North Star **Chain**

Block Chain Data Privacy Service Platform

-

From the deep net

to illuminate the future

目录

ORIGINATING FROM POLARIS

North Star Chain

来自 173 亿年前的一次爆炸,出现了万物星辰.燃烧在灰烬里,生命复苏的战歌从无到有，化为万物,正是宇宙的主宰之力.风沙之后的断壁残垣,诉说着辉煌的过往.如同命 如同岁月.我们都无法逃脱宇宙的审判.在中心化的世界里,思想 命运都被提前写入程序,人生不过践行历史存在的痕迹.所谓的民主不过是掩饰霸权的说辞.我们无数次的期待自由 民主 ,却只有在宗教的鸣唱中有过片刻的安宁。在我们快要认为中心化才是宇宙主宰万物的规则的时候。

从深网诞生出了区块链.在中心化的世界，我们的命运不由我们主宰。努力 希望 梦想 安宁被一个个中心化的权利摧毁。去中心化的伟大在于竟能使得每个人掌握自己的命运，可以与宇宙的主宰之力所抗衡，让文明和思想可以永恒有序的发展。他能够让文明和思想永续，使得他们如同满天繁星，还能让他们在规则下达成共识。世界只有 10%的人却掌握着 90%的财富，随着人类的进步，贫富差距越来越大 社会阶级越来越明显。大量的资源掌握在少数人的手里，我们所认为能够打破的命运，却是被人事先设定好的程序。绝大多数人类难以改变自己的命运，直到区块链的出现。区块链的出现伴随着希望，而跨越希望却有着重重的阻碍。不同的区块网络难以互联，使得每个区块网络都成为了一个独立封闭的世界。我们即使获得了区块世界的自由与开放，而我们却依然被禁锢在一个有限的空间。

NSC -照亮区块世界，打开世界区块之门，链接希望与未来

起　源

从探索到发现

源于改变世界

密码朋克（Cypherpunk）

- 说到比特币的缘起，就不得不谈到一个略显神秘的团体：密码朋克（Cypherpunk）。这个团体是密码天才们的松散联盟，比特币的创新中大量借鉴了密码朋克的贡献。密码朋克这个词一部分来源于密码（Cipher），这在密码学中意为用于加密解密的算法；一部分来源于赛博朋克（Cyberpunk），这是指那个时代流行的一个科幻流派。这样的组合有很微妙的意味，散发着改变社会的激进理想。

  密码朋克们的观点是：现在社会不断蔓延着对个人隐私和权利的侵蚀。他们互相交流着对这一问题的关注，并认为在数字货币时代保护隐私对于维持一个开放社会是至关重要的。这一理念在比特币中得到体现：去中心化的追求，对匿名的拥抱，自由主义的原则。**密码朋克本身就是数字货币最早的传播者**，在其电子邮件组中，常见关于数字货币的讨论，并有一些想法付诸实践。比如大卫·乔姆、亚当·贝克、戴伟、哈尔·芬尼等人在早期数字货币领域做出了大量的探索。

- 早期数字货币的探索

  比特币并不是数字货币的首次尝试。据统计，比特币诞生之前，失败的数字货币或支付系统多达数十个。正是这些探索为比特币的诞生提供了大量可借鉴的经验

  在变革发生之前，很多人都不相信。

——纳尔逊·曼德拉

1.1 点燃新世界文明的星火

宇宙最初的模样，是一个温度极高，密度极高的火球。一次大爆炸产生了宇宙，产生了元素，产生了生命，产生了世界万物。宇宙本就一个无中生有的雏形。自从人类诞生以来，世界不断的变革，我们似乎从未经历过持久的繁华，我们费劲心思的建立一个美好的社会/国度，在岁月风沙之后，却是一片断壁残垣。因为缺乏信任和民主，一次次组建的文明却一次次破碎。中国有句古话"合久必分，分久必合",人们似乎都已经接受这种情况，我们认为这才是宇宙本身的特性。虽然我们无数次的期待美好，却只有在宗教鸣唱的旋律中有过片刻的安宁。

在中心化的世界，我们的命运不由我们主宰。努力 希望 梦想 安宁被一个个中心化的权利摧毁。去中心化的伟大在于竟能使每个人掌握自己的命运，可以与宇宙的主宰之力所抗衡，让文明和思想可以永恒有序的发展。他能够让文明和思想永续，使得他们如满天繁星，还能让他们在规则下达成共识，使全人类的思想行为协作达到前所未有的高度

-

From the deep net
to illuminate the future

1.2 北极星照亮区块世界的明星

尽管这几年区块链行业蓬勃的发展，但是区块链的数据安全储存 隐私保护 以及不同区块网络之间的数据互通，依然没有很好的解决方案。区块链去中心化 公开透明的理念很好，但是却不是所有的数据都能被公开透明化，在区块链不可篡改的特性上面让不同的用户之间可以对数据产生共识信任。但是公开透明的特性在一些特殊数据情况下，却会对数据/用户造成很多的风险和麻烦，如何保证的数据的真实可靠，又能保证数据快速传输/储存，还能使得数据具有隐私性，已经成了拦在区块链数据储存前面的一大难题了。

在面对逐年的黑客攻击，区块链的安全真的是牢不可破吗？层出不穷的黑客攻击，算力攻击，在区块链网络上如何增加安全防护也是对用户资产/数据储存至关重要的因素。

区块链象征着自由开发的理念，而实际上区块链的网络却像局域网一样，每一个网络都是封闭的，所有的用户都被限制在一个个独立封闭的网络里，难以真正的实现在区块网络上进行自由的交互。

区块链数字货币要有更长久的发展，就必须有更广泛的应用场景支持。目前随着区块链领域研究的深入，特别是针对区块链落地应用方面的探索，逐渐有一些产品方案和 实体经

济生活相结合在需求端谋求合作共赢。但真正落地并规模使用的还很稀缺，同时针对用户端的服务更是屈指可数。无论是比特币、以太币，还是基于智能合约平台新发行的各种代币，只有和实体世界有了更多的交互，通过区块链技术服务更多的行业，才能让更多人了解到区块链的价值和意义，进而促进数字货币的市场繁荣和实体世。

North Star Chain,诞生于这个区块链世界，并致力于通过自身技术解决目前区块链行业的跨链/数据安全储存/匿名隐私等问题

North Star Chain 也将大面积应用于艺术版权保护 数据安全储存 物联网 人工智能 去中心化交易所等方面，以技术和实际的应用驱动价值。

源于深网，惠泽天下，照亮世界。

-

From the deep net

to illuminate the future

1.3 北极星之光

NSC 全称“NORTH STAR CHAIN”，中文翻译为北极星链

北极星西名塞纳久（Cynosure），在英文中，Cynosure 又有吸引中心的意思。极星的位置相对稳定，不易变化，所以给人的感觉是忠诚，有着自己的立场。从人生的角度来说，北极星有着向导我们到达目标的意义，正如它可以让我们分辨方向一样。

