

2017

# Kcash 数字货币钱包 白皮书

V4.0  
2017.12



# 目录

<b>1</b>	<b>内容摘要</b>	<b>2</b>
<b>2</b>	<b>项目背景</b>	<b>3</b>
2.1	数字货币发展历程	3
2.2	用户和市场痛点	4
2.3	使命和愿景	6
<b>3</b>	<b>产品介绍</b>	<b>7</b>
3.1	多区块链资产管理	7
3.2	数字货币兑换和交易	8
3.3	KCASH 及 KCHAIN 平台	10
3.4	人工智能与物联网	13
3.5	数字货币银行卡	14
<b>4</b>	<b>技术特点和创新</b>	<b>16</b>
4.1	ZERO-KNOWLEDGE PROOF 零知识证明	16
4.2	SHA512-ZERO 算法加密技术	16
4.3	RING TOPOLOGY HUB 环状拓扑中继技术	16
4.4	NOBLOCK 技术引擎	17
4.5	NO-LOCALCOIN 兑换网络	18
4.6	ZEROPAY 闪电支付网络	19
<b>5</b>	<b>项目规划</b>	<b>21</b>
<b>6</b>	<b>团队介绍</b>	<b>22</b>
6.1	创始团队	22
6.2	天使投资人	22
<b>7</b>	<b>代币细则</b>	<b>23</b>
7.1	代币发行计划	23
7.2	商业模式	24

# 1 内容摘要

Kcash 数字货币钱包 (以下简称 Kcash) 是一款打通数字货币和实体世界的钱包应用,旨在解决用户管理多种数字货币的不便、兑换交易过程繁杂、价值传输不畅、区块链性能不足以及应用场景不足的问题, Kcash 拥有独有的跨链和跨合约技术,并结合自有的高性能公链为数字货币领域提供强大的基础设施,促进数字货币的应用与发展。

一方面, Kcash 通过对多种区块链资产类型的支持,提供了安全便捷、去中心化的一站式管理方案。用户可以使用 Kcash 对比特币、以太币等主流数字货币进行统一存储、管理和兑换交易,不仅能够完全掌控自己的数字资产,而且极大的降低了数字货币的使用门槛和管理负担,有效促进了数字资产的灵活应用。

一方面, Kcash 拥有一条高性能的区块链 (简称 Kchain), 支持图灵完备的智能合约。Kchain 主链是非图灵完备的智能合约, 专为数字资产提供安全的金融服务, 避免了图灵完备的智能合约带来的巨大安全风险; Kchain 同时拥有可一键定制的侧链, 侧链支持图灵完备的智能合约, Kchain 提供专有的跨链和跨合约技术, 将主链和侧链链接在一起。无论是 Kchain 上的合约资产, 还是非 Kchain 上的资产, 都能通过 Kcash 具有的跨链及跨智能合约的技术自由的完成价值传递和兑换。Kchain 是一条为数字资产发行、兑换、价值传递等金融属性而生的区块链, 同时具备一键配置生成图灵完备的侧链的功能, 让企业专心于自己的商业逻辑, 而不用担心数字资产的安全及区块链的高成本高难度研发。而 Kcash 平台在 Kchain 的基础上, 为 Kchain 上的数字资产提供分布式算力及分

布式数据接口，极大的丰富了区块链的实用性。

另一方面，Kcash 通过和银行及发卡机构（Visa，Master 等）合作，共同发行数字货币银行卡。用户可以通过 Kcash 在线申请虚拟或实体银行卡，使用任一数字货币对银行卡充值，就能在全球数千万的银行卡受理网点进行线上线下的消费以及 ATM 提现，省去了用户换汇及管理多种法币的麻烦，也极大的扩充了数字货币的应用场景。有了 Kcash Card，任何数字资产都有了链接现实世界的桥梁，不再是飘在空中的梦想。

随着区块链技术和数字货币市场的持续发展，Kcash 作为区块链平台，将为更多新项目提供支持，帮助其区块链资产的管理和流通，为提升生态效率和促进市场繁荣贡献一份力量。

## 2 项目背景

### 2.1 数字货币发展历程

2008 年，中本聪在比特币论坛发表了题为《Bitcoin: A Peer to Peer Electronic Cash System》的论文，首次提出区块链的概念，并由此构建了交易信息加密传输的技术基础和比特币网络。从 2009 年比特币数字货币平台建立至今，比特币系统稳定运行，自动实现了从发行到交易流通的过程。同时，区块链作为基础支持技术，逐渐独立出来应用于更多场景，诞生了多种基于此概念的数字货币，比如莱特币、狗狗币、瑞波币等。

2015 年，随着以太坊开源项目带来的智能合约平台概念，实现了各种不同

类型资产及合约的注册和转移，方便了数字货币的发行和流通，极大程度的丰富了数字货币类型。特别是从 2017 年初开始，通过 ICO 的方式，各种代币层出不穷，带来了数字货币市场新一轮的繁荣。截止到目前（2017.12），在 Coinmarketcap 有统计的数字货币类型已经接近 1000 种，总市值突破 3000 亿美元。

## 2.2 用户和市场痛点

### ● 数字货币管理不便：

尽管数字货币市场在快速发展，但对于数字货币的存储和管理，仍然没有很好的解决方案，如何安全备份一种数字货币的钱包密钥或地址私钥，就已经是拦在用户面前的一大门槛。现在面对越来越多的数字货币类别，用户进行不同资产配置或分散投资时，管理门槛进一步提升，而应对的策略——要么是针对不同类型的数字货币，安装不同的去中心化钱包分别管理；要么是索性放在中心化钱包或者交易所里，让中心机构代为管理。前者给用户使用和管理带来了极大不便，后者又存在一定的安全隐患（中心机构被攻击，或经营不善倒闭等情况将带来资产损失）。如何更好的兼顾安全性和便利性，是该领域服务商一直努力的方向。

