Hcash

HyperCash 中文白皮书

Hcash 重塑价值

版本：0.8

2017 年 6 月 8 日

目 录

摘 要

Hcash, the cryptocurrency of distributed ledger in both blockchain and blockless based(directed acyclic graph) systems.

以比特币[1]为代表的基于 UTXO 的区块链和以以太坊[2]为代表的基于账户的区块链向我们打开了新世界的大门。比特币和以太坊的成功，证明了区块链技术的价值和未来的巨大潜力，同时在这个过程中我们也看到了区块链技术在一些方面存在的先天不足。从 2015 年开始，一些非常有潜力的但是并不基于区块的分布式账本系统底层技术也逐渐走入我们的视野，如 DAG（Directed Acyclic Graph）有向无环图[3]。毋庸置疑，未来是去中心化的数字世界，比特币或者以太币或许会成为区块链分布式账簿的基础货币，而基于 DAG 技术基础的货币或许会是 IOTA[4]或 Byteball[5]以及其它新兴数字货币。然而无论如何，这几种基于完全不同系统的货币目前除了在中心化的交易所上进行兑换之外，并不能在这两种完全不同体系的分布式系统中自由流通。

我们将创建一个新的分布式去中心化账本系统，连通基于区块的分布式账本和不基于区块的分布式去中心化账本系统，让所有这些去中心化的分布式账本之间的信息与价值自由流通，而 Hcash 则充当了不同系统之间价值流通的载体，我们称之为：超级现金。

一、系统特性

在我们的设想中，Hcash 将建立一个新的底层技术平台用以链接各种不同的区块链技术，从而让基于信任的价值在不同的区块链系统中自由流通。

Blockless Based Blockchian　　*Block Based Blockchain*

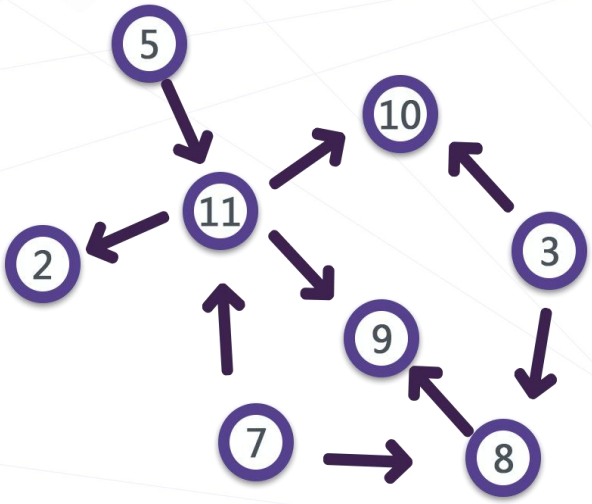
1.1. Hive composed of blockchain and DAG systems

Hcash 是区块链和 DAG 系统的双重侧链。实现基于区块链和基于非区块的分布式系统信息与价值的互联互通。其中 Hcash 是跨平台价值互通的媒介，而 Hcash 平台本身是跨平台信息交换的载体。

基于 Hcash 系统的设计特点，Hcash 在系统初始设计阶段已经考虑到了对基于区块链的系统（包含基于 UTXO 和 Account Based）和 DAG 为基础的分布式账簿信息的读取。

与此同时，Hcash 的货币体系设计也兼容 Zcash 的透明地址与暗地址以及 Byteball 的 Whiteball 与 Blackball 的地址体系。因此，在不久的将来，可以基于 Hcash 实现区块链与 DAG 系统之间直接发送或接受明(White)暗(Black)代币。同时，也能够在 Hcash 客户端之间实现基于零知识证明的完全加密通信。以及其他一系列激动人心的特性。

