华克金区块链方案白皮书

开辟区块链数字资产的“黄金时代”

WCG

WORLD CRYPTO GOLD

华 克 金

前言

黄金具有着所有货币中最高等级的流动性。黄金不仅在人类 5000 年的历史上，被不同文明，不同种族，不同地域，不同时代，不同政体的社会公认为财富的最高形式，它也必将在未来的社会担当起经济活动最基本度量衡的重大历史重任。从国际市场来看，黄金正赶上一个长期大牛市行情，这对机构和个人投资者对黄金市场的预期树立了良好信心。要实现“藏金于民”，必须“藏金于市”。也就是说，要建设一个良好的、多元化的黄金市场，必须先让老百姓了解黄金，将黄金投资作为重要投资理财手段。而随着互联网的发达，黄金交易也迎来了一场货币革命。如今，区块链技术可以让你像刷卡一样地“刷黄金”。

华克金环球组织宣布基于区块链技术的黄金交易测试中取得重大进展，并将在推出基于区块链的黄金交易产品“华克金 WCG”。这将为黄金现货市场带来实实在在的信任价值增值。

在传统黄金市场中，资产所有权往往是不透明的。然而区块链科技能够提供“更高水平的可追溯性与审计”，提供不被篡改的所有权记录，使得黄金所有权更加清晰透明，并为交易者和投资者提供更加流动的买卖市场。使用区块链分布式账本，意味着黄金交易所有权可以被分成很多小份。使用区块链技术黄金所有权被保存在一个数字账本上记录所有交易。

传统黄金定价机制问题严重，这包括黄金交易不透明、效率低和人为操纵的问题，这是近代黄金交易发展的巨大阻碍。黄金的保存和携带不仅不方便，成本和风险更是难以估计。因此区块链的“黄金时代”将颠覆传统意义重大，市场期待已久。

依托于区块链技术的黄金交易平台对于市场具有里程碑的重要作用。首先，投资者更加信任“数字化黄金”，通过区块链平台进行黄金交易可以有效消除交易双方对黄金定价制度和资产真实性的质疑，从而扩大黄金市场交易深度，提高交易量。不久前，伊斯兰国家金融市场发布新规，允许伊斯兰金融市场使用数字黄金投资，帮助区块链黄金平台开辟了一个潜在的巨大市场。

如今，华克金 WCG 投资者将不再只是依附于“纸黄金”和“黄金储备银行”等仅部分基于真实资产的衍生产品交易平台，而是通过供应黄金的区块链产品手握坚实的后盾。

市场需求旺盛和选择范围扩大将进一步提高流动性，反过来又会增加流通量。这个良性循环的过程可以增强黄金作为抵押品和交易手段的功能。“有效性越高，价值就越大。”

区块链技术开辟数字货币新时代。如果所有黄金交易最终都通过区块链平台进行交易，投资者以电子购买、销售、持有现货黄金。分布式账簿机制有效进行及时结算和资产所有权的确立，统计实际的黄金储蓄数量将变得简单。各国中央银行对区块链技术和数字货币的兴趣也越来越大。这意味着会有越来越多的国人走走在数字货币探索全球最前沿。

目录

第一章 . 华克金 WCG：点对点的智能经济生态系统

1.1 摘要

比特币已经证明了点对点的电子货币系统的可行性，并且可以在不需要信托或是中央印钞厂（金融机构）的情况下完成支付过程。但是比特币的一些缺点也使得其成为电子经济的基础变得困难。为了使得整个经济系统能够建立在对等的基础上，必须要做到以下几点：

1. 快速的处理数以千计的交易量
2. 提供一种产生收入的方法
3. 有可行的方法来增加新特征
4. 能够在可移动设备上运行

而华克金 WCG 则满足了以上所有要求，同时还消除了比特币的工作量证明 Proof of Work (POW) 所需要的算力机制与竞赛。华克金 WCG 是基于 100% 的权益证明 Proof of Stake (POS) 的加密货币。

1.2 简介

关于华克金 WCG 最根本的革新就是透明锻造 (Transparent Forging)，这是华克金 WCG 最核心的改造（创新），使其每秒能处理上千次的交易量。只有透明锻造 (Transparent Forging) 这种解决办法，能让整个网络来预测哪个节点会锻造下一个区块，从而能够直接的传输交易并且能保证交易中的即时确认，这就消除了网络速度的瓶颈问题。

