



VHKD 白皮书 White Paper

构建全球数字货币自由流通体系
提供下一代跨货币价值转移服务

V1.0

目录

01 执行概要	01
02 简介	
2.1 全球数字货币市场概述	02
2.2 VHKD 设计原则	03
2.3 商业机遇和技术挑战	05
03 VHKD 技术架构	
3.1 VHKD 区块链技术基础架构	06
3.2 底层区块链式结构介绍	08
3.3 分布式共识机制	09
04 VHKD 流通机制	
4.1 资金流动过程	10
4.2 储备金机制证明	11
4.3 挑战与解决方案	14
05 VHKD 发行方案	
5.1 方案介绍	15
5.2 发行优势	16
5.3 日常运营管理	16
06 主要应用场景	
6.1 VHKD 目标用户	18
6.2 VHKD 购买 / 赎回渠道	18
6.3 场景应用	19
07 未来规划	20
08 附录	
8.1 VHKD 项目的法律结构	21
8.2 风险声明和免责声明	21
09 参考	22

01 执行概要

2017年下半年各国对数字货币市场重重打压，数字货币直接兑换法币被大多数国家禁止，一度引起了投资者的质疑和恐慌。在此背景下，一种可以稳定代替法币的数字货币就非常关键。本篇白皮书介绍一款可与法定货币锚定的数字现金 VHKD，为法币与数字货币兑换提供渠道，帮助投资者规避数字货币整体下跌风险，方便资产跨域流通。

USDT 最早开辟了数字货币锚定法币价值模式，但是公众信任危机频发，信用严重缺失。有了 USDT 的前车之鉴，VHKD 在设计上会更加出色：更安全的资金托管制度、更透明的财务信息披露，更严格的审计流程、更健全的承兑网络和更丰富的应用场景。通过运用区块链技术特有的数据加密、时间戳、分布式共识和经济激励手段，在节点无需互相信任的分布式系统中实现去中心化信用的点对点交易、协调与协作，从而解决中心化机构普遍存在的高成本、低效率、数据存储与储备资金不安全的问题。

我们将在白皮书中详细介绍 VHKD 的设计原则、技术架构、流通机制、发行方案、应用场景及未来规划。需要说明的是，区块链技术本身不是一个全新的技术创新，而是作为一系列技术的组合（包括点对点通讯，密码学，区块数据结构等）产生的模式创新。VHKD 将持续打破区块链技术与现实世界交融的局限，逐步形成一个在全球具有影响力的区块链生态经济系统，提升行业效率，促进社会的高效协同发展。

战略合作、商户申请请联系我们：apply@vhkd.io

VHKD 官网：<http://www.vhkd.io>

02 介绍

2.1 全球数字货币市场概述

数字货币是金融科技创新驱动下产生的新型货币形式，自问世以来便受到了国内外学者、政府和民众的广泛关注和重视，吸引了从计算机科学、密码学、经济学、货币学等不同角度的研究和分析，数字货币在信用构建、发行机制、流通机制、交易成本和交易安全方面具备独有的特征。在以比特币为代表地数字货币系统中，中央银行的角色不再存在，没有发行主体，没有任何人或机构能够控制它的发行，货币发行和交易流通地职责由所有节点共同承担，信用信息被每一个节点记录，不会被篡改。

数字货币的理念和技术体系为货币金融体系开创了全新模式，在过去八年间数字货币市场向世人展现了惊人的生命力。据不完全统计，截止至 2017 年 12 月，全球共有 1370 种数字货币，总市值超过 6000 亿美元，这一数字还在不断攀升。预计到 2027 年，全球将有 10% 的 GDP 会通过区块链技术存储。作为数字货币底层技术，区块链正在形成一次历史性全面颠覆性的技术变革和商业革命，它打开了“互联网 + 金融”的战略机遇之门。



图 2.1-1 全球数字货币总市值走势图

具有去中心化特性的数字货币解决了跨地区跨币种的价值流通问题，也在一定程度上避免了法币存在的通货膨胀问题。然而以比特币、以太坊为代表的传统数字货币也有其局限性。一方面，数字货币的流通会对传统货币体系产生冲击，价格波动较大，存在较大的金融风险，因此不适合做为稳定的支付手段，接受此类货币支付的商家将会面临资产浮动较大的风险；另一方面，其成本和效率都有潜在隐患，节点通过掌握全网超过 51% 的算力就有能力成功篡改和伪造区块链数据，这将会引起一系列安全风险。此外，数字货币是一种信用货币，本身不具有价值，其背后是发行者的信用问题，发行主体不同，其背后的信用保证不同。

面对上述问题，Tether 公司发行了与美元 1:1 锚定的数字货币 USDT，开辟了数字货币锚定法币价值模式，为法币与数字货币兑换提供渠道，帮助投资者规避数字货币整体下跌风险，以期解决数字货币波动较大及法币充 / 提的入口问题。但是时间证明 USDT 似乎面临许多挑战，如疑似超发严重、黑客盗币、用户无法顺利地通过 Tether 公司兑换美元等，USDT 也逐渐出现了信用缺失的极端情况。

综上所述，如何保证其价值恒定无波动、无 51% 攻击的技术风险、信用可靠、不会被随意超发滥发，也不会出现 USDT 这类锚定法币的数字货币所面临的公众信任危机，将是数字货币领域又一大挑战。当你阅读本篇白皮书时，可能会感觉耳目一新，我们将针对此类问题提供一种安全、创新的解决方案，并在下文进行深入探讨。

2.2 VHKD 设计原则

毋庸置疑，稳定币值的数字资产在当前环境中是不可或缺的，无论是从技术角度，还是行业应用角度都还面临着很多挑战。基于上文涉及到的问题，我们提出了一个猜想，是否存在一种数字货币，既能提高价值资产流通效率，又能解决公众信任危机，还可以安全可靠地在线下流通？

在接下来的方案里，由 VDAC (Virtual Digital Asset Corporation) 发行的数字货币 VHKD 就可以很好的规避这些问题。VHKD 是一种可自由交易的新型数字现金，其开创性地将港元 (HKD) 与可溯源、公开化的区块链技术相结合，推出具备价值锚定、流通交易、服务兑付属性的数字资产。VHKD 严格按照 1:1 保证金储备港币，每发行 1 个 VHKD，账户上

将会有 1 港元的储备金保障。与 USDT 不同的是，VHKD 在机制层面把风险控制到最低，在设计原则上规避了“超发”风险。

简单地讲，VHKD 完整生命周期是由“发行”、“流通”、“兑付”、“冻结”这四个环节构成的，使得其可以在 P2P、匿名、安全、去中心化的环境中自由交易。同时，为了避免“人为超发”风险，在整个生命周期里，我们引入去中心化的审计模式，确保 VHKD 在公开、透明的环境下良性运行。

接下来将详细论述 VHKD 设计原则：“发行标准”、“流通标准”、“兑付标准”、“冻结标准”、“审计标准”。

• **发行标准：去中心化**

区块链最本质的特征是利用去中心化特性重构信任体系。VHKD 是政治去中心化（分布在全球的网络节点确保信息不可伪造和篡改）、结构去中心化（没有基础设施性的中心失败点），基于 PoW 机制来实现分布式共识，通过分布式账本能安全地存储交易或其它数据，数据采用带有时间戳的链式区块结构存储。任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。基于 VHKD 区块链的智能合约，无需任何中心化机构的审核，严格按照 1:1 储备金构建的去中心化数字现金。

