一号币（yibitcoin）白皮书 v1.3

目录

一、简介

一号币 yibitcoin （简写：YTC）是一种基于“点对点”(peer-to-peer)技术和去中心化的区块链。YTC 可以帮助用户即时将一号币发送给世界上任何一个人。

“YTC”由一号币社区在 2016 年 5 月 13 日发布， 采用 POW+VPOW 工作模式，每 2.5 分钟产生一个区块，每个区块 25 枚一号币，每挖出 20 万个块产量减半，总量 1.5 亿，其中 1000 万枚用于 POW 挖矿，1.4 亿用于 VPOW 虚拟挖矿。YTC 基于区块链加密技术，深度改进了原算法存在的安全性问题，并使得区块确认速度大幅提升，优化了交易体验。POW+VPOW 采矿方式仅需普通电脑和客户端就能处理交易和维护网络安全，达到节能和安全的目的。

二、发展规划

一号币是建立在一号池的基础上产生的区块链，一号池与聚币网于 2016 年 4 月 7 日达成战略合作伙伴，将共同推动一号池的发展以及一号币在区块链领域的发展，同时一号币的应用也会逐步对接。

一号池在 2016 年 3 月 31 日上线 ,仅仅 7 天时间就达到 150G 的算力，全网目前排名第四，一号池未来的规划是吸引全球 30%以上的莱特币算力，以及全球 30%以上比特币算力，成为全球最大的莱特币矿池及比特币矿池。

三、特点：

1：以一号池为支持，对接实际应用

2：交易速度快,确认时间平均为 2.5 分钟

3：超快链接节点，支付转账速度更快

4：网络监视器，查看最新区块信息

2009 年，中本聪提出比特币的概念，自那以后，比特币已迅速在主流应用和商业用途中传播开来，成为首个吸引大量用户的数字货币，是数字货币史上的里程碑。不过从完成交易的角度来看比特币接收的情形，我们可以发现一个重要问题，就是比特币区块确认交易的时间过长，而传统的支付公司已找出使买卖双方实现比特币交易零确认的解决方案，但这一解决方案通常是要在协议之外采用可信赖的第三方完成交易。

比特币提供假名交易，实现发送者和接受者之间一对一交易的关系，并能永远记录全网发生过的交易。比特币只是提供低层次的隐私保护，这点在学术界众所周知，尽管有此不足，许多人仍然相信区块链记录的转账历史。

基于中本聪成果，YTC（一号币）是一个以保护隐私为要旨的加密区块链。我们在比特币概念的基础上进行了一系列的改进，由此诞生出一个去中心化和具备良好加密数字货币，它支持防篡改的即时交易，又有能为一号币网络提供服务奖励制的点对点次级网络。

四、钱包

一号币的钱包基于比特币钱包的基础上开发，采用 Scrypt 算法，系统采用工作量证明机制（POW+VPOW）来分发资产，以鼓励用户保证网络，不仅“至简”而且“至坚”，坚如磐石。一号币的钱包在安全性上对一些细节做了改动，在安全性方面针对 OpenSSL 漏洞和最

近披露的一些漏洞进行封堵，这些漏洞可能影响通过 SSL 使用 RPC。

五、 推动区块链发展

近年来，区块链技术正在经历快速发展，并吸引了超过 10 亿美元的投资规模。而我们认为，最值得重视的是，区块链正在走进金融机构、大型企业、政府决策层的视野，大有从“草根力量”引发经济变革的态势。一号币的发布势必会加速区块链技术的进一步发展。

1.定义

区块链（Blockchain）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案主要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（block），每个数据块中包含了一定时间内的系统全部信息交流数据，并且生成数据指纹用于验证其信息的有效性和链接（chain）下一个数据库块。区块链是一种类似于 NoSQL（非关系型数据库）这样的技术解决方案统称，并不是某种特定技术，能够通过很多编程语言和架构来实现区块链技术。并且实现区块链的方式种类也有很多，目前常见的包括 POW（Proof of Work，工作量证明），POS（Proof of Stake，权益证明），DPOS（Delegate Proof of Stake，股份授权证明机制）等。

2.特征

结合定义区块链的定义，需要有这四个特征我们才能认为：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively maintain）、可靠数据库（Reliable Database）。并且由四个特征会

引申出另外 2 个特征：开源（Open Source）、匿名性（Anonymity）。如果一个系统不具备这些特征，将不能视其为基于区块链技术的应用。而一号币完全符合这些特征，所以我们说一号币的问世进一步的推动了区块链技术的应用。

3.意义

在网络中每个人都能够认可和确认的方式，将某一部分价值精确的从某一个地址转移到另一个地址，而且必须确保当价值转移后，原来的地址减少了被转移的部分，而新的地址增加了所转移的价值。这里说的价值可以是区块链（比如一号币）也可以是某种实体资产或者虚拟资产（包括有价证券、金融衍生品等）。而这操作的结果必须获得所有参与方的认可，且其结果不能受到任何某一方的操纵.在如此纷繁复杂的全球体系中，要凭空建立一个全球性的信用共识体系是很难的，由于每个国家的政治、经济和文化情况不同，对于两个国家的企业和政府完全互信是几乎做不到的，这也就意味着无论是以个人抑或企业政府的信用进行背书，对于跨国之间的价值交换即使可以完成，也有着巨大的时间和经济成本。但是在漫长的人类历史中，无论每个国家的宗教、政治和文化是如何的不同，唯一能取得共识的是数学（基础科学）。因此，可以毫不夸张的说，数学（算法）是全球文明的最大公约数，也是全球人类获得最多共识的基础。如果我们以数学算法（程序）作为背书，所有的规则都建立一个公开透明的数学算法（程序）之上，能够让所有不同政治文化背景的人群获得共识。一号币就是数学算法的产物，它的存在不但可以推动金融领域，甚至可以彻底

颠覆我们对世界的认识。

也许我们现在正处在一个重大的转折点和工业革命所带来的深刻变革几乎相同的重大转折的早期阶段。不仅仅是新技术指数级、数字化和组合式的进步与变革，更多的惊喜也许还会在我们前面。这些数字化的数据信息还在以比摩尔定律更快的速度增长。区块链技术将不仅仅应用在金融支付领域，而是将会扩展到目前所有应用范围，诸如去中心化的微博、微信、搜索、租房，甚至是打车软件都有可能会出现。因为区块链将可以让人类无地域限制的、去信任的方式来进行大规模协作。一号币也将一起参与其中，让我们一起成为一号币和区块链发展的见证人

六、价值及预估

一号币的价值与一号池是密不可分的。一号池每月所收取的所有手续费均用来换取一号币，我们会将这些手续费用于在市场上换取等值的一号币，并将这部分一号币按比例免费的发放给所有持币用户。一号池比特币算力和莱特币算力分别达到 30%时，一号币的价值预估如下：

一号池比特币算力和莱特币算力分别达到 30%时收益情况表

一号池挖矿手续费收取 4%		
	BTC	LTC
一号池每天挖出	1080	4320
一号池每天可收	43.2	172.8
一号池每月可收	1314	5256
一号池每年可收	15768	63072

从上表看出，一号池每年预计获取大约为 15768 个比特币和 63072 个莱特币，这些一号池手续费全部用来从交易平台换取一号币，并免费按比例赠送给持币用户。

七、分发方式

一号币采用 POW+VPOW 模式，其中 1 千万枚 POW 模式采用实体矿机通过 scrypt 算法挖矿才可以获得，剩余 1.4 亿一号币采用 VPOW 模式，即通过获得虚拟矿机产出虚拟算力，通过虚拟算力进行挖矿产出一号币。虚拟矿机可在一号池官方网站通过比特币交换获得。

八、相关

一号币官方 1 群: 218665247

一号币官网：www.yibitcoin.com

一号池官网：www.yihaochi.com

一号币社区

2016 年 5 月 13 日