### ● 交易和兑换门槛高：

目前数字货币的交易和兑换，主要通过交易所完成，这对非专业用户是很高的门槛——注册交易所需要严格的实名身份认证；交易数字货币需要学习相关流程和操作步骤，充值和提现通常还会有一定限制；数字货币之间的兑换，需要先用数字货币换为法币，再用法币买入另一种数字货币。

另一种方式是类似 LocalBitcoins 这样的服务商 提供场外的数字货币交易，有买卖需求的用户各自报价，大家只需像使用 C2C 商城一样，看到合适价格，一对一交易。但不足的地方是，为了保证交易双方不违约，交易过程中数字货币通常需要托管在平台方，这又衍生出平台方可能违约的风险，主观盗币或客观因黑客攻击等原因造成损失。

## ● **区块链性能不足及设计不合理：**

2017.8 月比特币发生了第一次大型的分叉，产生了 BCH，随后几个月，不断的有人对比特币网络进行分叉。以太坊网络因为发生 DAO 事件 硬分叉为 ETC 和 ETH。这里原因是什么呢？

1、比特币性能严重不足，BCH 打着为比特币扩容的旗号对比特币进行了硬分叉；

2、算力越来越集中，本来应该去中心化的系统沦为一家控制，随意操纵区块链网络，违背了区块链去中心化的初衷；

3、以太坊的智能合约，是区块链非常大的进步，但是这种设计理念却有一个巨大的问题，即把金融逻辑和业务逻辑耦合在了一起。不难想象将微信的聊天记录写在银行的数据库中是一种多么糟糕的设计。

所有，当比特币网络储存容量不够，以太坊智能合约出现漏洞的时候，整个金融系统居然需要分叉才能继续工作。对于超过上千亿美金的系统来说，这简直就是一场灾难。

## ● **区块链开发成本高、算力浪费大、连接现实世界难：**

区块链技术的大力发展，未来将有各行各业的企业使用区块链技术，而区块

链开发成本高将使企业望而却步；POW 的挖矿模式，由于算力竞争激烈，被淘汰的矿机被当做垃圾扔掉，极为浪费，而 POS 机制又无法具备 POW 的去中心化优势；区块链技术本身很难知道现实社会的数据，比如温度多少、股价多少、天气如何等等数据，虽然一些矿工可以提供一些常用的数据，但是由于现实世界数据种类复杂繁多，矿工无法提供企业想要的的数据，而企业如果完全自己提供这些数据，又做不到去中心化的特性，很难让人信服，导致区块链连接现实世界难；

- **应用场景缺失：**

数字货币要有更长久的发展，就必须有更广泛的应用场景支持。目前随着区块链领域研究的深入，特别是针对智能合约方向的探索，逐渐有一些产品方案和实体经济生活相结合，在企业端谋求合作共赢。但真正落地并规模使用的还很稀缺，同时针对用户端的服务更是屈指可数。无论是比特币、以太币，还是基于智能合约平台新发行的各种代币，只有和实体世界有了更多的交互，才能增加数字货币自身的价值，进而促进数字货币的市场繁荣和实体世界的效率提升。

## **2.3 使命和愿景**

Kcash 致力于为大众提供一个安全、便捷、高效的数字资产平台，通过打通数字货币与实体世界的连接，让每一个人随时随地便捷的使用你的数字资产，丰富区块链技术和数字货币的应用场景，推动其服务于商业进步和社会发展。

## 3 产品介绍

Kcash 是未来的支付宝，主要的服务载体是由 Kchain、钱包 APP、数字货币银行卡三部分组成。通过 Kcash 平台的产品和服务，为企业提供了快速部署高效区块链解决方案的服务，同时实现对比特币、以太币、各种代币及企业自己数字代币的一站式管理、简单方便的完成数字货币的交易和兑换，而且能将数字资产与银行卡进行绑定，实现数字货币和实体世界的无缝连接，让你的数字货币应用于各种交易消费场景，真正激活你的数字资产。

Kcash 立足全球，在遵守各国现行法律和政策的前提下，对接支付机构、发卡机构，为用户提供合规安全的产品和服务。

### 3.1 多区块链资产管理

通过 Kcash 的钱包 APP，能为用户提供多区块链资产的统一管理，它具有以下几个特性：

- **一站式管理**

Kcash 通过一个钱包 APP 里统一管理多种数字货币，不仅支持比特币、以太币等主流资产的存储和管理，也支持以太坊、Achain、Kchain 等智能合约平台的标准协议，快速增加基于各平台发行的代币。在减轻用户管理负担的同时，也为 ICO 新项目提供钱包服务支持，让项目团队更专注于核心服务。

- **去中心化服务**

Kcash 秉持区块链的核心要义，为用户提供去中心化的数字货币存储方案，



钱包密钥和所有类型货币的地址私钥信息都存储在用户本地系统里。同时，Kcash 提供便捷的密钥备份方案——用户只需进行一次备份，记下 12 个单词，保存到安全的地方。即使后续增加数字货币种类，用备份的 12 个单词就可恢复所有类别数字货币资产。

### ● 多重安全保障

除了让用户完全控制钱包密钥，Kcash 还针对不同规模的数字资产管理，提供多重签名技术保障和两步授权验证，用户可以选择在转账交易时进行手机验证码、指纹、活体等验证方式，全方位保证数字货币资产安全。

