



Whitepaper

ver. 1.41 CHI/ZHO

目录

概述.....	3
XNDA 特点.....	5
多数现代加密数字货币面临的问题及我们提供的解决方案：	6
BITGUN	11
T.N.T.....	15
XDNA 基金会	18
时间线及区块奖励分配.....	20
参考列表	23
鸣谢.....	24

概述

现如今虚拟世界正面临一场名为加密货币的风暴，数字货币正牵动着世界上数百万人的心。比特币的成功激励了无数的数字货币爱好者们，这导致了现在几乎每天都有大量新的数字货币诞生。

然而百分之九十区块链项目的质量都不尽人意，有时甚至不堪入目。逐利者牺牲他人谋取金钱；诈骗犯不断克隆较有名气的数字货币；伪造名字和标识成普遍现象；能自我隐藏的病毒被写入源代码和二进制代码中——加密世界从来没有像现在一样充满危险。

在这场数字货币的狂欢中，用于投机的替代币不断被制造，千篇一律。针对上述现象，追求高品质且具有专业素养的加密爱好者们想出了一个主意：在数字世界构建一个众人闻所未闻的全新项目。

这个项目结合所有成功数字货币优势，同时充分考虑到其瑕疵和缺点。

这个项目适用于数字货币矿工、投资者，而且即使是对数字现实时代数一无所知的一般人也可受益其中。

这个项目不仅给数字世界带来了切实利益，同时也给现实世界带来实在的好处。

这个项目赢得了所有用户的心，并与以太坊（Ethereum）、达世币（Dash）、小蚁（Neo）、巴比特（Zcash）、门罗币（Monero）及其他区块链。并肩齐行。

在项目推进过程中，我们遵守以下原则：

- 项目将致力于解决一些有关现代加密数字货币的具体问题。
- 项目必须满足矿工和投资者的需求。
- 项目应为人类带来切实利益。

坚持上述原则，我们创造的将不仅仅是一种数字货币，而是在虚拟世界和现实世界间搭建一个可持续的供应链。这条供应链将与现实世界中其他链条紧密相连，如事件链、关系链、家庭关系和高科技的区块链。

没有这些区块链的生活无法相信，为此我们自豪地向您展示全新的革命性的数字密码加密货币——XDNA。

XNDA 特点

BitGun

创新原则——区块报酬动态变化

T.N.T

高级多层次主节点概念——三倍主节点技术

XNDA 基金会

非商业性慈善电子加密货币基金

产品规格

- 产品名/股票代码：XDNA
- 算法机制：PoW/POS
- POW 持续时间：1440000 区块
- PoW 区块链报酬：动态变化，4-511 XDNA
- 开采前保护：前 720 区块
- 散列算法：Keccak 算法
- POW 算法下 XDNA 预估供应量：138,000,000
- POS 启动块：1440001
- POS 相位持续时间：无上限
- POS 区块报酬：记 XDNA 每 525600 区块减少 4 个硬币直到报酬为 1 个 XDNA
- POS 区块报酬分配：负载均衡算法
- POS 算法下 XDNA15 年内预估供应量：228,000,000
- 挖矿前总量：971,712 XDNA (占 0.7%的 POW 总供应量)
- 区块大小：1MB
- 单区块花费时间：1 分钟 (DGW3)
- 交易确认次数：6
- 到期时：需 60 次确认

多数现代加密数字货币面临的问题及我们提供的解决方案：

在 20 世纪末，21 世纪初，比特币出现在人们的视野中。它的出现影响了地球上每一位进步人士——所有的这些人都在关注着比特币的发展和新型数字货币的发明及应用。然后，在加密数字货币领域中（如在任何其他高科技领域一样），存在着许多问题。例如可扩展性、安全性、微交易网络堵塞以及其他问题。这些问题通常都是本身自带的，已知的方法无法有效地解决它们。除了与加密数字货币相关的基本问题外还有一些细微的瑕疵，其中一些瑕疵在项目中已根深蒂固，被固定在几个项目中，而其他小问题带来的影响还在被低估。

这些小问题都是由对加密数字货币的粗略分析所引起的。

1. 长时间的交易确认

考虑到我们所处的世界是动态发展的，任何超过 30 分钟，甚至 60 分钟的等待时间都是一种负担不起的奢侈品。

2. 支持 POW 算法 ASICs 的出现

考虑到设备成本，哈希算法的应用如 Scrypt、X11、Sh256 和其他的一些加密算法，使得绝大多数人无法挖掘。此外，ASICs 的应用对系统的分散化造成相当大的损害，这与 Satoshi Nakamoto 本人制定的一般原则正好相反。