去中心化的区块链技术，无需第三方介入，点对点直接交互，使得高效率、无中心化代理、大规模的信息交互方式成为现实，也不需要担心信息泄露。

• **流通标准：便捷高效**

自由、便捷、高效是 VHKD 的核心价值之一。VHKD 流通渠道广泛，持币用户不仅可以在线上自由流通，也可以线下使用 VHKD 购物或兑付法币。在转账速度方面，比特币每秒交易笔数峰值为 7 笔，以太坊为 25 笔，相比之下，VHKD 独特的区块链技术避开了传统拥挤的网络传输通道，收发速度远超主流数字货币，实现网络区块立即确认，1 秒内到账。

• **兑付标准：刚性兑付**

刚性兑付是确保资产价值安全的基石，也是 VHKD 的核心价值。无论持币用户何时何地提出兑付需求，发行方必须要在短期内完成用户的兑付，才能保证用户资产的安全。持币用户可以在线上兑换港元，也可以通过 VHKD 线下网络覆盖点，在指定商铺兑换港元。发行

方将严格按照 1:1 储备金与合作商铺形成承兑约束，确保用户可以实时购买 / 兑换 VHKD。1:1 的承兑约束是 VHKD 具有保值避险属性的关键，不会因市场供需而产生巨大的价格波动，保护用户权益；同时，强大的线下网络覆盖保证用户可以随时随地兑付。这些特征与 USDT 有本质区别，并且优于任何锚定法币的数字货币。

- **冻结标准：依储备金支出金额冻结**

冻结规则是保证 VHKD 平稳属性的关键，也是避免“人为超发”风险最有效的规定。持币用户在兑换时，发行方将冻结收回的 VHKD，被冻结的 VHKD 均可在公开的区块链浏览器查询；与此同时，资金账户将会按 1:1 的储备金支付给用户，资金账户的储备金信息也可随时查阅，保证 VHKD 与港元的价格始终严格保持 1:1 的兑换比例。

- **审计标准：公开透明**

为了将风险降至最低，必须引入公开透明的审计标准，这主要发生在发行、兑付两个环节。VHKD 的发行与兑付流程及储备金的证明将在接下来的内容中详细介绍，整个流通环节将被第三方权威会计事务所按照国际审计标准进行审计，并对公众定期公示，公开透明，支持随时查询，欢迎监督。

有了 USDT 前车之鉴，我们可以发现 VHKD 的设计原则优于任何一款锚定法币的数字货币。VHKD 利用区块链上的智能合约将去中心化更进一步，开辟的全新的数字货币锚定法币价值模式，为法币与数字货币兑换提供渠道，方便资产全球流通，依靠其便捷、高效、安全等特性将会给整个区块链行业，甚至所有有需求的用户带来全新的体验。

2.3 商业机遇和技术挑战

VHKD 主要优势是可以为跨境资产提供流动性和便利性，并且无价格波动的风险，但是机遇与挑战并存。

我们意识到 VHKD 虽然在政治上和结构上是去中心化，但是并非所有事物都需要去中心化。出于对储备资金安全及法币兑付的需要，VHKD 在逻辑上是中心化的：一个公认的发行方，承担着储备金托管及刚性兑付的承兑责任，并且需要不断开拓和维护承兑网络，以保证 VHKD 的流动性和跨货币转移的便利性。

VHKD 区块链的安全依赖于散列函数、椭圆曲线等非对称密码算法，然而随着数学、密

码学和量子计算技术的发展，传统密码学中的一些基本安全假设，如大素数分解问题、离散对数问题、椭圆曲线上的离散对数问题等，可能会变得越来越脆弱，密码算法安全问题也越来越突出。除此之外，VHKD 的工作量证明 PoW 共识过程高度依赖区块链网络节点贡献的算力，这些算力主要用于解决 SHA256 哈希和随机数搜索，因而一般意义上认为这些算力资源是被“浪费”掉了。同时被浪费掉的还有大量的电力资源，进一步凸显了资源消耗问题的重要性。

因此，如何弱化逻辑中心化的影响并能有效汇集分布式节点的网络算力来解决更多的实际问题，是 VHKD 区块链技术面临的商业和技术挑战。我们目前已经开始尝试解决此类问题，未来的潜在发展趋势是设计行之有效的交互机制来汇聚和利用分布式共识节点的群体智能，这将为下一步创新奠定更加坚实的基础。

03 VHKD 技术架构

VHKD 的底层区块链是去中心化系统各节点共享的数据账本，每个分布式节点都可以通过特定的散列算法和 Merkle 数据结构，将一段时间内接收到的交易数据和代码封装到一个带有时间戳的数据区块中，并连接到当前最长的主区块链上，形成最新的区块。该过程涉及区块、链式结构、散列算法、Merkle 树和时间戳等技术要素。VHKD 设计初衷是构建全球数字货币自由流通体系，考虑到行业特点和未来扩展的可能性，我们对 VHKD 区块链做了六分层设计。