### ● 多语言支持

Kcash 钱包 APP 计划将支持中、英、日、韩等主流数字货币市场的多种语言，为打造世界级钱包应用扫清语言障碍。

## 3.2 数字货币兑换和交易

Kcash 钱包 APP 通过独创的 NO-LOCALCOIN 兑换网络，以及对接交易所 API，为用户提供简单、便捷、安全的兑换和交易服务。

### ● 无风险货币兑换

Kcash 基于 Kchain 平台开发 NO-LOCALCOIN 兑换网络，通过智能合约和跨链网关和跨智能合约技术，实现无风险的数字货币兑换服务（具体细节参见技术特点部分描述）。用户通过 Kcash 进行数字货币间的兑换，由平台方或其他第三方创建兑换的智能合约，由合约机制监控和执行兑换过程，规避了参与各方在

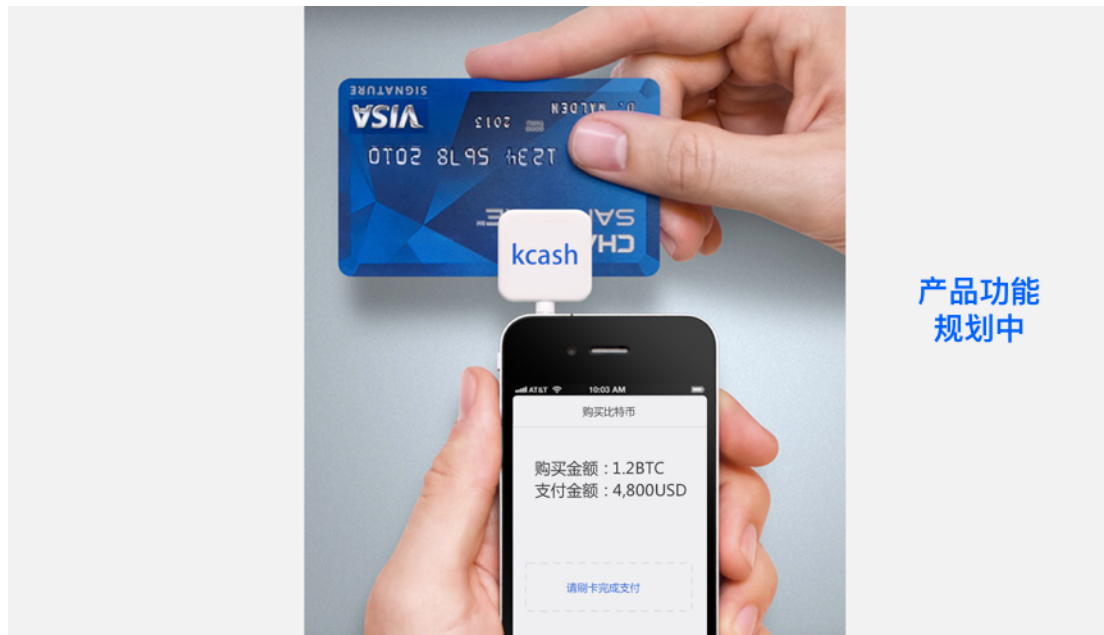
交易过程中的违约风险。相比于中心化的平台服务，智能合约避免了平台方主观的违约风险或客观遭受攻击给用户带来损失。即使是对于 ICO 新项目发行的代币，只要 Kcash 钱包一旦支持，就能通过钱包服务进行无风险的兑换交易。在 Kchain 上，有标准的各种数字资产兑换服务，各种数字资产可以自由兑换。

## ● 简单方便的交易

通过交易所来买卖数字货币，有一定的进入门槛和学习成本。Kcash 通过对接交易所 API，为用户提供最优的市场价格和简单的操作体验——Kcash 通过优化筛选机制，给用户呈现简单的买入价和卖出价，用户只需输入数量，就能像在电商平台一样方便的完成交易。

## ● 便捷的入金工具

Kcash 通过对接支付服务商，给用户提供了刷卡消费通道和手机刷卡器。用户想要购买价值 100 美元的比特币时，只需在 Kcash 的钱包 APP 里发起购买交易，通过 APP 和刷卡器连接，使用美元银行卡刷卡完成交易。Kcash 后台通过交易所 API 将 100 美元转到交易所账户，在交易所完成购买比特币的交易后，将比特币转回到用户的钱包里。整个过程，就如同线下刷卡消费一样简单。



### 3.3 Kcash 及 Kchain 平台

Kchain 主链是非图灵完备的智能合约，专为数字资产提供转账、兑换、交易等专业的金融服务，类似比特币的区块链网络，Kchain 预先生成了很多金融相关的智能合约，在主链上，不能随意发布智能合约，彻底解决了数字资产的安全性问题。Kchain 主链专注于数字资产的金融功能，而不是复杂的商业逻辑。这样设计的优势是安全和高性能，没有冗余的数据。

在 Kchain 的设计理念中，数字资产和商业逻辑是分开的，在 Kchain 的主链上，只有数字资产本身，只能完成数字资产专业的金融功能。如果这个数字资产需要一些去中心化的数据或者挖矿服务，可以在 Kchain 主链的数字资产生成合约里配置好相应的功能函数，同时在 Kcash 平台上，生成提供该数据或者挖矿的算法，并存入相应数量的 Kcash 代币，一同发布在 Kcash 平台上，这样就会有 Kcash 的 APP（手机或者 PC 端）去中心化的用户会运行该数据程序或

者挖矿程序为该数字资产提供数据或者挖矿服务，赚取 Kcash 代币和对应的数字资产。比如，一个合约的数字资产是为农作物提供保险服务，即当连续几个月的降雨指数低于某一数值，就返还给买保险用户一定的数字资产。在这个案例中，智能合约需要知道每天的降雨指数，如果这个指数由官方提供，则有官方欺诈及官方被攻击的风险，该指数数据无法得到信任。而官方可以在该智能合约中配置好相关函数，同时在 Kcash 平台上公布获取算法及存入一定的 Kcash 代币，平台上的 Kcash 用户发现运行该程序可以赚取不错的 Kcash 代币及该合约的数字资产，他们就会为该数字资产提供去中心化的数据提供服务，同时，该程序还可以具备挖矿的功能，只要官方发布的程序具备该功能，用户还可以获得一定的该数字资产，当运行一段时间后，用户发现即使官方不提供额外的 Kcash 代币，由于提供该数据和挖矿服务能获得官方的数字资产，收益也不错，他们会继续为该资产提供服务。对于官方，可以简单的付出一些成本，就可以获得去中心化的算力、数据和挖矿服务；对于用户，可以赚取不错的数据和挖矿收益，当然，用户是需要预先存入一些 Kcash 的保证金以承诺不提供假数据，如果系统发现用户作弊，将会回收用户获得的收益和没收用户的保证金。我们称这种挖矿的形式为合约挖矿。我们都知道，当一些新项目的数字资产发布的时候，买卖的深度通常是不够的，那么当用户需要消费 1 美元的数字资产时，要花费额外的数字资产才行，而有了我们 Kcash 平台的合约挖矿，项目方可以提供兑换挖矿的程序，即挖矿的用户提供该项目的数字资产与 Kcash 代币的兑换服务，这样用户使用该项目数字资产的时候，该兑换服务会将该数字资产兑换为深度足够的 Kcash 代币用以消费，同时获得项目方补贴的 Kcash 代币和挖矿的相应数字资产的矿工费。有了这一类的服务，就算是新上线的项目，也能完成用以现实世界消费的

商业逻辑。

当然，很多项目需要的不仅仅是简单的数据服务和挖矿服务，他们需要自己的区块链以完成自己的商业逻辑。在 Kchain 上，也很简单，项目只需要在自己的数字资产合约中配置好相应的数据，比如区块链的模式、区块大小、共识机制、挖矿模式等等，并存入一定的 Kcash 代币，那么 Kchain 的矿工就会发现该需求，如果矿工觉得收益合适，就会切换一些算力生成该侧链去支持该项目的区块链赚取 Kcash 代币及对应数字资产，如果发现支持该数字资产不划算，就会抛弃该数字资产。在这个逻辑下，矿工总是可以自动的配置自己的算力去获取不错的收益，同时当某种数字资产的算力竞争过于激烈或者矿机主发现自己的矿机已经被该数字资产的算力淘汰的时候，他们就会自动的把算力换到一些没那么竞争激烈的数字资产上，使得矿机可以重复利用而不被当垃圾一样淘汰。对于项目方来说，可以简单到存入 Kcash 代币就可以获取去中心化的侧链及相应的算力支持。当一条侧链出现数据故障或者完全死掉后，也完全不会影响主链的运行，并且侧链拥有自己独有的算力，这条侧链完全为自己的商业逻辑服务，不用担心网络拥堵的问题。这种方式，将数字资产与商业逻辑完全分开，解决了性能问题，也使数字资产更安全。比如，加入主链发生了重大事故，因为侧链上有详细的数据，可以恢复用户的数字资产；如果侧链发生了重大事故，那么也只是商业数据发生了意外，完全不影响用户的数字资产，并且项目方可以通过备份侧链的数据用以恢复侧链。在 Kchain 上，生成并运行区块链就是如此的简单、高效、安全，最重要一点，就是简单配置，就可以获得强大的去中心化算力，这是自己研发并运行自己的区块链所无法媲美的。在这种设计框架下，如果有一天侧链的性能不足，需要对区块链进行扩容，那就非常简单，所有矿工都愿意升级，毕竟侧链上

只是商业逻辑，不涉及数字资产本身，维持老的链并不能像 BCH 分叉 BTC 一样获取双份的数字资产收益，因为数字资产在主链上并不会进行分叉。

如果项目方的商业逻辑利用现在的区块链技术还是无法满足性能要求，该怎么办呢？很简单，同样在 Kcash 平台上，可以提供连接主链合约与自己中心化服务的程序，存入 Kcash 代币，发布在 Kcash 平台上，就会有 Kcash 用户提供算力去提供这种连接的服务。

在整个设计框架中，项目方的数字资产都是完全去中心化的，具备非常值得信任的公信力。Kchain 和 Kcash 平台的架构设计，彻底解决了区块链性能的问题、开发区块链成本和难度高的问题、算力浪费的问题、各种中心化与去中心化的商业逻辑结合的问题、区块链连接现实世界的问题等等。

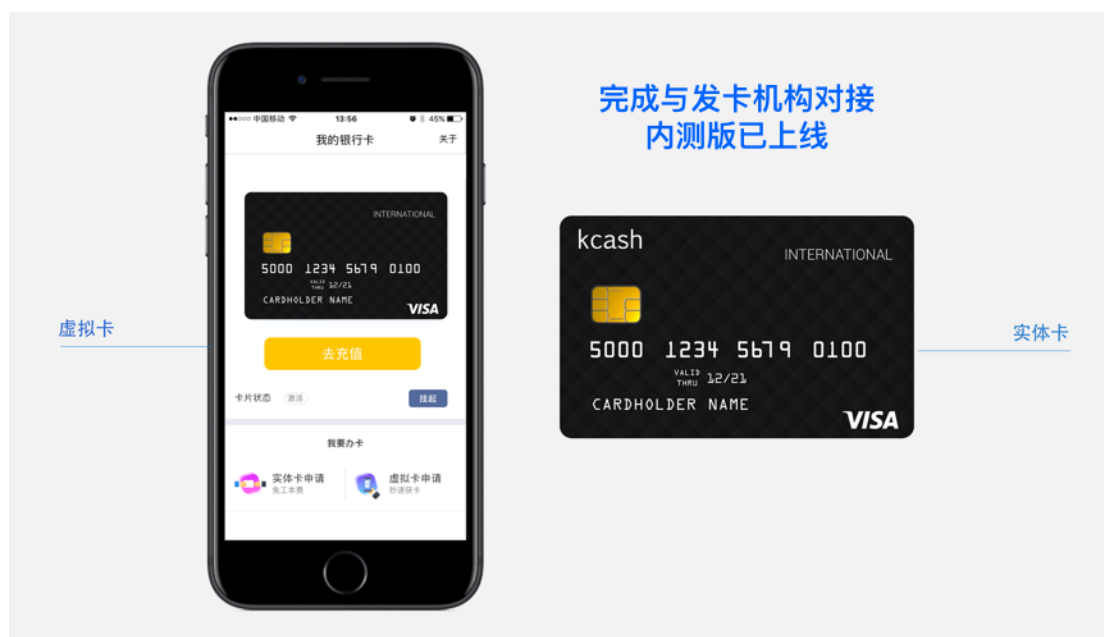
### 3.4 人工智能与物联网

人工智能和物联网的世界就要到来，然而却缺不了区块链，更缺不了区块链上的数字资产。少了数字资产，就不能自由的完成各种服务、价值的传输及兑换。区块链是人工智能和物联网最好的载体。想象一个场景，未来某一天，你坐在一辆自动驾驶的轿车中，你的手机需要充电和 WIFI 服务，你需要支付轿车的费用，你需要支付车上的零食，你还需要看某个付费的节目。每一项服务都有自己的服务商，拥有自己的数字资产无疑是最好的接收支付的方式，你的手机可以通过近场通信（或者蓝牙等）自动连接上这些设备，你只需要告诉你的手机你的需求，它会自动的支付所有的服务，同时它会自动的支付充电和 WIFI 的服务。这里会遇到一个问题，这么多的服务，无论服务商的数字资产有没有在 Kchain 上，

Kchain 网络会通过自己独有的跨区块链和跨合约技术，自动完成各种数字资产之间的兑换。Kchain 将成为沟通这一切的基础设施。

### 3.5 数字货币银行卡

为了将数字货币和实体世界连通，Kcash 通过和发卡机构合作，在钱包 APP 里提供银行借记卡的开卡功能，支持用户申请开通实体卡或虚拟卡，用数字货币充值，进行实体世界的交易和消费。目前，Kcash 团队已经和发卡方建立了合作关系，已有支持数字货币充值的银行卡，样式如下：



数字货币银行卡具有以下几个特性：

- **秒速开卡**

用户只需在 Kcash 钱包 APP 里进行在线申请，选择实体卡或虚拟卡类型，填写基础的 KYC 信息，即可完成开卡。虚拟卡在开卡成功后即时生效，用户可以立即使用；实体卡需要一定的制卡周期，通常 2-3 周能送到用户手里。



## ● 实时换汇

当用户需要用银行卡进行线上或线下交易时，通过 Kcash 的钱包 APP 可以将存储的任一数字货币，根据当前市场汇率，转换成相应法币充值到银行卡里进行交易。这样，用户在自己的钱包账户里始终持有数字货币资产，只在需要消费或交易时进行实时转换。

## ● 广泛的应用场景

通过 Kcash 发行的银行卡可以进行线上线下交易，无论是国内外电商的线上支付，还是境内外的转账汇款，都能提供较于传统渠道更优的费率和更高的效率。同时，Kcash 的银行卡还支持在全球几千万受理网点进行消费，也可以在 200 多个国家和地区的 ATM 机上提取当地货币，这为出国留学、旅游及商务活动等场景提供了极大的便利。

典型应用场景举例如下：

跨境电商购物——当用户在境外电商平台购物，需要用外币支付订单时，只需将实体或虚拟卡绑定到对应的电商平台账户，就能实现用数字货币充值银行卡，然后用银行卡完成支付；

境外旅游消费——当用户出发到境外旅游时，使用数字货币向 Kcash 开通实体银行卡充值，即可在境外进行消费和外币取现，从而免去了换汇的麻烦；

跨境汇款——无论是因为在外留学、工作、或者生意往来，需要在境内外进行转账汇款的操作，都可以通过 Kcash 钱包使用数字货币进行转账，对方在当地即能实时的消费或取现，转账速度和费率大大优于传统服务商。



## 4 技术特点和创新

### 4.1 Zero-Knowledge Proof 零知识证明

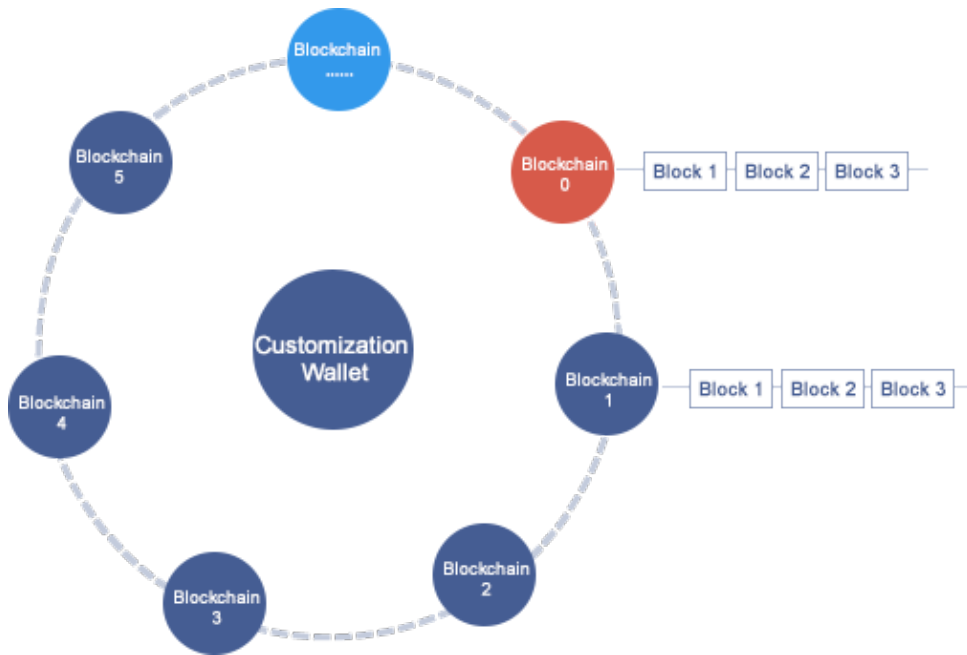
Zero-Knowledge(零知识证明) 它指的是证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。而 Kcash 正是利用零知识证明技术完成了跨链和跨智能合约技术。

### 4.2 SHA512-ZERO 算法加密技术

SHA (Secure Hash Algorithm，译作安全散列算法) 是美国国家安全局 (NSA) 设计，美国国家标准与技术研究院 (NIST) 发布的一系列密码散列函数。通过对 SHA512 加密技术的定制，研发出属于 Kcash 独家使用的 SHA512-ZERO 加密技术，保证对 Kcash 网络的数据安全。

### 4.3 Ring Topology Hub 环状拓扑中继技术

Kcash 的 Ring Topology Hub 技术将多条链连接到一个 Hub 上，让数字资产终端轻松实现一键跨链和转换。环状的优势在于拓扑结构对资源的消耗比星型、树形要小很多。节点少、距离近可能不明显，但是距离远、节点多，环网的这一优势会很明显。大体的设计结构如图所示：



## 4.4 NOBLOCK 技术引擎

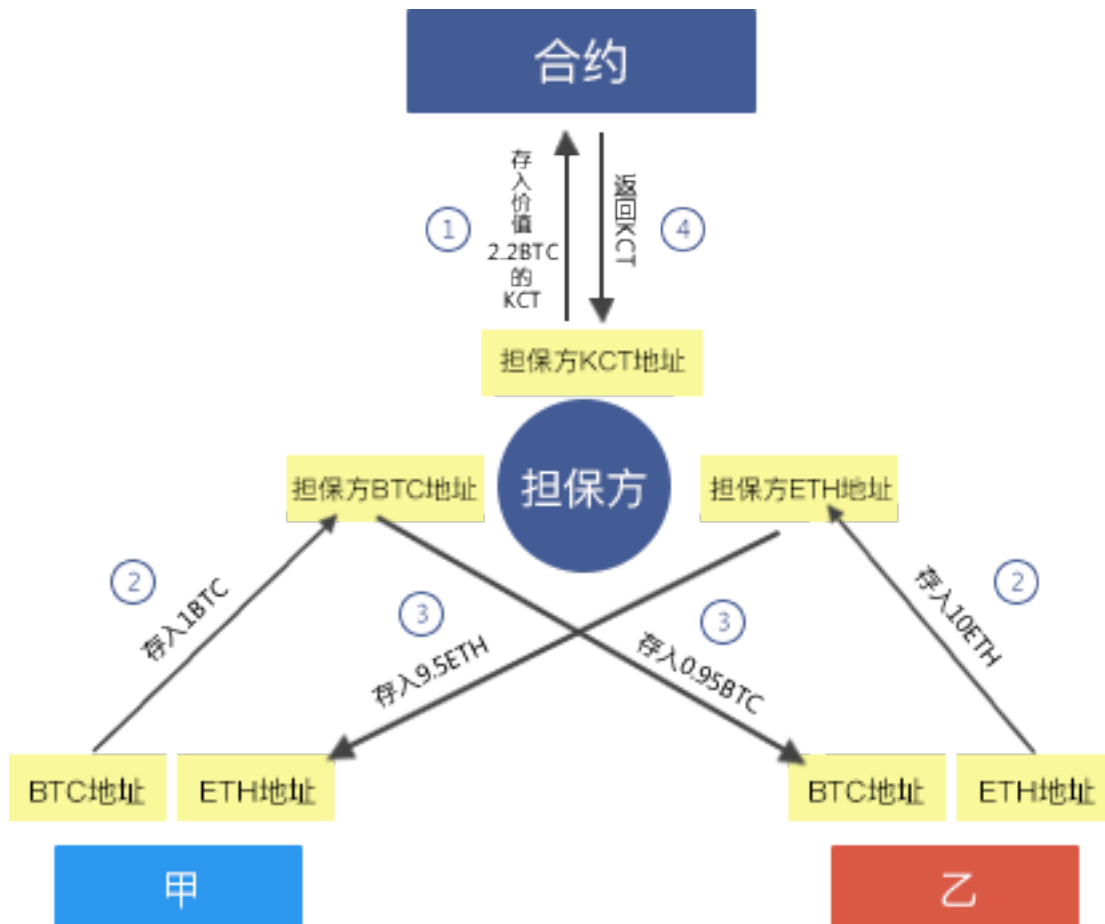
Kcash 独创的 NOBLOCK 技术引擎能让轻钱包真正实现最轻的目的。目前轻钱包有一个巨大的问题就是要接收区块链网络的区块 BLOCK 信息，由于区块链网络通过数据同步冗余来实现数据的安全性，轻钱包的网络请求占用大量的网络带宽。

我们的设计思想是让区块链浏览器成为我们的区块 BLOCK 数据源，自己不再同步区块 BLOCK 数据。而使用区块链浏览器的数据源会带来一个问题，就是数据源的正确性怎么能够保证。我们采用了 BCBP(Block Chain Browser Pool) 区块链浏览器池的设计架构，设计示意图如下：



## 4.5 NO-LOCALCOIN 兑换网络

NO-LOCALCOIN 兑换网络是基于 Achain 区块链平台通过定制智能合约和跨链网关技术，实现无风险数字货币兑换。Kcash 平台或持有 Kcash 代币的用户都可以创建兑换智能合约，通过创建合约提供担保服务，以合约机制来规避各方违约，避免中心化托管机构的仲裁偏颇，让参与三方都没有损失风险。合约创建者促成兑换交易后，获取相应比例的担保回报。整体流程示意如下：



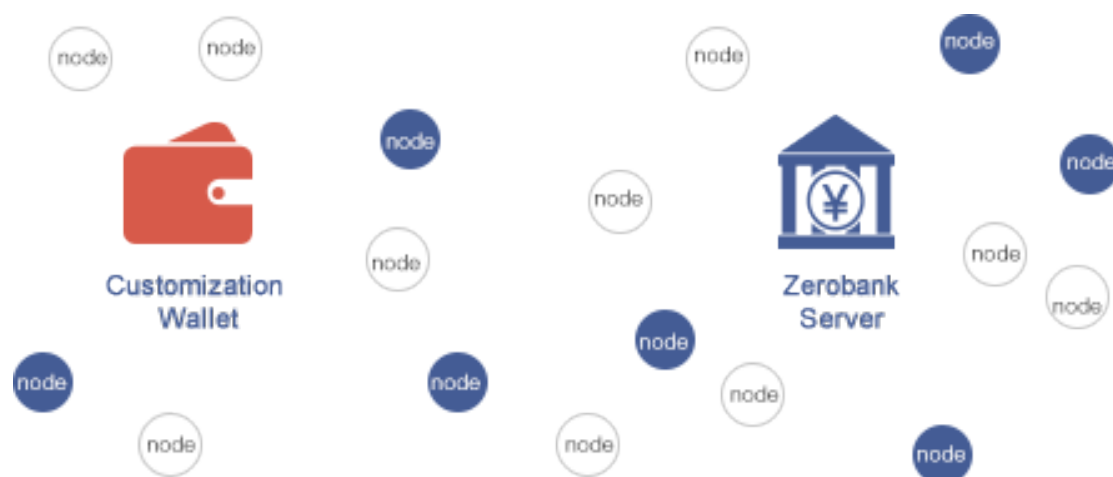
## 4.6 ZeroPay 闪电支付网络

区块链的去中心化会带来支付效率不高的问题。我们通过以下技术实现 Kcash 闪电支付网络（本质是基于现有区块链网络构建 Kcash 的 VPN 子网），转账秒级确认，保证实时刷卡消费不受区块链的影响，技术设计重点如下：

- 定制移动客户端，Kcash 用户的区块链转账做 SHA512-ZERO 加密标志；
- 开发企业级区块链节点，随时检测 Kcash 用户的区块链活动，进行合法性校验、流量分析等。企业级节点 7X24 小时不间断检测，提供给服务器用户的余额变化分析，并上报给 Kcash 服务端；

- Kcash 服务端接收企业级区块链节点分析结果，用户发起刷卡请求时，已经能实时明确用户是否已经真实发起区块链转账请求，防止恶意双花。

图例（蓝色的节点是我们在全球部署的嗅探节点）：



## 5 项目规划

步骤	时间	里程碑	功能服务
第一阶段	2017Q4	钱包 APP1.0	支持 BTC , ETH , LTC , ACT 及基于以太坊等平台发行的主流代币管理
第二阶段	2018Q1- 2018Q2	KCASH 代币 上线交易所 ; 发行数字货币 银行卡	1. KCASH 代币上线交易所 ; 2. 发行数字货币银行卡 , 连通数字货币和银行卡 , 支持线上线下交易 ;
第三阶段	2018Q3- 2018Q4	Kchain 上线 币币兑换	1. Kchain 主网上线 , 支持智能合约、侧链项目和钱包算力平台 ; 2. 基于 Kchain 平台智能合约 , 实现无风险担保交易
第四阶段	2019Q1- 2019Q2	DAPP 平台 对接交易所	1. 丰富 DAPP 平台 , 打造应用生态 ; 2. 对接交易所 , 支持 APP 内便捷的买卖数字货币 ;
第五阶段	2019Q3 及以后	持续迭代	1. 优化货币转换和交易的服务 , 完善数字货币银行卡的使用流程 ; 2. 完善 Kchain 主链与侧链的技术 3. 探索和银行金融机构合作 , 为用户提供多样化的创新服务

## 6 团队介绍

### 6.1 创始团队

**祝雪娇**，Kcash 项目创始人，毕业于清华大学，获得硕士学位。8 年技术研发经验，全栈工程师，连续创业者；2011 年开始接触研究比特币和区块链技术，随后联合创建 YardWallet，自主开发了比特币支付网关、比特币钱包以及版权认证系统，具有深厚的区块链技术积累和行业认知。

**刘锬**，Kcash 联合创始人，毕业于北京大学，获得信息管理和经济学双学士学位。8 年互联网产品从业经验，曾担任网易有道产品主管，YardWallet 联合创始人，钱袋宝产品总监，参与比特币钱包、POS 收单和移动支付等多个方向从 0 到 1 项目的创建，在传统支付和区块链领域都有深入的研究和实践。

**余水**，Kcash 联合创始人，毕业于南开大学，7 年管理咨询经验，曾任和君咨询业务合伙人、北京惠远咨询创始合伙人，为多家 A 股上市公司提供战略规划及商业模式设计、组织变革与升级、人才培养等服务

### 6.2 天使投资人

近 30 位支付行业公司高管鼎力支持 Kcash，作为天使投资人给予了 Kcash 项目资金、行业资源、业务发展建议等多方面的支持和帮助，他们是 Kcash 长期快速发展的坚实后盾和有效助力。天使投资人详细名单参见后续官网公布。

## 7 代币细则

### 7.1 代币发行计划

Kcash 发行的代币名称为 KCASH，发行总量 10 亿，具体分配方案如下：

比例	分配方案	明细
20%	预售	用于 Kcash 项目后续开发、人才招聘、市场推广等。 此部分资金的使用需要定期公示。
30%	挖矿	用户可以在 Kcash 平台上，为 Kcash 及 Kchain 提供算力、数据支持、挖矿等服务以获得奖励。该部分一共 30%，分八年挖矿完成，永不增发，前四年每年释放 5%，后面四年每年释放 2.5%。
5%	用户激励	用于激励用户下载、推广、存币、消费、转账等行为的奖励。
10%	发展基金	作为 Kcash 发展备用金，用于后续项目开发和业务生态建设，以及国际业务发展。此部分资金的使用需要基金会决议，并提前做公示。
15%	创始团队	为回报创始团队在数字货币领域的探索 and 开发，以及今后维护 Kcash 产品技术和运营发展的付出，发放代币做为回报。代币发行时此部分代币将被智能合约锁定，1 个月后解锁，每月解锁此部分的 3%。



5%	早期投资人	早期投资人对 Kcash 发展过程中在财力、资源、战略规划、人才辅助等方面做出的贡献，发放代币作为回报。代币发行时锁定，上交易所后一个月开始，每月解锁此部分 20%，5 个月解锁完成。
15%	机构投资人	用于回报企业投资人，以及建立和合作企业的业务合作。代币发行时锁定，上交易所后一个月开始，每月解锁此部分的 2%，分 50 个月解锁完成。

## 7.2 商业模式

### ● 数字资产消费的 Gas

在 Kchain 上，任意数字资产的创建和转账需要消费掉 Kcash 代币作为 Gas 矿工工费。

### ● 算力费用

在 Kchain 上，如果项目方需要快速的生成一条侧链，他们需要往配置合约资产的合约里存入一定的 Kcash 代币，以吸引矿工为其提供算力。同样，如果项目方需要用户提供去中心化的算力、数据支持和挖矿服务，项目方也需要预先支付一定的 Kcash 代币。

### ● 兑换费用

用户要完成不同数字资产之间的兑换功能，需要支付一定的兑换费用以获得去中心化的兑换服务。

## ● 手续费用途

用户通过 Kcash 绑定的银行卡在商家消费，VISA 或 Master 等服务商会向商家收取相应的交易手续费（这笔费用会受到消费地区、消费类型、消费金额等因素的影响而不同），然后再分配一定比例给 Kcash 作为分润收入，我们预估平均交易手续费分成后收益为 1% 左右（实际情况可能会有变化）。假设，Kcash 用户 100 万，平均每个用户每月消费 100 美元，一年交易总金额 12 亿美元，手续费分润收入 1200 万美元。

用户通过 Kcash 绑定的银行卡在商家消费，VISA 或 Master 等服务商会向商家收取相应的交易手续费（这笔费用会受到消费地区、消费类型、消费金额等因素的影响而不同），然后再分配一定比例给 Kcash 作为分润收入，我们预估平均交易手续费分成后收益为 1% 左右（实际情况可能会有变化）。假设，Kcash 用户 100 万，平均每个用户每月消费 100 美元，一年交易总金额 12 亿美元，手续费分润收入 1200 万美元。

Kcash 团队会每月拿出上述银行卡交易分润的不少于 35% 部分用于购买 KCASH 代币，回购代币存入发展基金地址，用于后续项目开发和产品生态建设。

## ● 手续费抵扣

当用户通过 Kcash 进行数字货币兑换交易时，可以根据 KCASH 当前市场价值，使用其进行手续费的抵扣。后期，Kcash 团队将通过和交易所合作，尽可能让 KCASH 可以部分抵扣数字货币交易手续费。

## ● 用户激励

持有 Kcash 代币的用户，都可以在 Kcash 的货币兑换服务里，担任合约创

建者的角色，通过促成兑换交易来获取手续费收入（具体机制参见 NO-LOCALCOIN 兑换网络描述）。

通过 Kcash 钱包绑定银行卡的用户，每次消费都将获得本次交易手续费 10% 的返现，Kcash 自动以 KCASH 代币的形式发放到用户钱包里。这样不仅让用户获得了返现折扣，也进一步拓展了 Kcash 代币的用户群。

**联系方式：**

官方微信号：kcash01

官方 QQ 号：1546285452

官方 QQ 群：661265047

Twitter：<https://twitter.com/Kcashofficial>

Facebook：<https://www.facebook.com/KcashOfficial>

Telegram：<https://t.me/KcashOfficial>