DashCash白皮书

全球数字现金完美解决方案

你的资金，你做主！
一秒之内即可完成支付，手续费不到一美分。
任何金额、任何时间、 任何地点。

全球下一代终极隐私保护点对点的数字现金系统

数字货币趋势

全50年前，如果有人告诉你，人类可以登上月球，你会相信吗？
10年前，如果有人告诉你，机器的智慧会比人类更上一层楼，你会相信么？
现在，如果有人告诉你，未来数字货币将成为全球主流的支付工具之一，你相信么？
2008年11月1日，中本聪发布比特币白皮书，标志着比特币的诞生。
2013 年 10 月，在加拿大启用了世界首台比特币自动提款机。
2017 年 12 月 18 日，全球最大的期货交易所——芝加哥商品交易所（CME）推出BTC交易。
2019年2月底，美国纳斯达克将比特币和以太坊指数加入全球数据服务。
2019年3月12日，谷歌、黑石、淡马锡、罗斯柴尔德家族已联合成立高达800亿美金的区块链数字货币投资公司。
2019年3月19日，世界500强公司AVNET公司宣布支持BTC支付。区块链技术将引领全球金融变革，全球将进入数字货币支付时代。
中本聪名言“如果你不相信，不明白，我也没有时间说服你”。
数字货币势不可当！

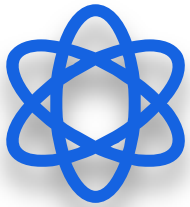
当前数字货币的模式

POW模式为代表的比特币，需要实体矿机参与，矿机耗费大量的电力资源。根据Digiconomist的比特币能耗指数，截至2017年11月20日，全球比特币挖矿的年耗电量约为29.05TWh。这意味着比特币挖矿现在使用的电量已经超过了159个国家的年度用电量。比特币通过竞争算力来获得区块奖励。矿机算力技术的升级，矿机不断贬值，由于利润巨减，恶性竞争的结果让没有优势的参与者只能被迫而承受巨大的经济损失。

POS将成为主流！

POS与POW区别

POS机制简单说就是一个根据你对区块网络提供服务量来给你区块奖励的体制。不同于比特币POW机制，使用矿机算力来解答数学难题获得区块奖励，POS机制是持币者对网络提供服务量来获得区块奖励。POS机制下获得区块奖励与持币者对网络服务贡献有关，没有电力消耗的高成本。并且POS机制下的网络转账更快、更便宜，所以成为了新的发展方向。



安全机制

另外，POS 币的挖矿和利息有很大不同，POS 挖矿的时候，我们的币是还在自己手里的。而我们在银行拿利息的时候，我们已经把钱出借给银行。POS模式比银行更安全！

POS大势所趋

从2018年起，包括ETH在内的很多数字币都开始从POW转向POS，主要是因为在POW机制下，在人类资源紧缺的当今时代，矿机挖矿耗费了全球大量的电力资源；矿工因消耗巨大算力从而抬高了手续费成本，不利于快捷流通；矿机算力恶性竞争，传统矿机不断淘汰，由于利润巨减，成本的抬高，很多大型矿场倒闭，这使得整个网络面临着瘫痪的威胁。诸于以上原因，POW转向POS将是大势所趋。

新一代数字货币诞生！

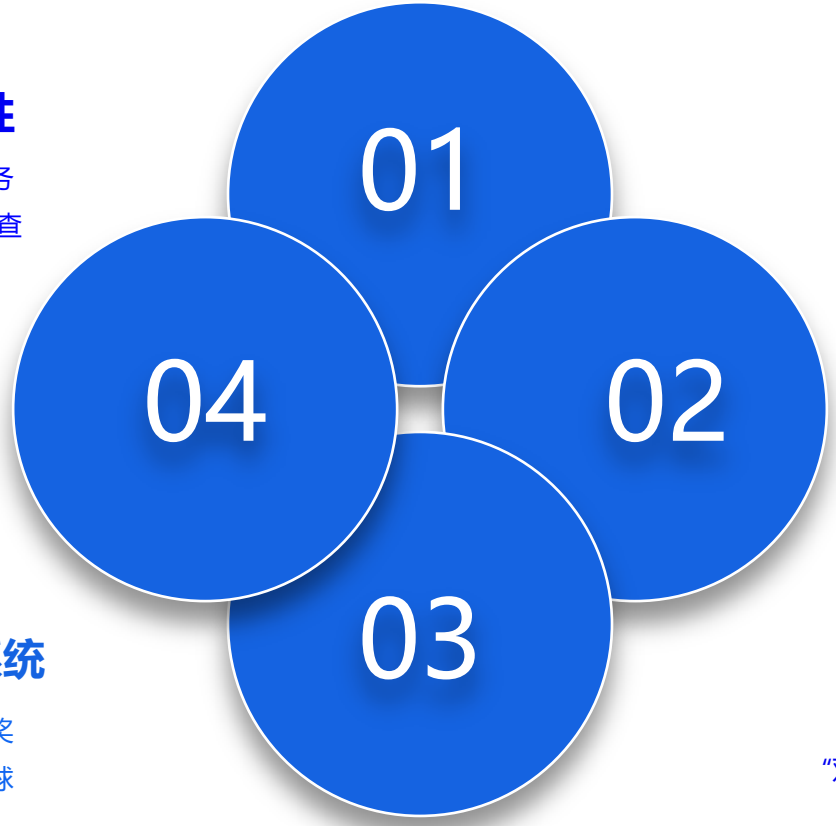
在全球资源紧缺的时代，随着科技的进步，为了提高区块链网络的效率，人们正在开发其他能源消耗更少的技术，如服务量证明和闪电网络。新一代计算机奖励机制POS模式应运而生，2018年5月DashCash团队开启了对POS模式更深入研发，对POS模式进行优化与升级，全球首家全新POS主节点全奖励机制的DashCash诞生！