3. 即时挖矿

项目启动初期，开发商带头挖掘大量加密电子货币，但这些开发商们却延迟对外公告这些资源的开发。

4. 开采前的问题

开发人员在第一个块中获得了大量的电子加密货币代币。不幸的是，开发电子加密货币的人倾向于设定一个较高的矿前百分比，然后使用它来谋取个人利益，在货币交易后的前几天卖出大量的代币。这与以下几个问题密切相关。

5. 新加密电子货币的开发人员往往缺乏资源，而将他们的项目视为纯粹的个人致富手段，而不愿将他们的项目应用于慈善当中。

事实上，考虑到最成功的项目应该是市场资本化，于是很少有人会想到在慈善领域运用电子货币。同时，世界上仍有许多人需要食物、饮用水、药品和其他一些必需品。

6. 每个区块中的大部分报酬都是支付给开发商的，一些电子加密货币的创作者使用一小部分区块报酬用于解决一些麻烦，但在一些项目中用于解决麻烦的费用往往会过高。

7. 矿工回报的明显减少

随着哈希网的增加，挖矿难度也随之增加，反过来导致矿工们的“工资”减少。第二个问题是由一个非常明显的原因造成的：矿工收入与货币价格成正比，与哈希网总数成反比。

8. 主节点成本

主节点成本过高导致“普通矿工”无法正常挖矿，而在成本太低的情况下，投资者常常对收益缺乏兴趣。

我们创作 XDNA 的目的在于：

1. 解决部分上述问题，消除现有电子加密货币的弊端。
2. 追求矿工与投资者的和谐。
3. 为现实世界带去实际利益。
4. 改变矿工收入减少现状，提升网络容量。

第一个问题的解决方法：

为克服交易速度缓慢的问题，在 XDNA 代码中设置了 60 秒的区块时间。

DurkGraveWave3 算法将在每个区块上提供网络故障校正。

只有 6 次确认是交易验证所必需的，因此 XDNA 在世界上任何地方的任何交易都不会超过 6 分钟。

XDNA 还利用了即时发送[1]，一种及时交易机制，允许主节点立即广播给定的交易，并在接受者的钱包中立即显示余额。

第二个问题的解决方法：

POW 哈希算法 Keccak 在 POW 网络功能阶段被用于实现网络一致性。该算法已被证明为足够完美，可以与不同厂家的 GPU 一起使用。此外，该算法不受 ASIC 支持，所以世界各地的矿工都可以使用 GPU 安全地维护 XDNA 网络，而不受产业采矿中心巨大容量的威胁。

不过为什么 Keccak 可以做到？

首先，该算法不受 ASICs 支持。

第二，采矿过程中，您可以有效地使用“红色”和“绿色”卡。

第三，Keccak 可用于双采矿，这使得您可以多样化地使用采矿设备。

第四，2012 年哈希算法 Keccak 在由美国国家标准与技术协会（NIST）主办的密码哈希算法比赛中夺得奖项。

我们不创造一个流行的哈希算法，它是一个众所周知基本序列算法。在选择 Keccak 之后，我们向电子加密货币领域的科学家们致敬，是他们创造了该算法。众所周知，没有科学家和他们的研究成果，就不会有加密电子货币，因此就不会有 XDNA。

我们向 Keccak 算法的作者：Guido Bertoni、Joan Daemen、Michael Peeters 和 Gilles Van Assche 致以衷心的感谢。

第三个问题的解决方法：

为防止即时挖矿，XDNA 的区块报酬将会设置在前 720 区块。

第四个问题的解决方法：

一些加密电子货币的创造者在第一个区块中最多可获得 50% 的货币供应量。

XDNA 团队有一个具有实际意义的哲学理念，所以在 POW 或 971,712 XDNA 中，我们的矿前挖掘只有预估总量的 0.7%，

您可以在一些板块中了解更多关于 XDNA 矿前挖掘分配信息。

第五个问题的解决方法：

XDNA 团队一致认为需要大量的人在阳光下进行操作。充足的矿前部分，即 350,000 XDNA 将用于创建慈善基金——XDNA 基金会。这将通过筹集和分配资金来帮助世界各地的各种组织和需要帮助的人。与国际社会紧紧相连，我们创造的将不只是一种加密电子货币！