通过比特币直接赚钱的方法，就是推断它的期货价值（未来价格）。WCG 有一种革新机制使交易费用得以循环，即用交易费来奖励锻造出目前区块的节点。就目前而言只有三种方式生成交易费：任意消息、WCG 转移和别名注册，但是随着 WCG 增加更多的特征，每一个参与锻造的 WCG 账户所生成的收入也会持续增加。因为 WCG 拥有一种实用的机制来通过它的投票系统获得更多新的特征，希望社区能同意增加更多有前途的新兴的特征，相应的，也会增加交易费用的数额以及 WCG 的实际利率。

通过把所有的这些特点与可扩展的框架相结合，WCG 已经完全成为一个完善且成熟的点对点经济的基础。从微交易，到投资回报产出、公开 IPO、瞬时交易，以及所有 WCG 所能实现的事情。

第二章 . 比特币的问题

2.1 区块链大小

比特币的区块链是完全按顺序生成的数据区块，它包含了自从比特币在 2009 年 1 月上市以来所有的电子分类账簿。四年之后的 2013 年 1 月，比特币的区块链已经占据了 4 千兆字节 (GB) --- 大约是将一部两个多小时的电影刻在一张 DVD 光盘上所需要的数据量。仅仅在一年之后的 2014 年 1 月，比特币的区块链已经膨胀到 3 个百分点 ---13 千兆字节 (GB)。比特币的区块链正经历着指数倍的增长，因此又必须要修改原始的比特币协议来应对不断增加的区块链。

2.2 每天的交易量

在 2013 年底，比特币的交易量最高达到了每天 70,000 的峰值，或是平均每秒一个交易量 (TPS)。目前的比特币标准区块在一兆字节，是由称之为“全节点”的客户端每隔十分钟产生的，将目前比特币网络总承受量局限在最大 7TPS。把这个与 VISA 的网络工作相比，它的承受能力可以达到 10000 TPS，你就会发现比特币不能与如今所存在的相抗衡。

增加比特币系统的公共使用量会使比特币很快达到每日交易量限额，并且会阻断其更多的增长。为了防止这种情况的发生，比特币软件开发者正在研发一种“lite node”客户端，声称能够简化支付验证节点而不会被区块的尺寸寸所限制。为了在相同的平均十分钟里能操控更多的生产量，SPV lite node 不会在他们处理的区块里进行全面的安检，相代替的是对那种竞争的矿工的散列列且多样的区块链进行检查，并假定由大多数矿工所生产区块链版本是正确的。用比特币麦凯恩的话来说就是“没有确认所有东西西的真伪，仅仅是因为 SPV 信任大多数的矿工是诚实的。只要大多数是诚实的，SPV 就能工作，但全节点确实提供了更好的安全性。例如，你开了个在线店，你就会感觉到运行全节点是有意义的。

2.3 交易确认时间

2013 年的大部分时候比特币的交易确认时间是 5 到 10 分钟。自从中国的银行不许再受理任何比特币的公告一出，比特币的平均交易时间就明显的增加到 8 到 13 分钟，以后的交易时间每时每刻都充满着不确定因素。中国的银行预算比特币一天可以产生大约 650,000 的交易量并且交易确认的时间最长达到 20 多分钟。因为最终确定比特币的交易需要很多的认证，因此在用比特币购买资产的过程结束之前会很耗时。

2.4 中心化的疑虑

比特币难度的增加以及网络 hashrate 的结合成为新手们进入的很大阻力，并且给现存的矿机减少了利润。比特币所采用的区块奖励机制驱动了创建更大、更专业的挖矿设备，以及对大型矿池的依赖。这已经导致了”中心化”的结果，因为越来越少的人控制着越来越多的算力。这不仅导致了比特币本身设计时要避开的这种算力结构，而且表明单个挖矿设备或者矿池有能力占据网络总算力的 51% 并且实施 51% 攻击。只需要 25% 总的网络 hashing power 的攻击也是存在的。2014 年 1 月初，GHAsh.io 由于其矿池算力接近 51% 而不得不减少其矿池算力。几天之后，该矿池的算力减少至整个网络算力的 34%，但是随后算力马上又增加了。1 月份第三周，比特币两个最大的矿池的算力已经达到了网络总算力的 60% 了。