DashCash全球下一代终极隐私保护点对点数字现金系统

DashCash比比特币的优势？

高匿名性

DashCash通过匿名发送技术，通过去中心化网络服务器“主节点”混淆交易的方式，使得交易无法被追踪查询，进而实现高匿名性。



即时发送

比特币网络需要花费10分钟甚至数个小时来确认交易，DashCash能够被即时发送。

主节点网络系统

通过此系统，根据DashCash对主节点的贡献来获得奖励。借助创新型POS奖励机制，DashCash可以向全球用户提供非信任制和去中心化服务。

网络更安全

DashCash全节点奖励机制从本源上避免了算力攻击与“双花”的产生，使的DashCash网络更安全。

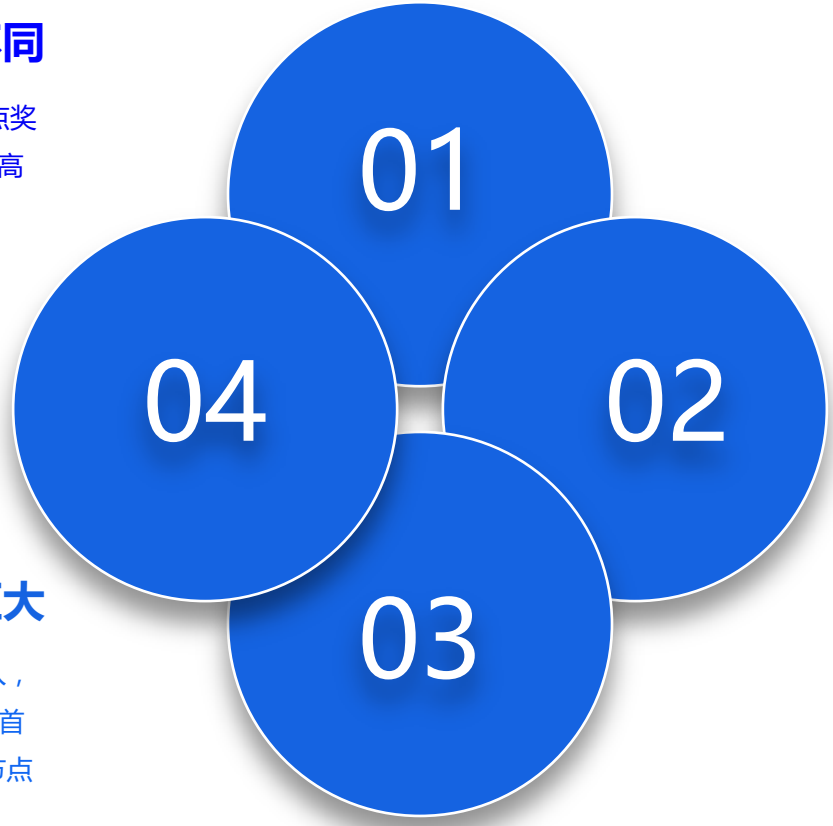
DashCash比Dash优势？

奖励比例不同

与Dash主节点45%奖励机制不同，DashCash主节点奖励达到100%。更多的主节点发展空间意味着更安全高效稳固的网络体系。

潜力更巨大

由于全节点奖励机制，全球会有越来越多主节点加入，从而使DashCash网络更稳固与去中心化，由于全球首创首个全节点POS奖励模式，低成本的主节点与全节点奖励机制，必然使主节点数量以倍数增长！