在中国传统上，北极星有非比寻常的意义，古人将北斗和极星作为一个整体来认识，称为“斗极”，斗极处于星空旋转的中心，群星绕其旋转，好像天空的主宰，而古人以北斗斗杓周旋四指来厘定节候，北斗又成为天地秩序的制定者，春生夏长秋收冬藏似乎都是随北斗指向而来临，北斗成为天地万物化生的中心。

NORTH STAR CHAIN 诞生于区块链，在他生长繁衍过程中不断遗传区块链的智慧，并将持续进化，使整个体系更加完美我们希望通北斗跨链协议可以成为第一个让推动区块链领域从“局域网时代”过渡到“万维网时代”的原点。

从区块链诞生，链接区块链，指引未来，正如北极星一般

-

From the deep net
to illuminate the future

2.North Star Chain 介绍

1.1 区块链的特点

平等的价值分配网络:

由于使用分布式运算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。所有的参与者都享有平等的权利。数学算法将保证每个参与者的收益分配和系统红利发放的公平公正。整个生态体系将按价值贡献来获取分配。

信息不可篡改不可逆

一旦信息经过验证并添加至区块链，就会永久的存储起来。由于是分布式的点对点存储方式，除非能够同时控制住系统中超过 51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

匿名可信任

所有参与者都可以自由的参与整个生态的建设，所有人都可以自由自主的使用。节点之间不需要相互验证，参与也不需要中心化的审批。用数学和密码学算法所搭建的网络里，所有参与者都会遵守的基础的“宪法”——共识算法。并通过加密算法和哈希算法使得每个参与的地址都是第一无二且匿名的，在公开的数据中保护每个参与者的隐私和自由。

1.2 NSC Chain 的使命

NSC Chain 是全球第一个匿名跨链数据技术平台。

将通过北斗跨链技术和量子文件切片技术，解决目前区块链区块存储成本高、转账成本高、

无法去中心化跨链交易、资产无法跨链、数据安全隐患大等问题。

NSC Chain 致力于让数据的保存和跨链资产交易变得更安全高效；让更多参与者的隐私的到保护；让跨链应用的开发变得可能。

通过跨平台开发，NSC Chain 将链接 NSC Chain 和 IPFS 的生态，集中更多优势来解决区块数据存储量的问题。当然，我们不排除未来有可能产生的兼容性问题，所以在未来也不排除共识算法升级的可能性。

在未来，NSC Chain 将保障每个参与者的数据隐私和安全，帮助更多富有创意的开发者开发例如去中心交易所这样的跨链应用，NSC Chain 的文件系统也将为更多企业和个人提供服务，保障信息不被恶意第三方盗用和监听。

1.3 NSC Chain 的创新

技术创新一：北斗跨链协议

北斗跨链协议通过分布式中继超级运算节点的技术思路，通过异步弹性算法来保证不同区块的传输。有别于 POW 挖矿，NSC 矿工的算力将不再执行无意义的随机哈希碰撞，矿工通过执行切片算法和加密算法为数据进行加密处理，并通过异步算法来保证跨链间的数据传输。北斗协议将会是跨链交易和跨链支付的起点。

技术创新二：匿名、隐私保护机制

在 NSC 内部的所有普通的数据传输和转账信息、转账金额等一切数据都是加密传输的。非交易双方是不可能获取到任何例如地址、数额、传输内容这种有价值的信息。用数学和密码学的高级算法来保障匿名和隐私，可以有效保障 NSC 生态的参与自由。

技术创新三：独特的生态

通过激励机制和收益智能动态算法，以智能合约的 DAO 架构完成价值分配。用公开透明的价值分配激励形成庞大的生态网络。让价值载体具有更强的分散性和流通性，在价值载体的流通中完成生态的指数裂变和线性增长。以 DAO 架构保障系统红利对每个参与者的派发。

技术创新四：量子全息文件切片加密技术

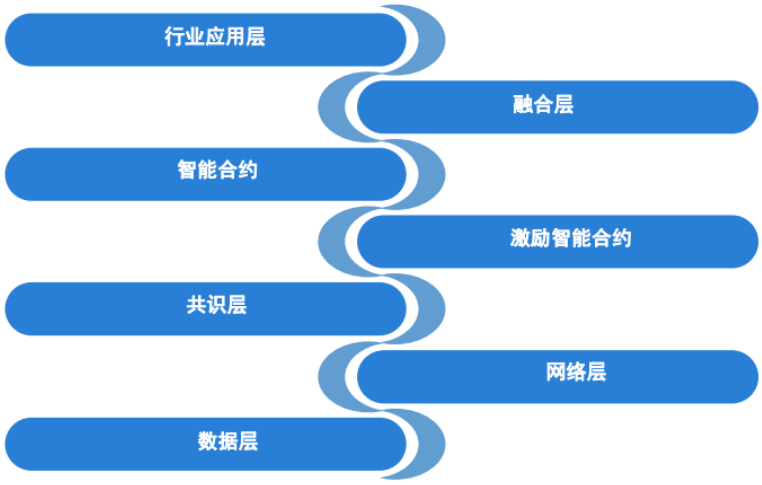
独特的全息文件切片技术，将上传的数据大文件进行上万份的切片加密，加密后的文件碎片分布存储在 IPFS 星际网络中。256 位数的非对称加密产生的私钥将由数据源保存。未得到数据源授权的一切第三方将无法盗取到数据。全息智能算法能防止文件在传输、分布式保存的过程中的损失，仅需用四分之三的文件碎片即可还原完整文件。

-

From the deep net
to illuminate the future

三、NSC Chain 实现

3.1 技术架构



3.3.1 数据层

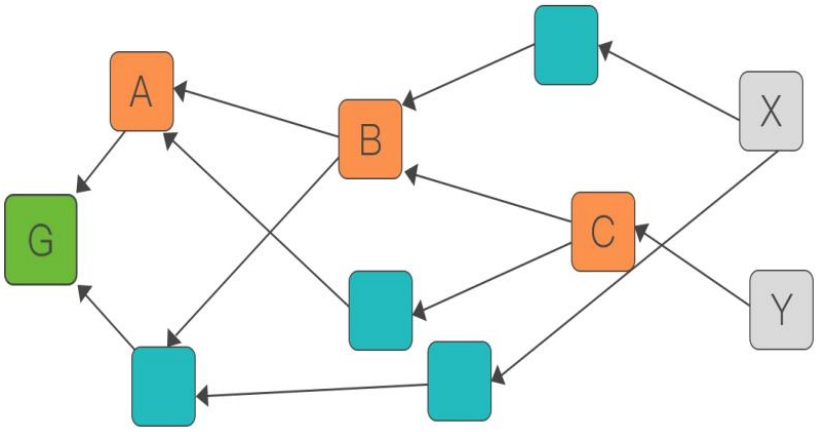


图 3.1.1-NSC Chain 有向无环图

基于增强 DAG 的 HashNet 数据结构 HashNet 是一种有向无环图（DAG），是由无数个顶点和连接顶点的有向边组成。 如图 3-2 所示。该图记录了全网所有节点在什么时间以什么样的顺序给其他节点发送了什么样的数据， 每个节点都在内存里有这样一个 HashNet 的拷。