2.5 工作量机制对资源的消耗

现有比特币的交易确认以及创造新的比特币用于流通需要大量的计算算力持续的操作。这种电脑算力是由那些“矿工”们通过所谓的矿机进行操作的。比特币矿工们相互竞争来为整个比特币的区块链增加下一个新的交易区块。这是通过”哈希值“来完成的 --- 将过去十分钟内所有发生的比特币的交易捆绑，并尝试将它们编译到一个区块数据中，而这个区块含有一个特定数目的连续 0 的随机数。绝大多数矿工哈希计算所产生的区块都不包含该目标 0 值，因此它们需要作出轻微的改变并继续尝试。为了成功找到区块而进行的大量的尝试称之为”gigahash”，也即挖矿设备是用每秒钟能够进行多少 gigasashes 来分级的，表示为”GH/sec”。第一个产生准确区块的矿工将会收到 25 个新的比特币 s 的奖励，按照目前的价格来计算为 $25,000。这些在矿工之间为了获得奖励的竞争，将会每隔 10 分钟进行一次又一次的重复。到 2014 年初，每天产生的作为奖励的比特币的价值在 350 万美金。

看到如此多的奖励，矿工之间展开了激烈烈的军备竞赛，以便增加获得奖励的概率。起初，比特币是用普通计算机的中央处理器 (CPU) 来挖矿的。后来中门的图形处理单元 (GPU) 也被用于增加速度。再后来是现场可编程门阵列 (FPGA)，紧接着则是专用集成线路 (ASIC) 芯片。ASIC 技术是比特币矿工的顶级技术，然而军备竞赛则产生了各种各样的 ASIC 芯片。目前的 ASIC 芯片是 65nm 单元的，是基于纳米级的晶体管。它们被 2014 年初的 28nm 的 ASIC 和 2014 年中的 20nm 的 ASIC 所替代了。其中的一个例子是 Butterfly Labs”Monarch” 28nm 的 ASIC 芯片，它能提供的算力为 600GH/sec，电力消耗为 350 watts，价格为单片 $2100。Hashblaste 刚出来的预定芯片则含有 3 个 20nm 的 ASIC 芯 <0505> Tj E 片，能提供的算力为 3300 GH/sec，能耗为 1800 watts.

大多数的挖矿设备都将在 2014 年中旬升级到该性能标准。目前支撑比特币运行的挖矿设备构架是惊人的。比特币的 ASIC 是愚蠢的 --- 它们只能进行比特币的区块计算，并无其他用途，但他们能够以超级计算机的速度进行那种计算。2013 年 11 月，福布斯杂志撰文写道”全球比特币的算力是 500 个最顶级超级计算机联合算力的 256 倍”。2014 年 1 月中旬 , blockchain.info 显示支撑比特币运行素需要的持续算力为 18

million GH/sec。在一天 86,400 秒内，这意味着矿工们为了找到能够获得 350 万美金奖励的区块，将会有大约 1.5 万亿的尝试区块被生成和拒。因此大约有 99.99999999 % 的比特币的算力并没有用于治疗 DNA 模型的癌症或者 E.T 的无线电研究 --- 相反，他们被完全的浪费了。

矿工为了支持比特币所小号的电力和成本是巨大的。如果所有的比特币的挖矿设备都拥有“Monarch”级别的能力 -- 除非它们升级，否则不会达到这样的级别 --- 这 30,000 个设备将耗资 63,000,000 美金，而且每天持续消耗的电力超过 10 兆瓦，也即是每天消耗的电费好过 3,500,000 美金。而真实的数目比目前的还要大，因为支持比特币运行的挖矿设备相对比较低效。随着比特币从目前的一秒钟一个交易增大至最大一秒钟 7 个交易，这些数字也正以指数倍数在向上增长。

2.6 持有工作量机制虚拟币的资源耗费

除了大规模的电力消耗之外，单纯的持有比特币也有一些隐性支出。对于每个区块资金，生成区块的实体都需要固定的津贴。在写这篇文章的时候，津贴是 25 个比特币，为今年比特币的总供给量提供了 10% 的膨胀率。对于持有价值 1000 美元的比特币有些人而言，今年需要花费 100 美元一个的比特币“支付”给矿工们，来保证网络的安全运转。

