完美的交易所安全与速度解决方案

白皮书（Beta）

Version 1.7.1

最终以官网公布的白皮书为准

目录

摘要

BITARK 首创黑客免疫交易技术 BITARK KO SOLUTION，旨在为全球的交易所提供百分之百杜绝黑客入侵，以及千万笔/秒的超高频交易解决方案，只需要 7-10 套服务器，便可服务全球 224 个国家和地区。

BITARK KO SOLUTION 是从底层 CPU，到密钥机，到操作系统，再到密钥策略管理系统、用户管理系统、分布式容灾管理中心等系统软件实现软硬件完美结合，为数字加密货币交易所提供终极安全保障的解决方案。

我们已经打造一个示范性的交易所——BITARK，并将于今年夏天发起百万美元黑客悬赏活动，以事实来证明我们技术的可靠性。

BITARK 交易所已经启动欧盟体系的布局与注册工作，2018 年 1 月即进入上线部署的测试阶段，BITARK 上线后将开发部署人工智能客服和人工智能投顾。

一、数字资产市场概况

1.1 数字资产市场现状

随着区块链 ICO 的爆发，数字资产交易的活跃度和交易量呈井喷式增长。根据数字资产市场统计网站 CoinMarketCap 在 12 月 7 日的数据显示，数字资产币种数上千种，总市值超过 2 万 7 千亿人民币，与 2017 年年初 100 亿总市值相比增长了 270 倍。

1.2 数字资产交易所现状

CoinMarketCap 12 月 7 日的数据显示全球的交易所数量超过 7185 所。其中，中心化数字资产交易所是当前市场的主流模式，其交易过程：用户将法币或代币充值到交易所的银行账户或钱包地址中，交易所对用户账户进行 IOU 记账，类似白条，用户之间交易的是白条，用户向交易所申请提现，资产提现成功后，才真正完成其交易。在提现之前，用户要承受交易所安保能力、数字加密货币和法币托管能力以及运营者商业道德三重风险。同时，该方式下数据进出、响应效率、准确性等交易所核心要素难以匹配实际市场需求。许多交易所面对快速增长的业务，因不堪重负而出现卡顿或掉线等现象，造成用户体验差。

虽开源社区已有基于区块链技术搭建的分布式交易所，如 Ripple、BitShares、Openledger 等，但去中心化交易所存在交易效率太低、用户体验太差等缺陷，以至于无法满足市场需求。因此对去中

心化交易所的需求开始凸显出来，但类似 EtherDelta 交易所还远不能满足市场需求。

随着全球数字资产在短期内的飞速发展，给参与者带来巨大收益，也吸引了大量新用户参与数字资产交易。与此同时，随着 ICO 等方式融资的火爆，每天有数百万甚至数千万美元的新数字资产被创造出来，交易需求急速增长，中心化交易平台存在的问题也被更多人所关注，其中亟待解决的问题包括：

1.入侵盗窃风险：中心化交易所，其硬件采用通用型服务器，软件多数采用开源的 Linux 操作系统，而这些都是黑客攻击的重点对象。由于开源软件、服务器托管、内部人员作案等等因素，交易所无法百分百避免黑客攻击，以保护用户资产安全。交易所安全事件几乎每年都在上演，比如著名的 Mt.Gox 事件，造成灾难性后果，直接导致交易所倒闭，用户资产丢失。（可参考附件一）

2.易受攻击：无论中心化交易所或分布式交易所，都很容易遭受网络阻塞或 DDOS 等拒绝服务攻击。特别是中心化节点的存在，容易成为被攻击的焦点，需花费巨大代价来避免拒绝服务攻击，而成本终将由平台用户来承担。

3.承载风险：现有所有交易所都是采用普通服务器来构建，服务器集群规模越大任务执行效率就越低，且没有做全球范围的分布式布局（服务器集群的数据同步是一个大问题），导致交易所的承载不能满足市场需求。譬如 2017 年 12 月 1 日，最离奇的暴跌发生在全球最大交易所 Bitfinex，许多币种跌幅一度达到 90%，几近归零。迄今尚

无证据显示此为交易所人为造成，其有可能是负载太大，超过交易所承载能力，导致交易数据错误，引发用户抛售。此类案例近年来比较多。

4.决策风险：去中心化交易所，在执行决策时易发生决策失误。即便有技术手段保证财产安全，也需耗费时间处理，造成潜在的损失。

二、BITARK KO SOLUTION 技术解决方案

2.1 打造金融级安全性交易平台

三类安全保障

交易所最核心的要求是确保资产存储及交易安全。依托强大的技术团队，我们从底层布局，采用软硬件结合的方式，打造金融级安全解决方案 BITARK KO SOLUTION，以确保加密货币交易所安全。