第六个问题的解决方法：

每个区块报酬的 1% 将用作对开发者团队的补偿，这与矿池所使用的佣金数量相当。

我们不做疯狂的矿前挖掘，我们也不做首次公开发行，我们没有需要隐藏的。区块报酬的 1% 就是我们的满满诚意。

第七个问题的解决方法：

最后需要解释一下 XDNA 最初产生的原因。为了解决矿工报酬减少的问题，我们研发了一种基于哈希网总量来改变区块报酬的特色工具——BitGun，由 XDNA 的一位开发者命名而来。

BitGun 的原理是，不同于传统的区块奖励分配方法，而是在逐步多阶段区块增加奖励，允许矿工接收相对稳定的奖励（在一定限度内）以维持 XDNA 网络功能。

您可以在相关章节了解更多关于 BitGun 的有关信息。

第八个问题的解决方法：

为吸引矿工和投资者们建立 XDNA 主节点，我们开发了一个系统，允许同时运行三种类型的相互作用的主节点。每种类型的主节点需要不同数量的货币作为担保，并且报酬的多少个不相同。我们已将这个系统命名为 T.N.T——三倍节点技术。

您可以在相关章节了解更多关于 T.N.T 的内容。

BitGun

为改变长期以来建立的与全算力成反比的矿工奖赏范式，我们开发了 BitGun 的高级特性。

通常情况来讲，矿工的报酬直接取决于网络全算力，这意味着较大的哈希网会每个矿工的报酬降低。换句话说，如果网络中的 GPU 数量增长 1000 倍，那么给定时间内平均矿工的报酬将减少 1000 倍。一些电子加密货币使用非线性相关性，但它们的原理保持不变。网络全算力越高，每个矿工接收的越少。BitGun 使用另一种方法——随着总网络全算力的增加，区块奖励逐渐增加，使得平均矿工报酬保持相对稳定。

BitGun 就是这样运作的。

每个区块奖励的多少在区块生成的每一时刻都会发生变化，这取决于前 24 个区块所记录的总平均希特网。

每个区块奖励的多少是随着一组反映斐波那契数列的“等级”而发生变化。总共有 15 个等级。

表 1 给出了由哈希网总数定义的级别和相应的区块报酬多少。

对于区块报酬的自动改变，XDNA 哈希网的总量必须克服表中相应的阈值。

使用这种方法有什么好处呢？

与传统的区块报酬计算方法相比，BitGun 允许我们在一定时间内稳定矿工所收到的酬金数额。随着网络全算力的充分增长，平均报酬略微减少，但仍比传统的报酬分配系统要多得多。

表 1:

等级	全网算力(Th/s)	区块报酬
1	1	4
2	2	5
3	3	7
4	5	9
5	8	11
6	13	15
7	21	20
8	34	27
9	55	39
10	89	57
11	144	85
12	233	131
13	377	204
14	610	321
15	987	511

表 2 表示的是在传统计算方法下使用 Nvidia GTX 1080Ti GPU 和 BitGun 的 24 小时平均回报对比。

表 2:

	1080ti 预计报酬	XDNA/1080ti/每 天	XDNA/1080ti/BitG un/每天
等级 1-5	1,000	4.032	4.032
	3,000	1.344	2.352
	5,000	0.8064	1.8144
等级 6-10	10,000	0.4032	1.512
	30,000	0.1344	0.9072
	50,000	0.08064	0.78624
等级 11-15	150,000	0.02688	0.5712
	300,000	0.01344	0.68544
	450,000	0.000896	0.45696

