MomoCash 白皮书

一个专注隐私、分权和可扩展性的加密货币

Alemic su - alemic@momocash.org CTO
Landon Leakey - landon@momocash.org COO

摘要：这是一款以中本聪所开发的比特币为基础，改进并添加了诸如双层奖励制网络—也称为主节点网络，等多项新功能的加密数字货币,包括 POW 分权。其中还包含为提高可互换性的匿名支付（PrivateSend），和在不依赖中心权威下实现即时交易确认的即时支付功能（InstantSend）。

1. 介绍

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。

比特币提供匿名交易，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，MomoCash 是以保护隐私为要旨的加密数字货币。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的和具备良好匿名性的加密数字货币，它支持防篡改的即时交易，又有能为 MomoCash 网络提供服务奖励制的点对点次级网络。

2. 主节点网络

全节点是运行在 p2p 网络上的服务器，让小节点使用它们来接受来自全网的动态变化。这些全节点需要显著的流量和要消耗大量成本的其它资源，由此在一段时间内会观察到比特币网络上的这些节点数量呈现稳步下降的趋势,使区块广播的时间需要额外增加 40 秒。为解决这问题，提出了许多方案，例如引入微软研究的新奖励计划和 Bitnodes 激励计划。这些节点对网络的健康而言十分重要，它们能让客户端同步和通过全网快速广播信息。我们提议增加次级网络，名为 MomoCash 主节点网络。这些节点将具有高可用性，而且在为网络提供符合一定要求的服务后能够得到主节点服务奖励。

2.1 主节点奖励计划——成本和奖励

比特币网络全节点锐减的主要原因是缺乏对运行节点的奖励。随着时间的推移，全网接入的用户会更多，对带宽的需求会更高，对节点运行者的资金需求也更多，结果使运行全节点的成本提高。考虑到成本的上升，节点运行者必须要降低他们的运行成本或者运行轻客户端，但这样完全不利于网络健康。

正如比特币网络一样，主节点是全节点，但不同的是主节点必须对全网提供一定的服务，并需要一定量的押金才能加入。押金不会丢失，在主节点运行时也是安全的。这可让投资者为全网提供服务的同时，赚取一定的投资收益，减少了价格的波动性。

运行一个主节点，需要存储 1000MOC。当主节点生效时，它可为全网的客户端提供服务，并以利息的形式获取奖励。这就使得用户为这项服务投资，但同时得到一定的回报。主节点获取的收益是来自同一个矿池，大约有 45%的区块奖励纳入到这个计划中。

考虑到主节点奖励计划的奖励率是固定的百分比，还有主节点网络节点存在波动的事实，预计主节点奖励会根据当前生效的主节点总数作出变化。通过以下的计算公式可计算出运行主节点一整天的收益：

$$(n/t)* r*b*a$$

n: 运行者控制的主节点数

t: 主节点的总数

r: 当前的区块奖励（当前平均奖励是 5MOC）

b: 平均每天的区块数，当前 MOC 网络每天区块通常是 576 个

a: 主节点的平均奖励（平均每个区块奖励的 45%）

运行主节点的收益公式：

$$((n/t)*r * b*a*365) / 1000$$

（式子中的变量与上述相同）

运行主节点需要成本，这在网络上创建了生效节点的硬限制和软限制。目前有 10 万 MOC 流通，只有 30 个节点可能可以在网络上运行。软限制由配置节点所花的成本和平台的滞留量所致，因为 MOC 是流通的货币，而不仅仅是为投资所用。

2.2 确定顺序

使用特定的确定算法创建主节点的伪随机排序。使用为每个区块设计的工作量证明机制的哈希算法，挖矿网络可以提供支持这个排序的安全性。

选择主节点的代码：

```
For(mastenode in masternodes){
    n = masternode.CalculateScore();

    if(n > best_score){
        best_score = n;
        winning_node = masternode;
    }
}

CMasterNode::CalculateScore(){
    n1 = GetProofOfWorkHash(nBlockHeight); // get the hash of this block
    n2 = Hash(n1); //hash the POW hash to increase the entropy
    n3 = abs(n2 - masternode_vin);

    return n3;
}
```