更安全

POW模式存在，始终无法从根本上避免51%算力攻击与“双花”攻击。DashCash全节点奖励机制从本源上避免了算力攻击与“双花”的产生，使的DashCash网络更安全，POS机制最核心的逻辑就是——谁持有全球过半主节点的数量（需拥有超过总量51%的硬币），谁就有网络的控制权。要攻击DashCash必须建立超过全球半数以上的主节点，这需要耗费大量资金获从市场买进51%以上的DashCash，由于DashCash总流通有限，DashCash被大量主节点拥有者持有，这使得攻击变的不可能，这就是POS奖励机制相对POW的先天性优势。就连以太坊网络创始人Vitalik Buterin都计划将以太坊由POW转向POS！

超级结算能力

当数以万计的全球主节点加入DashCash网络，DashCash的每秒处理能力将达到百万笔以上（而比特币系统每秒处理3-4笔交易，每笔交易需要10分钟甚至数小时），DashCash全球节点覆盖源自于独特的全节点奖励机制，DashCash将引领区块链3.0时代的到来！当拥有全球上万个主节点网络时， DashCash网络每秒处理结算能力将达到百万笔，将更适合于全球商用，甚至可媲美任何支付系统。

DashCash概述

DashCash（达世现金）是一种具有高度隐私的去中心化加密货币，具有开源代码，允许每个人参与DashCash主节点网络建设。 DashCash英文简写：DSC，总量恒定：3.68亿，每年产量递减8%，预计下世纪末即2180年左右产完，每分钟出一个快；出1个块即完成转账确认；转账速度：1秒；建立主节点需存币：10000个；主节点POS区块奖励：100%。

安全网络

DashCash主节点网络建设，使用达世现金能够有效保护隐私和账户安全。

方便快捷

DashCash网络为全球用户提供即时私人交易，不可追踪以及无需额外费用。

匿名支付与高度隐私保护

DashCash以中本聪所开发的比特币为基础，改进并添加了诸如POS奖励制网络---也称为主节点网络等多项新功能的去中心化点对点的加密数字货币。还包含为提高可互换性的匿名支付（Darksend），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（InstantX）。

DashCash理念

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，DashCash（达世现金）是全球领先的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，又有能为达世现金网络提供服务奖励制的点对点网络。

主节点网络

全节点是运行在 p2p 网络上的服务器，让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。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。

如何建立主节点？

您需要存入钱包10000个DashCash（不锁定，随时可支出变现），一年花费几十美金购买一台服务器，通过几步简单操作，运行起DashCash节点服务器就可以获得主节点奖励，主节点类似于比特币矿机，不同的只是奖励机制，当然您可以随时将存入的资金支出变现，也可以保留继续升值，当您支出变现，主节点将停止运行而关联的区块奖励也将停止支付。

建立主节点方式如下：
选择 1：托管主节点
运行个人服务器要求用户对区块链及操作系统有一定的了解。考虑到不是每位用户都具备这样的知识积累，一些社区成员面向用户提供了有偿的托管服务。换言之，借助托管服务的用户只需存入主节点保证金并缴纳托管服务费就能获取区块奖励了。如需了解主节点托管设置的相关知识，请咨询提供相关托管服务的社区成员。
选择 2：自行运营主节点
对达世现金托管服务网络的运行原理有着深入了解（或好奇）的用户可以在个人托管服务器上自行运营主节点。这要求用户采取多个步骤，并承担架设、安全防护和维护服务器及保证金的责任。如需了解创建自行运营的主节点的相关知识，请参考官网主节点创建在线教程。

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10000DashCash。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100%的区块奖励纳入到这个计划中。
考虑到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: 当前的每个区块奖励（当前奖励是21 DashCash，出块数量逐年递减8%），b: 平均每天的区块数，当前DashCash网络每天区块通常是1440个，a: 主节点的奖励（每个区块奖励的100%）。运行主节点的收益公式：((n/t) * r * b * a * 365) / 10000（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。软限制由配置节点所花的成本和平台的滞留量所致，因为DashCash是流通的货币，而不仅仅是为投资所用。
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服务量证明机制的哈希算法，主节点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。

主节点服务量证明机制

非信任制的Quorum：
当前DashCash主节点网络需要10000 DashCash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总量50%的DashCash。这将极大提高币价，所以获得如此多DashCash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InstantX，InstantX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。

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，我们的首个成功应用是 Darksend（匿名发送）和 InstantX（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。

攻击者控制的主节点数 / 总的主节点数	一轮检查次数	成功率 $(n/t)^r$	需要的DashCash
1/2300	6	6.75e-21	1,0000
1000/2300	6	6.75e-15	1,000,0000
10/2300	6	6.75e-09	10,0000
100/2300	6	0.01055%	100,0000
500/2300	6	0.6755%	500,0000

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。

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Darksend和InstantX。

在钱包中发送10000DashCash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10000 DashCash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10000DashCash。