如上表所示，在全网算力低的情况下，奖励几乎是相同的，但是随着全算力的增长，BitGun 的优势十分明显。

图 1 展示的是使用基于全网算力总量的 Nvidia Geforce GTX 1080ti GPU 的日均报酬比较。

对 1-8 级进行数学建模。对于这个建模，我们采取的是以下条件：矿工从每个区块得到报酬；单个 GPU 的全算力在 Keccak 算法下为 1.35gh/每秒。

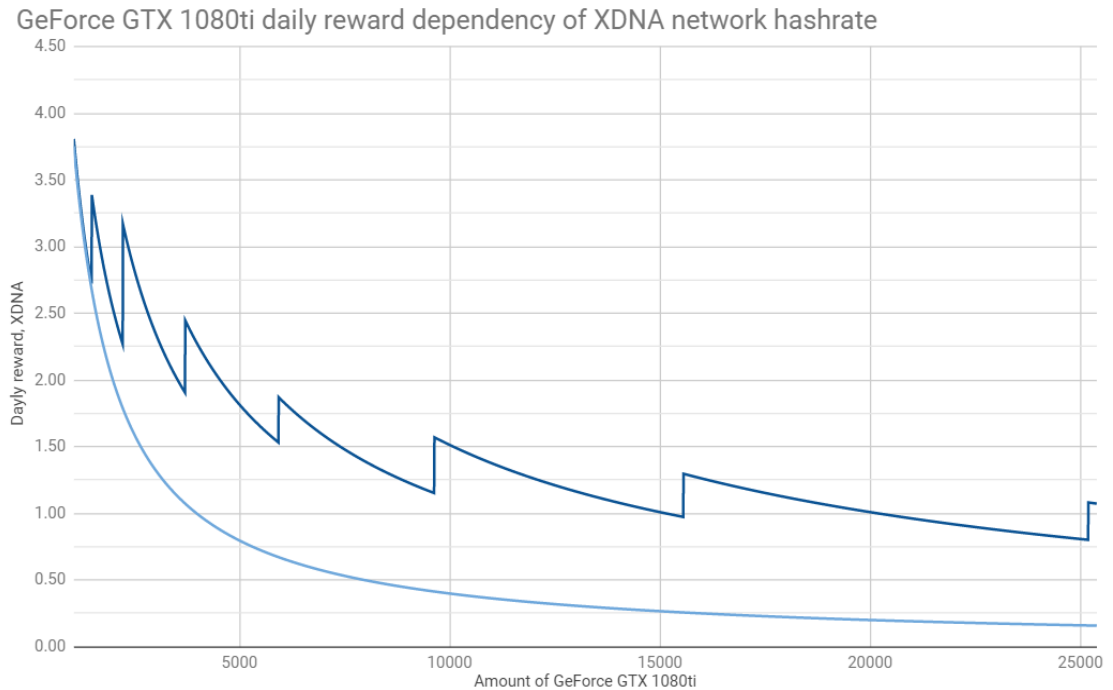


图 1

正如我们所看到的那样，即使全网算力显著增加，每个给定的 GPU 将在某个 BitGun 等级持续接收相对稳定的报酬，这个报酬远远大于使用传统系统计算的报酬。

这些建模结果对 2—14 级是有效的，并且可以在任何时间间隔内与模拟结果相近。

这种方法的新颖之处主要在于它改变了矿工收入与哈希网的伪线性反比关系。

BitGun 还有另一个不明显的优势。如果 ASKIC 矿工使用的 Keccak 算法升级了，XDNA 不用改变它的一致性和算法，也不用为了让矿工高兴而实行硬叉方案，只需要稍微修正 BitGun 的一些参数就行了。

哪怕全网算力突然增长 1000 倍，世界各地的矿工也有望得到一份相当不错的报酬。

T.N.T

若仅仅依靠世界前列的电子加密货币最先进的方面，我们建议使用主节点来确保网络的稳定性。

然而，考虑到在不同的项目中创建和使用主节点的经验，我们在 XDNA 上矿工和投资者的愿望及实现的可能性放在第一位。为了使每个人都能建立一个主节点，我们已经开发了三种类型的节点，每种类型都需要不同数量的 XDNA，并且能够带来大量收入。这个系统被称为 T.N.T——三倍节点技术。