示例代码还可以进一步扩展为主节点排序，“第二”，“第三”和“第四”个主节点的计算依此类推。

2.3 非信任制的 Quorum

当前 MOC 网络大约具有 30 个生效的主节点，而需要 1000 MOC 担保才可成为一个生效的主节点。我们创建了一个系统，其中没有一人能控制整个主节点网络。例如，如果有人想控制 50％的主节点网络，他们将不得不从公开市场上购买 3 万个 MOC。这将极大提高币价，所以获得如此多 MOC 是不可能的。

在拥有主节点网络和担保条件的前提下，我们以非信任制的方式使用该次级网络进行高度敏感的任务，其中没人能控制网络的演变结果。从总池中选择 N 个伪随机主节点来执行相同的任务，这些节点可以充当裁判，过程无需整个网络的参与。

例如，一个非信任制的 Quorum 发现 InstantSend，InstantSend 会使用 Quorum 确认交易和锁定输入。

另一个例子是，非信任制的 Quorum 可以利用主节点网络作为金融市场的去中心化预言者，这让实现去中心化的合同成为可能。例如苹果公司的股价在 2016 年 12 月 31 日超过 300 美元的话，就提交公约 A，否则提交公约 B。

2.4 角色和服务量证明机制

主节点可以向网络提供任意的额外服务。正如在概念中指出，我们的成功应用是 PrivateSend（匿名发送）和 InstantSend（即时支付）。使用我们称之为“服务量证明”的机制，可以要求这些节点处于在线状态，即使在正确的区块高度上也要作出响应。

恶意者也可以运行主节点，但不会对网络提供任何实质性的服务。为了减少这些人使用系统做出对自己节点有利事情的概率，必须 ping 剩余网络以确保它们保持活跃。这项工作通过主节点网络在每个区块选择 2 个 Quorum 来完成。Quorum A 检查 Quorum B 每个区块的服务。Quorum A 是与当前区块哈希最接近的节点，而 Quorum B 是远离所说区块哈希最远的节点。

主节点 A（1）检查主节点 B（2300） 主节点 A（2）检查主节点 B（2299） 主节点 A（3）检查主节点 B（2298）

检查网络就是要验证节点是生效的，这由主节点自身完成。全网区块的 1%会受到检查。这使整个网络在一天中会被检查大约 6 次。为了保持这个系统是非信任制的，我们使用 Quorum 系统中随机选择节点，但我们最少也需要六次检查来排查一个恶意节点。

为达到欺骗系统的目的，攻击者需要在一轮中被选中六次。否则，欺骗的目的就被系统发现，使其不会得逞，其它节点也是这样。

表 1 在服务性证明机制失衡的情况下，一个独立的主节点欺骗系统的概率

n:攻击者控制的主节点数 t:全网主节点总数 r:区块链深度 基于 Quorum 系统，主节点的选择是伪随机的。

Attacker Controlled Masternodes / Total Masternodes	Required Picked Times In A Row	Probability of success	MomoCash Required
1/2300	6	6.75e-21	1,000 MOC
10/2300	6	6.75e-15	10,000 MOC
100/2300	6	6.75e-09	100,000 MOC
500/2300	6	0.01055%	500,000 MOC
1000/2300	6	0.6755%	1,000,000 MOC

2.5 主节点协议

主节点使用一系列扩展协议在全网进行广播，包括主节点消息 announce 机制和主节点消息 ping 机制。这两类机制用来确认全网节点处于生效状态，除了它们，执行服务量证明机制需求的还有 PrivateSend 和 InstantSend。

在钱包中发送 1000MOC 到特定地址，就激活代码自然生成能在全网进行广播的主节点， 随之次级私钥生成，它是用来对其它所有信息进行签名，另外在运行单机模式时还可用来完全锁定钱包。

