



RICH CASH COIN
WHITE PAPER



目录

- RICH CASH 的诞生背景
- RICH CASH 的必要性
- RICH CASH 的 On – Line 平台
- RICH CASH 的交易计划
- RICH CASH 网络
- RICH CASH 操作证明
- RICH CASH 模块形成与补偿系统
- RICH CASH 暗号化算法
- RICH CASH 海绵构造
- RICH CASH INSIDE
- RICH CASH 交易的处理与认可
- RICH CASH POLICY



RICH CASH 的诞生背景 1

- 世界化的网络公司从原有的Off - Line 营销方式转换为On - Line方式。
现有的 Off - Line构造是通过人与人见面的方式来进行，受时间与地点的限制。为了实现世界化扩散利用On - Line 商场，各种 SNS，公开市场，社会化电子商务方式来进行On - Line上的营销。 这样可以解决地点与语言上的障碍使世界变为一体。
- 虽然物流与流通正在向往世界化时代进展，但是在结账方面因为各国家的限制与手续费变得困难。为了解决这一问题 RICH CASH 诞生为支付结账的手段。
- RICH CASH是任何人都可以自由的交易的支付结账手段。
- 全世界的有名企业都在步入虚拟货币市场。所以，RICH CASH设立了利用虚拟货币的 On - Line 网络公司。
- 因为是网络形态所以根据销售量产生佣金。为了支付销售量与佣金但是各国的货币不同所以各国需要有分社。虽然也有用美元支付的公司，但是问题在于兑换手续费昂贵。
- 以网上购物为标准将世界连为一体，原本设立分社是网络营销事业的短处，但是变成 On - Line 国际虚拟货币交易所可以支付销售额与佣金。
- RICH CASH是综合两种营销的优点的媒介体。



RICH CASH 的诞生背景 2

Token交易将会活性化集资，群众募资，金融商品的块环链上的交易。通过客户端轻松的解决安装过程，降低使用者的不便。

试图尝试所有可能的块环链技术的软件，其中p2p数码货币的使用频度将会最高。(Ryan X Charles)

我们已经经历过在流通市场的货币的用处与极限,并了解在不动产市场上金融的重要性。RICH CASH COIN 运用了 Nxt 与 Wave 币所提示的方式来在两种市场上执行货币应有的角色，并且克服原有的极限。

原有的极限指

1. 以小规模的资金很难参与投资
2. 即使参与了投资也很难持续的观察事业进行状况
3. 不能担保分配利益的透明性，并且分配的名次下降

这一方面的难处在于

1. 在流通市场与不动产市场使用的虚拟货币或代币需要隔离，因为两个市场的利益与危险性不同。
2. 在两个市场上使用的虚拟货币可以互相补充么？

我们通过Ripple 与 Wave 解决上例问题，通过交易计划公布 RCS 的有用性。

- - 定制token的形成，删除，传送
- - 分散token交易所，对等卖价与买价
- - 可以随意交换定制token。(asset-to-asset trading). 可以制作成与各国货币联动的token，重现传统性的基本。



RICH CASH 的必要性

- 虽然为了价值的传送, 主要网络token的使用非常自然, 但也会发生一些问题。如果流动性与机动性使用大量虚拟货币的话会给出售者带来相当的负担。
- 为了完化妨碍作为分散货币储存库的使用的非稳定性时使用的token的总量是(哪怕是在技术开发初期始点)要有限制的。
- 如果公开制作国家别的中央化块还链货币的话, 就会将有外部金融机构的登场。他们的角色是扩张实际货币资产缺少的流动性, 提供 KYC/AML. 维持支付基础是为了分散块还链的完全外协加工。
- 将国家级货币记录在块还链的方法曾在 Nxt块还链上的 CoinUSD token里尝试过。就像 Ripple 的网关的接收方式一样。这样的战略将会与新登场的块还链竞争, 诱导其与金融机构开起的块还链共事。
- 金融机构与企业是构现块还链的社区化计划的效果性框架。无法提供高频度交易是块还链的特性。中央化的解决方法将回瞬间解决大量的交易, 但此非必须。块还链应当运营的圆滑。例如发行群众募资货币后应将金融流量容入社区里进行管理。
- 作为将与速动器在未来出世的商品, 虽有投资一定金额的方式但也是存在明确的阶段的。基本方式的投资者很难倒卖出自己投资的金额。相反块还链为基础的系统里倒买会相当自然。块还链中RCS的交换与转移是允许的。
- 证券的发行受金融监督员的管制。预测货币价值的上升或得利时, token可以与证券比较。但块还链式拥有完全不受规则的限制的特性所以比起证券更加容易发行与交易。
- 每个人对虚拟硬币的价值观不同的原因有以下几点。
- 某些资产的价值在将其保管起来后流入的阶段性的现金的流动预测金与现金流入的各个期限的因利润率的折扣的金额的总和。将买入的资产保有后的纯利润用公式表现如下。
- 在上面的公式中IRR称为内部纯利润, 主要用做自己到达的资本的的利润。此利润中隐藏风险, 因投资的危险度商议价值。
- RCS赋予致谢价值的变动性完化与安全。



RICH CASH的 On - Line 平台

- 全球性网络公司把所有业务做成能够在网上商城里交易的平台。
在这个网上商城里购买, 退货, 佣金支付等所有货币的功能都是使用 RICH CASH来结算与支付的系统来使其一元化。
各国家不同货币所发生的问题与不便的事况因 On - Line 国际暗号货币交易所质品的使用每个人都可以轻松的加入。
使得国家间的外汇交易变得简便, 交易与市价的差异和利益的蓝图能够实现, 也使本国货币也能够现金化。
- RICH CASH是通过 On - Line 网上商城将全世界构现成了一个购物城。将各国的商品作为质品登陆后, 让世界各国的人们购买品质好的异国性的商品或普遍但又不方便购买和无法购买的商品轻松到手的平台。
初期平台登记的商品为化妆品, 绿色食品, 美容商品(护肤), 名牌(车, 包, 表, 钱包, 皮带等), 预计商品将会阶段性的扩张。
这样的商品是以如果买家想买就会形成交易, 当国就可以轻松配送的系统。
- 贩卖方式构现成消费者阶层与网络市场营销阶层也可以使用的方式。
- 全世界商品成为一体, 全世界消费者成为一体的平台。购买方式是以 RICH CASH来实现的。
- RICH CASH 成为将全球统一的一个连接点。



RICH CASH 的交易计划 1

- RICH CASH 会成为 On - Line 商场的中心货币，将会有30万名不同国籍的会员使用 RICH CASH 。购买商品与支付佣金时将只会使用 RICH CASH。
- 现在并没有可以维持30万名会员可以周期性交易的虚拟货币，有明确的使用处并且有充分的交易量的 RICH CASH 和大部分的虚拟货币相比时明显优越。
또한, On - Line 商场的全球化网络阶层与一般阶层融为一体来接近市场的竞争力与消费者的权益。这将增加消费者与会员，并且 RICH CASH 将成为最优秀的虚拟货币。
- 阿里巴巴, amazon.com 等网上商城以网络营销，不需要经营分社便可以流通物资。因为网上商城并不是network方式，所以不需要支付佣金，只需要 visa与 master card支付销售额。
- 运用两种营销方式的长处创造新的一种营销平台， RICH CASH 来解决销售额与佣金兑换的问题。



RICH CASH 的交易计划 2

- 第一次先开采发行量200,000,000RCS使用在流通市场。通过联动交易时使用的货币的市价来维持虚拟货币的内在价值。网上购物的消费者购买商品时一般不会使用现金，都是使RCS，需要的RCS超过市价时，因Airdrop保有虚拟货币的使用者将会有利益，虚拟货币的市价将会维持货币的市价。经营网上商城的利益将提升虚拟货币的价值。
- 并且会使用在不动产市场。将考虑Target不动产的投资规模来流通市场，并且提供可以交换已完成的建筑的房间权力。即，以目标不动产开发时需要的资本与投资利益的限制内决定虚拟货币发行量。决定在RCS 投资不动产1号的事业计划书里仔细讨论。
- 在两个市场上使用的虚拟货币将另外指定最初交易的钱包，让相互不受干扰的限制性的管理。需要管理者的许可便可以相互交换。
- 通过不动产开发钱包的虚拟货币将使用在购买不动产，中介费，租金，管理费的支付。
- 到了一定时期Target投资不动产的总投资金额达到200,000,000RCS时不动产投资虚拟货币将通过hard fork与coin swap转换为不动产专用虚拟货币，这个过程大约需要1年6个月到2年左右可以达成。
- 使用在流通市场的RCS以登载为原则，使用在投资不动产的RCS以Private sale为原则，考虑相互间价值的warranty来策划。



RICH CASH 的交易计划 2

- Target 不动产
- 事业名 RCS 永登浦新筑公寓事业
- 地 址 首尔市 永登浦区 永登浦1街 121-3
- 区 域 1种区域单位(一般商业)
- 面 积 237.92坪
- 总面积 1,587.52坪
- 容积率 590.41%(预计)
- 房间数 商铺一间 公寓 162号 (9.42坪 138号, 11.37坪 24号)
- 销售额 30,153,860,000韩元
- 土地费 9,000,000,000韩元
- 工程费 8,173,897,000韩元 关联工程费 1,271,919,000韩元 税收以及公共缴费 814,439,000韩元
- 卖出费 2,850,646,000韩元
- 保存登记 245,880,000韩元
- 金融费 2,525,385,000韩元
- 事业利益 3,626,477,000韩元
- 出售性 优秀

- 现况
- 土地 土地合同已签并允准使用土地
- 施工 아이렉스 建设公司 트윈建设公司 意向参与施工 预算施工费中预定bidding
- 金融 水协中央会 驿三金融中心, 0K存款银行, 有利银行 债权人团 意向参与
- 委托 国际信托 韩亚资产信托 木槿花信托 韩国信托 意向参与信托
- 为了节省信托费与金融费进行担保信托代理物(资本50韩元为条件)
- 出售 担保2个月之内出售(全额接收未出售物量) 请有收购意向的人提前上交意向书
- 策划 5/24日 永登浦区政厅接收审议书 与负责人进行口头协议并批准
- 开工与出售 预想 2018年 10月



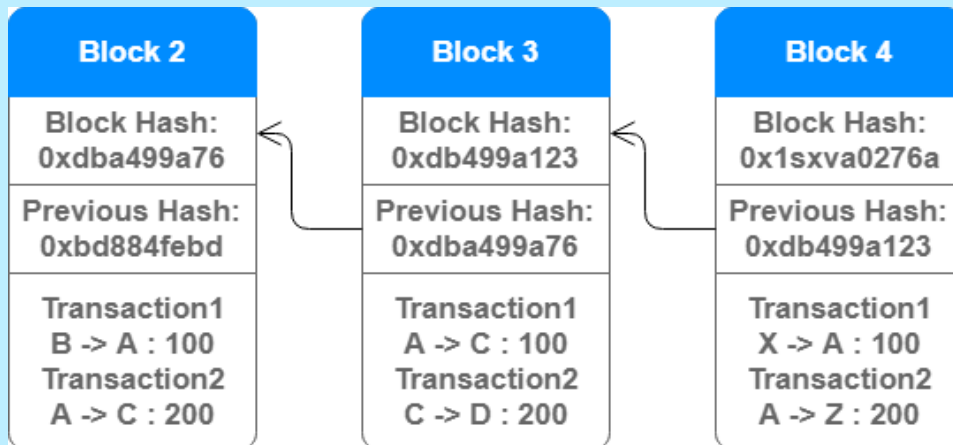
RICH CASH 网络

区块链网络大角度分为，区块链数据切换点和区块链和客户。

数据切换点保管交易，负责认证起到分散协议的作用，客户会生成事务交易，起到确认交易明细的作用。

数据切换点具有两种数据库，一个是保管所有的正确交易的区块链交易保管数据库，另一个是所保存的交易适于软件的程序保管数据库。

数据切换点所持有的上面的第一个DB，就是叫区块链的特殊构造设计。记录交易的区块链，通过P2P网络而传播，在许多的区块链中，根据事前所商议的方式，把正确的砌块连接在以前的模块上。





RICH CASH 操作证明

RICH CASH采用基本操作证明方式的和的算法。

操作证明是利用keccak散列函数来寻找暗号散列值的过程。

RICH CASH的操作证明方式与比特币相似。

但是，现有的操作证明方式因大量的交易，模块形成时间为10分钟。

RICH CASH为了克服这些问题，使用Keccak (Shah-3) 散列函数，采纳了CPU操作证明方式(Proof of Work)。

但是，以公开开采为目的的模块形成时间为5分钟，一日可形成的模块数为288个，模块补偿为40 RCS，一日最大开采补偿数量为 11.520 RCS，一个模块为增加难易度的标准。

RICH CASH的特点为，有结账的功能与技术上的部分可以以5分钟为单位形成最多模块数，并且有补偿数量可以进行公开开采。

以结账为目的的虚拟货币一般100%都使用在先开采，RICH CASH是80%为先开采，20%为公开开采。已经在市场流通的虚拟货币外可以通过自由的开采来参与，这样可以确保用户。

公开开采的2.2亿 RCS的总开采期限设定为52年。

虚拟货币的起初 0 ~ 9 block为止补偿为 0 RCS，

第 10 block的补偿为8.8亿 RCS

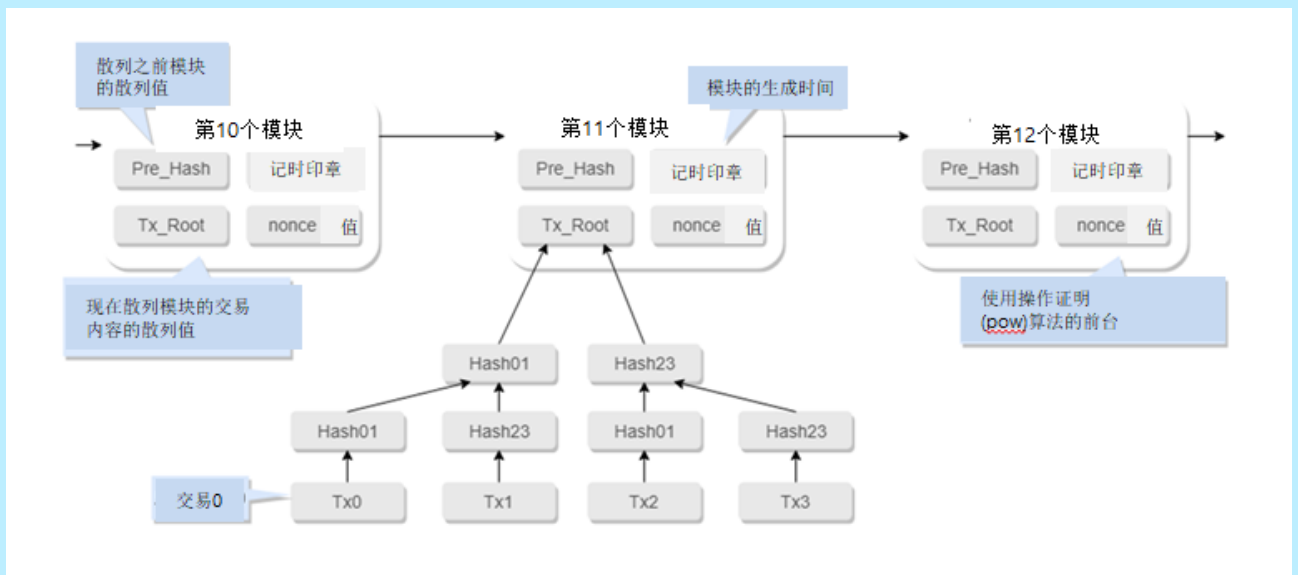
第 11 之后各block的补偿为8 RCS

开采的总额为2.2亿 RCS时(5,500,010 blocks)，各block补偿为 0 RCS。



RICH CASH 模块形成与补偿系统

RICH CASH 的模块形成时间为 5 分钟以内。一日形成模块数为 288 个，模块补偿体系为 40 RCS ， 一日最大开采补偿数量为 11,520 RCS ， 以一个模块为标准来增加难度度。





RICH CASH 暗号化算法

加密算法中散列函数(SHA : Secure Hash Algorithm)是在短信代码或电子签名等多种领域中必需的加密算法。1993年发表 SHA-0 后, 发表了SHA-1, SHA-1的变形 SHA-2系列的 SHA-224, SHA-256, SHA-384, SHA-512 等。

SHA-1是SHA 函数中最经常使用的函数, 与TLS, SSL, PGP, SSH, IPsec 等多种保安协议与程序上使用。SHA-1代替之前经常使用的MD5来使用。但是, 发生了针对 SHA-0 与 SHA-2 的攻击, 因此发现了MD5的脆弱性。与SHA-1没有太大区别的SHA-2也是不知道什么时候会被攻击。比特币使用分类为SHA-2的SHA-256算法。

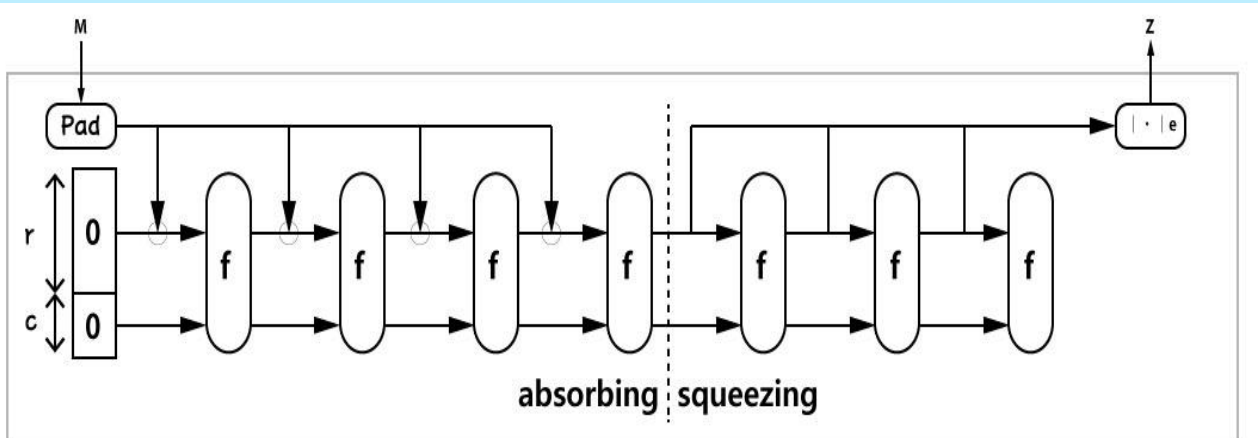
因此产生了SHA-3。

SHA-3是美国国立标准技术研究所(以下 NIST)在2015年8月发表的加密散列函数。

SHA-3是以SHA-1, SHA-2为基准补充散列算法的缺点, 通过5年间收集的64件加密算法比较分析, 选定最合适的一个来进行的。

其结果为下届SHA-3散列算法 Keccak被选定。

SHA-3是用 SHA3-224, SHA3-256, SHA3-384, SHA3-512的4个散列函数与称作 SHAKE128, SHAKE256的2个可扩展的函数来构成。因为以海绵的构造来形成所以称作海绵函数。



SHA-3的海绵构造



RICH CASH 海绵构造

SHA-3是以海绵构造来利用保有 bit顺序的的函数与填充信息的填充函数来打印信息摘要。

b bit定为 $b \in \{25, 50, 100, 200, 400, 800, 1600\}$ ，以 $b=r+c$ 来分为 r 的bitrate与 c 的保安参数。

r 是比 b 要小的整数定义为 f 函数的输入bit， c 是拥有 $b-r$ 值的整数。

信息经过填充函数为了成为 r 的倍数来填充，把信息除以 r bit的值与 r 的 XOR验算值使用于 f 函数的输入。

之前 f 函数的值的信息与 XOR后的 f 函数使用的过程反复中进行吸收信息。

概要	Keccak 海绵函数
设计者	Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche
体现	可扩张输出函数(XOF),即拥有任意的输出长短的散列函数的一般化
构造	海绵构造
早期	b 是 25, 50, 100, 200, 400, 800 或者为1600 bit的 KECCAK - $f [b]$ 排列中之一。FIPS 202 与 SP 800-185 使用标准范围内最大排列 的 KECCAK - $f [1600]$ 。但是在有限的环境下会使用更小（更轻）的排列。 参
参数化基准	容量 c 与 bit率 r
例子	例子标示为KECCAK [r , c] ，容量 c 决定一般攻击下的保安强度。即，保安水准为 n bit的情况下容量为 $c = 2n$ ，合成为 $r + c$ 是 25, 50, 100, 200, 400, 800 与 1600 bit中为排列的宽。地
地位	在3GPP TS 35.231, FIPS 202 与 SP 800-185为标准化的SHA-3 竞争中胜出



RICH CASH INSIDE

海绵构造的SHA-3可以打印出所有SHA-2可以打印的大小的信息，完备了暗号学函数需要具备的特征，所以可以在所有使用SHA-2的地方使用。

另外, SHA-3拥有较高的双联结构, 采用接近存储器的方式, 所以效率非常高。

比起原有的SHA-2 散列算法要安全。

在所有的平台上比起原有的SHA-2 散列算法处理速度要快。

SHA-3可以扩张打印的长短。

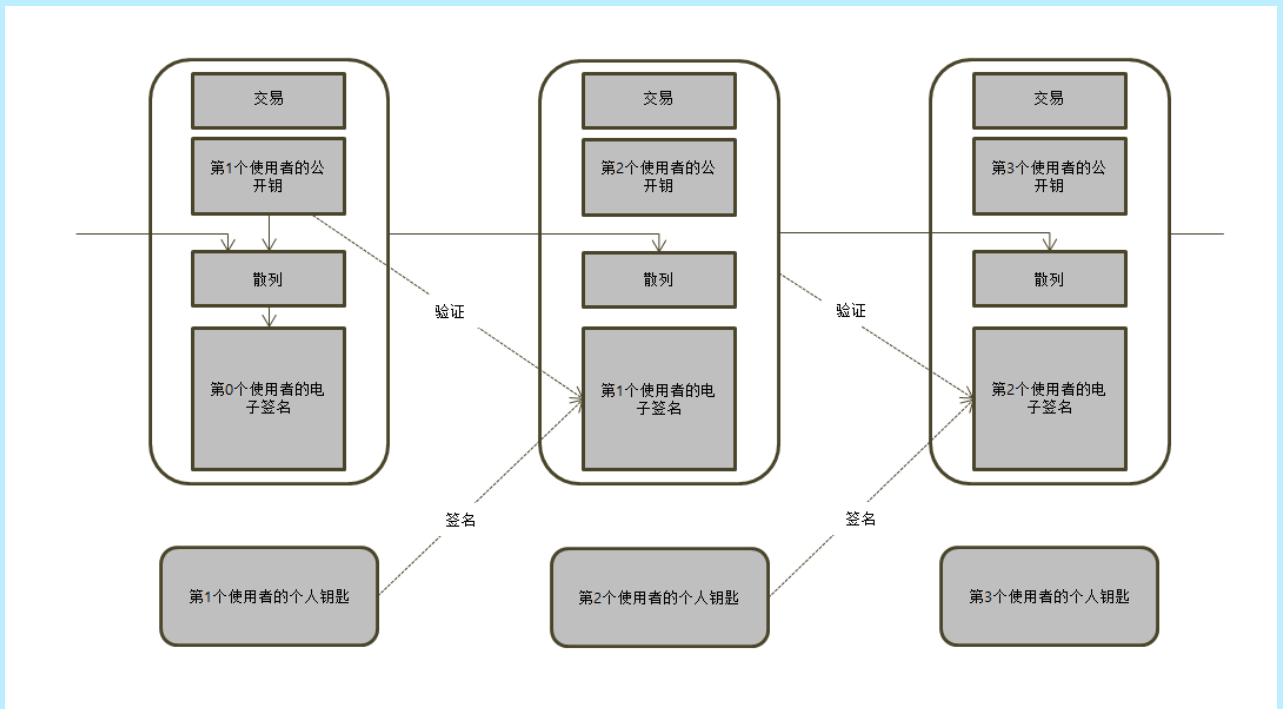
Keccak Tree 散列函数比 MD5 散列算法的性能要高，在处理速度方面也比较性的优越。

Cycles / byte	Algorithm	Strength
4.79	keccakc256treed2	128
4.98	Md5	< 64
5.89	keccakc512treed2	256
6.09	Sha1	< 80
8.25	Keccakc256	128
10.02	Keccakc512	256
13.73	Sha512	256
21.66	sha256	128

主要散列算法的性能比较表



RICH CASH 交易的处理与认可



- 1) 使用者使用个人钥匙申请转账交易。
- 2) 发行相应转账交易A的散列值的识别代码。
(TxID) - 通过这些, 可以立即确认转账明细, 通过识别代码, 可以确定哪些旗下的开采者能够参与开采。
- 3) 将转账交易A明细放入自己的存库中保存。
- 4) 开采者成功散列目标值并且有生成模块的权限时便可以在新的模块上吧转账申请明细从‘优先顺序’开始发行。
- 5) 装有转账交易A的模块传播到网络上。
- 6) 转账交易A收到1次确认(confirmation)。



RICH CASH 交易的处理与认可

- 7) 通过网络下载此模块后开采者获得生成模块的权限可以生成下一个模块。
- 8) 传播到装有转账交易A的模块。
- 9) 转账交易A收到2次确认。
- 10) 收到转账的主体认可转账内容时变成确定转账(Settlement)。

中本聪设计的比特币程序是各转账需要确认6次才可以使用。

先生成的模块到达之前生成新的模块时块环链分歧的话先采纳更长的块环链，不能链接模块的块环链会消灭。

比特币设定为6次确认的原因因为装有交易的模块形成后添加5个模块时，其块环链将会活下来，这样一来，此交易便不会发生问题。

这时，装在已经消灭的模块里的交易会回到原来的状态等待装到下一个模块里。

比特币模块形成的平均时间为10分钟，像这种验算量多的操作可以同时形成模块的情况较少。

并且长度相同的块环链发生冲突时过一段时间块环链的长度会有所改变来消除冲突。

实际过去一年发生的分歧都会在2~3个模块内解决。

还有，很多事业家在交易领域中为了满足使用者来调整确认阶段，让在1~2次确认中完成转账。

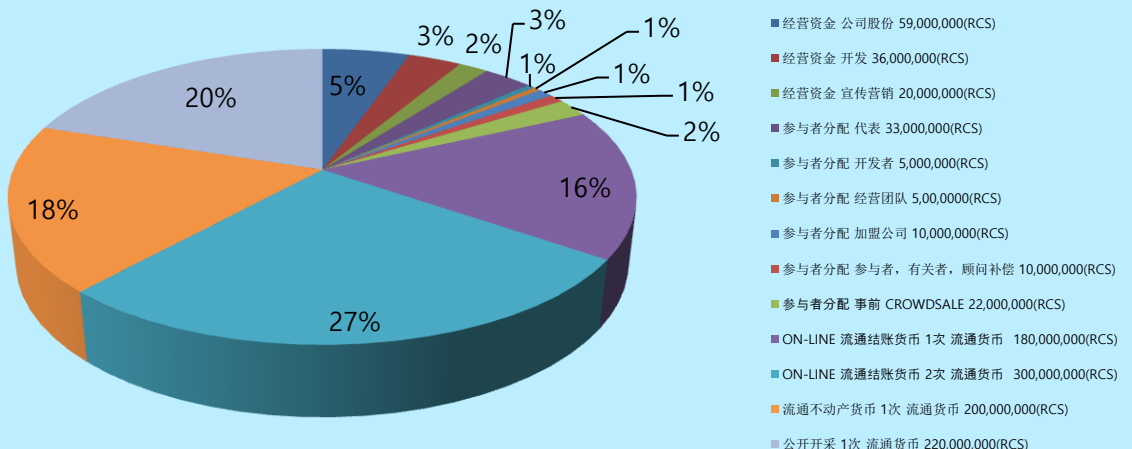


RICH CASH POLICY

- COIN NAME : RICH CASH
- COIN 简称 : RCS
- COIN 单位 : 小数点以下8位数
RP1(小数点1位数) , RP2, RP3~ RP8(小数点8位数)
- RICH CASH 算法 : Keccak (SHA-3)
- RICH CASH 使用处 : On - Line 商场支付, 不动产流通虚拟货币
- RICH CASH 总埋藏量 : 11亿 RCS
- RICH CASH 公开开采量 : 2.2亿 RCS
- RICH CASH 先开采量 : 8.8亿 RCS

RICH CASH COIN的分配如下.

区分	分配区分	分配货币数	比率
经营资金	公司股份	59,000,000(RCS)	5.36%
	开发	36,000,000(RCS)	3.27%
	宣传营销	20,000,000(RCS)	1.82%
参与者分配	代表	33,000,000(RCS)	3.00%
	开发者	5,000,000(RCS)	0.45%
	经营团队	5,000,000(RCS)	0.45%
	加盟公司	10,000,000(RCS)	0.91%
	参与者, 有关者, 顾问补偿	10,000,000(RCS)	0.91%
ON-LINE 流通结账货币	事前 CROWDSALE	22,000,000(RCS)	2.00%
	1次 流通货币	180,000,000(RCS)	16.36%
流通不动产货币	2次 流通货币	300,000,000(RCS)	27.27%
	1次 流通货币	200,000,000(RCS)	18.18%
公开开采		220,000,000(RCS)	20.00%





RICH CASH POLICY

RICH CASH以 keccak (SHA-3) 算法为基准。

总发行数为11亿 RCS ， 用于结账的数量为 8.8亿 RCS 作为先开采。

RICH CASH 设定为可在多种交易所登载，为了预备RICH CASH的价值上升，设定2.2亿RCS作为公开开采。

在难易度上升的情况下想要开采的话需要高结构的开采器，为了让所有人可以容易的开采，开用了keccak (SHA-3) 算法，要比ETH和LTC的生产性好。

开采时发热的温度只有ETH的 30% ， 可以长时间的使用。

模块形成时间为5分钟，一日可以形成288个模块，模块补偿为40 RCS ， 一日最大开采补偿数量为 11,520RCS ， 根据最大模块数与模块来提供补偿。

RICH CASH 的特征为作为实用货币与在技术上的方面以一个模块为基准提升难易度并可以公开开采。

RICH CASH 作为生活货币会在多样的平台上运营。

RICH CASH 为了实现分散化的世界，连接定义的共同体。 通过连接共同体做一个新的世界。

RICH CASH 在社会，政治上才有的共同体(Community)连接的经济上的关系，新的定义了国家定义的现有的经营系统，定义的各共同体会比以前更密集的连接。

并且，不仅仅是现实世界(Real world)还连接虚拟货币世界(Crypto-world)进行无限的扩张 (Infinite scalability)。

Coin Name	Richcash Coin
Abbreviation	RCS
Algorithm	keccak (SHA-3)
Time Between Blocks	300 sec (高难度)
Block Reward	40 RCS
Total Coin	1,100,000,000 (11亿 RCS)
daily block count	288 blocks
mining coin per a day	11,520 RCS
Rewardable Last Block	5,500,010
Expectation time until Last Block generated	52 years 117 days 6 hours and 10 minutes
maximum block size	2M
pre-mined coin	880,000,000 (8.8亿 RCS)