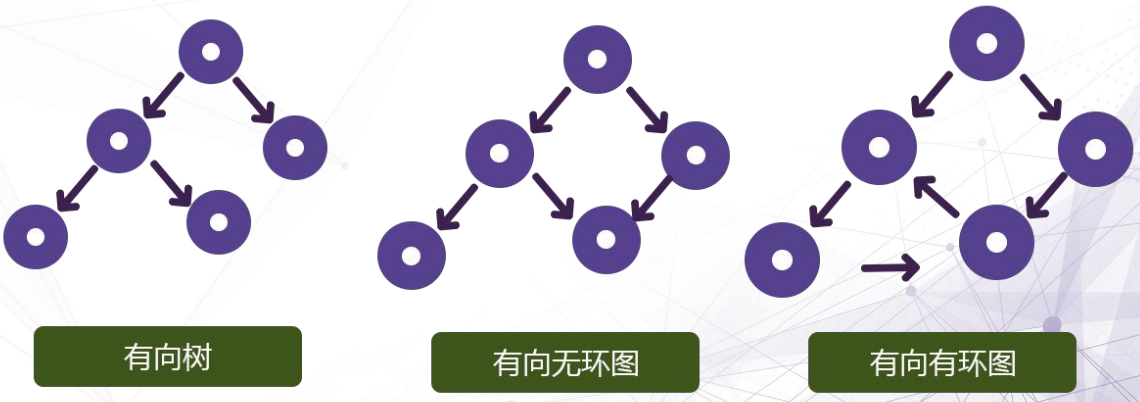
关于有向无环图



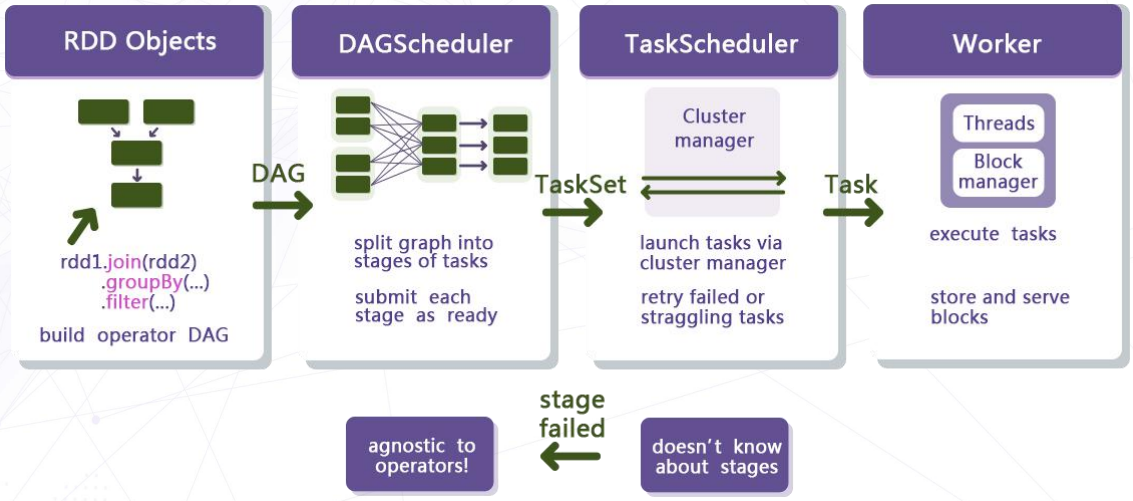
在图论中，如果一个有向图从任意顶点出发无法经过若干条边回到该点，则这个图是一个有向无环图（DAG 图）。

因为有向图中一个点经过两种路线到达另一个点未必形成环，因此有向无环图未必能转化成树，但任何有向树均为有向无环图。

DAG 图是一类较有向树更一般的特殊有向图，下图给出了有向树、DAG 图和有向图的简单示例。在大数据领域中，DAG 通常用于大数据框架比如 Hadoop、Storm、Spark 的执行引擎。