1. 负载较轻的节点：需要 1,000 个 XDNA
2. 中等节点：需要 3,000 个 XDNA
3. 完全节点：需要 5,000 个 XDNA

在 POW 算法下主节点将获得以下奖励（节点类型不同，奖励也不相同）以维持网络稳定性并执行附加功能：

1. 负载较轻的节点：占总区块报酬的 3%
2. 中等节点：占总区块报酬的 9%
3. 完全节点：占总区块报酬的 15%

在 POS 算法下，主节点奖励比例保持不变，但数量将由负载均衡算法确定。

尽管主节点的任务是保持网络稳定性，但它们也是一种极好的投资方式。

通过一系列的计算，我们确定了不同类型的主节点的盈利回报。

值得一提的是 BitGun 的等级直接影响主节点盈利——在较高全算力下区块报酬增加，因此主节点收入也随之增加。

图 2 展示的是，基于网络中的主节点数量，不同主节点类型在不同的 BitGun 等级上的回报计算结果。

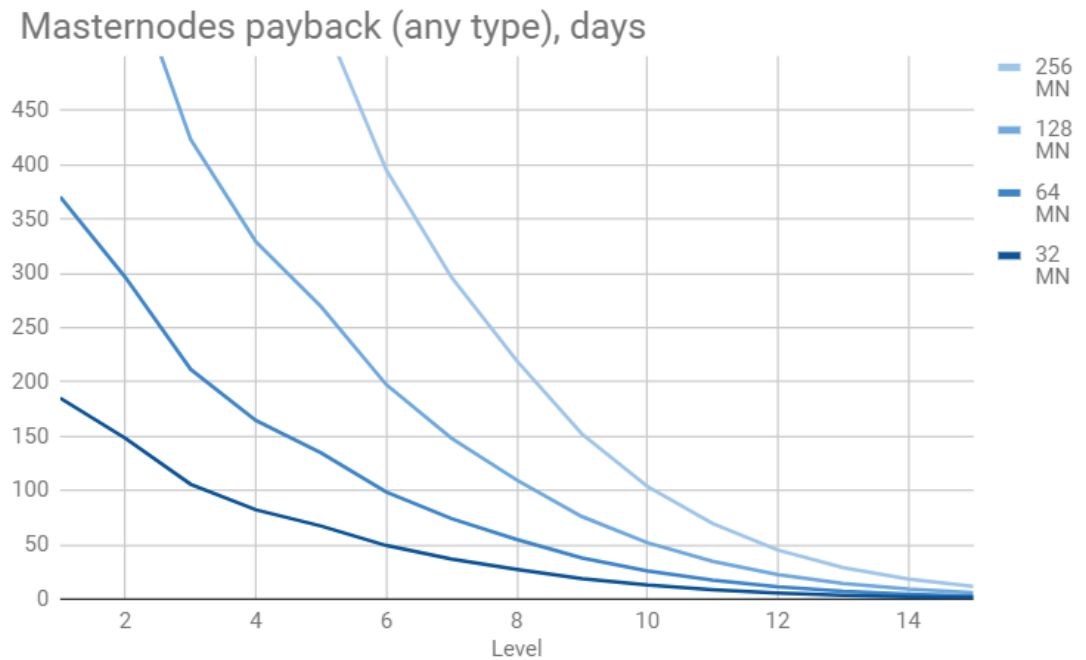


图 2

我们还计算了一组 50 个主节点的每日主节点支出，基于网络中它们的主节点类型和 BitGun 等级（图 3）；当每种类型的 100 个主节点存在于网络中时，基于每种主节点类型的 BitGun 等级，计算它们的投资回报率（图 4）。

Masternodes payments per day, XDNA (for 50 MN of each type)