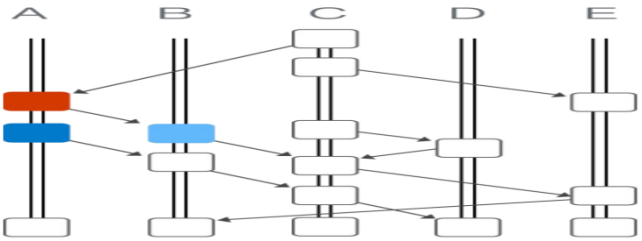


图 3.1.2: HashNet 数据结构图

上图中有 5 个计算机节点 A, B, C, D, E， 每个节点拥有一个放置顶点 vertex(也叫 event) 的柱子。 最新发生的事件， 会被放置的在图顶部，HashNet 是随时间向上增长。

3.1.2 网络层

NSC Chain 底层通信网络采用 P2P 架构， 然后在其上加入了节点间匿名访问机制来确保信服务的隐私保护性。P2P 是英文 Peer-to-Peer 的缩写， 称为“ 对等网”或“ 点对点”技术。IBM 将 P2P 定义为：“ P2P 系统由若干互联协作的计算机构成， 且至少具有如下特征之一： 系统依存于边缘化（ 非中央式服务器） 设备的主动协作， 每个成员直接从其他成员而不是从服务器的参与中受益； 系统中成员同时扮演服务器与客户端的角色； 系统应用的用户能够意识到彼此的存在， 构成一个虚拟或实际的群体。”在 P2P 系统中， 每一个节点（ Peer） 都是平等的参与者， 承担服务使用者和服务提供者两个角色。 资源的所有权和控制权被分散到网络的每一个节点中。 P2P 技术使得网络上的沟通变得很容易、 很直接， 并且把对中间服务器的依赖减少到最小。 P2P 技术改变了“ 内容”所在的位置， 使其从“ 中心”走向“ 边缘”。 也就是说它改变了互联网现在以集中式的网站为中心的状态， 资源不保存在服务器上， 而保存在所有用户的 PC 机上。 P2P 技术使得终端不再是被动的客户端， 而成为具有服务器和客户端双重特征的设备。 因此 NSC Chain 具有去中心化的特性。

3.1.3 共识层

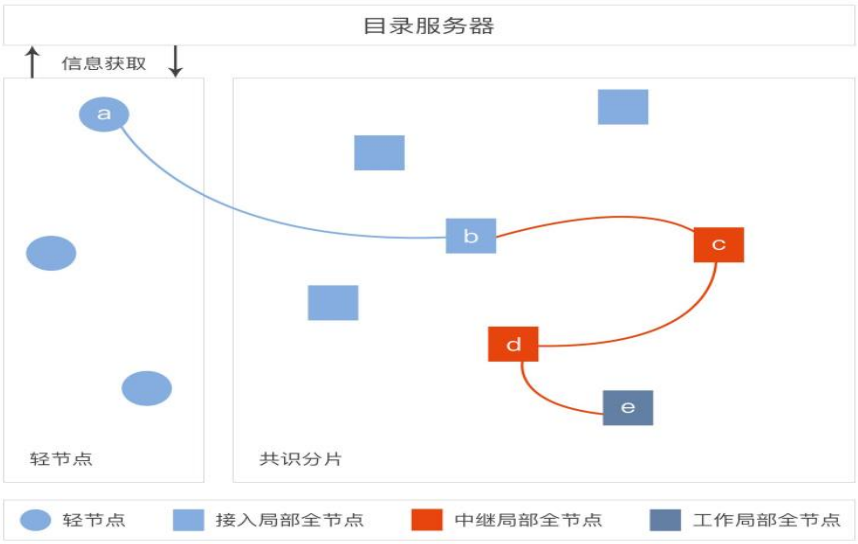


图 3.1.3: NSC Chain 匿名通信网络的基本原理图

NSC Chain 使用 DPOS 来实现区块链记账和数据交换的共识机制。DPoS(Delegated Proof of Stake) 中文名叫做股份授权证明机制（ 又称受托人机制 ）， 它的原理是让全网代币持有人进行投票， 由此产生至少 21 位代表作为系统的区块生产者， 我们可以将其理解为 21 个(可无限扩展)超级节点或者矿池， 而这 21 个超级节点彼此的权利是完全相等的。 从某种角度来看， DPoS 有点像是议会制度或人民代表大会制度。 NSC Chain 任一出块时间仅有一个代表有权生产区块， 如果代表不能履行他们的职责（ 在预定一段时间内未能生成区块 ）， 他们会被除名，网络会选出新的超级节点来取代他们。

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。 DPoS 机制要求在产生下一个区块之前， 必须验证上一个区块已经被受信任节点所签署。 相比于 PoS 的"全民挖矿"， DPoS 则是利用类似"代表大会"的制度来直接选取可信任节点， 由这些可信任节点（ 即见证人)来代替其他持币人行使权力， 见证人节点要求长期在线， 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， 非常适合企业级的应用。

3.2 匿名算法

零知识证明算法

Zero-Knowledge(零知识证明) 它指的是证明者能够在不向验证者提供任何有用信息的情况下， 使验证者相信某个论断是正确的。 而 NSC Chain 正是利用零知识证明技术完成了跨链和跨智能合约技术。