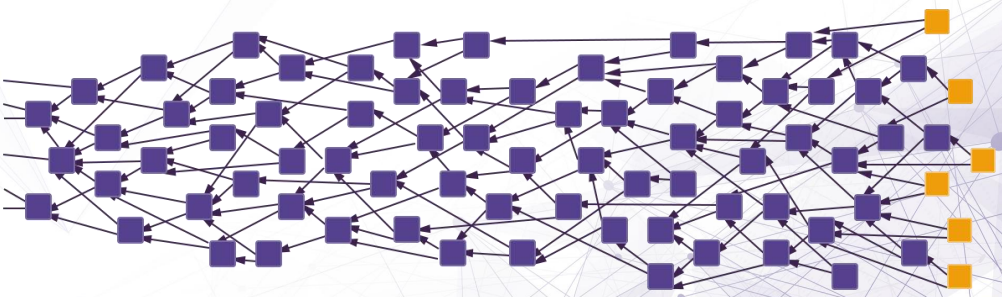


在大数据领域中，DAG 通常用于大数据框架比如 Hadoop、Storm、Spark 的执行引擎。下图为 Spark 的运行架构：

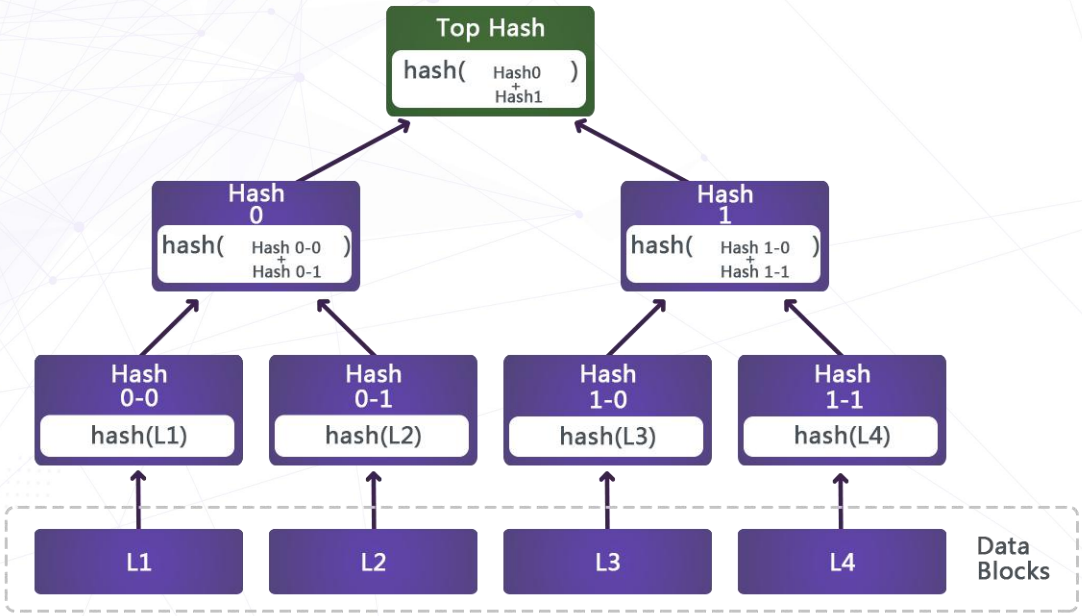


各个 RDD 之间存在着依赖关系，这些依赖关系形成有向无环图 DAG。DAGScheduler 对这些依赖关系形成的 DAG，进行 Stage 划分，划分的规则很简单，从后往前回溯，遇到窄依赖加入本 Stage，遇见宽依赖进行 Stage 切分。完成了 Stage 的划分。DAGScheduler 基于每个 Stage 生成 TaskSet，并将 TaskSet 提交给 TaskScheduler。TaskScheduler 负责具体的 task 调度，在 Worker 节点上启动 task。

最近，随着区块链技术的发展，也有部分新兴后区块链系统底层框架的数据结构采用了 DAG 来实现，比如 IOTA[4]，其核心数据结构就是名为缠结的 DAG 图，解决了物联网领域海量大数据存储及分布式计算的问题。



传统的区块链比如比特币、以太坊还是采用基于诸如默克尔树这样的二叉树数据结构：



Hcash 试图建立两个完全不同底层数据结构系统之间的通道，从而在底层技术层面兼容主流的区块链技术标准。这种挑战无疑是非常大的。Hcash 的技术团队由深耕大数据、云计算以及密码学和区块链领域多年的技术专家组成。我们有信心能够克服各种障碍，实现系统的设计目标。

1.2.Hybrid. PoW+PoS

数字货币社区的协同一直是一个难以解决的问题，众所周知的比特币协议升级斗争在过去两三年的时间内一直影响着社区的发展。而类似于 Zcash 的过分中心化的数字货币则排除了社区其他成员的参与权。

Hcash 参考了 Decred 和 Dash 的部分理念，提出了 Instant-Open-Governance（即时开放治理系统），所有持币者可以通过 PoS 挖矿机制参与社区的重大决定，包括协议的更新和升级。更为先进的是，Hcash 提供了一个平滑的执行方式，一旦投票通过，所有的决定将会被记录在区块链上且强制执行，这样就避免了矿工、矿池、交易所、钱包服务商的协同难题。PoW[6]机制的存在是为了防止早期投资者在 PoS[7]分发机制中所占的收益比重过高，同时 PoW 是目前已经被证明最能够有效地保障基于区块链的系统安全机制。虽然它不可避免的要消耗一部分能源，但是，从有效地保障系统安全的角度考虑，我们认为是值得的。并且，PoW 和 PoS 的挖矿过程是有机结合起来的，二者共同保证了系统的安全性。

首先以一种传统的 PoW 方式开始挖矿，矿工相互竞争来解决密码谜团。根据这种实施，挖出的区块不包含任何的交易（它们更像模板），所以赢得的区块将会仅仅包括一个 header 和该矿工的奖励地址。这时候，系统将会切换到 PoS。基于这个 header 的信息，一组随机的 validators 被挑选出来对这个新的区块进行签名。手中持有币越多的 validator 被选中的概率就越高。一旦这些被选中的 validator 全部完成对该区块的签名，该模板就成为了一个完整的区块。如果一些被选中的 validator 不可用于对该区块进行签名，那么将会被选中对下一个区块进行签名，然后再选出新一组的 validators 等等，直到该区块获得正确数量的签名。手续费将会被分配给矿工和参与该区块签名的 validator。

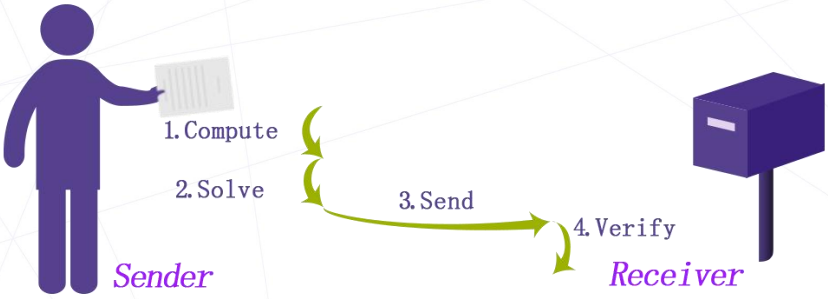
对于 PoW[6]，合格的区块可以表述为：

F(Nonce) < Target

其中 Nonce 是随机元素，Target 是合格区块的量化，每个记账节点的 Target 一致。此外 PoW 的成功运行还需要配合如下两条约定，

1、Best chain 原则：将最长的链条视为正确的链条。

2、激励原则：找到合格的区块有奖励收益。



第 1 条约定为硬性规则必须遵守，共同的目标是找到一致性账本，而最长的链条代表最大的工作量，如果没有这条约定，每个人都只会构造自己的区块链，无法达成一致。第 2 条为工作量激励，既然记账有成本，那唯有收益才能驱动大家都去记账，参与记账构造区块变成投资行为，其成本和收益风险在第 1 条约束下形成博弈，驱动所有节点按约定规则诚实地构造区块，最终达到纳什均衡。