在两台独立的机器上使用次级私钥让冷模式成为可能。主要的“热”客户端对 1000 MOC 的输入进行签名，此过程包含使用二级私钥对信息进行签名。 之后，“冷”客户端能发现包含次级私钥的信息并将主节点激活。这让“热”客户端失效（客户端关闭），这样攻击者访问激活后的主节点也不可能获得窃取其中的 1000MOC。

主节点开始运行时，会向全网发送“主节点广播”信息，

包含有：

信息：（1000MOC 输入，可访问的 IP 地址，签名，签名时间，含有 1000MOC 的公钥，次级公钥，用于捐赠的公钥，捐赠的百分比）

此后每隔 15 分钟，一条 ping 信息会对外发送，证明节点生效中。

信息：（1000MOC 的输入，签名（使用次级私钥），签名时间）

随着时间的推移，网络会移除失效的节点，让该节点不再被客户端利用或再用于支付。节点也可以不停地 ping 网络，但如果它们的端口不打开，最终会被标记为失效状态，不再用于支付。

2.6 主节点列表的广播

进入 MOC 网络的新客户端必须发现当前全网活跃的主节点，这样才可以使用它们的服务。一旦它们加入网状网络，它们的节点就会收到请求主节点列表的指令。设置缓存的目的是让客户端记录主节点及其当前状态，因此当客户端重新启动时，他们只需简单加载该文件，不需重新请求主节点的完整列表。

2.7 使用挖矿进行支付和强制规定

为了确保每个主节点都获得应有的区块奖励，网络必须强制每个区块支付奖励给正确的主节点。如果矿工不愿意的话，他们的区块必须被网络拒绝，否则作弊就会产生。

我们提出一个策略，就是一个主节点代表一个 Quorum，选择其中优胜的主节点然后广播它们的信息。信息得到 N 次广播后，会选择同一目标接收者，这样达成共识后选中的区块要对该主节点支付奖励。

在网上挖矿时，矿池（矿池的作用是将单独的矿工整合起来）使用 RPC API 接口获取生成有关区块的信息。为了向主节点支付奖励，必须添加次级接收者到 GetBlockTemplate 来扩展接口。矿池之后广播自己的成功开采的区块，使自己和主节点之间保持同步。

3. 匿名支付

我们相信，为了能在客户端提高强度保护用户隐私，实现标准的非信任制是很重要的。例如 electrum，Android 和 iPhone 这些客户端，也会直接嵌入相同的匿名层和很好利用协议扩展性。这让用户使用坚实稳固的系统匿名发送资金时有着相同的体验。

PrivateSend 是 CoinJoin（提供匿名技术的软件）的改进和扩展版本。除了拥有 CoinJoin 的核心理念，我们还进行一系列的改进，例如去中心化、使用链接实现强匿名、相同面值和被动先进的混币技术。

在提高隐私和加密数字货币的可互换性时，最大的挑战是，无法做到加密整个区块链。在以比特币为基础的加密数字货币体系内，能看到哪些输出是没发送，哪些是已发送，通常将其称为 UTXO，全称是未使用交易输出。这让每个用户在公共帐本中都可充当诚实交易保证者的角色。比特币的协议是在不依赖第三方参与的前提下设计的，没有第三方的参与，仍能通过公共区块链随时读取用户信息实现审计是至关重要的。我们的目标是在不失去这些要素的前提下提高保密性和可互换性，我们坚信这是创建成功数字货币的关键。

使用数字货币范围内去中心化的混币服务，我们能让货币本身具备完全可互换的能力。可互换性是金钱的属性，决定货币的各单位要保持平等。当你以通货的形式接收资金时，资金不应该保留之前用户的使用记录，或者用户能很轻易地与之前的使用历史撇清开来，从而做到所有货币是平等的。与此同时，任何用户在不影响他人隐私的情况下，保证公共账本的每笔交易都是诚实的。