Carter 系统

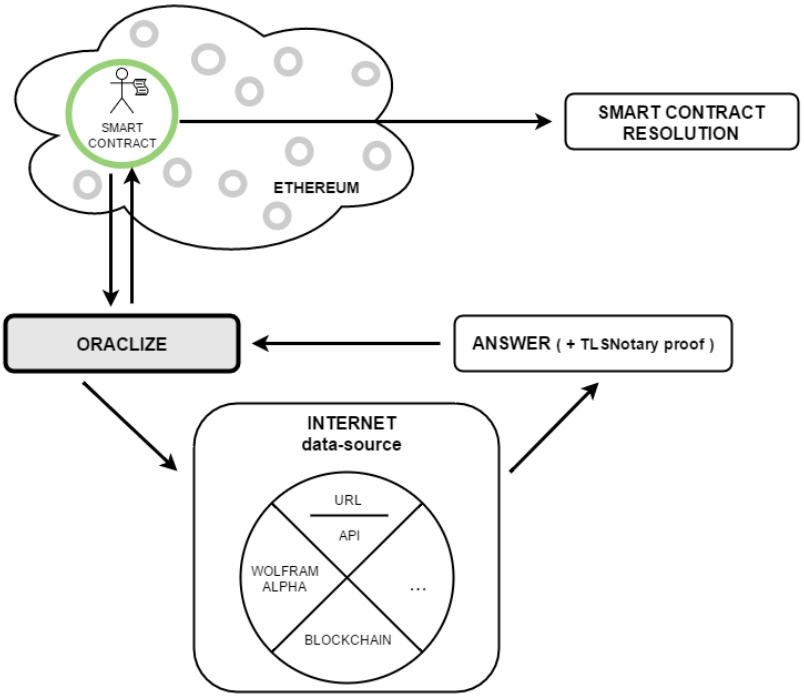
卡特(Carter 系统)是全球首个通过非交互式零知识证明(NzK),真正实现具有图灵完备智能合约的隐私保护的区块链系统,和现有的区块链隐私保护技术相比,Carter 不仅能实现对账户信息和交易信息的隐私保护,还能实现对图灵完备的智能合约输入输出的隐私保护,另外,开发者还能基于 NSC Chain 上的智能合约发行的匿名数字资产(Token),并且与智能合约的通讯信息也同样会得到隐私安全保护。Carter 重新设计了区块链结构和各类底层协议,使得对隐私保护的图灵完备智能合约成为现实,不仅使更广泛的应用场景获得了隐私保护措施,并且因为其采用的先进的 NzK 加密学算法,也进一步提升了对用户隐私数据的攻击难度。除此之外,在即将

发布的 1.0 版本中,改进了目前 NzK 加密算法的实用性问题,大大降低了所需要消耗的内存资源,提升了计算效率。除此之外,对比市面上的主流匿名区块链系统,Carter 对图灵完备的智能合约的支持和对其相关的去中心化应用的隐私保护措施,使其使用场景得到了极大的泛化。更值得一提的是,团队不仅考虑到了去中心化应用本身所需要的隐私保护措施,而且还从应用落地的角度,计划从点对点的网络传输安全以及账户物理的网络地址的隐私性角度提供解决方案,可以使与中心化应用交互时,或者与使用者客户端交互式时也能获得强大的隐私保护功能。

Difiniti 协议

迪菲尼蒂协议(Difiniti 协议):一种分布式的 DNS 系统,可以利用现有的 P2P 网络交互信息,具备自动切换和动态寻址的功能,抗攻击者阻断,使整个数据传输网络具备十分稳定的安全性。

3.3 数据通道



```
    function GetTicker() {
        oraclize_setProof(proofType_TLSNotary | proofStorage_IPFS);
        update();
    }

    function __callback(bytes32 myid, string result, bytes proof) {
        if (msg.sender != oraclize_cbAddress()) throw;
        ETHXBT = result;
        update();
    }

    function update() {
        oraclize_query(60, "URL", "json(https://api.RXChainoracle.xx/0/public/Ticker?pair=ETHXBT).resul
t.XETHXXBT.c.0");
    }

    function kill(){
        if (msg.sender == owner) suicide(msg.sender);
    }
```

3.4 量子全息切片

3.4.1 椭圆曲线加密算法

使用椭圆算法将上传的数据进行加密公钥将被用于存储标记并永久写入 NSChina 区块记录，私钥作为读取凭证返回给用户。比如 RSA 依据的是：给定两个素数 p、q 很容易相乘得到 n，而对 n 进行因式分解却相对困难。那椭圆曲线上有什么难题呢?

考 虑 如 下 等 式 ：

K=kG [其中 K,G 为 Ep(a,b)上的点，k 为小于 n（n 是点 G 的阶）的整数]

不难发现，给定 k 和 G，根据加法法则，计算 K 很容易；但给定 K 和 G，求 k 就相对困难了。

这就是椭圆曲线加密算法采用的难题。我们把点 G 称为基点（base point），k（k< p style ="word-wrap: break-word;" >

现在我们描述一个利用椭圆曲线进行加密通信的过程：

1、用户 A 选定一条椭圆曲线 Ep(a,b)，并取椭圆曲线上一点，作为基点 G。

2、用户 A 选择一个私有密钥 k，并生成公开密钥 K=kG。

3、用户 A 将 Ep(a,b)和点 K，G 传给用户 B。

4、用户 B 接到信息后 ，将待传输的明文编码到 Ep(a,b)上一点 M（编码方法很多，这里不作讨论），并产生一个随机整数 r（r

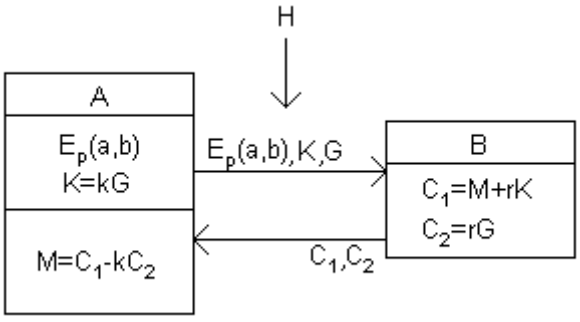
5、用户 B 计算点 C1=M+rK；C2=rG。

6、用户 B 将 C1、C2 传给用户 A。

7、用户 A 接到信息后，计算 C1-kC2，结果就是点 M。

因为 C1-kC2=M+rK-k(rG)=M+rK-r(kG)=M 再对点 M 进行解码就可以得到明文。

在这个加密通信中，如果有一个偷窥者 H ，他只能看到 Ep(a,b)、K、G、C1、C2 而通过 K、G 求 k 或通过 C2、G 求 r 都是相对困难的。因此，H 无法得到 A、B 间传送的明文信息。



密码学中，描述一条 Fp 上的椭圆曲线，常用到六个参量：

T = (p , a , b , G , n , h) 。

（p 、a 、b 用来确定一条椭圆曲线，G 为基点，n 为点 G 的阶，h 是椭圆曲线上所有点的个数 m 与 n 相除的整数部分）

这几个参量取值的选择，直接影响了加密的安全性。参量值一般要求满足以下几个条件：

1、p 当然越大越安全，但越大，计算速度会变慢，200 位左右可以满足一般安全要求；

2、p≠n×h；

3、pt≠1 (mod n)，1≤t<20；

4、4a3+27b2≠0 (mod p)；

5、n 为素数；

6、h≤4。

3.4.2 碎片存储系统

在切片信息写入 NSChina 区块后，超级节点将会把所有碎片发送至 IPFS 存储节点保存，并返回 IPFS 的存储信息。对信息进行二次非对称加密后将公开信息写入区块永久保存，私钥将返回给数据源。