对于 PoS[7]，合格区块可以表述为：

F(Timestamp) < Target * Balance

上面的 PoS 方式是目前 nxt[8][9]与 Blackcoin[10]所采取的 PoS 机制。最简化版本的 PoS 机制很容易引起财富中心化问题，同时对整个系统安全构成重大影响。

因此我们必须在考虑 Stake(Balance) 的同时，加入另一个变量来尽量避免由于单纯的参考 Balnace 所造成的中心化以及安全问题。与 PoW 相比，公式左边的搜索空间由 Nonce 变为 Timestamp，Nonce 值域是无限的，而 Timestamp 极其有限，一个合格区块的区块时间必须在前一个区块时间的规定范围之内，时间太早或者太超前的区块都不会被其他节点接纳。公式右边的目标值引入一个乘积因子余额，可见余额越大，整体目标值（Target * Balance）越大，越容易找到一个区块。因为 Timestamp 有限，PoS 铸造区块成功率主要与 Balance(Stake)有关。Hcash 的 PoS 机制将借鉴现有的 PoS 机制，在保障系统安全性的前提下，提高 PoS 的效率，着重提高用户在使用 PoS 机制时数字货币的安全性。

1.3.Hierarchy DAO Governance

去中心化自治组织（DAO）是密码学技术革命的最理想的产物。DAO 的源头可以追溯到 Ori Brafman 在《海星和蜘蛛》（2007 年）[12]中描述的组织的去中心化，和 Yochai Benkler 在《网络财富》（2006 年）[13]描述的“对等生产”（peer production）。但是这两个概念被与密码学货币相关的技术所连接起来，Dan Larimer 提出了 DAC 的概念，他将比特币看作一个 DAC。

关于 **DAC**

为了对 DAC 有一个明晰的定义，我们总结了 DAC 所必需的七点特征：

- 公开性，DAC 系统的设计公开透明，公开透明性是整个 DAC 系统的基石，一个暗箱操作的组织不能作为 DAC，现在的软件开源精神成为公开性的一个典型范例;
- 去中心化性，没有中心化个人和组织能控制整个 DAC，这条特性决定了自相似性，去中心化特性保证了 DAC 系统的生命力;
- 自治性，DAC 系统人人可以参与，参与者都是 DAC 系统的子公司或者子单元，并从自身角度促进 DAC 的发展。参与者的自发行为保障了 DAC 的运行;
- 价值性，DAC 系统必须是具有使用价值的，比如比特币系统的国际支付网络、匿名交易、避税、价值储存、不可冻结、不可监管的特性，这条特性决定了比特币 DAC 系统的盈利性;
- 盈利性，DAC 的参与者会获得 DAC 系统发展的奖励，盈利性由 DAC 本身的价值性确定;
- 自相似性，即使在只有部分 DAC 节点的情况下，DAC 系统仍能正常运作并发展，部分单元节点的摧毁不会影响 DAC 的发展，由去中心化性保证;
- 民主性，DAC 系统核心协议的改变需要绝大多数单元的投票才能完成，去中心化特性和自治性决定了 DAC 必须是一个能够民主投票的系统。

Vitalik 将 DAC 概念进行扩展，提出了更为普遍的 DAO 概念（分布式自治组织），不受监管的众筹和服务拆分是 DAO 的构成要素，还有密码学技术管理层和基于信任的自动化，这使得 DAO 能够运行起来，正如 Stan Larimer 所说“在一组商业规则的控制下，不需要人类的参与”。然而这种理想状态下的自治组织，如果在系统设计阶段不进行严格的把控，也会造成非常严重的后果[11]。2016 年 6 月，史上最大的以太坊众筹项目 The DAO，这个众筹超过 1.5 亿美元的分布式自治组织，因为代码漏洞，遭受黑客攻击，在当时损失超过 360 万以太币，当时的价值超过 6000 万美元。并引发 ETH 社区分裂，造成现有的 ETC 与 ETH 双链共存局面。

在 Hcash 的系统内，有 5%的代币会发送到一个 DAO，由 Hcash 的全体持有者通过即时动态投票来决定资金的用途，例如，开发钱包等基础设施建设，或者进行公开推广等商务公关活动，DAO 的形态为 Hcash 社区提供了源源不断的活力与积极向前发展的动力，同时，Hcash DAO 的代码会进过严格的审核并在初期加入必要的人工干预（由基金会邀请第三方进行代码安全审核）。以保障 DAO 在早期的资金运用过程中不出现重大失误。