为了提高可互换性和保持公共区块链的诚实性，我们提议使用先进的非信任制去中心化混币技术，为了保持通货的可互换性，这项服务直接整合到这个货币体系中，对于每个用户而言都可容易和安全使用。

3.1 Coinjoin 通过账户可追踪资金流向

一个简单的策略是在现有的比特币基础上整合 Coinjoin，就是单纯将交易合并在一起。通过追踪联合交易的用户资金流向就会将用户的身份暴露出来。

图 2：例如将 2 个用户的交易整合为 Coinjoin 交易 [11][12]

在这项交易里，0.05 个比特币使用混币技术对外发送，为了追踪这笔资金的来源，仅需要把右边的数额加起来再和左边的数额匹配就可得知。

重新组合交易

0.05+0.0499+0.0001(fee) = 0.10BTC.

0.0499+0.05940182+0.0001(fee) = 0.10940182BTC.

随着更多用户加入到混币的过程中，获得结果的难度会以指数级增长。然而，在以后某个时间点结果还是可以被追踪出来，匿名性失效。

3.2 直接链接和中继链接

在 Coinjoin 其它实现的应用里，用户先把资金匿名化，最后把交易发送到知道发送者身份的平台或个体，这点是有可能实现的。但这打破了匿名性，能让其它人往前追踪用户的交易，我们称这类型的攻击为“中继链接”。

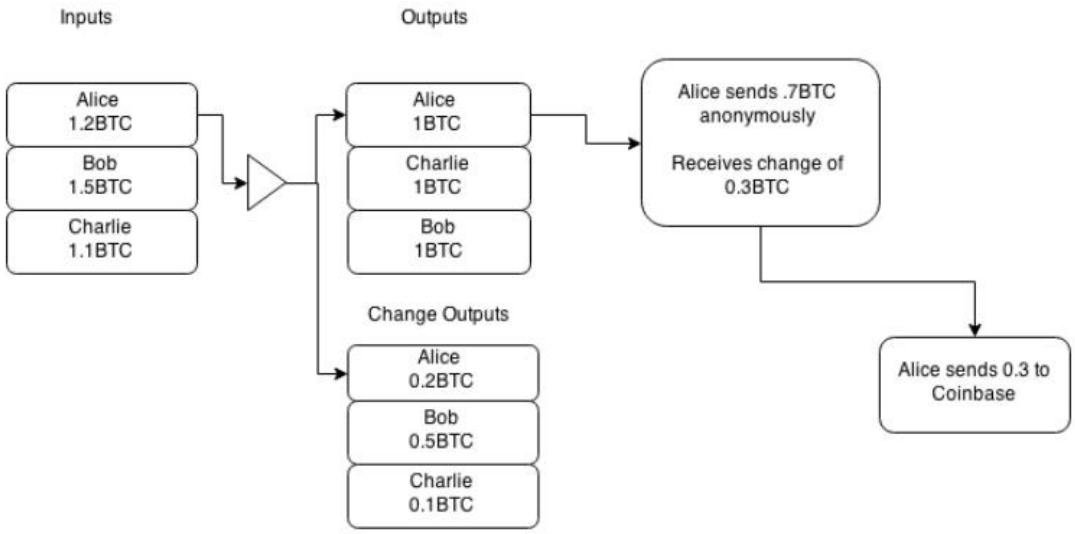

图 3： 中继转换链接

在这个例子中，Alice 匿名发送 1.2BTC，分别以 1BTC 和 0.2BTC 对外输出，然后从 1BTC 的输出中再对外输出 0.7BTC，剩余 0.3BTC，这 0.3BTC 输出发送到可识别对象去，但实质上 Alice 已经将 0.7BTC 成功匿名发送出去。

为了确定匿名交易的发送者身份，要从“交换交易”环节开始，通过区块链往前追溯，直至找到“Alice 匿名发送 0.7 个 BTC”。一旦找到的话，你会发现那是你的用户最近匿名购买了东西，从而看透这个匿名交易。我们称这种类型的攻击为“中介转换链接”。