3.1 VHKD 区块链技术基础架构

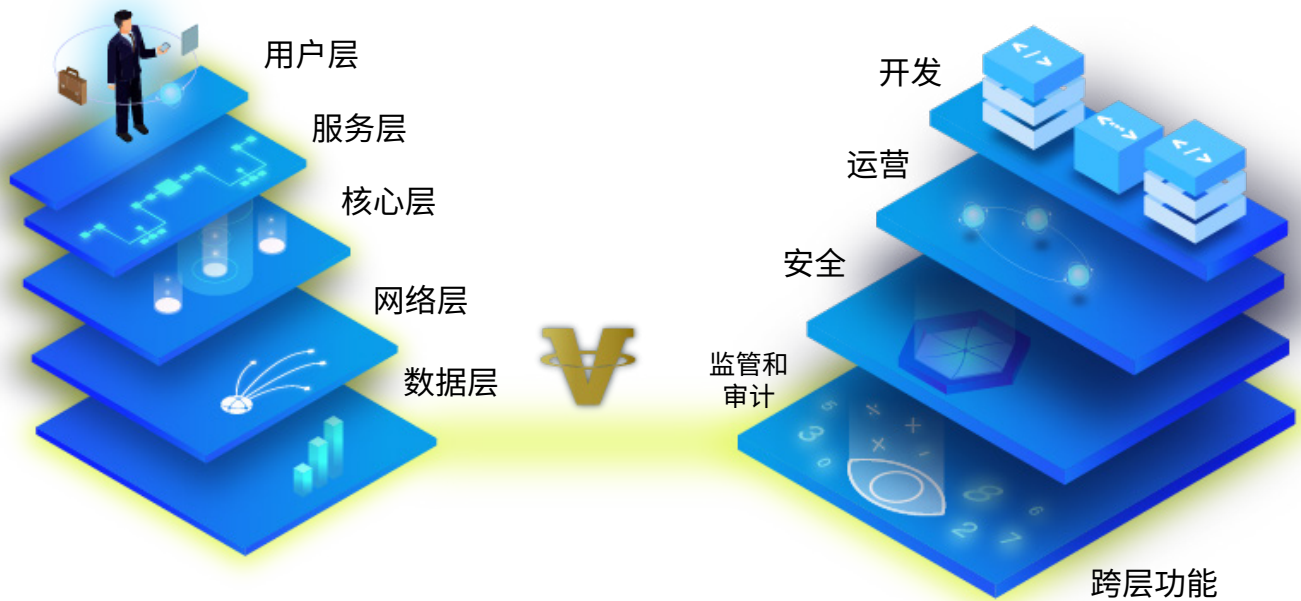


图 3.1-1 VHKD 底层区块链技术基础架构模型

VHKD 底层区块链基础架构模型如图 3.1-1 所示，由数据层、网络层、核心层、服务层、用户层及跨层功能组成。其中，数据层封装了底层数据区块及相关的加密和时间戳等技术；网络层则包括了分布式组网机制、数据传播机制和数据验证机制等；核心层主要封装网络节点的各类共识算法、各类脚本和智能合约，是区块链可编程特性的基础；服务层包含接入管理、节点管理、账本管理；最顶层是用户层，封装了区块链各种应用场景和案例，包含用户功能、业务功能、管理功能。

其中跨层功能包含开发、运营、安全、监管审计功能。

- 开发：IDE、测试管理、构建管理。
- 运营：服务目录、策略管理、异常和问题管理、交付管理、跨链服务管理
- 安全：认证和身份管理、授权和安全策略管理、隐私保护
- 监管审计：监管支持、审计实现

3.2 底层区块链式结构介绍

取得记账权的矿工将当前区块链接到前一区块，形成最新的区块主链。各个区块依次链接起来，形成了一条从创世区块到当前区块的最长主链，从而记录了 VHKD 区块链数据的完整历史，能够提供 VHKD 区块链数据的溯源和定位功能，任意数据都可以通过此链式结构顺藤摸瓜、追本溯源。VHKD 区块链式结构如图 3.2-1 所示。

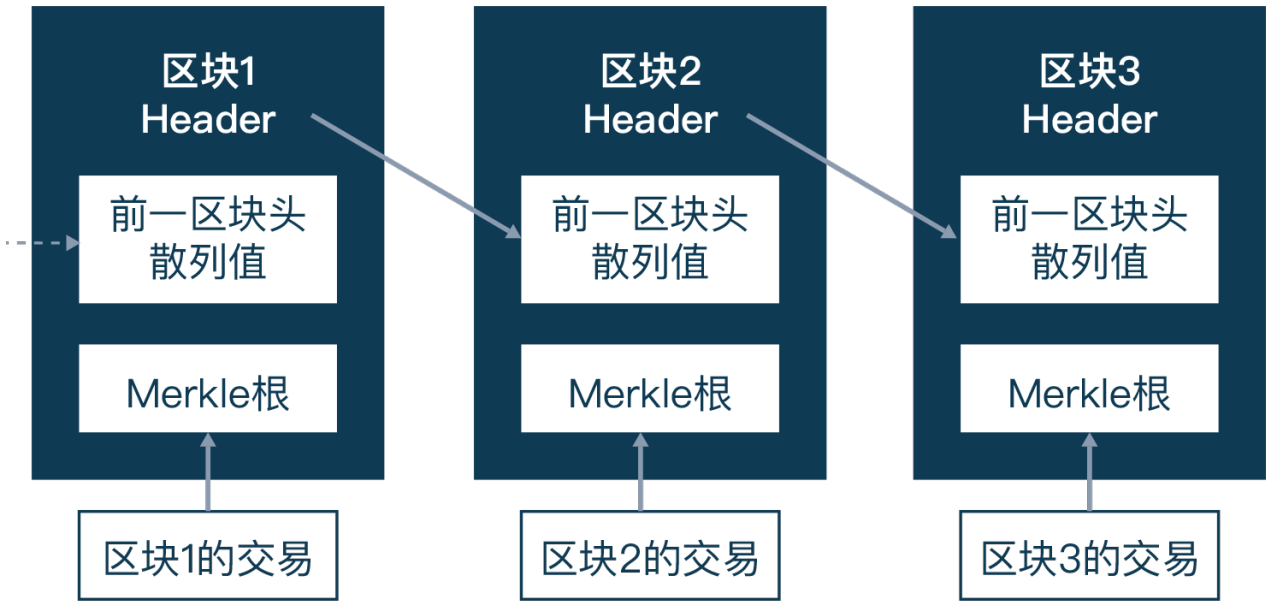


图 3.2-1 VHKD 区块链式结构

Merkle 树是区块链的重要数据结构，其作用是快速归纳和校验区块数据的存在性和完整性，如图 3.1-1 所示。VHKD 采用二叉 Merkle 树，其每个散列节点总是包含两个相邻的数据块或其散列值。Merkle 树通常包含区块体的底层（交易）数据库、区块头的根散列值（即 Merkle 根），以及所有沿底层区块数据到根散列的分支。Merkle 树是自底而上构建的，运算过程一般是将区块体的数据进行分组散列，并将生成的新散列值插入到 Merkle 树中，如此递归直到只剩最后一个根散列值并记为区块头的 Merkle 根。每个区块体中记录的交易数目大约有 1000 多甚至 2000 个。采用 Merkle 树的数据结构来记录交易信息，极大地提高了区块链的运行效率和可扩展性。

要证明区块中存在某个特定的交易，只需要找到一条从特定交易到 Merkle 根的路径即可。以图 3.2-2 所示的 Merkle 树为例，要证明交易 K 是记录在该区块中的有效区块，可以通过生成一条仅有 4 个 32 字节散列值的 Merkle 认证路径来完整验证，即（HL、HLJ、HMNOP、HABCDEFGH），如图 3.2-2 中深色标注的散列值。再计算另外 4 个散列值