1.4. Hidden Zero Knowledge Proof

零知识证明 （被称为“zk-SNARK”）是实现 Zcash 的匿名特性的核心技术。“零知识证明”的定义是：证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

考虑到 Hcash 的海量数据交互量，我们采用一种安全性是基于计算离散对数的困难性的鉴别方案，可以做预计算来降低实时计算量，所需传送的数据量亦减少许多。为了产生密钥对，首先选定系统的参数：素数 p 及素数 q，q 是 $p-1$ 的素数因子。$p \approx 2^{1024}$，$q > 2160$，元素 g 为 q 阶元素，$1 \leqslant g \leqslant p-1$。令 a 为 GF(p)的生成元，则得到 $g = a(p-1)/q \bmod q$。由可信赖的第三方 T 向各用户分发系统参数(p, q, g)和验证函数（即 T 的公钥），用此验证 T 对消息的签字。

对每个用户给定惟一身份 I，用户 A 选定秘密密钥 s，$0 \leqslant s \leqslant q-1$，并计算 v = g−s mod p；A 将 IA 和 v 可靠地送给 T，并从 T 获得证书，CA = (IA, v, ST (IA, v))。

协议如下：

（1）选定随机数 r，$1 \leqslant r \leqslant q-1$，计算 x = g r mod p，这是预处理步骤，可在 B 出现之前完成；

（2）A 将(CA, x)送给 B；

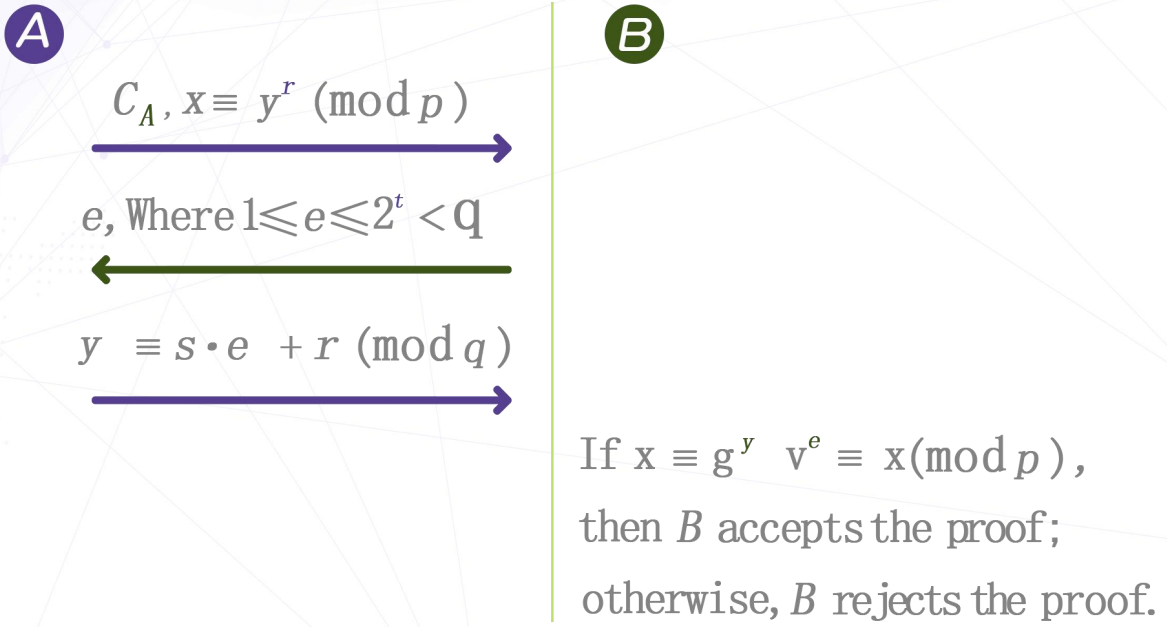
（3）B 以 T 的公钥解 ST (IA, v)，实现对 A 的身份 IA 和公钥 v 认证，并传送一个介于 0 到 2 t − 1 之间的随机数 e 给 A；

（4）A 验证 $1 \leqslant e \leqslant 2$ t，计算 y = (s e + r) mod q，并将 y 送给 B；

（5）B 验证 $x = g^{y} v^{e} \bmod p$，若该等式成立，则认可 A 的身份合法。

安全性基于参数 t，t 要选得足够大以使正确猜对 e 的概率 2^{-t} 足够小。建议 t 为 72 位，p 大约为 512 位，q 为 140 位。

此协议是一种对 s 的零知识证明，在认证过程中没有暴露有关 s 的任何有用信息。



Hcash 将会借鉴 Zcash 的零知识证明技术，不单单在资产转移的过程中可以实现双向加密，还可以应用到很多其他对交易隐私要求极高的领域。Hcash 在客户端集成了即时通信功能，它不但能够利用暗地址实现代币的跨平台转移，也可以在日常的点对点（P2P）通信中利用零知识证明的机制实现高度的隐私通信，更能够跨越平台实现诸如从 Hcash 客户端到 Byteball 客户端的加密通讯。