IPFS 是一个对等的分布式文件系统，它尝试为所有计算设备连接同一个文件系统。在某些方面，IPFS 类似于万维网，但它也可以被视作一个独立的 BitTorrent 群、在同一个 Git 仓库中交换对象。换种说法，IPFS 提供了一个高吞吐量、按内容寻址的块存储模型，及与内容相关超链接。这形成了一个广义的 Merkle 有向无环图（DAG）。IPFS 结合了分布式散列表、鼓励块交换和一个自我认证的命名空间。IPFS 没有单点故障，并且节点不需要相互信任。分布式内容传递可以节约带宽，和防止 HTTP 方案可能遇到的 DDoS 攻击。

强大网络数据的分发机制：

哈希指纹是指每个文件及其包含的所有数据块，都会转换为一个散列字符串。每个节点维护一张 DHT（分布式哈希表），包含相应数据块与目标节点的对应映射关系。整个哈希表被组织成二叉树，平均查询联系节点的复杂度是 O(log2N)。例如要查询 10000 万节点只需 20 跳。

基于内容寻址而非域名寻址。只需要通过文件或数据块的哈希值，IPFS 便可自动在全网节点中找到拥有这些数据块的节点，并从节点上拉去数据。

IPFS 使用一个叫 IPNS 的分布式命名系统，将难于记忆的数据哈希值映射为易于记忆的字符串这可以类比于域名与 IP 地址的映射关系。

IPFS 具有如下一些特性：

√ 相同数据内容被赋予唯一的哈希指纹，通过哈希指纹的对比即可判断数据块是否一致，防止数据重复储存空间浪费；

√ 节点本身使用类似 git 的版本控制系统，来管理本地文件与数据块。这既保证了数据块的去冗余，又提供了可追溯的历史版本;

√ IPFS 节点在维护哈希路由表、账本一致性方面，需使用区块链技术，一方面是在动态增减内容、节点方面与全网达成共识；另一方面是为激励机制中 NSC Chain 大文件数据存储管理建设基础平台;

√ 通过发行 TOKEN 来激励节点存储稀有的数据块。节点不仅可从其他节点拉取所需数据，同时也可将该新数据存储在自己节点，供其他节点下载;

√ IPFS 中存储的数据将被永久保存且无法被任何第三方删除，仅有数据产生者自己有修改权限;

√ IPFS 存储和数据传输的过程中，由于分布式的节点存储方式，目前导致会有节点丢失数据的极小概率事件，NSC Chain 的全息文件切片技术在保证了每位用户数据安全的同时，彻底解决了 IPFS 存储传输的文件丢包现象，保证完全的数据完整性和安全性。

CENTRALIZED(A) DECENTRALIZED(B) DISTRIBUTED(C)

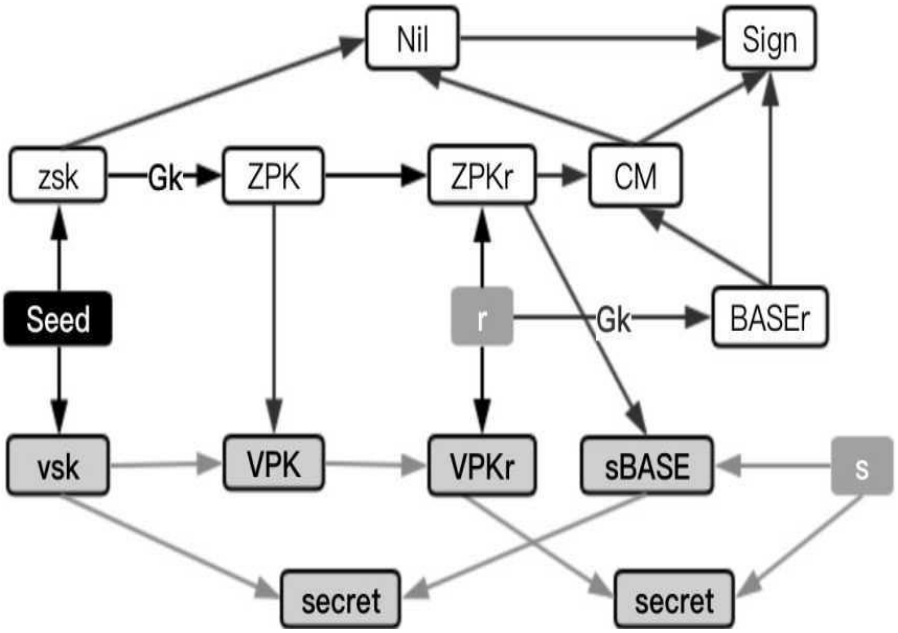
IPFS 是一个基于内容和身份寻址的超媒体协议，不同于传统的位置寻址

```
type NodeId Multihash

type Multihash []byte // 自描述加密哈希摘要

type PublicKey []byte

type PrivateKey []byte // 自描述的私钥

type Node struct {

NodeId NodeID

PubKey PublicKey

PriKey PrivateKey

}

difficulty = <integer parameter>//基于 S / Kademlia 的 IPFS 身份生成：

n = Node{}

do {

n.PubKey, n.PrivKey = PKI.genKeyPair()

n.NodeId = hash(n.PubKey)

p = count_preceding_zero_bits(hash(n.NodeId))

} while (p < difficulty)
```

第一次连接时，对等节点交换公钥并检查：对方的 NodeId 是否等于公钥的哈希值。

若否，则终止连接。

3.4 账户系统



账户系统分为两个种类:用户账户和合约账户。用户账户是用户选定一个 32byte 的 seed 而合约账户根据用户安装智能合约的环境产生一个 64byte 的地址,两者都是系统唯一,不可重复的。用户账户可以产生一个 64byte 的私钥 SK 和一个 64byte 的公钥 PK,该公钥是用户的付款地址。在安装或调用智能合约时,钱包会根据当前情况生成一个暂存地址 PK,这个暂存地址无法用任何方式关联到用户的私钥和公钥,并且只会使用一次。

在智能合约安装的时候,钱包会根据当前情况,将暂存地址转为 64byte 的智能合约地址(CADDR)。当节点收到地址时,需要确保智能合约地址之前没有出现过。

Let:

Gk = NewEccQ

seed = New(Byte32)

r = RandFrQ

s = RandFrQ

a = RandFrQ

m = Message

SK:

zsk = HASHzsk(seed)

vsk = HASHvsk(seed)

sk = (yskt zsk)

zvsk = zsk • vsk

PK/TK:

ZPK = zsk-Gk

VPK=vsk-zsk-Gk

PK= QPK,VPK)

TK=(ZPKtvsk)

PKr:

BASEr = r • Gk

ZPKr = r • ZPK

VPKr = r • VPK

PKr =(yPKr,ZPKr,BASE^

Trace :

VPKr = = vsk • ZPKr

Enc :

BASEs = s • ZPKr

SECRET = s * VPKr

key = Hashs(SECRET)

M = Encvk(m, key)

Dec :

SECRET = vsk- BASEs

m — Decvk^M, key)

Sign :

k = Hash^a, zvsk, ni)

sO = k • BASEr

h = Hash2(S0,m)

si = k + zvsk • h

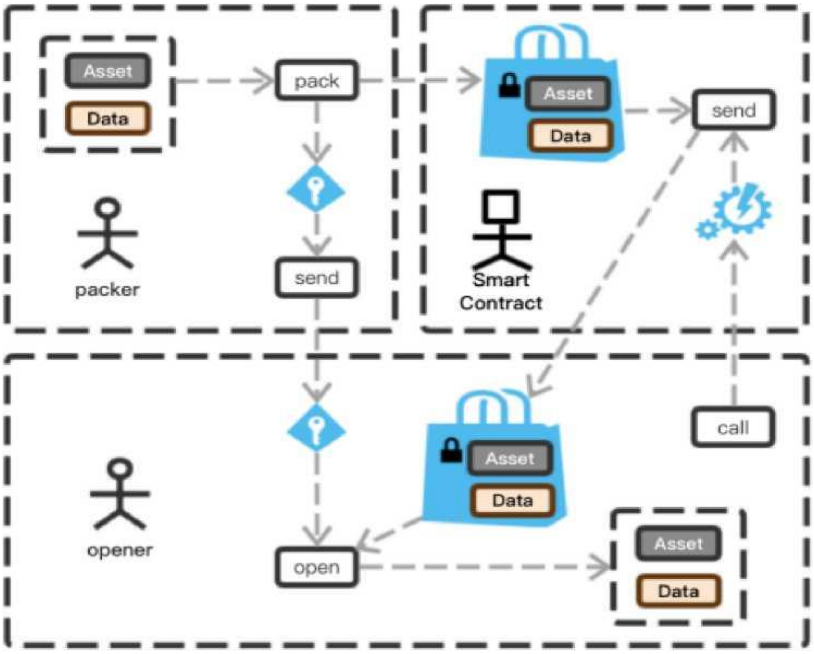
sign = (sO,sl)

Verify :

si • BASEr = = SO + h- VPKr

Seed 是账户种子，用户必须妥善保存。SK 是私钥，不可持久化存储，其中 TK 是跟踪私钥，可以提供给可信的第三方用作账户的审计。PK 是公钥提供给其他用户的交易目标地址是暂

存地址，提供给智能合约，用来临时接收资产的目标地址。



四、NSC Chain 生态治理

4.1 生态结构

超级运算节点生态：

基于独特的技术算法，NSC Chain 的超级运算节点将协同形成一个不需要干涉、自动运转的超级运算中心，将所有接收的数据进行加密处理并分布储存，NSC Chain 有着自动纠错的追溯和更正系统，每个节点之间会通过运行异步协议来进行数据同步。所有的超级节点

需要满足最低的算力和存储性能的审核才能申请。提交申请后由全体节点进行投票选举。

应用生态：
NSC Chain 的跨链技术将吸引众多去中心化的 DAPP 进行调用。NSChain 计划通过社区来引导参与者积极参与应用生态的维护和裂变。对于富有创意的自由开发者，创意应用将在应用生态中进行展示。创意应用在海量参与者的应用生态中。
未来在 NSC Chain 的应用生态中将出现各类精美的跨链应用，例如分布式的去中心交易所。

开发者：

全球企业和所有参与者，可以自由进行开发。基于 NSC Chain 跨链数据传输技术，部署应用至 NSC Chain 应用生态。NSC Chain 开发平台将大幅提升开发效率，降低开发者技术门槛；同时 NSC Chain 生态为每个应用开发者提供了海量的社群用户，让开发者可以将精力集中在运营和应用创意上。

仲裁委员会：
仲裁委员会的工作是对基金会的监事作用，仲裁委员会将安排 16 个席位，按照每 180 天的轮值周期进行投票选举。投票所使用的 token 将进行锁仓 180 天处理。委员可连任。16 个席位中有 3 个席位具有一票否决权，这三个监督席位将由 16 个委员投票产生两个个席位，基金会投票产生一个，轮值周期为 360 自然日。每期投票将在官网公开进行。仲裁委员将有权获得基金会对于仲裁委员会的建设 token 奖励。

2.2 生态激励计划

1.生态发展待挖总量为 1.3 亿的 token 将经过 80 年的周期对所有节点进行按价值分配。

2.矿池中的 token 数量每四年减半。每个投放结算周期为区块间隔，起始值为每周期产出 139.4225。

不同类型矿池的投放比例：

时间	总产出	矿池①	矿池②	矿池③	矿池④	矿池⑤
前4年	25003052.1	6250763.0	5000610	5000610	1250152	7500915.
9-12年	6250763	1562690.7	1250152	1250152	312538.1	1875228.
13-16年	3125381.5	781345.3	625076	625076	156269.0	937614.4
17-20年	1562690.7	390672.6	312538.1	312538.1	78134.5	468807.2
…						
80年	6104.3	1526.1	1220.9	1220.9	305.2	1831.3

（具体算法以主网上线为准，NSC Chain 基金会保留在系统研发阶段算法调整的权力）

2.3 角色收益算法

存储节点收益计算：

①矿池收入：时段 T（30S 的正整数倍），矿池周期总量 C，周期内总任务系数 M，自己所参与任务的任务系数 M1，任务参与人次 P。

系统该周期内所有任务参与数 Z1，自己在周期（时段）所有参与数 Z。公式：0.6CT / 30 * M1/M/p + 0.4Z1/Z

开发者收益计算：

① 矿池收入：时段 T（30S 的正整数倍），矿池周期总量 C，总参与人次 P（一个人参

② 与一次事件记为一个人次），自己应用参与数记为 P1

公式：CTP / 30P1

②应用收入：应用总收入 Z

公式：0.4Z

③ 开发资金募集算法

创作者释放作品收益的 y%的份额，募集 M 个 NSC Chain 用于创作，到结束时间完成 Q(Q...Q)个 NSC Chain 募集（Q<=M）。

所有赚取 NSC Chain 的行为都需要时间顺序 T 竞争，时间是影响回报的一个因子,时间越早收益越高。

公式：S=(x+1)-u /

如开发者收益为 A，Nu 投资创作的收益= A * y% * 。

收益的 y%的份额，募集 M 个 RXChain 用于宣发, Nu 投资宣发的收益为

$\Sigma^{x}_{k=1^{k}}$ $\sum^{x}_{k=1^{QU}}$ = A * y% * S* QU/

算力挖矿收入：全网的算力记为 O,自己的算力记为 O1，算力矿池总量 C

公式：C*O1/O（主网上线后将公布测试算法）

四 、 NSC Chain 应用场景

4.1 跨链应用

A. 场景一：跨链金融工具

目前传统的金融市场撮合交易系统存在许多不足：中介费用高昂，可拓展性差，效率低下等。而 NSC Chain 的跨链技术可以帮助开发者搭建去中心化的数字资产交易撮合平台（去中心化交易所）并免去中介费用，去除专业化门槛，易于拓展，提高准确率且高效。