(图 3.2-2 中虚线框标注)，可以通过比较计算出的 Merkle 根与记录在区块头中的 Merkle 根是否一致，来验证交易是否记录在此区块中。

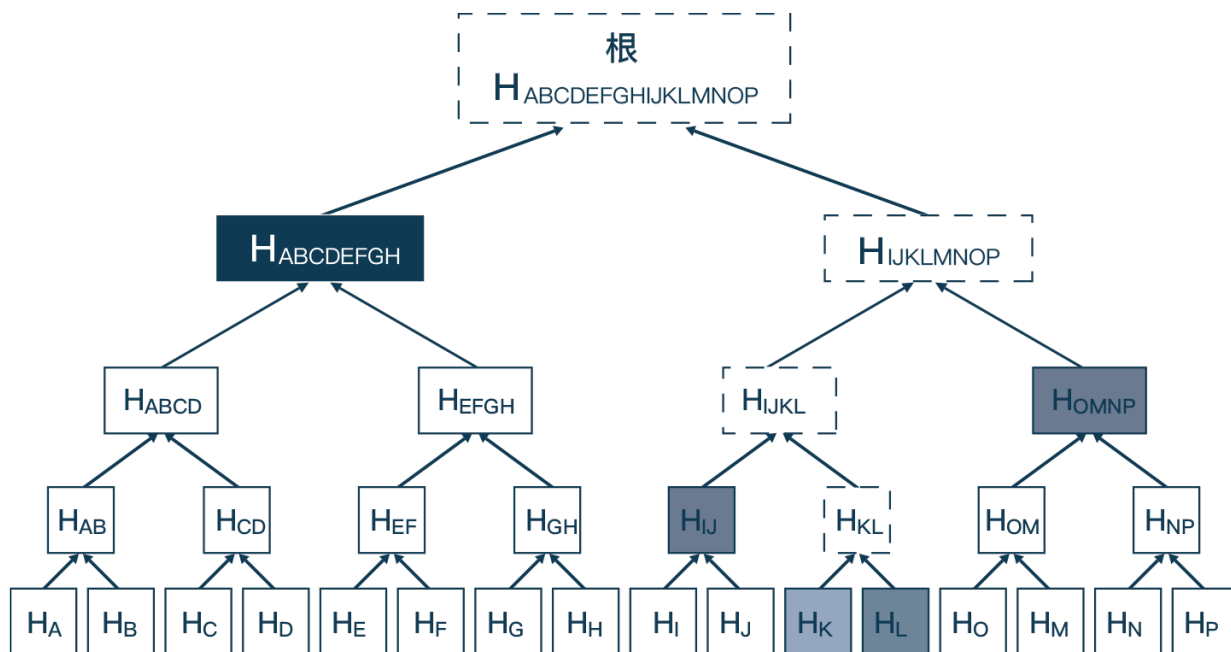


图 3.2-2 VHKD 二叉 Merkle 树路径

3.3 VHKD 分布共识机制

VHKD 采用依赖节点算力的工作量证明机制（PoW 共识机制）来保证 VHKD 网络分布式记账的一致性。工作量证明机制通过对交易的验证和结算在全网达成共识，保证了系统安全，其核心思想是通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性。

VHKD 系统中，各节点基于各自的计算机算力相互竞争来共同解决一个求解复杂但验证容易的 SHA256 数学难题，最快解决该难题的节点将获得区块记账权和系统自动生成的 VHKD 奖励。一般来说，PoW 共识的随机数搜索过程如下：

步骤一：搜集当前时间段的全网未确认交易，并增加一个用于发行新 VHKD 奖励的 coinbase 交易，形成当前区块体的交易集合。

步骤二：计算区块体交易集合的 Merkle 根记入区块头，并填写区块头的其他元数据，其中随机数 Nonce 置零。

步骤三：随机数 Nonce 加 1，计算当前区块头的双 SHA256 哈希值，如果小于或等于目标哈希值，则成功搜索到合适的随机数并获得该区块的记账权；否则继续步骤三，直到任一节点搜索到合适的随机数为止。

步骤四：如果一定时间内未成功，则更新时间戳和未确认交易集合，重新计算 Merkle 根后继续搜索。

PoW 共识机制是具有重要意义的创新，近乎完美地整合了 VHKD 系统的发行、交易支付和验证等功能，并通过算力竞争保障系统的安全性和去中心性。

04 VHKD 流通机制

4.1 资金流动流程

我们将完整的资金流动生命周期简化为 8 个阶段，如图 4.1-1 所示。

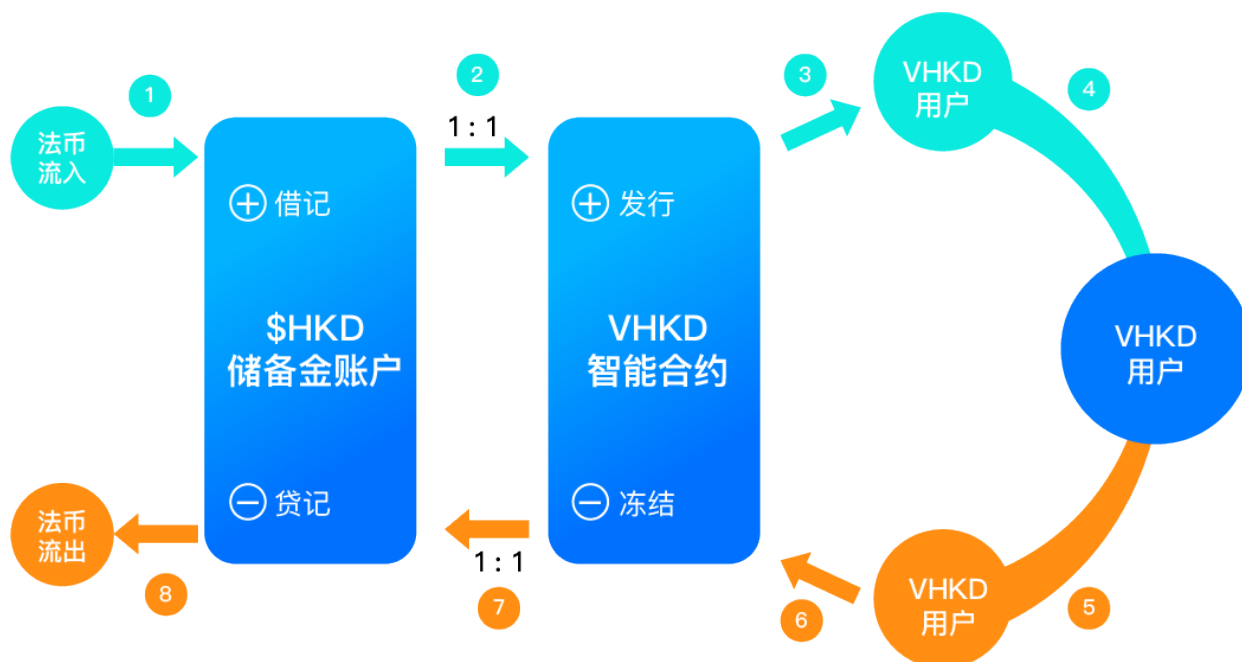


图 4.1-1 资金流动流程图

第①步：法币流入

用户通过兑换渠道将港元（或其他法币币种兑换成港元）存入 VHKD 储备金账户；

第②步：1:1 兑换

由 VDAC 完成资金核算并在多方机构进行备案，通过 VHKD 智能合约按第①步流入的

港元 1:1 发行新的 VHKD（例如有 \$100 HKD 流入储备金账户，则相应发行 100 个新的 VHKD，储备金账户借记 \$100 HKD）；

第③步：发送 VHKD

将新的 VHKD 发送至用户提供的资产地址，此时市场上就会有对应数量的 VHKD 在流通，且储备金账户资产余额 =VHKD 流通量；

第④ - ⑤步：转账交易

此时用户可以用 VHKD 进行转账、购物消费、购买其他数字货币、或用于存储等多种场景；

第⑥步：赎回申请

用户通过兑换渠道将 VHKD 发送至指定地址赎回法币，需要完成后面两个赎回流程才可以刚性兑付；

第⑦步：1:1 赎回

VHKD 智能合约将用户发送至指定地址的 VHKD 进行冻结，由 VDAC 按照此次冻结的 VHKD 进行 1:1 的 HKD 核算（例如有 100 个 VHKD 申请赎回，则会冻结此 100 个 VHKD，储备金账户贷记 \$100 HKD），并在多方机构备案；

第⑧步：法币流出

储备金账户核算无误后将港元（也可按用户要求兑换成其他法币）汇入用户指定银行账户（或支付现金），完成赎回兑换流程。我们与境外银行有深度合作，需要注意的是，因各银行规定不同，到账时间不同，具体时间依银行公布为准。

4.2 储备金机制证明

储备金的风险控制主要发生在发行、兑付两个环节，VHKD 发行与兑付环节的风险控制由其链上的智能合约及储备金审计制度完成。在发行环节上，智能合约按用户支付的法币金额规定 VHKD 的发行数量，同时储备金账户需储备等额港元法币；在兑付环节上，当用户完成兑付后，被收回的 VHKD 依智能合约会被冻结，同时储备金账户支出等额港元法币。VHKD 流通数量与银行账户储备金不仅会被多方机构备案，还会被第三方权威会计事务所按

照国际审计准则进行审计，支持区块链浏览器实时查询，定期公示审计报告，公开透明，共同监督。

接下来将介绍一种简单明了而又行之有效的创新证明机制来证明 HKD 储备金总额 \geq VHKD 流通总量，即储备金 $\geq 100\%$ ，从而证明储备金的安全性。

我们理念是在保护用户隐私的前提下，公开所有平台数据：储备金账户实时余额、VHKD 流通总数，以及所有节点数据，并由审计机构定期审计。审计过程非常严格，但同时也会保护用户的“绝对隐私”。

- 首先证明 VHKD 流通总量是真实有效的，从逻辑的完备性上讲，需要证明：
 - (1) 数据未被伪造：未伪造用户、未伪造用户余额。

因为用户数量与 VHKD 流通总量没有必然关联，所以伪造用户数量没有任何意义；用户是将港元 1:1 兑换为 VHKD，若接收到的 VHKD 数量不符，用户会第一时间发现并反馈；若伪造用户拥有的 VHKD 余额增多，会造成储备金 $<100\%$ ，相当于稀释了储备金率，得不偿失，所以不会伪造用户余额。

- (2) 用户统计未被遗漏：未直接遗漏用户、未间接遗漏用户

直接遗漏用户是指在区块链浏览器公布的数据里找不到自己，这种情况用户会第一时间发现并反馈；间接遗漏用户是指两个或两个以上用户对应的是同一条数据，上文提到过 VHKD 采用二叉 Merkle Tree，Hash 算法保证每个 User_id 字段唯一且固定不变，具有天然的唯一性且不可伪造。构建完 Merkle Tree 后，根节点的余额与区块链浏览器公布的地址余额相同，即可证明用户未被遗漏且余额准确。

以上两点即可证明 VHKD 流通量真实有效。

通过图 4.1-1 资金流动过程图可以得出以下观点：我们把新发行的 VHKD 命名为 N_VHKD，把冻结的 VHKD 命名为 F_VHKD，流通中的 VHKD 命名为 C_VHKD，三者之间的逻辑关系在任何时间都应为：

$$C_VHKD=N_VHKD - F_VHKD$$

其中 C_VHKD 可直接在区块链浏览器中查看实时数据，即 VHKD 实时流通量总额。

- 其次论述 VHKD 与 HKD 法币 1:1 的逻辑关系：

(1) 将用户购买 VHKD 而流入储备金账户的港元命名为 In_HKD，此时会有 1:1 发行新 VHKD，即 $In_HKD = N_VHKD$ ；

(2) 将用户赎回港元而流出储备金账户的港元命名为 Out_HKD，此时会有 1:1 冻结的 VHKD，即 $Out_HKD = F_VHKD$ ；

(3) 将储备金账户实时余额命名为 R_HKD，则有 $R_HKD = In_HKD - Out_HKD = N_VHKD - F_VHKD = C_VHKD$ ，即 $R_HKD : C_VHKD = 1:1$ ，在任何时间流通中的 VHKD 总量与储备金账户的余额都是 1:1 的关系，逻辑关系成立。

- 最后要证明储备金账户余额 (R_HKD) 是真实有效的，我们选择被第三方权威会计事务所按照国际审计准则进行审计，并支持公开查询。审计流程有以下步骤：

- (1) 审计者核查 VHKD 全部流通中的资产：

VHKD 会向审计者提供所有公开的地址，并对这些地址进行签名。签名时的区块哈希将是签名信息的一部分，因此能够被当做时间戳证明签名的时间。这些签名的了的公开地址将在随后被确认，审计者将通过 VHKD 区块链去获得这些地址在某个时间点的所有 VHKD 数量；

- (2) 审计者审查 VHKD 储备金账户余额与 VHKD 全部流通中的资产一致性：

VHKD 会向审计人提供每一个用户通过 Hash 算法加密处理的地址信息而生成 Merkle 树。审计人将公布 Merkle 树根节点的哈希，并确认储备金账户的港元总余额大于所有流通中的 VHKD 数量。

- (3) 用户自行确认他们的账户被包含在了审计人获得的数据之内：

我们将向用户提供审计时用户地址的 VHKD 数量，以及到根节点上的所有节点哈希。我们也将提供产生这些节点哈希的具体方法，用户可以确认自己的 VHKD 被包含在本次审计当中。

- 用户可以查看审计者审核过的地址信息

(1) 审计时间：也就是审计者使用的时间戳显示的时间。

(2) 用户 ID：是用户在系统内唯一标识符。

(3) 随机数：是这次审计为每个用户随机生成的数，当下次审计时，即使用户地址余额不变，生成的用户节点哈希也会变化。

(4) VHKD 数量表示在审计发生时您地址所拥有的 VHKD 数量。这是我们向审计者提供的您地址的资产信息。

(5) 备注由审计者公布的用户审计的根节点哈希值信息。

(6) 资产证明是你的节点到根节点的所有哈希，以及相邻节点的哈希。在直接路径上的哈希值显示时有一个 * 号，用来区别相邻节点的哈希值。通过这些哈希，你能确认你的节点被包含在这个根上。

4.3 挑战与应对方案

政策风险：作为一项创新型技术，VHKD 要实现与现有货币金融体系的融合可能会面临不同国家复杂的法律和合规问题；我们了解到各个国家的监管机构对数字资产的监管与规范采取了多种方式，包括根据某些实际业务内容，将数字资产定义或归类为虚拟货币、加密货币或数字货币。我们认为 VHKD 是一种新兴的创新型另类资产，因此数字资产不应被称为钱或货币。然而，由于我们服务于想用港元（HKD）结算的用户，且因此接入了法定货币的金融体系。在不同时期我们可能会对各政府机构所采取的监管方式有些分歧或误区，但是，我们会一直全面遵守各国的规章制度，并定期与监管机构和同行探讨数字资产业务的最佳方法。在任何一个 VHKD 流通的地区，VDAC 都将遵守当地的相关法律法规，包括但不限于注册、审批、备案等相关手续。

存在安全漏洞风险：用户可能会被盗币。安全漏洞的出现有两种可能：一是 VHKD 区块链的安全依赖于散列函数、椭圆曲线等非对称密码算法，然而随着数学、密码学和量子计算技术的发展，传统密码学中的一些基本安全假设，可能会变得越来越脆弱，但是如果 VHKD

区块链上的密码被破解，那就意味着所有数字货币（包括比特币）将被破解，以目前的科学发展阶段来看，这种情况不会出现；二是用户在不安全的钱包或交易所存储 VHKD，导致被盗，这种情况出现的可能性最大，因为私钥在用户手上。

储备金账户可能被冻结：这个风险与其他传统的金融机构一样都可能会面临，但是请放心，与我们合作的银行机构也在为其他交易所和钱包服务商提供服务，并且我们已经得到合法合规的承诺保证。此外，我们不会违反各国银行法律规定，以保护我们的声誉和用户。

资不抵债破产风险：可能会因公司经营不善出现破产风险，但是 VHKD 的储备资金是安全的。若出现破产情况，我们会将市场上流通的 VHKD 全部赎回，并从储备金中按 1:1 向用户支付法币，银行账户出入金流程是受严格的内部政策约束的。

05 VHKD 发行方案

5.1 方案介绍

VHKD 采用代理承兑发行方案，一级市场（即授权商）全部交由 Virtual Digital Asset Corporation (VDAC) 发行。VDAC 是由多个世界顶尖金融集团发起的联盟组织，联盟成员来自全球各地，以国际商业公司形式注册于塞舌尔共和国；VDAC 先后在中国大陆、香港、澳门、美国、法国、西班牙、日本、韩国、越南等几十个区域设立了服务网点，服务范围覆盖东亚、东南亚、欧美等区域，在实现跨境汇款、价值跨境转移上具有得天独厚的优势。用户可以通过任意网点随时购买 / 兑换 VHKD，资金来去自如，且无价格波动风险。

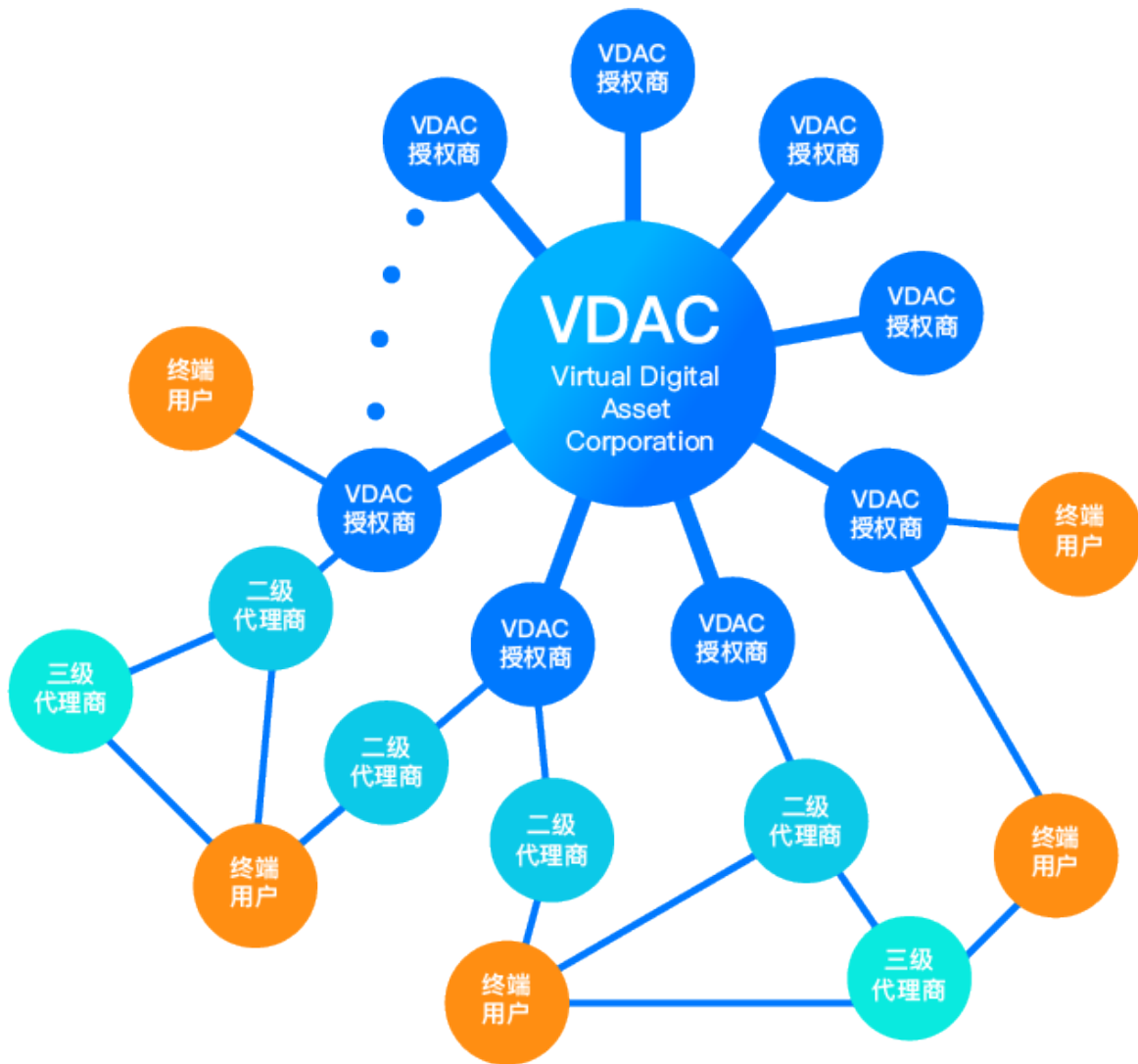


图 5-1 VHKD 发行方案

5.2 发行优势

采用授权代理发行方式的优势有：

- (1) 通过代理制的承兑约束，保证 VHKD 与 HKD 的兑换比例维持平稳，避免出现类似 USDT 波动大的问题；
- (2) 以 VHKD 为基础的承兑通道建立在众多国际机构的经济网络上，这些机构的相互协作使得交易能够与现实世界快速交融，为世界各地不同需求背景的用户提供更加快速、便捷的金融服务；
- (3) 省去银行中间环节，跨域资金自由流动，这将会填补银行领域的巨大空白。

5.3 日常运营管理

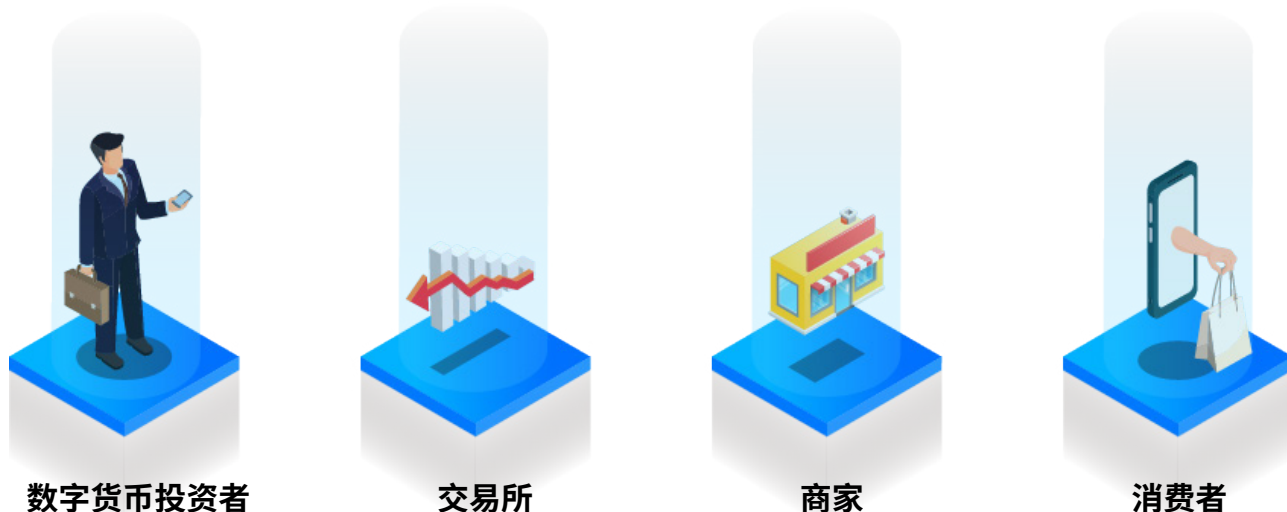
VDAC 的日常运营主要分为财务管理、市场推广及法务事项。联盟成员将通过以下各项控制活动对日常运营进行管理，但各项控制活动不仅限于此：

管理内容	职责描述	审核机构
财务管理		
运营预算审核	每年制定VDAC运营预算，由联盟成员财务管理委员会负责审核。	联盟成员财务管理委员会
合同签订	合同条款经过审核后，由决策委员会审核，审核后由VDAC执行合同签订。	决策委员会
收入审核	VDAC的收入来源主要是提供商业服务，由联盟成员财务管理委员会进行核准并记录，由独立人员进行对账。	联盟成员财务管理委员会
支出审核	VDAC所有支出需经过联盟成员财务管理委员会审核，并做好相关账务处理。	联盟成员财务管理委员会
账务处理	账务处理应由联盟成员财务管理委员会负责审核，并且每月形成财务报告。	联盟成员财务管理委员会
披露事项	定期披露资金使用情况，VHKD的落地情况应定期向联盟成员汇报。披露事项需经过决策委员会审批。	决策委员会
市场推广		
新增推广渠道	由PR管理委员会对新增推广渠道进行调研，经过调研后审批确定新增的推广渠道。	公共关系管理委员会
推广服务合同签订	新增推广服务渠道，需要经过PR管理委员会审批后签订合作协议。	公共关系管理委员会
危机公关处理	维系投资者关系，当出现紧急事件，需要由PR管理委员会商讨公关处理，由决策委员会同意后方可对外披露。	公共关系管理委员会
法律支持		
合同的拟定与审核	由独立法务机构对各类业务合同条款进行审核	法务支持委员会
法律咨询	确保VDAC的业务开展符合各个国家的法律、法规的基本原则，符合该国政策	法务支持委员会
法务处理	代表VDAC处理各类诉讼或非诉讼法律事务，维护联盟成员的合法权益	法务支持委员会
法律事务外联	参与重大事故的处理工作，解决已发生的法律问题，负责与外聘律师、法律顾问的联络、配合工作。	法务支持委员会

行业合作是我们成功的关键，VDAC 将提供透明的财务管理，聘用第三方机构提供相关工作审计报告，合规治理和监督，并保持高标准的诚信和道德的商业行为，遵守相关的法律法规，协助 VHKD 进行商业落地。

06 主要应用场景

6.1 VHKD 目标用户



- **数字货币投资者：**VHKD 是一种很好的保值避险工具，可以让投资者更从容的面对突发行情，搬砖套利更便捷；
- **交易所：**接受 VHKD 作为充值手段增加了一种入金方式，可以规避存储法币带来的不便之处，省去与银行对接的时间成本和人力成本，提高交易效率和转账速度。
- **商家：**作为兑换商，则有可能成为多家交易所的充值代理。VHKD 实时到账，减少传统金融机构手续费负担，并能帮助用户解决数字货币变现的难题，增加店铺额外收入，提高经营效益。
- **消费者：**可在兑换网站或线下门店充值港元，兑换商按照用户的指示直接将 VHKD 打入到用户提供的地址，完成充值。跨境资产来去自如，不受任何机构限制，方便携带。

