这是一个全新的区块链时代

在比特币诞生之前，全球信息传递都是通过互联网的TCP/IP（传输控制协议/因特网互联协议）协议来实现高速低成本的传输，但是随着互联互通技术的发展（互联网、物联网、VR/AR），人与物体、人与信息的交互方式更加多样化，更多的实体被数字化或者代币化，仅仅是信息的分享和传输并不能满足经济社会的发展，因此当实体被数字化或者代币化之后，人们越来越关注到价值转移以及如何点对点传输这些资产和价值。

在2008年10月31日，Satoshi Nakamoto 第一次发布了比特币的白皮书《比特币：一种点对点网络中的电子现金》，并提出了通过去中心化的比特币网络实现价值转移。在比特币体系中，全网参与者均为交易的监督者，交易双方可以在无需建立信任关系的前提下即可完成交易。区块链技术改变了我们获取和分享信息的方式，创造了一个新的分布式、点对点的生态社会。

在比特币网络出现之前，我们一直无法在不借助于第三方受信机构的情况下，通过互联网进行点对点的价值的转移和传输。比特币网络则是运行于信息高速公路上面的第一个 Value Transfer Protocol（“VTP 协议”）。目前，随着区块链技术的成熟，区块链的应用场景不仅限于比特币和以太坊，BitcoinNC试图将区块链链上和链下相结合，形成第三个区块链的生态环境，进一步使用 VTP
协议实现点对点价值传输。

自2009年以来,随着比特币的价值被越来越多的人所接受、价格不断地提升,币市逐渐成为全球投资者的投资圣地.究其原因在于相较于其他行业投资门槛的不断提高、投资利润空间的不断压缩以及过多的政策干预,而区块链技术跨时代的象征意义和币市价值低洼成了资金不断涌入的根本原因。

目前市场上把区块链技术主要划分为三个时代:

 第一个时代即以BTC为代表的一种点对点的电子现金系统。

 第二个时代即以ETH为代表的开放的智能合约完整解决方案。

 第三个时代即以解决 ETH
性能不足,容易出现区块拥堵问题,努力实现更好的商用价值的公链集群。

可以推断，在经历了币市前期近十年的疯狂投机后，后面十年将迎来价值投资的黄金时期，而此时如何选择一个低估且优质的项目成了首要任务，亦如比尔盖茨当年

投资可口可乐一般。

什么是BNC？

BNC，全名BitcoinNC ，比特容量，是基于 Proof Of Capacity (以下简称：POC）的新型加密货币。

BNC是一个区块链的数字资产及应用平台，它提供了一套全新的 Proof Of Capacity，并在系统底层提供了数字资产 BitcoinNC Asset 与数字身份 BitcoinNC ID 等功能，使得人们可以非常方便地开展资产数字化业务，而不仅仅是在区块链上创建原生代币。

BNC通过以硬盘容量大小
作为共识基础，让其生产更趋向去中心化方式使其更加安全可信，让人人都能参与到加密货币的生产中，通过数学产生信用，通过数学产生价值。

BNC选择计算机硬盘挖矿是一个颠覆性的创新，计算机中能够作为挖矿设备有CPU、GPU和硬盘三种。CPU、GPU最后都避免不了成为AISC矿机，同时CPU、GPU会造成了大量的能源浪费，而硬盘天然有着抗AISC且省电的特性，硬盘只需通过简单的扫盘就能保持其运作，
BNC选择硬盘挖矿，完美避开了CPU、GPU的缺陷，单台矿机最大挖矿容量8T，避开了部分POC币种，发展到一定阶段后，小户进不了场，都是大户在玩，重蹈POW挖矿的覆辙，小容量PC矿机，更容易布局生态，走进千家万户，实现中本聪人人挖矿的构想，POC挖矿的革命已然打响，下一波牛市将会诞生POC龙头币种，拭目以待！

BNC特点

1.确定性：
程序的行为是确定性的，达成一致共识，在设计系统时排除了非确定性的因素。

2.时间：
BNC基于POC机制提供了基于区块时间戳的系统调用，可以将整个区块链看成一个时间戳服务器，并取得任意一个区块被构造时的时间戳。

3.随机性：BitcoinNC的运行有两种方式来获取随机数：

（1）每个区块在被构造时，共识节点都会对一个随机数达成共识并填充到区块的字段中，挖矿程序可以读取到任意区块的字段

（2）挖矿程序可以利用区块的散列值作为随机数的生成手段，由于区块的散列值具有一定的随机性，这种方式可以得到一个较弱的随机数。

4.数据源：BitcoinNC提供了两种确定性的数据源：

（1）区块链账本

程序可以通过互操作服务来访问到整个区块链上的所有数据，包括完整的区块和交易，以及它们的每一个字段。区块上的数据都具有确定性和一致性，所以可以安全地访问。

（2）合约存储空间

部署在 BitcoinNC 上的每一个节点都有一个仅可由该节点本身来存取的私有存储区，BitcoinNC的共识机制确保了每一个节点上的存储状态都是一致的。 对于需要访问链外数据的情况，BitcoinNC没有提供直接的方式，需要通过交易来将链外数据发送到链内，从而转化成以上两种类型的数据源，才能被访问。