计算机世界里，凡是软件都有漏洞！单靠软件保护存储安全是不可靠的。我们将采用软件和硬件结合的方式，以金融级安全措施隔绝黑客。

1. 硬件保障：

1）定制 CPU：从最底层计算机硬件开始布局

独立设计专用指令集，在主机里运行的程序必须通过自主研发的编译器编译方可运行，黑客采用通用的编译器编译的程序将无法运行，这从根本上杜绝一切可能存在的入侵行为。

2）金融级密码机：先进密钥管理技术

主要用于实现对主机应用层数据加解密、消息来源正确性验证、密钥管理等，是金融数据安全保护级别的一种有效物理工具，具有完善的密钥管理体系，其特点：能提供由全硬件噪声源产生的真随机密钥（其它交易所提供的均为伪随机密钥）；能有效防止通信信道上的主动攻击行为；以物理方式封闭敏感信息使其变为不可读信息；硬件芯片在遭遇拆解时具有自我销毁功能；符合 FIPS 140-2 Level3 国际标准，具有高安全性。

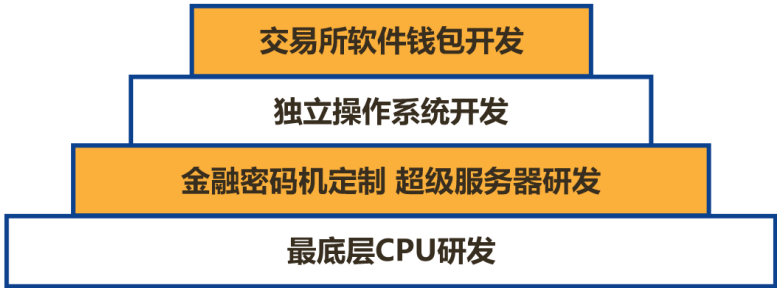
3）专用 U 盾：多重安全保障

专用 U 盾与密码机等设备实现物理隔离用户核心信息和私钥，硬件芯片在拆解时均具有自我销毁功能，没有用户的安全设备，即便窃取硬件也无法从芯片中获得私钥，从而确保用户资产安全，杜绝可能的监守自盗。

2. 软件保障：

操作系统和交易所软件全部为独立自主开发的非开源软件，如钱包、交易系统、密钥策略管理系统、用户管理系统、去中心化式存储管理系统、去中心化容灾管理中心等等。在文件和通讯层面采用多种加密保护手段、双因子认证机制等交叉保护系统，使黑客无法侵入到操作系统，不给黑客任何可乘之机。

在文件层面、通讯层面也采用多种加密保护手段，确保层层严防死守，滴水不漏。



BITARK 安全金字塔模型

3. 策略保障：

1）分布式部署：避免数据安全隐患

采用去中心化模式的管理模式，系统分布式部署、多重签名及银行式授权操作机制，以保证安全，其中服务器采用分布式部署，多节点数据备份，确保数据安全，充分避免由于地域环境突发状况造成的安全隐患。

2）多重授权管理：杜绝内部交易隐患

交易所系统采用多重签名及银行式授权的操作管理机制，避免监守自盗。

3）欧盟 CC 认证：世界权威认证背书

软硬件安全性方面，已经邀请国内顶级安全专家为我们制订认证计划，国内的安全认证基础工作已经部署到位，欧盟安全认证也已经纳入计划之中，将以相关认证佐证 BITARK 无懈可击的安全性！

（关于通用评估准则 Common Criteria，简称 CC，请参考附件二。）

4）全球黑客大赛：用事实证明安全

BITARK 将携带团队研发的区块链交易安全技术，参与新一届的全球黑客大赛，进行“百万现金求黑”活动，用事实来证明我们核心技术的安全性能！

2.2 超高速交易性能

专用服务器

高速分布式算法

底层私钥智能识别技术

三项极速体验

1. 专用服务器

超高性能服务器，在芯片上优化 CPU 指令集以电路实现超速计算；在服务器内部，以带宽取代频率，优化通讯；在服务器群组上，以物理分组，计算与加密解密工作由特定机器执行。可避免因不断增加服务器数量，而导致任务执行效率降低。BITARK 专用服务器采用自主研制的 128 核 CPU、并配置 256G 内存及 2 个万兆网口。目前 BITARK 交易系统测试已达到 1 千万笔/秒的交易速度，且不出现卡顿、挂机等现象，可以满足用户高频交易需求。

2. 高速分布式算法

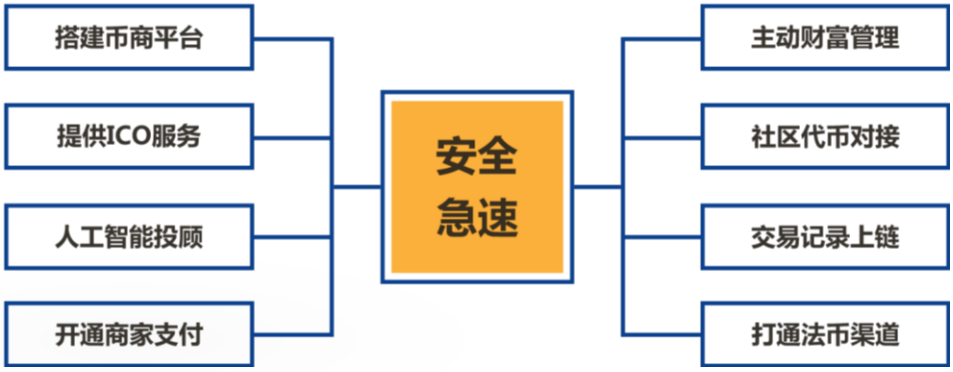
服务器群组物理分工，计算与加密解密工作，分别交给特定机器；大大提高工作效率。7-10 台服务器就可以布局全球提供服务。

3. 底层私钥智能识别技术

私钥无需像其它交易所那样加解密保存和调用，就无需在高频的加解密上耗费大量的计算资源，使得我们的服务器在速度上超过使用

普通商用主机和 Linux 系统的交易所。

三、BITARK 多功能服务延展



双核心驱动八项服务延展

3.1 人工智能投顾和人工智能客服

在 7×24×365 区块链交易市场中，客户耗费大量的时间和精力用于盯盘操盘等。对此，我们将采用人工智能，依靠交易所数据喂养，开发人工智能投顾工具，实现智能化操盘。届时客户既可使用传统方式操盘，也可设定智能助手辅助操盘，大大节省操盘时间。并将提供一系列的智能投顾策略，如通过比较收益率跟投其它智能助手，以获得收益及时效的最佳平衡点。

目前已经开发好人工智能客服的原型，在交易所运营后不久，即可通过短时间的迭代，完成人工智能客服的部署。我们的人工智能客服主要给客户提供交易问题的解答，以及数字加密货币方面的基础知识答疑。

3.2 交易记录上链

BITARK 交易所的所有记录都将通过区块链技术进行公开，主要为：

1. 所有交易记录都通过区块链技术进行分布式记录。

2. 将采用多条具有公信力的主链，进行交叉多头的交易记录。

3. BITARK 交易所可提供交易记录的对外 API 接口。

3.3 主动财富管理

BITARK 已经获得很多数字资产基金的支持，会形成一些优质的收益项目，我们将其收益率按照其对应的风险权重细分，根据客户的风险偏好，形成短期、中期和长期的加密货币资产包组合，动态匹配各种不同的投资者各阶段固定收益+浮动收益的投资需求。

3.4 搭建币商平台

OpenBazaar 平台是区块链领域唯一可用的 B2C 在线商场，但其页面加载非常慢，用户体验糟糕。我们将构建与交易所一体化的币商（Crypto-Commerce）平台，不仅提升消费体验，还可使用上架 BITARK 交易所的任何代币进行支付。产品可通过简洁的区块链业务逻辑销售到全球各地。

3.5 提供公开募集服务

我们将为客户的产品或品牌设计及公开募集提供服务，将其代币

将上架 BITARK 交易所。这样公开募集服务和币商平台就能遥相呼应，完成商家业务的闭环。

3.6 打通法币渠道

BITARK 团队已经研发了一款交易便捷的 OTC 交易系统，可以快速地进行 OTC 撮合交易，让法币与数字资产以最佳的方式进行迅速的价值交换。

3.7 社区代币对接

通过制定完善的社区代币奖励规则，将社区进行代币化，同时对接数字货币交易所，促进数字资产流转，区块链生态搭建。

3.8 开通商家支付

对接全球线上线下支持代币支付的商家，加速加密货币支付历史进程。

四、BITARK 代币设计及销售规划

4.1 代币设计

BITARK 提供 BARK 上限 100 亿枚，且永不增发。

BARK 为标准的 ERC20 代币。ERC20 的功能由 StandardToken 合约提供，包括安全检测在内的基础数学函数由 SafeMath 合约提供。

4.2 代币作用与回报机制

1.抵扣平台交易手续费

平台用户在发生交易费时，如使用 BARK 支付交易手续费，即可享受相关的优惠政策。具体执行标准见下表：

	第一年	第二年	第三年	第四年	第五年
折扣	50%	25%	12.5%	6.25%	无

2.接入平台的“燃料”

为确保平台的扩展性，平台将开放 API 接口，硬件服务等一系列接入服务，完善自我生态，与现有法币交易所接入时，BARK 将充当“燃料”特性，如对外提供 BITARK KOSOLUTION 解决方案将以 BARK 进行结算。

3.回报机制

交易所正式运营后，每个季度依据以下标准，将整个项目净利润的不低于 X%（见下表）用于回购 BARK 币，并全部烧毁，以回报所有持币用户。回购与烧毁记录将会第一时间公布，用户可通过区块链浏览器查阅，确保公开透明，直至销毁到剩余一半 BARK 币为止。

	一季度	二季度	三季度	四季度	五季度起
净利润回购率	40%	30%	20%	10%	10%

此后，每个季度我们会将整个项目净利润的 10%纳入社区发展基金。社区发展基金以 DAO（去中心化自治组织）的模式独立运作。

任何人都可以发起帮助 BITARK 发展的提案，提案通过则相应的资金就会马上拨付到帐。

4.3 代币分配比例及销售细节

BITARK 将于欧洲时间 2018 年 1 月 25 日在 BITARK 官网众筹，代币分配比例如下：

时间：BITARK 众筹时间暂定于欧洲时间 2018 年 1 月 25 日至 2018 年 2 月 5 日（结束时间）。

众筹：15%BARK 币（即 15 亿）用于众筹，兑换比例：1ETH=40000BARK，众筹目标 3.75 万个 ETH；

决策委员会：10%BARK 代币（即 10 亿）用于激励市场推广，基金会建设等，每月释放 20%；

顾问团队及私募：10%BARK 代币（即 10 亿）用于早期投资者，在公开众筹后锁定 6 个月；

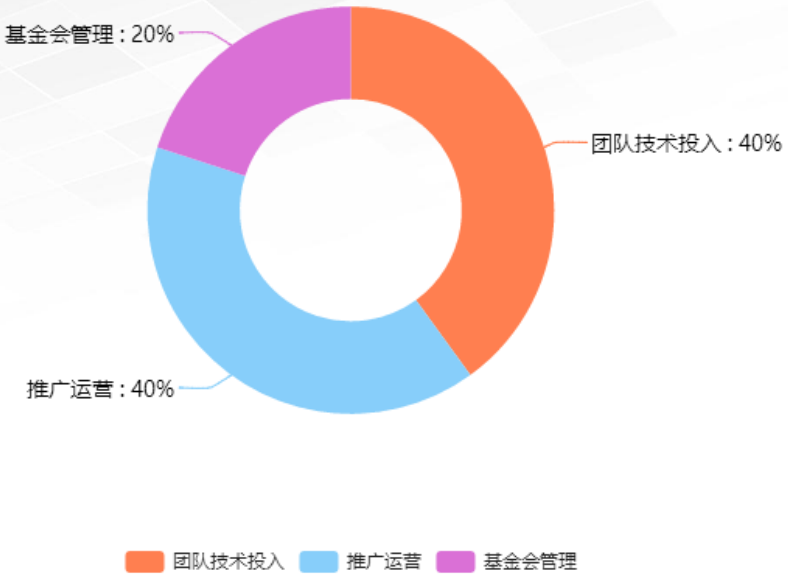
BITARK 团队：15%BARK 代币（即 15 亿），在公开众筹后锁定 12 个月；

代币燃烧：50%BARK 代币（即 50 亿）将用于系统固定收益比例的燃烧销毁，直至销毁完为止。BARK 将于燃烧机制结束后，上线多家交易平台。

4.5 资金使用计划

公开发售的资金，40%用于作为团队建设、产品开发、硬件投入；

40%用于运营推广，确保快速进入市场并累计客户；20%用于储备金，并交由 BITARK 基金会管理。



1.团队技术投入

第一阶段：完成香港、新加坡及欧洲的数据中心部署；

第二阶段：完成美、澳洲一体化部署的同时，建立欧洲研发中心。

2.推广运营

1）与现有代币项目合作；

2）与新立项目合作；

3）与传统金融市场合作。

3.产品方案

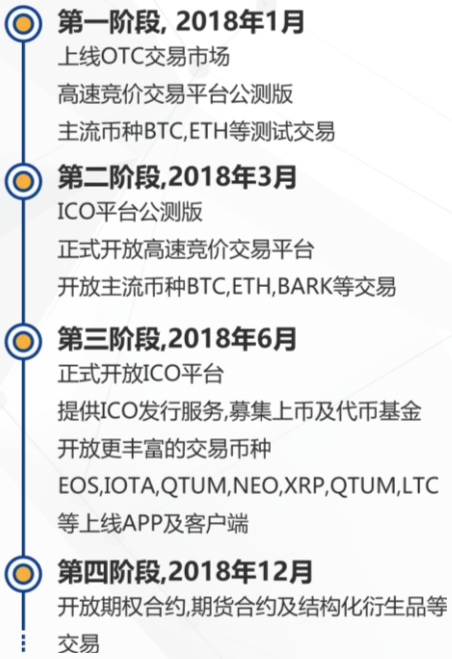
项目完成所有传统市场的所需的金融服务，如现货、期货、杠杆、期指等产品，同时探讨、研发适合区块未来可能出现的产品服务。

五、历程 & 规划 & 团队 & 顾问

5.1 历程

路线图

5.2 未来发展规划



未来发展规划图

5.3 核心团队

李于晨

奥克兰理工大学计算机科学、工商管理学士学位。比特币社区早期参与者，以太坊社区忠实爱好者，对区块链、物联网领域有深刻的研究。多年中国、日本大型上市公司高级管理经验。

李戈

法学学士学位，曾任职 DACA 区块链协会、微金融五十人论坛， 组织翻译并出版中国第一本中文区块链书籍《区块链：新经济蓝图及导读》，组织区块链主题演讲和学术交流活动五十多场；并参与策划清华大学 iCenter 区块链课程的设计和教学；参与举办 2016 微金融峰会区块链主题论坛；2017 贵阳数博会区块链主题论坛。先后承接多个国内外知名区块链项目的运营和推广。

丁丁

四川大学计算机科学与技术学士学位。领导某国有大型企业通讯设备研发，其单项成果达到行业全球第一；研发多个通讯系统项目应用于国际 500 强企业、政府、银行以及国有大中型企业。对密码学、区块链、物联网、AI、大数据有深刻的系统研究。

赵立宇

佳木斯大学材料成型及控制工程学士学位，日本东京大学宏观经济学

研究生。曾任富士康高级工程师，负责苹果手机全系列设备监制开发。担任三菱电机华南区经理期间，负责 SMT 手机项目管理及新市场开拓，热衷新技术在制造业领域的开拓。

林建峰

厦门大学软件工程学士，热衷于开源技术的开发与应用，擅长软件工程项目管理，精通 web 技术、底层技术及区块链技术。多年在某商业银行提供技术支持，负责软件开发及项目管理，并有丰富的区块链实践经验。

5.4 项目顾问&投资人

周朝晖

复旦大学毕业，中国狗狗币协会副会长、世界区块链基金会（WBD）投资研究员、DACA & 清华大学 iCenter 特聘讲师，DACA 区块链协会“区块链大学行”的公益宣传演讲的主讲老师之一。

累计各类演讲十几场，投资五十几个区块链项目。

主编：《如何投资数字货币》、《狗狗币：最宝贵的人生财富》

参编：《区块链开发与实例》、《区块链技术基础和应用实践》

在编：《ICO：1 分钟区块链投资》、《比特币全球电商平台 OpenBazaar》

公开发布 PPT：《全球区块链投资》、《为什么数字货币最近会跌》、《再见比特币》。

程迈越

乌镇智库理事、美国落基山研究所前合伙人、高级研究员、乌镇智库发起理事、国开金融（城镇开发）顾问 。

程迈越先生毕业于复旦大学、北京国际关系学院，以及美国普林斯顿大学威尔逊国际公共事务学院，被授予国际关系、经济学和公共政策的学士和硕士学位。20 余年来，程迈越先生先后供职于世界银行总部、能源和通信领域之顶尖跨国公司及国际著名咨询机构，长期与中国各级政府及大型国企合作，活跃于经济和金融分析、城市规划战略、直接投资/私募股权以及创业服务等领域。近年来，程先生参与了落基山研究所与发改委能源研究所、劳伦斯伯克利国家实验室和能源基金会(中国)共同担当的“重塑能源—中国（2050 年能源愿景）”项目，推动中美战略合作，寻求低碳发展和绿色能源领域的政策思路和解决方案。

比特币大使 —李威声

毕业于英国的皇家会计师，是知名的国际企业顾问。2004 年受中国国务院邀请代表海外华裔青年企业家在北京人民大会堂向国家领导发

言。 集演讲家，投资家，旅行家，评论家，作家于一身。是全球唯一与吉姆罗杰斯同台演讲的华人投资家；是全球首位用比特币环游世界并拍成纪录片的人，受邀在世界各地高峰论坛会发表［加密经济风暴］，［比特风云］全球宣传大使，世界区块链基金会（2017 年获世界卓越品牌）永久主席。

邓海韬

毕业于英国诺丁汉大学，获得信息技术与管理学硕士学位。中国知名天使投资企业德迅资本的投资总监兼董事长助理，2014 年创立志成资本，并荣获“2015 年新锐年青投资人”、“2016 深圳新锐投资机构”等称号。比特币项目早期参与者，以太坊社区忠实粉丝，对区块链技术和应用有深刻的认识和理解。曾参与筹备组建“数字资产抵押”项目“DIC”及担任中国首个非上市股权交易区块链项目“ShareX”顾问。

六、风险提示与免责声明

6.1 免责声明

本文档用于传达信息之用途，并不构成参与 BITARK 项目（BARK）的相关意见。

任何类似的提议或征价将在一个可信任的条款下并在可应用的

证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策的具体建议。本文档不构成任何关于证券形式的投资建议，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。

BITARK 项目明确表示相关意向用户明确了解 BITARK 的风险，一旦参与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。

BITARK 项目明确表示不承担任何参与 BITARK 项目造成的直接或间接的损失，包括：

1.因为用户交易操作带来的经济损失；

2.由个人理解产生的任何错误、疏忽或者不准确信息；

3.个人交易各类区块链资产带来的损失及由此导致的任何行为。

BARK 是一个平台使用的加密代币。BARK 不是一种投资，我们无法保证 BARK 一定会增值，甚至某种情况下会出现价值下降的可能，没有正确使用 BARK 的用户，可能丢失使用 BARK 的权利及 BARK 本身。BARK 不是一种所有权或控制权。

控制 BARK 并不代表对平台的所有权，BARK 并不授予任何个人任何参与、控制，或任何关于项目决策的权利。

6.2 风险提示

1.安全：项目初衷即基于安全理念规划的交易平台，但安全本身永远是相对的概念，如科技进步，自然灾害等不可抗力造成的损失等，

我们承诺尽一切可能保护您的资产安全。

2.监管风险：加密代币正在被或可能被各个不同国家的监管机构所监管，项目方可能会不时收到来自一个或多个监管的询问、通知、警告、命令或裁定，更甚者勒令暂停或停止 BITARK 开发或相关行动。由于监管政策随时可能变化，任何国家现有的对于 BITARK 公开售卖监管许可或容忍可能只是暂时的。在各个不同国家，BARK 可能随时被定义为虚拟商品、数字资产或证券等，因此在某些国家按当地监管要求，BARK 可能被禁止交易或持有。

3.密码学发展带来的风险：密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步或者技术进步，可能给基于密码学的系统（包括 BITARK）带来危险。这可能导致任何人持有的 BARK 被盗、失窃、消失、毁灭或贬值。在合理范围内，项目方将采取预防和补救措施，升级 BITARK 协议以应对密码学的任何进步。密码学和安全创新的未来是无法预见的，项目方和社区成员将尽最大的努力适应密码学和安全领域的不断变化。

4.竞争风险：交易所是一个竞争激烈的市场，现有的以及正在计划开发的交易所平台有数千个，其竞争将是很残酷的。在这个时代，不论拥有好的概念的创业公司还是成熟的公司，都会面临竞争的风险，然竞争是我们发展过程中的动力。

附件一：List of Bitcoin Hacks (2012-2016)

时间	组织名称	入侵手段	被盗比特币数量	损失
2017.06	Bithumb	一位员工的电脑被黑	不详	$870,000
2017.04	Yapizon	不详	3831	530 万美元
2016.08	Bitfinex	用户钱包	119,756	$66,000,000
2016.07	Kraken	一些用户账户被突破	多种数字资产	不详
2016.07	Bitmex	用户账户被突破	不详	不详
2016.07	ItBit	用户账户被突破	不详	不详
2016.05	Gatecoin	热钱包	多种数字资产	$2,000,000
2016.05	SimpleFX	邮件系统被攻击，给用户发了很多诈骗邮件		不详
2016.04	Yaykuy	遭受攻击并且阵亡		不详
2016.03	ShapeShift	inside job	多种数字资产	$230,000
2016.03	BitQuick	用户姓名、电话号码和邮件信息被盗	无	无
2016.03	Cointrader	热钱包	81 BTC	$33,600
2016.01	Cryptsy	不详	13000BTC 30 万 LTC	近 4 千万 RMB
2016.01	Bitstamp	热钱包	18,866	$5,263,614
2015.05	Bitfinex	热钱包	约 1500	约 36 万美元
2015.03	Exco.in	冷钱包/inside job	不详	不详
2015.03	Kipcoin	冷钱包/inside job	3,000	$690,000
2015.03	796	冷钱包/inside job	1,000	$230,000
2015.02	比特儿	冷钱包	7170 个比特币	$1,750,000
2015.02	台湾 Yes-BTC	不详	不详	不详。跑路
2015.01	Bitstamp	热钱包	19,000	$5,100,000
2015.01	Cavirtex	用户数据库被盗	不详	不详
2014.12	Blockchain.info（钱包）	用户钱包（bug，R values）	267	$101,000
2014.12	Mintpal	inside job	3,700	$3,208,412
2014.08	比特儿	不详。黑客潜伏数月	5000 万 NXT	1 千多万 RMB
2014.08	Cryptsy	inside job	多种数字资产	$6,000,000
2014.03	Flexcoin（钱包）	热钱包	1,000	$738,240
2014.03	Poloniex	代码 bug，用户提款到负数	12.3%的准备金	不详
2014.03	Bitcurex	不详	10%～20%的资金	不详
2014.03	Canadian Bitcoins	骗客服开启安全模式侵入	不详	$100,000
2014.03	CryptoRush	冷钱包/inside job	950	$782,641
2014.01	Mt.Gox	冷热钱包/inside job	850,000	$700,258,171
2013.12	Blockchain.info（钱包）	2-factor authentication	800	$800,000

		breach		
2013.11	Inputs.io（钱包）	冷钱包/inside job	4,100	$4,370,000
2013.11	BIPS（钱包）	冷钱包/inside job	1,200	$1,200,000
2013.11	PicoStocks	冷钱包/inside job	6,000	$6,009,397
2012.09	Bitfloor	未加密的钱包数据文件被盗	24000	25 万美元
2012.05 2012.03	Bitcoinica	不详	不详	不详
2012.03	Linode（主机托管）	inside job	46,703	$228,845
2011.08	My Bitcoin	不详	780000	约 80 万美元
2011.07	Bitomat	wallet.dat 文件的访问权限丢失	17,000 比特币	约 22 万美元
2011.06	Mt.Gox	安全漏洞	不详	不详

（主要来源：https://steemit.com/bitcoin/@michaelmatthews/list-of-bitcoin-hacks-2012-2016）

附件二：关于通用评估准则（Common Criteria）

关于通用评估准则（Common Criteria，以下简称 CC）标准源于世界多个国家的信息安全的准则规范。截至 2015 年 4 月份，CCRA 成员国总计 26 个国家，其中已有 17 个国家的相关政府机构拥有自己的评估认证体系可进行认证证书的颁发并接受互认（Certificate authorizing）。

CC 是专注于信息安全领域且具有奠基意义的一部标准。在标准所定义的同一个框架内，使用的是同一种专业语言，使得计算机信息产品的使用者能够用严格规范的方式来明确提出产品的安全功能的要求。同时，产品的研发商能进而实现这些所要求的安全功能或是声明他们的产品具有怎样的安全特性，实验室的测试评估人员也能评测产品是否真正地达到了研发商所宣称的安全功能。由此可以看出，CC 是为计算机信息产品的安全功能说明、实现以及评估提供安全保证的一部通用标准。

CC 在标准结构和撰写形式上一共包含三个部分，就像是一本书的三个大章。这三个部分在内容上可以说是唇齿相依、融会贯通、缺一不可的，如果其中任何一个部分被孤立起来，则不能独立地构成一个有任何应用价值的标准，孤立的部分也无法确保产品的安全性能有效地被评估出来。

CC 第一部分介绍了 CC 的基本思路和一般模型，定义了评估目标（Target of Evaluation，简称 TOE）、安全目标（Security Target，简称 ST）和保护轮廓（Protection Profile，简称 PP）这些重要的基本概念，并且规定了撰写 ST 和 PP 这类文档的格式及要点。评估目标简单说来就是要对此进行评估的对象产品。安全目标是对某个特定的评估目标提出的要其满足的安全功能要求（Security Functional Requirements，简称 SFR）和安全保障要求（Security Assurance Requirements，简称 SAR）。保护轮廓是对某一类产品提出的安全功能和安全保障要求。

CC 第二部分详细描述了可供 ST 或 PP 选用的安全功能组件，共分十一个大类，其中有安全审计、通信、密码支持、用户数据保护、标识和鉴别、安全管理、隐秘、TSF 保护、资源利用、TOE 访问和可信路径/信道。每一大类内，又逐步细分到不同的族、组件及组成要素。CC 第二部分提供的安全功能组件集合了当前信息安全产业界最普遍使用的技术方法，是非常有价值的可供参考的安全功能描述。然而，CC 第二部分既不强迫任何产品必须选用一些特定的安全功能组件，也不能保证所有信息安全产品所需的安全功能都已存在相应描述。CC 是有弹性可扩展的框架性体系，它允许 ST 或 PP 的作者按照 CC 第二部分提供的对已定义的安全功能组件的格式来定义描述新的安全功能组件。

CC 第三部分详细描述了可供 ST 或 PP 选用的安全保障要求。安全保障要求覆盖到对 ST 的评估准则、TOE 的开发、生命周期支持、指导性文件、测试、脆弱性评定在内的六个方面。根据在每个方面安全保障要求的数量多少和松紧程度，CC 第三部分中又定义了七个评估保障级（Evaluation Assurance Level，简称 EAL），每个评估保障级都是将六个方面的安全保障要求的细节按一定方式搭配并固定下来。从 EAL1 到 EAL7，在六个方面的安全保障要求由少到多、由松到紧逐渐递增。

CC 评估具有两个重要环节。第一步是对确定的安全目标的评估。安全目标可以遵从于某个保护轮廓（Protection Profile，简称 PP），也可以没有遵从的保护轮廓而是针对某个特定产品撰写的。提出安全目标和保护轮廓的基本准则

是根据某个或某类产品需要保护的信息资源的价值，以及此（类）产品使用环境受到敌意攻击的威胁程度，来选取合适的安全功能组件和安全保障级别。如果此（类）产品实现了所要求的安全功能组件，并且这些功能的设计和实现是达到了所要求的安全保障级别的，那么从理论（即 CC 的理想）上讲此（类）产品有能力抵御来自所处的使用环境的威胁，因而能够有效保护所拥有的信息资产。安全目标的制定应符合 CC 标准的第一部分一般威胁模型的方法。

CC 评估的第二步是对安全目标中所定义的 TOE 的评估。这一步的评估要点在于通过对产品的设计文档、代码实现、生产流程、使用安装、功能测试、脆弱性分析等等多个角度和方面来衡量判定此产品是否真正地实现了在其 ST 中所宣称的安全功能，是否真正地达到了所宣称的安全保障级。这里要强调指出的是，ST 中指定的安全保障级中包含的安全保障要求将贯彻覆盖到所选用的全部的安全功能组件。

对于 EAL1 到 EAL4 的 CC 评估，CCRA 还发布了通用标准评估方法论（Common Criteria Evaluation Methodology，简称 CEM），并被接纳为国际标准 ISO/IEC 18405。据作者所知，中国信息安全领域的专家们对 CEM 已作了中文翻译，目前尚未看到该部分发布为一个国家标准。

概括来讲，CC 评估是基于 CC 第一部分提出安全威胁模型，该模型根据产品面临的安全问题（假定、威胁和组织安全策略），确定安全目标，并根据 CC 第二部分的安全功能要求选择产品的安全功能，基于 CC 第三部分的安全保障要求开展 CC 评估。