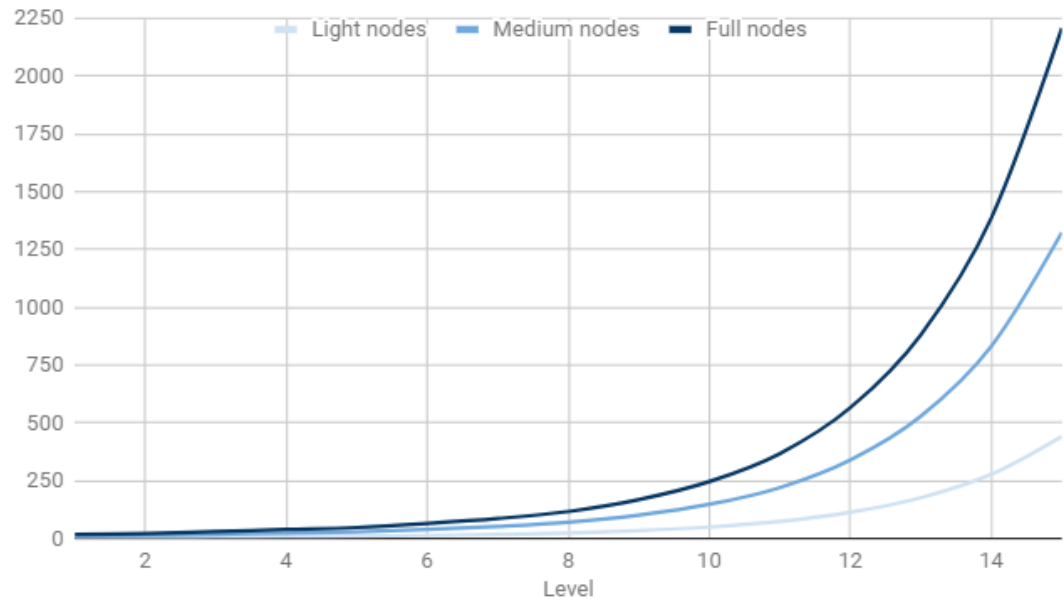


图 3

Masternodes ROI, % (for 100 MN of any type)