1.5. Hard. Quantum Resistance

在当前以比特币为代表的区块链系统中，SHA-256 哈希计算和 ECDSA 椭圆曲线密码构成了比特币系统最基础的安全保障，但随着量子计算机技术不断取得突破，特别是以肖氏算法为典型代表的量子算法的提出，相关运算操作在理论上可以实现从指数级别向多项式级别的转变，这些对于经典计算机来说足够“困难”的问题必将在可预期的将来被实用型量子计算机破解。

后量子密码（post-quantumcryptography），又被称为抗量子计算密码（quantum-resistantcryptography），是被认为能够抵抗量子计算机攻击的密码体制。此类加密技术的开发采取传统方式，即基于特定数学领域的困难问题，通过研究开发算法使其在网络通信中得到应用，从而实现保护数据安全的目的。后量子密码的应用不依赖于任何量子理论现象，但其计算安全性据信可以抵御当前已知任何形式的量子攻击。1997 年，IBM 的研究人员提出一种加密方案名为 Learning With Errors（LWE），意即伴随误差学习，由于要找到最近的通用格要很长时间，因而可以抵抗来自量子计算机的攻击。

基于 Ring－LWE 的公钥加密方案

相关参数选择及运算规则

方案中主要参数有 n，p，q。

n: 确定加密方案中多项式的最大次数。在保证计算效率和安全性的标准下，n 值越大越好，应该是 2k。

q: 大模数， 通常是一个正整数，q 值的大小与具体实例相关。q 值应该足够大， 这样才可以保证足够高的安全性，但是 q 值越大占用的系统资源就会越多，并会增加整数计算量。

p: 小模数，通常是一个小的正整数。

令 R = Z

q [x] /(xn + 1)，对于环中的两个多项式 f 和 g，表示为如下形式 f(x) = f0 + f1(x) +... + fn－1xn－1，g(x) = g0 + g1(x) + ... + fn－1xn－1，k ∈ R， 定义如下运算: k · f(x) = kf0 + kf1x+ ...kfn－1xn－1

$$f(x) \cdot g(x) = \sum_{k=0}^{n-1} \left(\sum_{i+j=k(modn)} f_i g_j \right) x^k$$

密钥生成

在该方案中加密公钥是 h(x)， 解密私钥是 f(x) 和 fp(x)，选取方法如下

选定多项式 f(x)，g(x)，满足

f(x) ·g(x) =0modq。

f(x) ·fq(x) = 1modq。

h(x) = fq(x) + 1。

公钥为（h(x)，g(x)）， 私钥为（f(x)，fp(x)）。

加密过程

该方案中加密时引入随机差错多项式 e(x)∈ Ψα，Ψα 是参数为 α 的某一高斯分布， 将明文转换为多项式 m(x) ，计算密文为: c(x) = h(x)·m(x) + g(x) ·e(x) 。

解密过程

接收到的密文是 c(x) ， 使用私钥 f(x) 和 fp(x) 对密文进行解密的步骤如下:

α(x) = f(x) ·c(x)= f(x) ·h(x) ·m(x) + f(x) ·g(x)·e(x)= [f(x) ·fq(x) + f(x)] ·m(x) +f(x) ·g(x) ·e(x) modq (1)= f(x) ·m(x)

fp(x) ·a(x) = fp(x) ·f(x) ·m(x) modp= m(x) (2)

其中在第(1) 步和第(2) 步的解密过程中有

可能出现解密失败，即当第(1) 步的系数不在区间（ － q2 ，q 2）内或者第(2) 步的系数在不在区间（ － p2 ，p 2）之间时便会出现解密失败现象，但是只要选取合适的参数，解密失败的可能性还是非常小的， 还可以采用像 NTRU 类似的避免解密失败的方法以减少解密失败的概率。