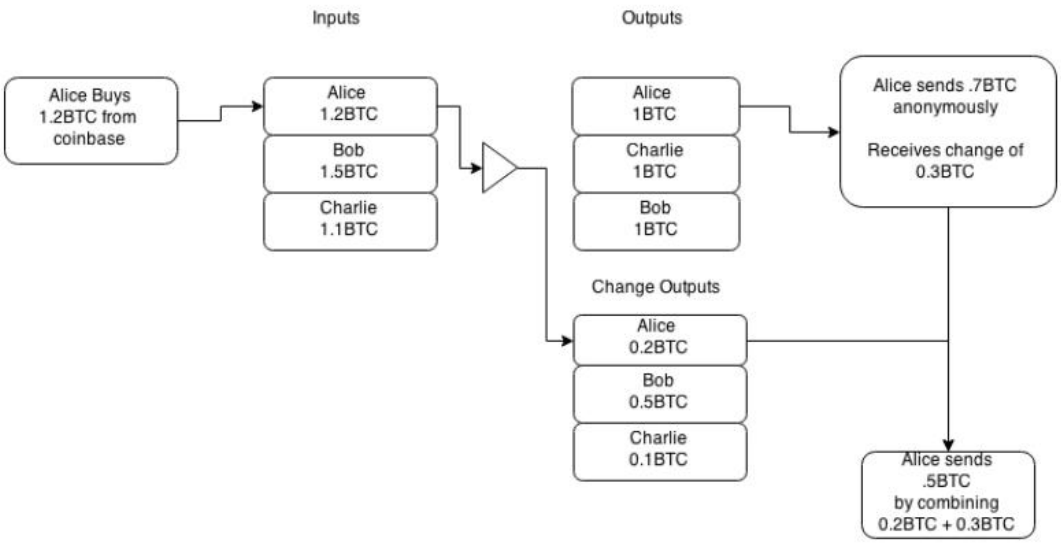

图 4：中介转换链接

在第二个例子中，Alice 在 coinbase 处花费了 1.2BTC，然后将这数额匿名化再以 1BTC 输出。接着，她又花费 1BTC，剩余 0.3BTC 再结合之前的 0.2BTC，组成为 0.5BTC 对外输出。

结合匿名交易和 CoinJoin 交易，将前后的整个交易历史整理一遍，从而可彻底看穿这个匿名功能。

3.3 增强的隐私和 DOS 防护

多方的交易可以合并为一个交易，PrivateSend 很好地利用了这点，它将多方的资金合并在一起对外发送，这样一旦整合后就无法再次拆分。考虑到 PrivateSend 交易是专门为用户支付设置的，这个系统是高度安全防盗窃，用户的货币是十分安全的。目前，使用 PrivateSend 的混币技术至少需要 3 方参与。三个用户的资金合并到一个共同交易，用户会以新的打乱过的形式对外输出资金。

为了从整体上增强系统的隐私性，我们提以使用 0.1MOC，1MOC，10MOC 和 100MOC 的相同面值。在每轮混币过程中，所有用户应该以相同面值的形式输入和输出资金。除了使用相同面值外，交易手续费会被移除，而且所有交易会分解成分散的、独立的、前后没有关联的小交易。

接下是应对可能的 DOS 攻击，我们提议所有用户在加入时把交易以押金的形式提交到矿池去，交易最后还是输出到用户，同时又可向矿工支付一笔高的报酬。也就是说，用户向混币池提高请求时，交易一开始就要提供押金。如果某个时候用户不合作了，例如拒绝签名，押金交易会自动在全网广播，若要在匿名网络上进行持续攻击，所付出的代价是极其高昂的。

3.4 被动的资金和区块链匿名

PrivateSend 每轮的混币限制为 1000MOC,并多轮混币才能匿名混合相当数量的资金。为了让用户体验方便和攻击变得困难，PrivateSend 以被动的模式运行。同时设定时间间隔，用户的客户端要通过主节点连接其它客户端。一旦进入主节点，用户要求需要匿名的面值数额会在全网依次排队广播，但是没有信息会将用户的身份暴露出来。