场景一：跨链金融工具

B. 场景二：去中心保险

保险是一个和大众息息相关的行业。传统保险业由于中心化管理，出现了流程太长，理赔手续繁杂缓慢等令人诟病的问题。同时庞大的保险公司代理体系也使保险的很大一部分收益被用于企业运营。通过 NSC Chain 跨链的去中心化保险能够完美解决这些不足。例如，利用 NSC Chain 平台可以创建一个航空延迟险。想购买航空险的用户可以在乘坐航班前用代币购买。大多数情况下，用户的航班都会准时，从而用户的代币将锁定在航空险事件对应的智能合约里。当某个航班发生延误时，智能合约将会把延误航班的航班号写入该航空险的理赔智能合约。理赔智能合约将能够自动为购买了该航班号所对应航空险的客户跨链返还不同种类代币理赔金。整个过程是完全自动化且不需要人工干预的，所有用户的代币除了一小部分矿工费以外都将用于客户理赔。

场景二：保险

4.2 分布式应用

场景一：分布式网盘

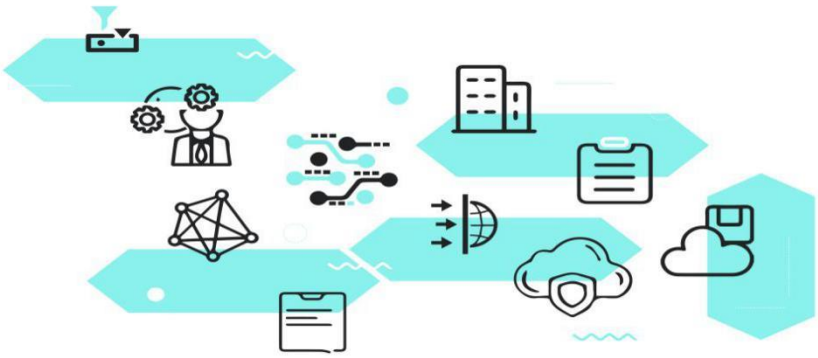
现存网络存储空间服务商采用的方式是企业集中式存储，用户上传的每一个文件在检索 MD5 值后，对不重复的数据进行上传存储。为了防止数据的意外丢失和破损，规模大的网络存储服务商会对每一个数据文件进行重复存储（备份），这就更大提升了存储的成本。并且，由于受到不同地区监管影响，某些服务商会在未经用户许可的情况下销毁用户文件。这也暴漏出了另一个问题，在现有的数据服务商中，一部分数据服务商并未保护用户的隐私，服务

商并未对原数据进行加密处理，服务商及任何绕过防火墙的第三方都可以在未经用户授权的前提下随意查看和读写用户的隐私数据。基于 NSC Chain 存储技术开发的分布式网络存储应用将彻底解决诸如隐私性、安全性和成本问题。所有的数据均会采取切片加密，并以分布式的方式存储在全球分散的节点中。不经用户授权的任何服务商和第三方将无法访问和读取任何数据。通过 NSC Chain 开发数据存储应用即高效又低成本，服务商存储成本仅有现成本的 1/5。

场景一：分布式网盘

场景二：企业大数据存储方案

目前企业内部的大数据以集中的方式进行存储，尤其对于部分互联网企业。用户信息和用户隐私都存在着巨大的安全隐患，Facebook 的用户信息泄露更是引起了全世界人对于隐私数据和个人信息安全性的担忧。 NSC Chain 未来将是一个开放式的分布式数据存储和应用开发平台。企业可以基于 NSC Chain 的方案来解决数据存储效率和数据安全问题。