Hcash 将会开发可与 OpenSSL 一同工作的 Ring-LWE 密钥交换协议，实现后量子时代区块链的安全问题。

1.6. Handy. Limited Blockchain with Unlimited Transaction

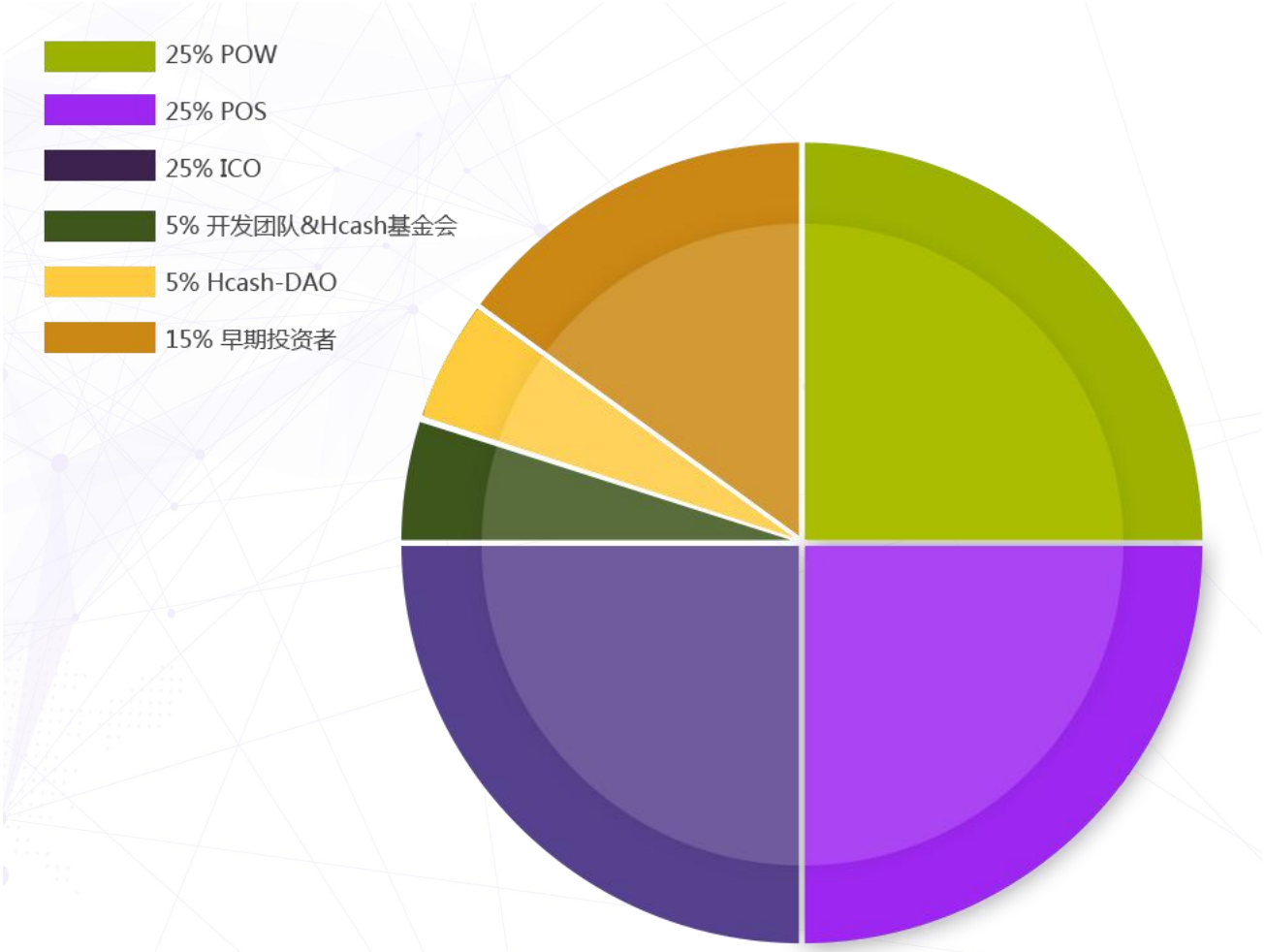
DAG 技术本身并不基于区块，因此不会受区块确认时间限制（例如比特币的区块确认时间是 10 分钟而以太坊的确认时间大约在 15 秒）。Hcash 在系统设计时由于需要考虑与基于 DAG 技术的区块链系统的交互，因此会借鉴 DAG 的特性与优势。在 Hcash 系统中交易的确认时间几乎是瞬时的。同时因为 DAG 并不基于区块，所以并不存在所谓区块大小的限制，理论上，单位时间能够容纳的交易量是非常庞大的（HTPS, Hyper Transaction Per Second）。而同时 Hcash 又需要考虑与基于区块的区块链系统的交互。所以 Hcash 能够实现在有限的区块体积下实现单位时间的海量交易。从而真正的实现“超级现金”的功能。

1.7. Haven. Limited token supply

Hcash **数量规划**

Hcash **的代币总量是固定的，总量无限接近 8400 万，总体分为六大部分。**

- PoW 产出 2100 万（25%).
- PoS 产出 2100 万（25%).
- 众筹（ICO）以及免费分发 2100 万(25%).
- 早期投资者（Pre-ICO）1260 万(15%).
- 开发团队 + Hcash 基金会 420 万(5%).
- Hcash-DAO 420 万(5%).



Hcash 的地址分为明地址和暗地址，分别对应 Zcash 的透明地址和 Byteball 的 Whitebyte 以及 Zcash 的 Z-Add 和 Byteball 的 Blackbyte。Hcash 的用户可以在自己的钱包或者客户端进行明暗地址的转换，但是 Hcash 的代币总数量保持不变。在系统默认定义中，PoS 产出的 2100 万币默认全部去到暗地址，此部分币可称为 HiddenCoin，PoW 产生的 Hcash 在矿池出块的时候也默认去到暗地址并成为 HiddenCoin。除此 50%的币之外其他所有的 Hcash 全部为明地址币，包括 ICO 以及免费分发，早期投资者，开发团队以及 Hcash 基金会持有以及 Hcash-DAO 所持有的所有币，全部为明地址币 Hcash。在不同系统之间转换或发送的时候可以按要求发送明地址币或暗地址币。