第三章 . WCG 的解决办法

3.1 密码学基础

WCG 的主要交易是基于 curve 25519 算法，该算法使用快速、高效、安全的椭圆曲线秘钥算法 (elliptic-curve Diffie-Hellman function) 生成了共享秘钥。这种算法最先是由 Daniel J. Bernstein 在 2006 年提出的。

WCG 中的信息签名是使用 EC-KCDSA(elliptic-curve Diffie-Hellman function) 来实现的，该算法是 IEEE P1363a 的一部分，是由 the KCDSA Task Force team 在 1998 年提出的。所有的算法都是基于平衡速度和安全来选择的，其秘钥长度为 32 字节。

3.2 加密算法

当爱丽丝给鲍勃发送了一份加密文档时，她：

1. Calculates a shared secret:

• shared_secret = Curve25519(Alice_private_key, Bob_public_key)

2. Calculates N seeds:

• seedn = SHA256(seedn−1), where seed0 = SHA256(shared_secret)

3. Calculates N keys:

• keyn = SHA256(Inv(seedn)), where Inv(X) is the inversion of all bits of X

4. Encrypts the plaintext:

• ciphertext[n] = plaintext[n] XOR keyn

Upon receipt Bob decrypts the ciphertext:

1. Calculates a shared secret:

• shared_secret = Curve25519(Bob_private_key, Alice_public_key)

2. Calculates N seeds (this is identical to Alice’s step):

• seedn = SHA256(seedn−1), where seed0 = SHA256(shared_secret)

3. Calculates N keys (this is identical to Alice’s step):

• keyn = SHA256(Inv(seedn)), where Inv(X) is the inversion of all bits of X

4. Decrypts the ciphertext:

• plaintext[n] = ciphertext[n] XOR keyn

注意：如果有人猜到文档的一部分内容，他们可以通过使用相同的密匙对来破译爱丽丝和鲍勃之间的信息。所以，建议分别为每一次的交流建造一对私钥和公钥。

3.3 区块链

同其他加密的货币一样，WCG 交易的总账是建立和储存在一系列列的区块里的，也就是所谓的区块链。每个区块链的备份都存放在WCG 网络的每个节点里，而且在每个节点上没有加密的每个账户都能够生成区块，只要至少一个新入账户的交易已经确认了 1440 次。任何账户只要达到了这个标准就会被视为”激活账户”。

在WCG 里，每个区块都包含着 255 个交易量，每个交易都是由包含识别参数的 192 字节的数据头开始的。

一个区块里的每个交易量都是是由 128 个字节所代表着。总共加在一起就意味着最大的区块大小有 32K 字节。所有的区块都包含以下参数：

- 一个区块版本
- 一个区块时间戳，从源区块开始的用秒来计算
- 之前区块的 ID
- 区块里所储存的交易数目
- 区块中总的 WCG 交易量
- 区块中总的交易费用
- 区块的负载长度
- 区块负载长度的散列列值
- 生成区块的账户公匙
- 区块的生成签名
- 整个区块的签名

每个链条上的区块都有一个”生成签名”的参数。激活账户用自己的私钥在原先的区块上签署“生成签名”。这就产生了一个 64 字节的签名，之后通过 SHA256 散列列该签名。哈希产生的前八个字节给出了一个数字，作为一个“hit”。这个“hit”与目前的目标值（是一个 64bit 的数字）相比较。如果计算出的“hit”值要比“目标值”低，那么就可以生成下一个区块了。

因此产生了“Proof of stake”的算法，因为对于每个激活账户来讲，“目标值”都是与它自身所确认的余额成比例的。一个持有 1000 个币的账户得到的目标值是持有 200 个币账户所得到目标值的 50 倍。因此，拥有 1000 个币的持有者产生的区块数是持有 20 个币的人产生的 50 多倍（从长远角角度来说）。

