量。

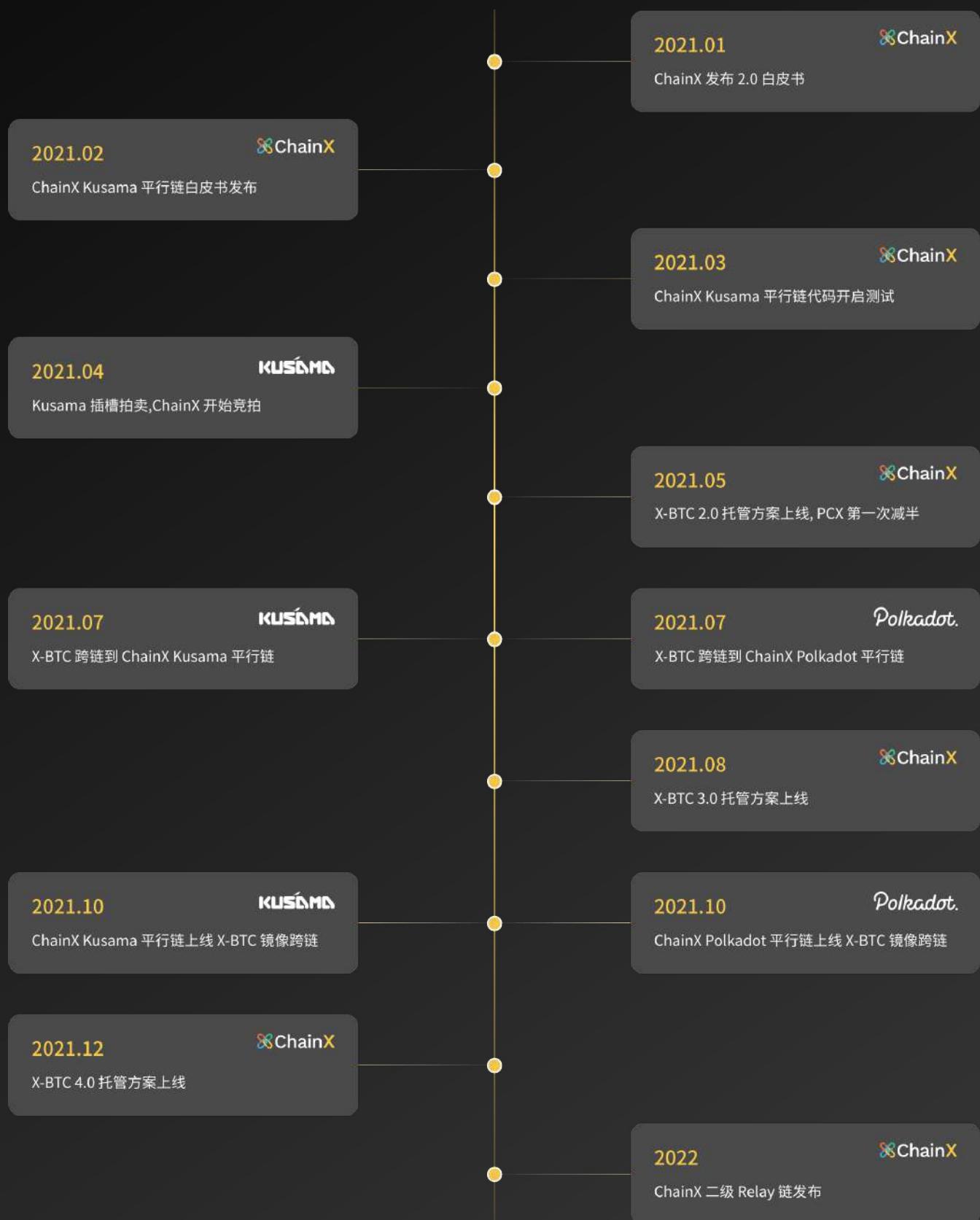
转接桥平行链

将各个转接桥拆分为独立的平行链，用于分担压力。

DAPP 平行链

社区开发的各类应用可以独立运行，并保持跨链通信能力。







<https://chainx.org>