二、开发路线图

由于 Hcash 着眼于建立新的技术标准并重新定义价值。所以 Hcash 所面对的技术挑战也是前所未有的，预计的开发路线图如下图所示：

Road Map for Development

h.cash

Hcash 与 Hsare

正因为我们需要较长的时间来实现 Hcash 的代码和功能开发，所以在 ICO 结束之后，所有投资人会先获得 Hshare 作为代币，该代币基于 Hyperledger 技术进行开发。而在 Hcash 主链上线之后，可以在任何上线 Hshare 的交易所或者 Hcash 官方团队与 Hcash 进行一比一兑换。并于大约 10 个月后完成所有的承兑与替换。Hcash 团队将使用技术手段销毁所有的 Hshare。在最后截止日期后所有的 Hshare 将被永久销毁。Hshare 的开源代码在 Hcash 的 GitHub 页面下，每一个人都可以阅读审核 Hshare 的源代码并确认 Hsahre 的发放总数量与 Hcash 白皮书所规定的 Hcash 数量一致。

三、项目风险与优势

3.1. Hcash 项目的相关风险

1．政策性风险

目前虽然多数政府对区块链相关产业态度明朗并持积极鼓励政策，但公有区块链天生的去中心化属性在与现有的中心化政府的法律法规下依然面临政府政策层面的很多不缺定性。

针对政策性风险 Hcash 团队将会采取如下措施：

- 在团队单独设立公共关系部门，积极与政府以及业内从业人员保持沟通协作，在法律框架下设计数字资产发行／交易／区块链金融／区块链应用等方面业务。
- Hcash 项目运营不涉及法定货币交易，但并不干涉第三方交易所开展 Hcash 兑法币交易业务，Hcash 团队只专注技术。

2．市场风险

Hcash 的终极目标是要实现价值在区块链系统中的去中心化自由流动，然而区块链产业刚刚兴起，项目的未来会面临各种各样的市场考验。

针对市场风险运营团队采取的应对方式为：

- Hcash 运营团队将定期的参与业内会议，并定期或不定期举行项目进展与发布会，与相关开发者沟通与交流目前的市场需求与前景预测，确保项目能够回应社区与市场的声音。

3. 技术风险

Hcash 要建立跨平台的新技术标准，这其中的技术开发难度是非常巨大的，这对于顶尖技术人才的需求以及科研的投入力度要求都是非常高的，如果把控不好，会影响项目进度甚至最终导致项目的失败。

针对技术风险运营团队采取的应对方式为：

- 紧紧依托国内外顶尖著名高校与区块链社区，与顶尖高校共建区块链技术创新实验室。基金会定期拨款，支持 Hcash 社区建设并与其他区块链社区开展深度合作，确保项目的技术风险可控。

4. 资金风险

资金风险是指项目资金出现重大损失，例如：资金被盗，在预定时间内因为人员与资金问题无法完成开发进度等等问题。

针对资金风险运营团队采取的避险方式为：

- 所有大额数字货币存储采取多重签名钱包+冷存储方式由基金会理事共同掌管。在 3/5 多重签名方式下，可以有效降低资金被盗以及被私自挪用风险。

四、免责声明

- 该文文档只用于传达信息之用途，并不构成买卖 Hcash / Hshare 的相关意见。以上信息或分析不构成投资决策。本文档不构成任何投资建议，投资意向或教唆投资。
- 本文档不组成也不理解为提供任何买卖行为或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。
- 相关意向用户明确了解 Hcash 的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。
- Hcash 团队不承担任何参与 Hcash 项目造成的直接或间接的资产损失。

五、参考文献

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/ bitcoin.pdf. Oct 2008

[2] Vitalik Buterin. Ethereum White Paper : A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper.

[3] Wikipedia. Directed acyclic graph. https://en.wikipedia.org/wiki/Directed_acyclic_graph.

[4] Serguei Popov for Jinn Labs. The tangle. https://iota.org/IOTA_Whitepaper.pdf, April 2016.

[5] Anton Churyumov. Byteball: A Decentralized System for Storage and Transfer of Value. https://byteball.org/Byteball.pdf,September2016.

[6] Wikipedia. PoW. https://en.wikipedia.org/wiki/Proof-of-work_system.

[7] Wikipedia. PoS. https://en.wikipedia.org/wiki/Proof-of-stake.

[8] "Nxt Whitepaper (Blocks)". nxtwiki. Retrieved 2 January 2015.

[9] mthcl (pseudonymous). "The math of Nxt forging" (PDF). pdf on docdroid.net. Retrieved 22 December 2014.

[10] Vasin, Pavel. "BlackCoin's Proof-of-Stake Protocol v2"

[11] http://www.8btc.com/dao-attack-lost-60-million

[12] Ori Brafman. The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations. 2006.

[13] Yochai Benkler. Wealth of networks: How Social Productions Transforms Markets and Freedom. 2006

[14]HOFFSTEIN J，PIPHER J，SILVERMAN J H. NTRU : A ring — based public key cryptosystem

[15]LYUBASHEVSHY V，PEIKERT C，REGEV O. On ideal lattice and learning with errors over rings