每轮的 PrivateSend 过程可视为增强用户资金匿名性的独立事件，然而每轮只限制 3 个参与者，因此观察者有三分之一的机会追踪交易，为了提高匿名的质量，会采用链接的方法，将资金通过多个主节点依次发送出去。

Depth Of The Chain	Possible Users
2	9
4	81
8	6561

表 2. N 轮混币中可能涉及的用户数

3.5 安全性考虑

由于交易合并在一起，主节点在用户资金流过时有可能进行“窥探”。由于每个主节点都被要求持有 1000 MOC 和用户选用随机主节点来部署他们的资金，所以“窥探”的影响性不大。通过区块链追踪交易的概率计算如下所示。

Attacker Controlled Masternodes / Total Masternodes	Depth Of The Chain	Probability of success	MOC Required
10/1010	2	9.80e-05	10,000MOC
10/1010	4	9.60e-09	10,000MOC
10/1010	8	9.51e-11	10,000MOC
100/1100	2	8.26e-03	100,000MOC
100/1100	4	6.83e-05	100,000MOC
100/1100	8	4.66e-09	100,000MOC
1000/2000	2	25%	1,000,000MOC
1000/2000	4	6.25%	1,000,000MOC

Attacker Controlled Masternodes / Total Masternodes	Depth Of The Chain	Probability of success	MOC Required
1000/2000	8	0.39%	1,000,000MOC
2000/3000	2	44.4%	2,000,000MOC
2000/3000	4	19.75%	2,000,000MOC
2000/3000	8	3.90%	2,000,000MOC

表 3.考虑到攻击者控制 N 个节点时，在全网追踪 PrivateSend 交易的概率

n: 攻击者控制总的节点数　t: 全网主节点总数　r: 区块链深度 主节点的选择是随机的

考虑到 MOC 的有限供应（此时此刻撰写白皮书时有 530 万个 MOC 在流通）和市场上低的流动性，在一次攻击中控制如此之多的主节点是不可能的。

通过遮掩主节点上发生的交易来扩展系统，也会大大提高系统的安全性。

3.6 使用中继系统遮掩主节点

在 3.4 一节，我们描述了使用 PrivateSend 多轮混币技术追踪单一交易的概率。这可以进一步通过遮掩主节点加以强化，使他们不能看到用户输入/输出方向。要做到这一点，我们提出一个简单的可让用户保护自己的身份的中继系统。

我们不让用户向矿池直接提交输入和输出的交易，而是让他们从全网随机选择主节点然后要求它将输入/输出/的签名中继传输到目标主节点。这意味着，主节点将接收 N 次的输入/输出和 N 组签名。每轮混币只为其中一个用户服务，但主节点无法知道究竟是哪个用户。

4. 使用 InstantSend 进行即时交易

使用主节点的 Quorum，用户能够发送和接收即时不可逆转交易。一旦 Quorum 形成，该交易的输入被锁定到对应的特定交易去，而目前全网交易锁定的时间是大约 4 秒。如果在主节点网络达成锁定的共识，所有与之冲突的交易和区块将被永远拒绝，除非它们能匹配当时锁定的交易对应 ID。

这将允许商家在现实商业中使用移动设备来替换传统 POS 机器，用户可像使用传统纸币一样快速进行面对面的非商业交易。这过程是没有中心权威的干预。此功能的广泛综述可以在 InstantSend 白皮书中找到。

5. 其他改进

5.1 Neoscrypt 算法

采用的挖矿算法是 Neoscrypt 算法。它是一款新的专为普通计算机硬件设计的内存密集型加密算法。 Neoscrypt 算法的主要作用是防矿机，它是一种主要基于 Salsa20 和 ChaCha20 算法,采用串联或并联运行模式。Neoscrypt 算法可以采用 CPU\GPU 挖矿,不仅支持 AMD 显卡,而且对 Nvidia 显卡也很友好。当 ASIC 突破此算法后，MomoCash 将采用改进升级 POW 算法。
跨链哈希运算的另一个好处是高端的 CPU 有着跟同级 GPU 接近的平均回报。GPU 消耗的功率已有 30-50%的下降，比大多数加密数字货币使用的 Scrypt 算法的功率少得多。