“目标”值并不是固定的。随着先前区块的时间戳的流逝，每秒钟都在增长。如果在最初的一秒钟内没有哪个账户的“hit”值是低于“目标”值的，则下一秒钟目标值就会翻。“目标”值会持续的翻倍直到一个活动账户的“hit”值有一个较低的数值。还有一个“基本目标”值会以 60 秒的间隔设定为目标值。正是因为这个原因，一个区块，平均产生的时间会在 60 秒。

即使在网络上只有很少的激活账户，他们其中的一个最终会产生一个区块因为“目标”值会变得相当大。通过将你账户的“hit”值与目前的“目标”值相比，你就可以估算出你的“hit”值还有多久能成功。

当一个激活账户赢得产生区块的权利时，就能将任何可获得的且未确认的交易放入区块中，并用所有需要

的参数来填充该区块。然后这个区块就会被传播到网络中作为一个区块链的备选。

每一个区块中的负载值、“hit”、产生的账户以及签名都能被网络上接收到它的节点所确认。每个区块参考之前的区块，区块形成的区块链可以用来追溯和查询网络中素有的交易历史，所有这些都会追溯到创世源区。

3.4 交易

计算每个 WCG 账户的余额需要对整个区块链进行扫描。尽管这听起来效率很低，但是就目前网络与 CPU 的速度而言，这并不是一个很大的计算量。处理这些工作需要 WCG 服务器因此也就允许了更低能耗的移动设备成为 WCG 的节点。

WCG 交易的细节如下所示：

1. 发送者指定了交易的参数。交易的种类有很多（发送钱币，创建别名，发送信息，发行资产或对资产下订单）但是任何交易的几个参数都需要指定。

• 发送账户的密码

• 交易的费用

• 交易的截止期限

• 随意的“参考”交易

2. 所有交易的输入值都要通过检查。比如：强制性的参数必须指定：交易费不少于零，交易截止日期不少于一分钟。

3. 如果参数核实的结果不出现意外的话：

• 通过所提供的密码来计算产生账户的公钥。

• 产生账户的账户信息可恢复，并且交易参数要进一步的验证。

1) 发送的账户的余额不能为零

2) 发送账户的确认余额不能低于交易额与交易费用的总和

• 如果交易账户有足够的资金提供给交易额

1) 产生一个新的交易，其类型与子类型值要设定为与已经产生的交易的类型相匹配（发送钱币，创建别名，发送信息等等）所有指定的参数都包含在交易对象中。唯一的交易 ID 也是随着对象的创建而生产的。

2) 交易是用发送账户的密匙所签署的。

3) 加密的交易数据被放置在信息里，信息用于指导网络节点来处理交易。

4) 交易被传送到网络上的所有节点。

4. 服务器会反馈一个结果代码: 交易 ID, 如果交易成功的话; 如果参数确认失败, 则反馈错误代码和错误信息。

3.5 交易确认

所有 WCG 的交易都被认为是”未确认的”，除非它们已经被包含在有效的网络区块中。新建立的区块会通过创建他们的账户分散到网络中。而且包含在区块里的交易就会得到确认。因为随后的区块会添加到现有的区块链，因此每增加一个区块就会对现有的交易进行增加一次确认。

在经过 10 次确认之后，WCG 交易被认为是可信的。如果出现问题，网络有可能重新组织最近的 720 区块，所以一个交易在 721 次的确认之后是不可逆的。而已经被确认了 1440 次的交易则被认为是永恒交易。

3.6 权益证明 Proof of Stake (POS)

在以前陈旧的 POW 模型中，网络安全是由节点通过“工作”来保证的，他们借用他们的资源（电脑 / 处理时间）来帮助加强网络，并且阻止恶意袭击。这些节点因为他们的“工作”而被奖励了一些区块的币，这些数量以及他们出现持续的时间都基于特定的网络。这种办法的弊端就是需要越来越多的时间处理（以及持续的能量）因为随着时间的流逝，指定的节点来支撑网络的运转就格外重要。

换句话说，随着网络越来越快的发展，单个节点来支撑网络的积极性就越来越少，因为他们潜在的奖金都被越来越多的节点所划分。一些节点用专业的、专有的和昂贵的硬件持续的增加资源投资，并且增加能量消耗。随着时间的推移，很讽刺刺的是，网络将会越来越中心化，较小的节点（工作量很小的节点）会退出，因为他们的奖金会流向更大的节点（那些能负担的起更多资源及能量的节点）。