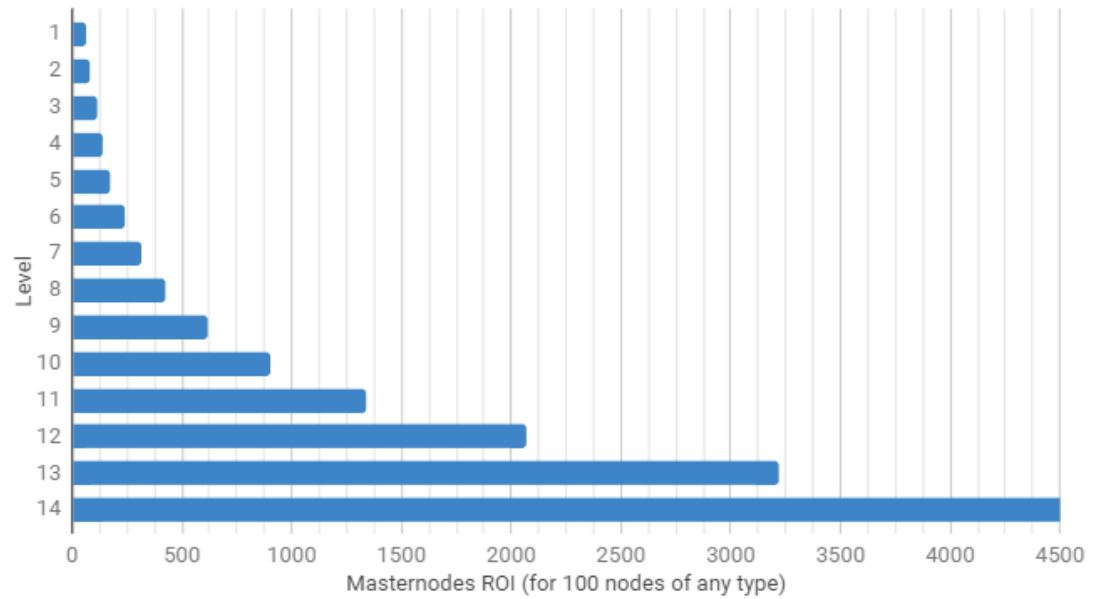


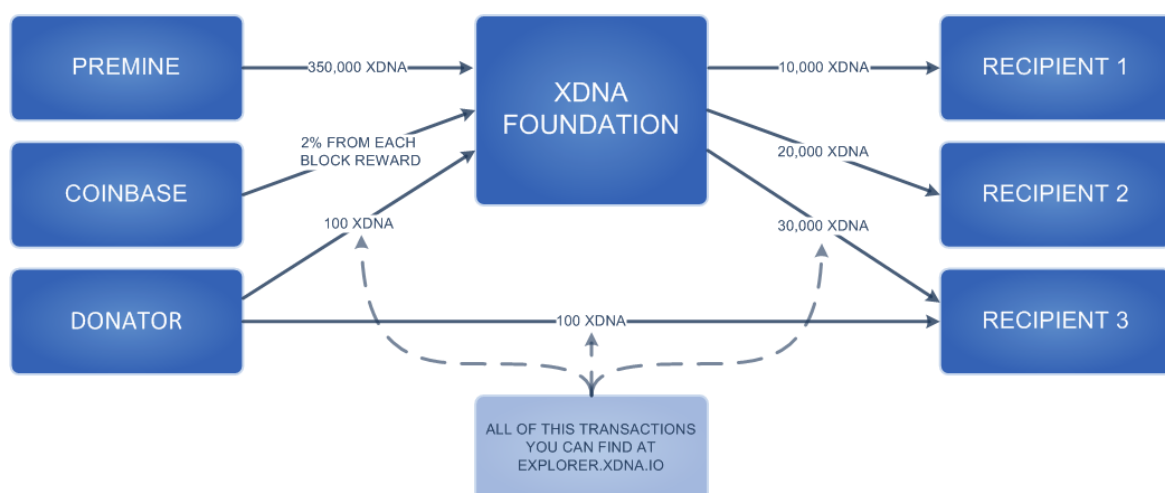
图 4

XDNA 基金会

我们在为这个世界考虑。我们知道还有许多慈善组织给需要的人提供免费的帮助，我们也想要成为它们中的一员，去帮助人们。

因此我们创建了 XDNA 基金会——一个电子加密货币慈善基金，旨在为一些组织和缺少基金或没有基金的基金会提供具有针对性的援助。

为启动这一项目，我们已经分配了 350,000 个 XDNA。所有资产被存入一个由基金会分配的特殊地址。基金会钱包中的 XDNA 数量是公开且受控的信息；打开区块浏览器并在相关区域搜索 XDNA 官方网站上的钱包地址就可以进行相关操作了。



这就是它的运作方式。

如果您所在的慈善组织资金较低，或者您是一个社会/社区项目协调员，一个青年运动队经理，又或者您只是需要 XDNA 基金会的帮助，以下几件事可以帮助到您：

在相关区域填写表格，简要描述你所在的组织，以及相关的问题和困难。

附上图片，写清楚具体内容，并尽可能地提供更多信息。

如果您认为您的请求是真实的且符合我们的目标，那么您的申请将被审查并标记为“正在考虑中”。待完成事实认证之后，XDNA 基金会管理层将会作出决定。如果您的申请被通过，我们将邮寄您（或面交）一个预先装入 XDNA 的纸质钱包。为了能够利用这些资金，您需要安装一个 XDNA 的电脑钱包，并 XDNA 储存进这个钱包。然后您就可以将收到的 XDNA 转换为现金或者比特币，并在你所选择的交易中使用它们。

如果你想使用 XDNA 去帮助人们或者一些组织，没有比这还要简单。在任何交易所购买 XDNA，并将其转入基金钱包地址。这真的十分简单。想把钱转入到另一个电子加密货币的基金会里？完全没问题，我们会把它换成 XDNA，并转移到基金会。

我们保证 XDNA 基金会里的任何一枚货币都不会被浪费掉。

如果世界上所有组织都用 XDNA 出售食物、水和医疗用品，或者用 XDNA 做慈善事业，那我们将携手把这个世界变为一个更美好的地方！请加入我们！

时间线及区块奖励分配

XDNA 的使用期可以分为两个阶段：即 POW 和 POS。在这两个阶段中，区块奖励的数额和分配有所不同。在 POW 期间，区块奖励有 BitGun 决定，以下为区块奖励分配原则：

- 矿工 70%
- 完全节点占 15%
- 中间节点占 9%
- 负载较轻的节点占 3%
- XDNA 基金会占 2%
- 研发团队占 1%

基于以上原则，POW 阶段的区块奖励分布如图 5 所示：

POW blockreward distribution

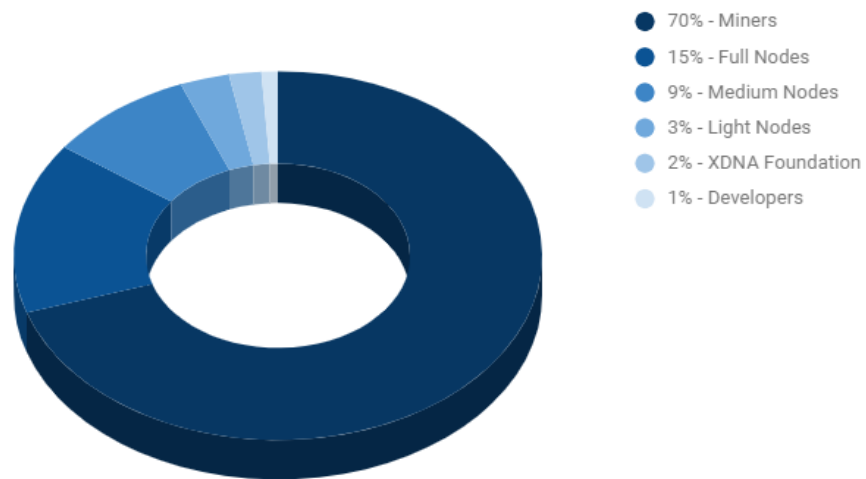


图 5

在第 14,400,000 个区块或接近 1000 天时，XDNA 将切换至 POS 阶段。在 POS 阶段，区块奖励一开始是 57 个 XDNA，等于第十个 BitGun 等级。