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：（10000DashCash输入，可访问的IP地址，签名，签名时间，含有10000DashCash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：（10000DashCash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。

主节点列表的广播
进入DashCash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。

使用区块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，网络强制每个区块支付奖励给正确的主节点。
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。

隐私保护

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。
Darksend 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。

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：例如将2个用户的交易整合为Coinjoin交易

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。

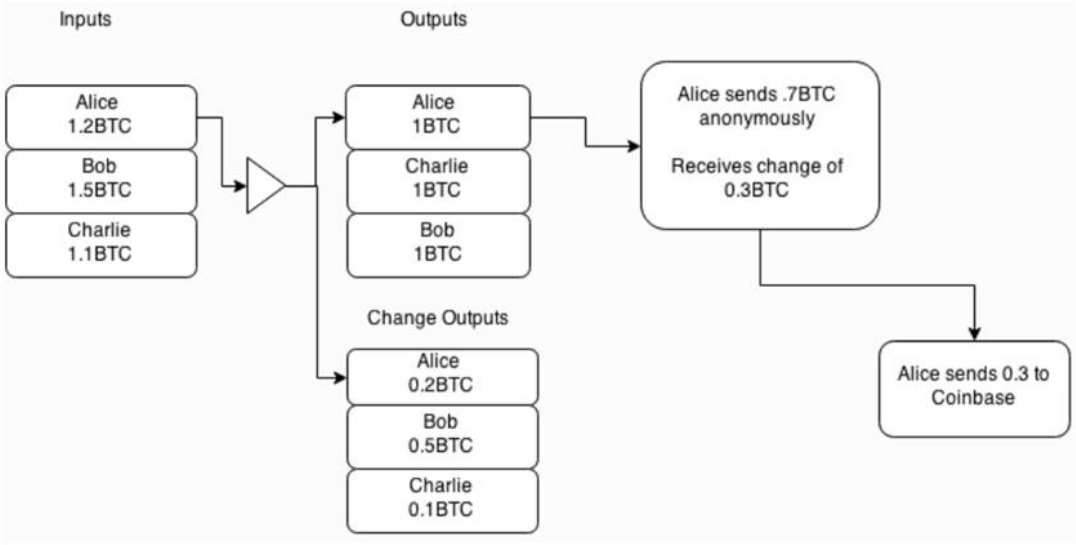
重新组合交易

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。

匿名支付

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： 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”。

安全性

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10000 DashCash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。

攻击者控制的主节点数 / 总的主节点数	一轮检查次数	成功率 $(n/t)^r$	需要的DashCash
10/1010	2	9.80e-05	10,0000
10/1010	4	9.60e-09	10,0000
10/1010	8	9.51e-11	10,0000
100/1100	2	8.26e-03	100,0000
100/1100	4	6.83e-05	100,0000
100/1100	8	4.66e-09	100,0000
1000/2000	2	25%	1,000,0000
1000/2000	4	6.25%	1,000,0000
1000/2000	8	0.39%	1,000,0000
2000/3000	2	44.4%	2,000,0000
2000/3000	4	19.75%	2,000,0000
2000/3000	8	3.90%	2,000,0000

表.考虑到攻击者控制N个节点时，在全网追踪Darksend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DashCash的有限供应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。

相关改进

使用中继系统遮掩主节点

在上面我们描述了使用Darksend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。

使用InstantX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。

区块奖励数量供应

DashCash采用另一种可降低区块奖励数量引起的通胀的方法，就是每年的供应进行8%的减产。DashCash的开取计划会在本世纪持续，慢慢直至到下世纪末，最终在2180年左右区块奖励才会停止。

混币技术

为了从整体上增强系统的隐私性，我们提以使用0.1DashCash，1DashCash，10DashCash和100DashCash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。

被动的资金和区块链匿名

Darksend每轮的混币限制为10000DashCash,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，Darksend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Darksend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。

区块链的深度	可能的用户数 (n)r
2	9
4	81
8	6561

表. N轮混币中可能涉及的用户数

全球新一代完美去中心化数字现金系统

匿名支付

匿名支付、混币技术，实现超级隐私保护。

即时发送

全球任何地方，任何个人，即时发送，一秒完成支付，像信用卡一样方便快捷！

稀缺增值

总量恒定，每年产量递减8%，极具稀缺与保值、增值！

商用价值

独有的主节点全奖励机制，当全球主节点达到上万个的时候，每秒可处理百万笔以上结算！

下一代全球数字现金系统

DashCash

全球数字现金完美解决方案！
技术改变未来，让支付变得更简单！

DashCash，你的资金,你做主!
一秒之内即可完成支付, 手续费不到一美分；
任何金额, 任何时间, 任何地点.

总论

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主节点激励模型，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。

THANK YOU

DashCash下一代全球领先的数字现金系统