说到这点，最近 GHash.io 矿池的算力已经非常接近比特币算力的 51%。这样的话，单个个体已经控制了区块链，去中心化的概念就完全消失了。在 WCG 所运用的 POS 模型中，网络的安全是由拥有”股份”的节点所维护的。

3.7 网络

WCG 的网络是由节点组成的。节点在本质上来说是任何贡献于网络的设备。任何运行 WCG 的 NRS 客户端 (WCG Reference Software) 的设备都是一个节点，并且因为源代码可以开发成本土的客户端，它们也会成为节点。节点可以分为两种类型：“有标记的”和普通的。每个标记过的节点都继承了基于标记账户所持有 WCG 数目的权重，可以只有 1WCG，或者，五百万到一千万的 WCG，是没有上限的。拥有权重越大的标记节点，其可信度也越高。

如果一个攻击者想要标记一个节点从而获得网络的可信度，然后用这种可信度去进行攻击，进入的阻碍（消耗 WCG）就会限制这些滥用。一旦投票系统得以实施，其它节点可以发起投票来禁止或是惩罚网络上的恶意节点。

3.8 透明锻造

为了解透明锻造，首先就要理解锻造本身的过程。对于激活的锻造账户，其锻造到区块的机会与它所持有的 WCG 数目以及网络上所有激活的锻造 WCG 数目是成比例的。也需要一定的随机性来消除对相对靠后的已知的锻造者的攻击，但是，对于相对靠前的而言，就需要尽可能的准确以减少对网络带宽的使用。

大拇指法则决定了一个账户每天能锻造到的区块量是（账户余额 /1000000000)*1440，以上的前提假设是：所有的 WCG 都在进行锻造，以及一天产生 1400 个区块。然而这两个数据一天内的变化是很大的。

由于锻造机会是计算出来的，因此就能够预计出那个账号锻造出下一个区块以及什么时候锻造出来。因为 hit 值已经确定，拥有多账户的人可以计算出哪个账户最有可能锻造出下一个区块，因此可以将所有的 WCG 转移到那个账号里。这就是为什么要选择有效余额而不是实际余额。一个账号存入资金时的时间延迟以及资金转移时的时间延迟都会减少 WCG 受攻击的有效数目。

通过储存来自所有账户的 hit 值，如果每个节点都知道哪个账户是处于激活锻造的，就有可能让所有的节点预测哪个账号会锻造出最近的区块。

因为每个节点都有基于可视节点和激活锻造账户变化的不同网络拓拓扑结构，所以并不是 100% 的准确，但这是事先的设计。当然也需要一些错误的因素来阻止攻击者通过计算出最近的区块锻造者而对 WCG 网络实施攻击。只要预测准确率接近 100%，网络拥堵问题就极大地减少，从而允许数以千计的实时交易。

透明锻造允许在去中心化的网络中存在中心化的操作。这是 WCG 最基本的突破。透明锻造允许每个用户客户端自动决定谁将产生下一个区块，然后他们就可以将把他们的交易发送至那个节点上。为了实现即时交易，允许额外的费用。透明锻造另一个同等重要的特点是协议杰出的安全性，它可以临时性的将产生一下个区块的节点的锻造能力减少至 0.

这个特性设计用于阻止拥有 90% WCG 数目的节点进行分支或者分叉。因此，如果一个节点拥有 90%

的 WCG 而未按照计划产生区块，系统就会临时的将其锻造能力减少到 0 以阻止可能的分叉。它的锻造能力就会分配给网络中剩余的节点，因此网络的能力还是 100%，所以，不管该潜在的对手它在其它分支上做什么，都会被高级的共识机制（还未披露露）所抵消。

透明锻造意味着什么？它意味着每个人都可以预测（很大几率）谁以及什么时候会产生下一个区块。这就给予了 WCG 很多优势：

1. 交易能够直接发送给即将产生下一个区块的锻造者（如果他愿意披露它在网络上的地址），因此节省了交易流量并很快接近 VISA / MasterCard 的交易量。