5.节点调用：BitcoinNC的节点具有相互调用的能力，但不能递归调用。

6.高性能：BitcoinNC 采用了轻量级的 VM（Virtual Machine）作为其节点的执行环境，它的启动速度非常快，占用资源也很小，适合像节点这样短小的程序。通过JIT（即时编译器）技术对热点进行静态编译和缓存可以显著提升虚拟机的执行效率。

7.拓展性：
BitcoinNC的节点之间的调用关系是静态的，无法在运行时指定调用的目标。

8.低耦合：
BitcoinNC的系统采用低耦合的设计，区块程序在执行时，通过互操作服务层与外部通信。

9.高效节能：
POC的挖矿经济模型使矿工成为生态利益的共同体、并用币作为新型生产资料代替了原本的电力消耗资源，使BNC整个生态不停的自动扩张。全球只要买得到硬盘的国家，人人可以参与挖矿。

BNC应用场景

超导交易：BitcoinNC未来会孵化区块链超导交易的项目。

智能基金：BitcoinNC未来会在智能基金项目上加大投资，它和基于以太坊的 TheDAO 项目非常相似，但试图通过一些方法来提高安全性，避免重蹈 TheDAO 的覆辙（被黑客攻破）。

跨链互操作：
BitcoinNC为跨链互操作的实现提供支持，不但可以实现跨链资产交换，还可以运行跨链分布式事务，在不同区块链上运行，并保证它们的一致性。

BNC分配机制

1、名称：BNC (BitcoinNC 比特存储)

2、发行数量5300万

3、开发团队：530万用于激励 BitcoinNC 的开发者和 BitcoinNC 的理事会成员（总量10%，预挖产生）；其中160万为创世区块，剩余370万分为12个次进行释放，第1次释放40万，第2~12次释放30万。

4、社区建设：265万（总量5%，随挖矿产生）

5、矿池总量：4505万（总量85%，随挖矿产生）

6、初始块大小：100 BNC/Block

7、出块时间：10分钟

8、减半机制：四年

9、发行价格：1美金=7RMB/BNC

10、容量抵押：1T容量抵押100枚代币

技术原理：

在 Plotting的时候，也就是为硬盘空间创建 plot 文件，同时会创建一个 nonces 。

24nonces是通过数据不停重复哈希产生的，这些数据包括账户ID等等。如果为Plotting分配越多的硬盘空间，那么就能存储越多的nonces。一个nonces 最终会包括8192个哈希表。这 8192个哈希表是成对出现的，每对被称为scoop。每个scoop会被分配一个从0到4095的标号数字。 在挖矿过程中，从0到4095计算每个scoop的标号数字。我们假设最终算出的数字是42，那么就要去编号为42的scoop里取出它里面的数据，利用这个数据计算出一个时间，这个时间被称为deadline。重复上面的过程，直到每个scoop都被计算过一遍，再从所有计算出的deadline里面，找出代表最短时间的、数值最小的那个 deadline。这个deadline 就代表了“自从上一个区块被生成之后，到生成下一个区块之前，系统必须等待的时间长度（多少秒）。如果在这个时间长度里面，没有人生成下一个区块，那么就获得了生成一个区块的权利，挖矿的奖励也就归你了”。

3.转账

Transactions，交易集合，不但给了每一笔交易的16进制数据，同时给了hash，交易费等信息。

Coinbaseaux，如果有想要写入区块链的信息，放在这个字段，类似中本聪的创世块宣言。

Coinbasevalue，挖下一个块的最大收益值，包括发行新币和交易手续费，如果矿工包含Transactions字段的所有交易，可以直接使用该值作为coinbase输出。

Target，区块难度目标值。

Mintime，指下一个区块时间戳最小值，Curtime
指当前时间，这两个时间作为矿工调节nTime字段参考。

Height，下一个区块难度，目前协议规定要将这个值写入coinbase的指定位置。

4.挖矿打包

矿工通过挖矿程序确认网络区块，每当收到一个区块后，即刻进行下一个区块的过程。

5.验证

将new block的json数据格式的Header给到矿工，矿工聚集算力给矿池算出new block需要的正确的Nonce，最后验证通过后矿池拿到出块奖励分发给矿工。

6.抗量子密码学机制

量子计算机的出现将对基于RSA和ECC的密码学机制产生重大挑战。量子计算机能够在极短的时间内解决RSA所依赖的大数分解问题和ECC所依赖的椭圆曲线离散对数问题。BitcoinNC是一种基于格的密码学机制，QS是Quantum Safe的缩写。目前，量子计算机尚无快速解决最短向量问题（SVP）和最近向量问题（CVP）的能力，格密码学被认为是抵御量子计算机的最可靠算法。

我们来计算一下BNC的整个市场的流通情况，每天全网大概能挖出14400个BNC，1T抵押100个BNC，相当于每天只能增加144T容量最多，这将是一个漫长的挖矿历程，基本对于早期的矿工，收益将是非常友好的，在加上四年减半，这简直是一个非常完美的经济模型，供需把控相当到位！

BNC的抵押经济模型，消除了矿工无限制抛售货币的可能性，CPOC挖矿将矿工绑定以作为生态利益共同体、并用币作为新型生产资料代替了原本消耗电力资源，使BNC整个生态不停的自动扩张。

BNC公链的发展路线