每 525600 个区块会减少 4 个货币（或每年大约），直到最终区块奖励变为一个 XDNA，这一时期大概需要 15 年，预计会发生在第 87984401 个区块上。

在 POS 阶段中，区块奖励采用负载均衡算法处理。主节点报酬比例将保持不变，但总的主节点报酬与赌注钱包报酬的比例将发生动态变化。

除此之外，每个区块奖励的 2% 将投入到 XDNA 基金会中，1% 将流入开发者基金。

由于我们无法预测在 POW 阶段的全网算力，所以无法计算 POW 阶段的最大货币供应量。为了估计这一点，我们使用了平均区块奖励，并在此基础上我们期望在 POW 阶段的总供应量大约为 138,000,000 个 XDNA。

在 POS 阶段的 15 年中，年区块奖励减少的数量 228,000,000 个 XDNA。

根据上述计算，18 年内货币总供应量约为 366,000,000 个 XDNA。

这一数量不包括开采前的 971,712 个 XDNA，这个数量约等于 7 天的供给量和平均区块报酬数量。

开采前数量是这样分配的：

- 350,000 个 XDNA——XDNA 基金会的创立
- 271,712 个 XDNA——开发团队的报销，这包括：
 1. 开发者的起薪
 2. 为种子节点租用虚拟专用服务服务器的租金
 3. 站点创建和域名权限
 4. 设计费用
 5. SSL 证书及项目创建期间的其他费用
- 350,000 个 XDNA——市场营销费用，包括
 1. 赠送礼物活动
 2. 社交媒体推广
 3. 吸引社群和市场竞争

4. 赞助费用
5. 线下媒体推广
6. 交易所挂牌费用
7. 加密电子货币单元的上市费
8. 纪念品生产
9. 通过博客、视频博客进行广告宣传
10. 纸质媒体及其他来自于市场方面的费用

Premine distribution (971,712 XDNA or 0.7% of POW supply)

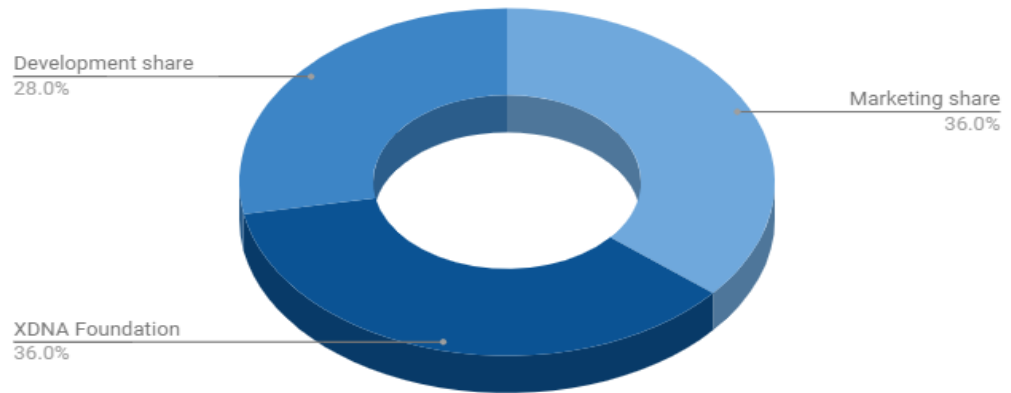


图 6

参考列表

1. DASH Masternodes <https://dashpay.atlassian.net/wiki/display/DOC/Masternode>.
2. Seesaw Reward Balance System Whitepaper. Revision 0.7e, January 24, 2017 <https://pivx.org>.

鸣谢

XDNA 团队感谢以下人士对 XDNA 项目的研究、开发、测试和支持。

S.F.Vakano

Gunbit

Kamir

George a.k.a. Commie

nullptr

a.kapone

koksoks

SiriS

Imbalance911

msbishop

TheUnknownHero

Allison

B52

oGrInGo

Satt

Kaseman

TeMbl4

marikun