2. 区块可以提前产生，并且在它们生效（时间戳生效）之前发送给大多数的锻造者，因此很大程度上就减少了孤立区块的概率。

3. 由于可以预测未来区块时间（区块速率），因此设定适当的费用来确保重要交易能够快速确认就变得有可能（不用在一个区块中花费太多）。

4. 也许最重要的是，网络能够检测出哪个锻造者没有参与到区块生成中来并采取相应的措施。

作为 100% 的 POS 货币，WCG 能够预防政府和可以获得很多 ASIC 的财团，而且有了透明锻造特征，甚至可以预防某些人购买绝大多数的币。所以到底是什么让 WCG 能成为下一代货币？并不是那些漂亮的特征，比如去中心化的交易、DNS 或是去中心化的应用商店，而是透明锻造机制（促成了这一点）。

3.9 交易费用

交易费是 WCG 如何再循环至网络的途径。现有的交易资金是通过发送 WCG、创建别名或者发送信息来产生的。

交易费用目前设定为每次支付最少 0.01 个 WCG，并且直到交易数目填满一个区块，1 个 WCG 的费用将足够将其包括在区块内。而且随着 WCG 价格的增加，最小的交易费用将下调至用户可以接受的程度。比特币的交易费为 0.0001 的 BTC，随着比特币价格的增加交易费将会变得越来越不实际。随着 WCG 价格的上涨，交易费也会逐渐降低，WCG 将会非常适合于微支付。到那时候，即使需要更小的单位，比如 milli-WCG，micro-WCG 甚至 femto-WCG，我们可以发行彩色币来表示任何内容。

3.10 回收磁盘空间

区块链的膨胀是一件大事，它与任何的加密货币相关，尤其是对那些像 WCG 交易量很大的来说。通常，添加到区块链的操作会按照他们使用的空间大小来收费，这也是为了限制节点故意膨胀区块链。

但是，随着时间的流逝，重新从源区块开始计算所有内容是很没有效率的。WCG 计划进行每年的检验点，它会为所有的节点创建一个起点去使用，其频率可以让 WCG 的股东们进行投票表决。通过使用电子签名，可以确保每年检验点的有效性。拥有资源越多的网络节点（比如专用服务器）也能继续支撑整个区块链，并且作为服务提供商而受到奖励。

（这是我的拙见）

举个例子，到 2012 年中期，比特币的区块链仍然保持在 1GB 大小内。而现在，仅仅一年半之后（2014 年的 1 月）随着比特币日趋增长的流行以及越来越多的交易，区块链已经膨胀到了将近 13GB 的大小。很明显，对于绝大多数的设备来说提供这么大容量的区块链是不可行的。即使是整个链条的传送就要花费好多小时，而且还要取决于网络连接速度。

3.11 设备可携带性

由于它是 Java 代码，POS 哈希散列列以及能够修剪和减少区块，WCG 非常适合于运行在小巧，低功率以及低功耗的设备上。安卓以及苹果的应用也正在开发中，而且 WCG 客户端 NRS 已经运行在低功率的 ARM 设备上了，比如 RaspberryPi。

将 WCG 应用于低功率或者联网设备是很容易的，比如说，智能手机。这些设备支持大部分网络。因为全球数以百万计的人已经拥有了智能手机，WCG 能够在这些设备中快速的得到应用从而来支持网络，而不用像传统密码学货币那样花费很多钱。

WCG 的特征，比如说瞬时交易使得智能手机成为一个理想的平台在日常消费中来使用 WCG（食品，燃料等等）。在这个领域，其它密码学货币也存在解决方法（比如，比特币），但因为需要大量的资源（算力）来维护网络，因此使用这些设备并不能对网络健康或稳定性带来帮助。而对于 WCG，任何有发送和接受交易功能且有一定算力的设备都能增加网络的稳定性以及去中心化。

第四章 .WCG 锻造技术

4.1 锻造及 WCG 的产出

锻造一个区块的机会取决于基础目标值 Base Target（对所有人都一样）、从上一区块开始的时间 time since the last block（对所有人都一样）以及你的账户余额 Balance。

机会 = 基础目标值 × 从上一区块开始的时间 × 账户余额

T = Tb × S × Be

where:

T is the new target value 机会

Tb is the base target value 基础目标值

S is the time since the last block, in seconds 从上一区块开始的时间

Be is the effective balance of the account 账户余额

4.2 WCG 锻造计算

我们从概率论的观点来讨论 WCG 的锻造机制，通过公估算出几个重要的参数，比如一个账户锻造到区块的可能性，一个账户锻造到最长序列列连续区块的长度，以及目前区块链胜过其它的可能性。

第五章 .WCG 特性

5.1 别名系统 – 与 DNS 类似

5.2 任意信息 – 任何人都可以发送任何形式的信息

5.3 资产交易 – 货币 / 股票交易

5.4 分布式计算

5.5 分布式存储

5.6 瞬时交易

5.7 混合服务

5.8 多重签名

5.9 服务供应商 – 区块链之外的服务

5.10 缩减 – 缩减膨胀的区块链

5.11 智能合约

智能合约的期望是将合约嵌入到有价值的且以电子方式控制的资产中。WCG 的只能合约可以用于发行分布式自治组织 DAC。DAC 可以作为 WCG 矿池。

5.12 双相支付

5.13 投票系统

对于 WCG 的可扩展性而言最重要的就是可以增加新特征。新特征使得 WCG 更具有活力并且会吸引较大的用户群。同时也备受期待的是，添加的特征越多，就会产生越多的交易费 --- 就增加了锻造的积极性，因此也就增强了网络的安全性。为了达到这个目的，WCG 建立了一个投票系统，它可以让整个社区投票达成共识来确定哪个特性应该被实施以及什么样的顺序实施。但是投票系统本身并不是严格的技术创新，因为这是每个区域都可以实施的 --- 但是 WCG 已经将其植入系统了，希望能很快成为现实。

任何人都可以根据自己的需要发起投票。发起投票的人需要确定投票内容和投票期限(与区块数目相关联)。用户可以用它来解决所有的问题，比如选择新的图标。添加新的特征必须要通过 WCG 股东们的投票决定允许。股东们也能投票决定别名转移和 WCG 的更小单位。也可以投票决定毁灭（冻结）特定的钱币，特别是小偷或黑客们的钱币。甚至可以通过明主投票来决定停止恶意攻击的节点。更进一步说，社区可以通过投票来决定是否需要发起投票来考虑个别用户或节点。

投票是根据所持有的 WCG 的数量来进行计算的。拥有较大交易账户的用户在这个系统里有较大的投票能力。为了防止这种情况，网络需要有健康数目的交易账户供用户选选择。另外，随着去中心化交易的实施，用户们也可以选择避免中心化交易。有了去中心化交易系统，就不存在中心化交易投票能力的问题了。

WCG 的投票系统是去中心化货币的重要组成部分之一。这里没有领导者，没有集权的实体，所有的决定都取决于民主化投票。另外，除了能够解决全球问题，投票系统还能够被资产股东用于资产交易功能。它能帮助资产股东达成共识。

5.14 WCG 发行量

WCG 的主币华克金总发行量为 9 亿（900,000,000)，其中有 6 亿分布于多个重签名储存库， 将由华克金环球组织散播到各个黄金收藏者账户，实现可信赖的去中心化资产管理和交易。另外还有 3 亿华克金乃作为储存收益，符合条件的账户里必须至少拥有 100 华克金，该账户每 172，800 个区块（约 120 天）将可获得额外 3% 的收益。此设计除了吸引收藏者，同时保证了支持者的奖励，有效地控制了市场上的流通量，创造了长远价值的保障。比起其他的加密数字资产拥有巨大的优势!

第八章 . 结论

华克金 WCG 将会引起巨大的电子经济变革，它们将替代全球 GDP 很大的比例。WCG 也确实拥有所有的强势特征来巩固它成为数字化黄金投资第一位。基于比特币的投资和开发是对于区块链 1.0 阶段的投资，其投资回报也是巨大的。但随着许多创新区块链协议的诞生，比特币不再是一个一家独大的数字资产。而接下来的日子，创新协议和区块链应用的投资将会是接下来的投资主题。未来产生 10 倍甚至 100 倍回报的投资机会在于发现并正确投资有价值的数字资产。拥有实体黄金作为后盾的WCG 会是一个即将被唤醒的数字资产市场。

比特币照亮了这条道路，WCG 紧随其后将更加夺目。

WCG

WORLD CRYPTO GOLD

世 交 金