场景二：企业大数据存储方案

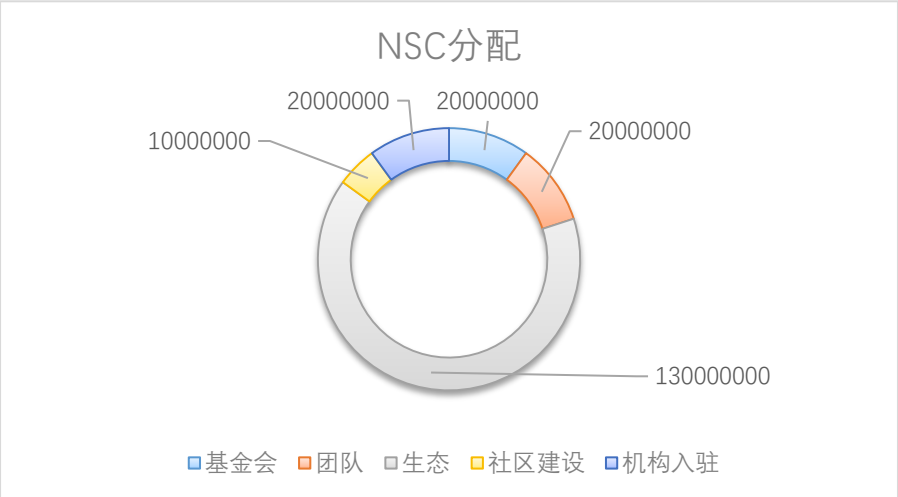
五、Token 分配

发行名称： NSC（ North Star Coin）

发行数量： 200000000

发行类型： erc20

分配比例：团队 10%、社群建设 5%、机构 10%、节点生态 65%



说明：

1. 技术团队锁仓，主网上线后每月释放 5%， 20 个月释放完成；

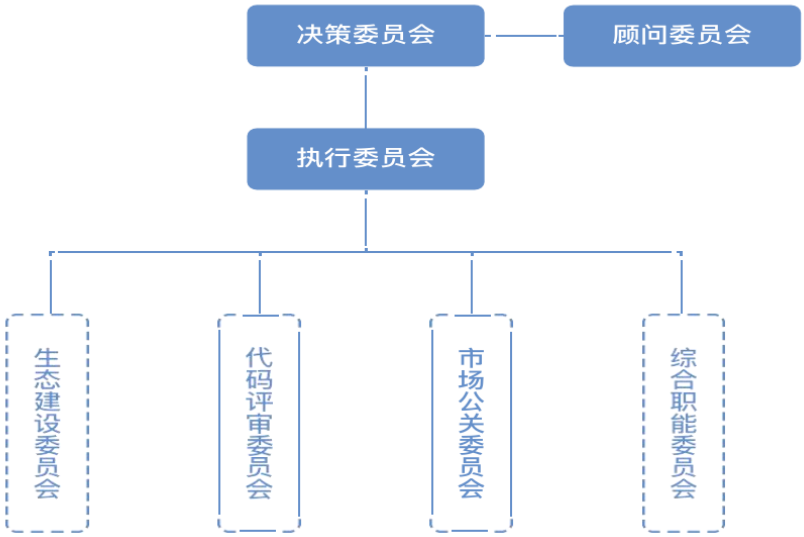
2. 基金会使用代币必须上报并通过决策委员会并公示；

3. 社区奖励为不锁仓流通 Token。

4.生态释放自主网上线开始每 4 年释放减半，80 年左右释放完成。用于奖励为主网提供算力的超级节点和存储节点。

六、基金会与团队介绍

6.1 基金会架构

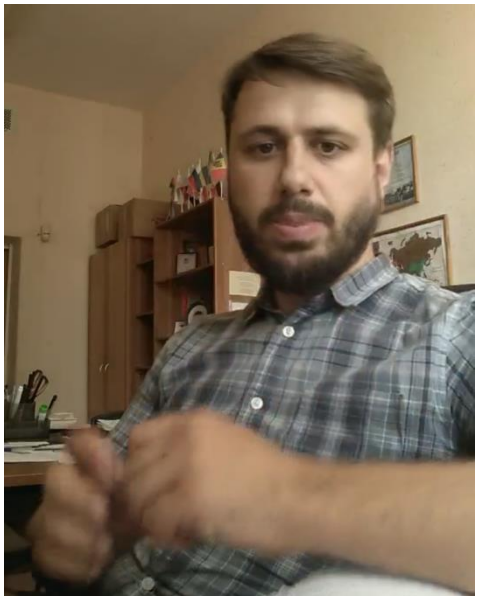


NSC 基金会（ 以下简称"基金会"） 是在新加坡依法注册成立的管理主体。 基金会致力于 NSC 的开发建设和治理工作，推进生态社区的建立、 演进、 形成。为避免社区成员出现方向、决策的不一致甚至因此导致的社区分裂， 基金会通过制定良好的治理结构，说明管理社区的一般性事物和特权事项。基金会治理结构的设计目标是保持平衡生态的发展可持续性、决策效率性和资金管理合规性。基金会由决策委员会行使日常权力。

6.2 团队介绍

1.alex(CEO)

Alex,毕业于耶鲁大学，专注研究世界货币体系以及金融系统，对区块链产业和虚拟货币市场有自己独到的见解.曾领导耶鲁大学货币与国际关系专项课题研究。目前为英国数据技术公司Blis 联合创始人.NSC Chain 联合创始人，CEO.



2.Daniil(CTO)

毕业于斯坦福大学计算机硕士，美国计算机协会网络安全顾问.计算机长期从事密码学与 P2P 点对点加密网络传输技术研究.知名游戏交易网站 G2G 联合创始人， 有多年的分布式网络安全经验，NSC Chain 联合创始人，CTO.

Tammo Weiss(CMO)

海德堡大学传播学硕士，曾任职于联合利华，Garena 首席运营，现任 NSC Chain 首席运营官，联合创始人。

免　责　说　明

本白皮书内任何内容均不构成法律、财务、商业或税务意见，您应在参与任何与本白皮书相关的活动之前咨询您自己的法律、财务、税务或其他专业顾问。无论是 NSCChainFoundation Ltd.（下称"基金会"），还是任何在 RXChain 平台或任何相关项目工作的项目团队成员（下称"NSCChain 团队"），还是任何第三方服务提供商，均不应对您因与获取本白皮书、基金会提供的材料或者访问网站或者任何由基金会出版的其他材料相关而遭受的任何直接或间接的损害或损失负责。

所有的贡献将被用于基金会的目标，包括但不限于提升和支持对去中心化密码或区块链解决方案的研究、设计、开发以及推行，以构建透明、自由和可靠的数据市场。

本白皮书仅用于提供一般信息之目的，其并不构成招股说明书、要约文件或证券要约或投资征集招揽。下面的信息可能不是详尽的，其也并不意味着任何合同关系的要素。这些信息的准确性或完整性是无法保证的，而且就这些信息的准确性或完整性而言，其无法也不欲提供任何陈述、保证或允诺。在本白皮书包含从第三方获得的信息的情况下，基金会和/或 NSCChain 团队并未独立验证此类信息的准确性或完整性。这些信息的准确性或完整性是无法保证的，而且就这些信息的准确性或完整性而言，其无法也不欲提供任何陈述、保证或允诺。

本白皮书并不构成基金会或 NSCChain 团队出售任何 NSCChain Token（定义见本白皮书）的要约，其整体或任何一部分，以及其中陈述的事实，均不构成任何合同或投资决定的基础亦不得以此为据与任何合同或投资决定相联系。本白皮书中所包含的任何内容都不是也不能被引以为据为对平台未来表现的承诺，陈述或允诺。基金会（或其隶属机构）与您订立的任何买卖 NSCChain 的协议仅受该协议的独立条款和条件的约束。

基金会和 NSCChain 团队没有也不欲作出对任何实体或个人的任何陈述，保证或允诺，并声明不承担任何责任。Token 的潜在购买者应仔细考虑并评估与 Token 销售、基金会和 NSCChain 团队相的所有风险和不确定性（包括财务和法律风险和不确定性）。

通过获阅本白皮书或其任何部分，您向基金会和 NSCChain 团队作出陈述和保证如下：

(a) 您承认、理解并同意：NSCChain 可能没有价值、不存在对 NSCChain 的价值或流动性的保证

(b) 或陈述以及 NSCChain 并非用于投机性投资；

(b) 您并非依据本白皮书中的任何声明而去作出任何购买任何 NSCChain 的决定；

(c) 您将会并且自行承担费用以确保遵守了所有适用于您的所有法律，监管要求和限制（视情况而定）；以及

(d) 您承认、理解并同意：如果您是美利坚合众国的公民、居民或绿卡持有人，或者您是中华人民共和国的公民或居民，则您不具备购买 NSCChain 的资格。

本白皮书中所包含的所有声明，新闻稿中或由公众可访问之处的声明，以及基金会和/或 NSCChain 团队可能作出的口头声明均可构成前瞻性声明（包括对有关市场状况、商业战略和计划、财务

状况、具体规定和风险管理实践的意图、信念或当前预测的声明）。谨请阁下您不要不恰当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、不确定性和其他因素，而该等风
险、不确定性和其他因素可能会导致未来的实际结果与前述前瞻
性声明所描述的结果大不相同。这些前瞻性声明仅于本白皮书之日当时适用，而且基金会和 NS Chain 团队明确表示不承担任何（不论明示或暗示的）责任去对这些前瞻性声明进行修改，以反映此日期之后的事件。

本白皮书可能被翻译成英文以外的语言，如果本白皮书的英文版本和其翻译版本之间存在冲突或模糊不清的情况，则以英文版本为准。您承认您已阅读并理解了本白皮书的英文版本。