6.2 VHKD 购买 / 赎回渠道

(1) 如果用户持有数字货币，可以在支持 VHKD 的数字货币交易所购买 VHKD，同时也可以通过相同渠道将 VHKD 兑换其他数字货币。



图 6.2-1 持有数字货币购买 VHKD

2. 如果用户持有法币，可以在支持 VHKD 的数字货币交易所（C2C）购买，也可通过线下合作商家店铺购买，同样支持相同渠道赎回法币。

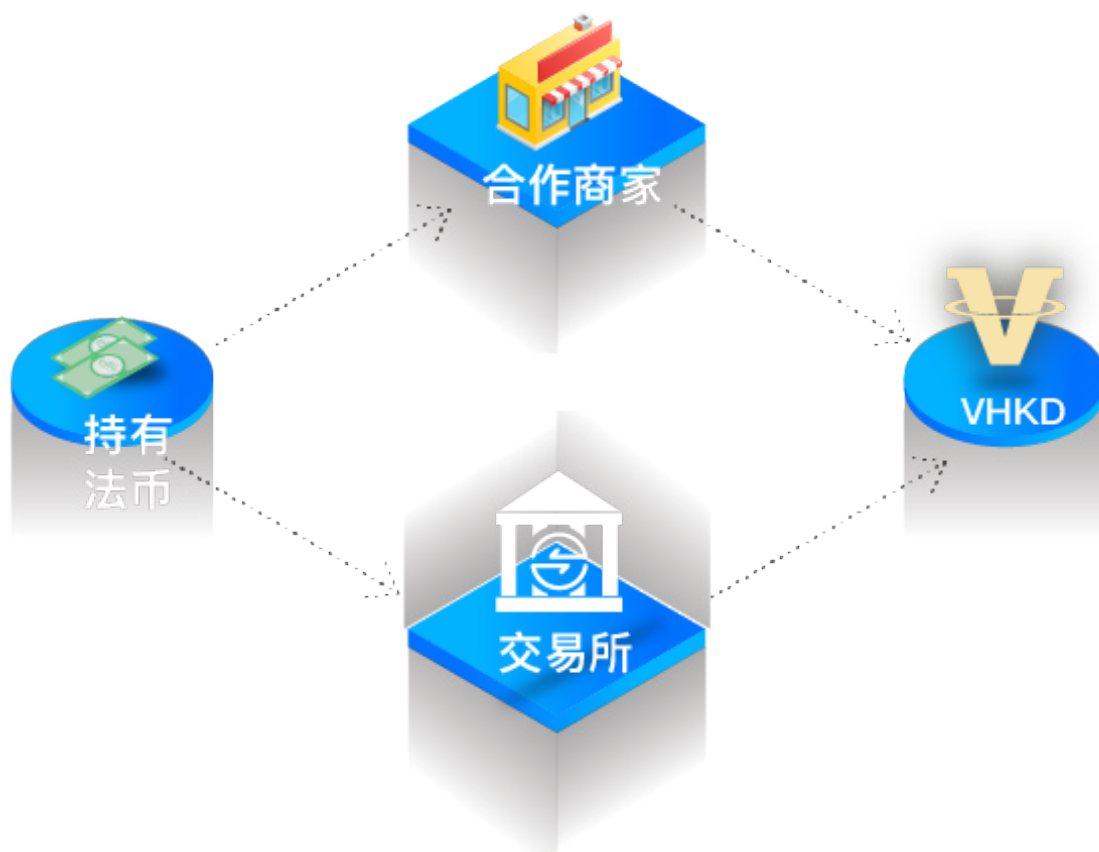


图 6.2-2 持有法币购买 VHKD

6.3 场景应用

在区块链出现之前，我们一直无法在不借助于第三方授信机构的情况下，通过互联网

进行点对点的价值的转移和传输。随着区块链技术的成熟，区块链的应用场景不仅限于购买数字货币，VHKD 将区块链链上和链下相结合，形成全新的区块链商业生态。

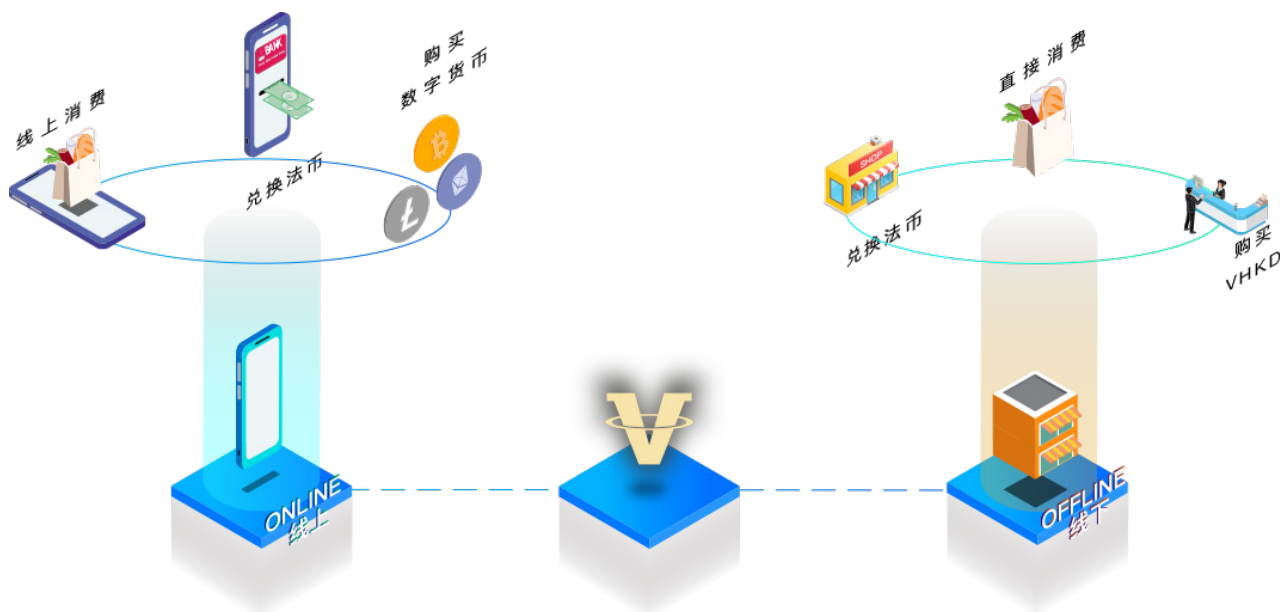


图 6.3-1 丰富的应用场景

VHKD 在香港、澳门、东南亚及欧美等地区有丰富的应用场景，如品尝美食、购买名表、澳门娱乐消费等等，用户还可以网上购物支付账单。VHKD 打通了数字货币和现实世界的连接障碍，其设计初衷就是为了解决用户多种资产管理不便、兑换交易过程繁杂和应用场景不足的问题，让数字资产真正应用到现实生活中。

07 未来规划

VHKD 致力于构建全球数字货币自由流通体系，提供下一代跨货币价值转移服务。我们的规划不仅仅停留在兑换港元层面，而是将 VHKD 定位于 1.0 阶段，未来将以韩元、日元、欧元等全球各大主流法币为切入点和基点，加入更多的创新元素，进而构建面向全球数字货币市场和外汇市场的全新货币生态体系，重塑经济与世界。

08 附录

8.1 VHKD 的法律结构

针对 VHKD 项目，Virtual Digital Asset Corporation (VDAC) 将作为独立的法律主体管理 VHKD 储备金，并全权负责 VHKD 的开发，技术，发行，维护，安保和宣传任务。但 VHKD 本身的运营和管理均完全取决并依赖于联盟成员社区自治，VDAC 只作为执行者，对 VHKD 的治理提出建议和方案，但并不享有超自然的或高出其他成员的权利或权威。

VDAC 在提供商业服务时所获得收入，将由 VDAC 无条件的自由使用，主要用于技术开发、市场营销、法律合规、财务审计、商务合作等用途。

VHKD 是建立在区块链上的完全分布式数字资产，全球任何人均能且只能通过消费 VHKD 来使用其功能，不受地理位置所限。VHKD 不具有物理实体存在，但依然很有可能会在全世界不同国家受到主管机构的质询和监管。为了满足和遵守当地的法律法规，VHKD 可能会在有些区域无法提供正常的服务。VDAC 将会尽力争取“沙箱政策”（sandbox policy）或者安全港待遇，为用户提供尽可能全面优质的服务。

8.2 风险声明和免责声明

除本白皮书外，VDAC 不对 VHKD 做任何陈述或保证（尤其对其试销性和特定功能）。任何人参与 VHKD 的承兑行为均基于其本身对 VHKD 的知识和白皮书信息的完全了解。在无损于前述内容的普适性的前提下，所有参与者将在 VHKD 项目启动之后按现状接受 VHKD，无论其技术规格、参数、性能或功能等。

VDAC 在此明确不予承认和拒绝承担下述责任：

- (1) 任何人在购买 VHKD 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；
- (2) 任何人在购买 VHKD 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取 VHKD；
- (3) VHKD 开发的推迟或延期，以及因此导致的无法达成事先披露的日程；
- (4) VHKD 源代码的错误、瑕疵、缺陷或其他问题；

(5) VHKD 未能实现任何特定功能或不适合任何特定用途；

(6) 未能及时且完整的披露关于 VHKD 开发的信息；

(7) 任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥（尤其是其存储 VHKD 的钱包私钥）；

(8) 任何人与第三方平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；

(9) VHKD 在任何交易所或承兑点的上市或退市；

(10) VHKD 被任何政府、准政府机构、主管当局或公共机构归类或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制；

(11) 未经授权认领 VHKD，或任何通过解密或破解 VHKD 购买者密码而获得的使用权限；

(12) 本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

09 参考

- 1.Nakamoto S. Bitcoin: A Peer-to-peer Electronic Cash System[J],Consulted,2009.
- 2.Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [M]. O’ Reilly Media Inc.,2014.
- 3.Narayanan A, Bonneau J, Felten E, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction [M]. Princeton University Press,2016.
- 4.Morabito V. Business Innovation through Blockchain: The B3 Perspective[M]. Springer,2017.
- 5.Walport M. Distribute Ledger Technology:Beyond Blockchain[R].Tech Rep,2016.
6. 中国区块链技术和产业发展论坛 . 中国区块链技术和应用发展白皮书 , 2016.
7. 谭磊 , 陈刚 . 区块链 2.0[M]. 北京 : 电子工业出版社 , 2016.
8. 朱建明 , 高胜 , 段美姣 . 区块链技术与应用 [M]. 机械工业出版社 , 2018.
- 9.<https://www.coinmarketcap.com/>