在密码学中，密钥导出函数（KDF）使用伪随机函数从秘密值（eg.主密钥）导出一个或多个密钥。KDF 可用于将密钥扩展到更长的密钥或获得所需格式的密钥(eg.将作为 Diffie-Hellman 密钥交换的结果的组元素转换为用于 AES 的对称密钥）。密钥加密哈希函数是用于密钥推导的伪随机函数的流行示例。密钥导出函数通常与非秘密参数一起使用，以从公共秘密值导出一个或多个密钥。这样的使用可以防止获得派生密钥的攻击者学习关于输入秘密值或任何其他导出密钥的有用信息；也可以使用 KDF 来确保派生密钥具有其他期望的属性，诸如在某些特定加密系统中避免“弱密钥”。KDFs 最常见的用途是将密码散列的方法来密码验证，我们将非秘密参数称之为 salt。KDFs 也通常用作多方密钥协商协议的组成部分，这些关键推导函数的示例包括 KDF1 和 ANSI X9.42 中的类似功能。特别的，基于 HMAC 的提取和扩展密钥导出功能（HKDF） 是一种简单的基于 HMAC 的 KDF，可用作各种协议和应用暴力攻击的难度随着迭代次数的增加而增加。迭代计数的实际限制是用户不愿容忍登录计算机或看到解密消息的可察觉延迟。使用 salt 可以防止攻击者预先计算派生密钥的字典。类似的，当下还有另一种方法叫做密钥强化（key strengthening），使用随机盐扩展键，但是不像密钥延伸一样可以安全地删除 salt。这将强制攻击者和合法用户对 salt 值执行强力搜索。

5.2 挖矿供应

MOC 采用另一种可降低挖矿引起的通胀的方法，就是每年的供应进行 7%的减产，这不同于其它数字货币的减半。另外，每个区块的供应量与全网的矿工数直接相关，更多矿工的参与意味着更少的挖矿奖励。

MOC 的开取计划会在本世纪持续，慢慢直至到下世纪中叶，最终在 2150 年左右挖矿才会停止。

6. 结论

本白皮书介绍各种旨在提高比特币协议的概念，这对于普通用户来说意味着，有更好的隐私性、可互换性、更少的价格波动和全网更快的信息广播。这一切都是

通过使用 two-tier 激励模型，而不是借用其它数字货币如比特币现有的 single-tier 模型来实现。使用这个可替代的网络设计让添加更多类型的服务成为可能，例如去中心化的混币技术、即时交易和使用主节点 quorum 的去中心化预言。

References

1. A peer-to-peer electronic cash system (2008)
2. http://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.pdf
3. https://www.cryptocoinsnews.com/3-solutions-instant-bitcoin-confirmations/
4. http://research.microsoft.com/pubs/156072/bitcoin.pdf
5. http://www0.cs.ucl.ac.uk/staff/s.meiklejohn/files/imc13.pdf
6. https://getaddr.bitnodes.io/nodes/incentive/
7. https://medium.com/zapchain-magazine/why-don-t-people-run-bitcoin-nodes-anymore-d4da0b45aae5
8. https://www.momocash.org/
9. https://explorer.momocash.org/
10. https://github.com/momopay/momo/blob/master/src/Masternode-pos.cpp
11. https://blockchain.info/tx/4eb3b2f9fe597d0aef6e43b58bbaa7b8fb727e645fa89f922952f3e57ee6d603
12. https://blockchain.info/tx/1694122b34c8543d01ad422ce600d59f8d8fde495ac9ddd894edc7139aed7617
13. http://en.wikipedia.org/wiki/NIST_hash_function_competition#Finalists
14. http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf