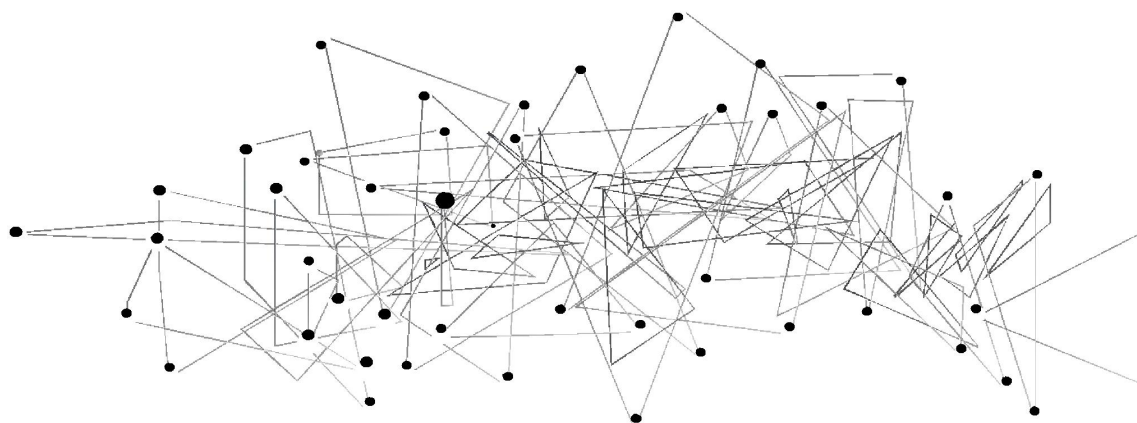


Zbc 数字资产交易所

Zbc.com 白皮书



目录

一 . 项目背景	3
1.1 市场现状.....	3
1.2 行业现状.....	4
1.3 项目愿景.....	5
二 . 平台特色	7
2.1 特色金融服务.....	7
2.2 cool shield 交易机.....	8
2.3 区块链媒体.....	9
2.4 数字资产游戏.....	9
三 . 平台概述	10
3.1 技术优势.....	10
3.2 安全优势.....	12
3.3 高便利性.....	14
四.会员体系	18
4.1 成为会员.....	18
4.2 会员权益与服务.....	18
五 . Zbc 积分体系	19
5.1 积分概述.....	19
5.2 积分功能.....	19
5.3 获取 Zbc 积分.....	20
六 . 风险提示及免责声明	21
6.1 风险提示.....	21
6.2 免责声明.....	22

一. 项目背景

1.1 市场现状

自从 2009 年比特币问世至今，数字资产无论规模还是种类，都经历了非常巨大的变化。

数字资产的总体市值，从 0 增长至今最高超过 7400 亿美元，预计还将迅猛增长。

而基于区块链的数字资产最早起源于比特币，而后出现了竞争币：莱特币和狗狗币等。

随着以太坊的出现，数字资产呈现了爆发式的增长，至今在各大交易平台交易的加密货币和通证 (Token) 已经超过了 2000 种。在新兴数字资产百花齐放的同时，比特币的市值占比也从最初的 100% 逐步下降到了目前约 35%。

数字资产交易，已经是一个全球 7x24 小时不间断，市值数千亿美元的市场。日交易额最高突破 488 亿美元，正常运营的交易平台也达到了近 300 家的规模，其中排名前二的交易平台最高日交易额已超过 40 亿美元。但是由于各类交易平台安全事故频发，用户风险意识逐步加强，绝大部分用户都注册了多家交易平台账号以达到分散风险的目的。由于交易平台项目启动门槛不高，费用成本也不是很大，这也就造成了当下大量劣质交易平台利用市场空缺滥竽充数的现状。综上所述，我们不难发现，虽然“巨头们”占得的市场份额不算小，但留给新兴优质交易平台的市場空间依然很大。如 2017 年下半年崛起的 Binance 和 Upbit，它们用了不足半年的时间，以其相对优质的用户体验就轻易跻身全球交易平台的前列。

随着区块链技术的发展以及通证 (Token) 经济模式的完善，除了数字资产市场本身的

增长以外，传统企业的上链与通证化也给交易平台市场提供了巨大的潜力。通证化是公司体制的变革，是未来各类机构的重要组织形态和机会，是可以将公司用户与公司权益的分配主体真正统一起来的经济模式，这个模式的应用已经初步形成规模。在不远的将来，极可能有数百万甚至上千亿美元的传统资产将转换成为数字资产。未来交易平台的交易产品和交易方式将更加多样化，交易平台市场总体交易规模也将有可能达到今天的数百倍，甚至数千倍。

1.2 行业现状

综观目前交易平台行业情况，各个交易平台的基础设施水平和运维能力参差不齐。尤其是以下几点，是市面上大部分交易平台都存在的问题。

- **缺乏完善的金融工具**

区块链行业的飞速发展使得数字资产金融工具的稀缺性更为明显。相较于传统金融业丰富的金融衍生品起到的风险对冲作用，大部分数字资产交易平台并没有完善的金融衍生品作为风险对冲、放大收益的工具。很多机构投资者因为缺乏此类金融工具而无法进入市场。

- **可用服务级别远达不到互联网项目标准**

大部分交易平台团队并不具备足够的高并发业务承载能力和经验。如多个日交易额全球排名前十的交易平台曾多次出现停止服务数小时，甚至在出现漏洞和故障后陷入数十小时不能访问的窘境。这在追求 SAL 99.99%的高可靠时代，是远远落后于互联网行业领先水平的。尤其在数字资产交易平台行业标准的服务时间是 7x24 小时不间断的背景之下，欠缺高并发业务承载能力，对投资者和用户造成的损失，实际上比任何其他互联网交易平台都要严

重。

- **用户操作体验差，安全性不足，长时间没有改进**

由于大部分交易平台采用的都是外包公司研发的代码，且交易平台团队本身只有简单的运营能力，而交易平台自身技术研发能力完全缺失或严重不足。这些交易平台在用户体验上，就相对刻板生硬，只能实现少量用户基本的交易需求。在最重要的交易平台安全性上漏洞百出，缺乏研发冷热隔离钱包、构建安全运维架构等最基本的能力。部分交易平台甚至没有二次验证的安全检测，用户的数字资产安全受到了极大的挑战。即使是目前相对大型的交易平台，也存在相当多的问题。

如在行情页面停留时间稍长便会出现内存泄漏，导致浏览器甚至电脑出现显著卡顿甚至崩溃。再如，某大型交易平台由于缺乏研发数字资产钱包的能力，在用户不知情的情况下，就将用户寄存于交易平台的资产托管至第三方钱包。

1.3 项目愿景

Zbc.com (Zbc 数字资产交易平台) 是一家依法注册于开曼群岛的全球化数字资产综合交易平台，提供币币交易、合约交易、债券、数字资产托管与清算、大数据分析、数字资产专业管理等综合服务。项目技术、产品团队成员来自于国际知名互联网上市企业，有着丰富的安全、高并发的技术积累，可以解决市面上大部分交易平台存在的技术、产品问题。金融产品参考摩根士丹利 (Morgan Stanley) ，芝加哥商业交易所 (CME) ，黑石集团 (Blackstone Group) 等国际知名金融机构的金融产品，随着投资者增多，他们的需求日益

多样化：保值（风险对冲），资产管理、流动性等等。这就对市面上现有的单薄的金融工具形成了挑战。基于这样的需求，我们金融产品团队力图去开发更多元化的金融工具及服务：合约（金融衍生品）、债券、托管、资产管理、策略组合等。我们将在金融服务多样化上一路走在市场前沿，以保持平台用户的高粘性。

二 . 平台特色

2.1 特色金融服务

2.1.1 合约

数字资产的合约是一个很好的风险对冲工具，它使得机构投资者更放心地进入数字资产的市场。对于矿工和普通交易者来说，合约也能在行情大幅波动时第一时间进行套期保值以减少损失。对于风险偏好较大的交易者，单边合约市场的高杠杆率可以来放大收益。基于数字资产合约市场的巨大需求，Zbc.com（Zbc 数字资产交易平台）也择机上线合约交易市场。

2.1.2 权利合约

权利合约与合约不同，权利合约给持有者某种权利去做什么事情，但权利合约持有者不一定必须行使权利。权利合约购买者通过支付一笔权利合约费给权利合约出售方，换取在未来某个时间以某种价格买进或卖出基于数字资产标的物的权利。权利合约允许交易者进行买开、卖开、买平、卖平操作。对于数字资产来说权利合约的加入使对冲与交易组合更加便捷。

2.1.3 债券

许多项目在进行首次募币之后，许多长期看好项目的投资者希望长期持币。项目方也希望投资者的投资倾向大于投机倾向。于是市面上出现了一些锁仓需求。基于此需求，结合传统金融工具，我们首创了数字资产债券。数字资产债券将为项目方提供锁仓工具，同时也提供给长期看好项目的投资者固定利息激励，促进双方共赢。由于债券是可以二级市场交易的，

用户也可以以一定价格转让给其他投资者换取流动性。

2.1.4 数字资产托管

随着全球持有 BTC、ETH 等头部数字资产的用户越来越多，数字资产的托管需求也迎市而生，Zbc 数字资产交易平台将会和第三方金融机构进行合作，为第三方的质押贷款、融资融券币、大宗交易、场外交易等业务进行数字资产托管服务。交易平台将会提供一个信息中介平台，为用户与用户、用户与第三方机构、机构与机构交换信息并撮合需求，在用户交易过程中提供数字资产托管服务以保证交易的顺利进行以及双方的资产安全。

2.1.5 投资组合

由于市面上项目众多且鱼龙混杂，加上区块链的技术学习门槛较高。很多用户缺乏时间、精力和能力去挑选优质项目。基于此，我们将开放投资组合的信息平台，让更多专业机构的投资策略加入进来，给用户多种可选的数字资产组合策略。包括但不限于：套利策略、量化策略、打新策略、指数策略等。由于平台托管，专业机构只有对计划调整的权限，并不能将用户的资产转移走。交易平台将每天公布各种策略的净值还有每周期的分析报告，以便投资者实时了解组合的实际情况

2.2 cool shield 交易机

Zbc 数字资产交易所顺应数字资产交易市场用户冷钱包存储的需求，和库神品牌达成入股合作，共同研发并发布了 Cool shield 交易手机。冷钱包存储功能是指将钱包离线保存的一种方法。玩家在一台离线的电脑上生成币的地址和私钥，并将其妥善保存起来。以后挖矿

或者在交易平台得到的币都可以发到这个离线生成币的地址上面。由这台离线电脑生成的私钥永远不在其它在线终端或者网络上出现。

Cool shield 的冷钱包存储功能是在库神冷钱包存储技术的基础上进行了改良和完善，提高了多币种存储的兼容性，在 Zbc 数字资产交易所进行交易的币 Cool shield 都能提供存储功能。

2.3 区块链媒体

Zbc 整合国内多家媒体资源，传递区块链技术相关知识，带来最新的数字资产交易咨询。Zbc 交易平台的策划团队将制作“寻找中本聪”系列节目。该节目视频将在美国、日本、加拿大等地相继录制视频追寻中本聪踪迹，探讨中本聪和比特币以及全球经济的关系，并将在节目中传递区块链最新技术资讯，和全球数字资产交易第一手资讯。采用传播手段大众传媒的方式助力推动区块链技术的前进。

2.4 数字资产交易

把数字资产交易植入游戏，相结合进行开发，通过娱乐获利，开创数字资产交易发展新方向。数字资产形式的泛娱乐游戏，Zbc 数字资产交易平台已经和知名游戏团队开发商达成合作协议，开发针对数字资产交易的竞技类，休闲类游戏，包括棋牌、开心农场等多种游戏形式。

三 . 平台概述

3.1 技术优势

项目团队核心架构师以及研发人员均来自于国际知名科技公司的中间件和底层通讯团队，人均具有十年以上的研发经验。团队经历了多年高并发业务实战检验，对于分布式系统的高可用(包括限流、降级、多机房架构等)有着非常深入的理解。在系统调优、问题诊断方面，团队同样聚拢了大量高端人才，核心成员之一便是某著名 JVM 诊断工具的作者。

3.1.1 高响应

由于在整体架构上借助公有云完备的基础设施，Zbc.com (Zbc 数字资产交易平台) 可以根据用户数量和规模变化快速伸缩相应的服务，带给用户最好的体验。同时我们通过数据专线将中心 IDC 的数据行情同步到了各区域 IDC 加速节点，以保证各个区域的用户体验同样高响应。同时交易平台充分利用了 CDN、缓存、内存撮合等技术手段，提升了整体性能，最大限度优化了用户体验。

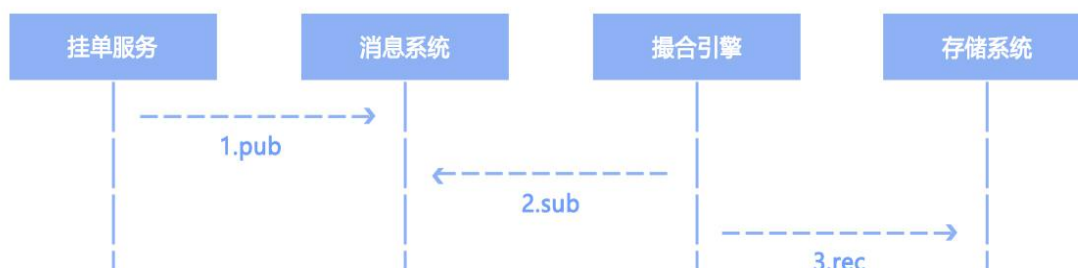
3.1.2 高吞吐

系统的整体吞吐一方面取决于最短板的服务，另一方面取决于整体的设计模型。交易平台的数据库服务及其他服务组件都在充分利用公有云服务的高性能的基础上，进行了调优。核心研发团队有多年的 Actor 编程模型实战经验，采用响应式架构设计，最大程度上保证了系统的吞吐和扩展。交易平台在撮合引擎的 15 实现上也经过多次优化改进，具备了相当优越

的撮合性能。

3.1.3 高可用

不可否认的是当前数字资产交易平台的可用性与传统证券系统相比仍有很大的差距，即便当日交易额排名全球前十位的数字资产交易平台，也有出现服务数小时不可用的情况，这对于互联网金融而言是不可接受的。所以从项目之初 Zbc.com (Zbc 数字资产交易所) 架构师团队就为产品确立了超越同行的高可用性要求——达到 99.9% 的可用性，即核心功能全年的不可用时间不超过 8.76 小时。这就要求主链路及链路上各个子系统的可用性均超过 99.9%，且链路越长可用性值要求越大。例如，



交易简化后大致涉及 3 个阶段：

- 挂单服务无状态（多实例），按交易币对分 TOPIC 发送买卖消息
- 撮合引擎无状态(每个币对一个实例)，按交易币对订阅买卖消息
- 撮合引擎对于买卖挂单消息进行撮合并向数据库记录状态

那么这 4 个子系统高可用性必须有更高的要求：

- 挂单服务无状态，通过注册中心负责监控或单独实现进程的监控与重启

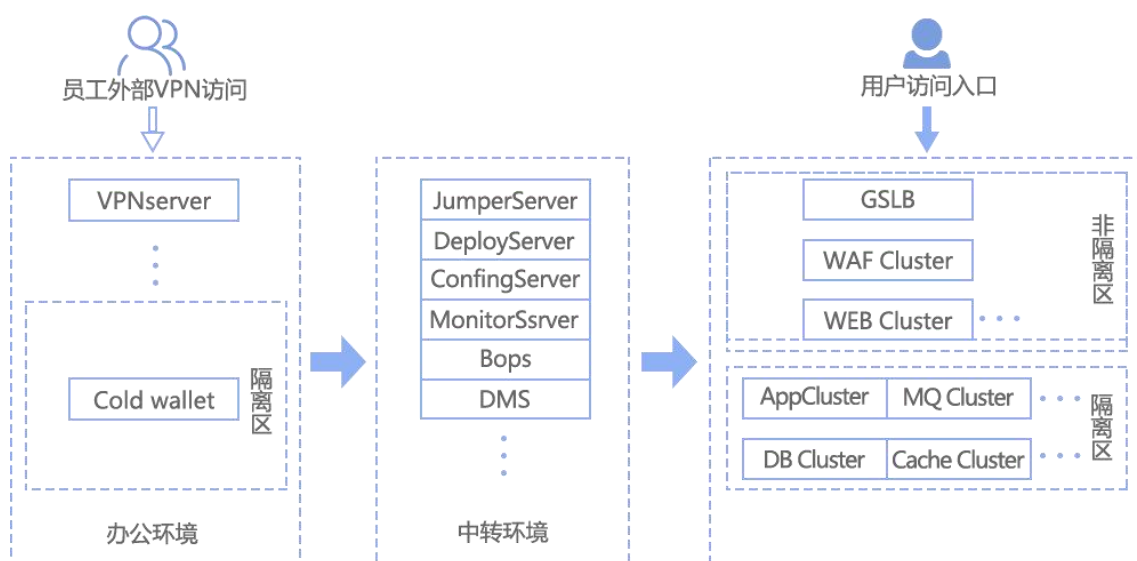
- 消息系统可采用公用云服务(或自己选型搭建集群)，且按交易币对进行服务隔离
- 撮合引擎无状态，可用进程监控与重启来秒级容错，但重启后，需根据数据库状态对消息进行基于 offset 的断点恢复
- 数据库基于公有云的服务，其本身提供了高可用保证

3.2 安全优势

对于交易平台而言，安全是重中之重。团队中的安全负责人是在行业具备相当影响力的安全专家，安全团队的人员配比要比一般的金融公司还要高出很多。除了自己的安全团队外，交易平台同时也会选择与其他第三方的安全公司或团队合作，如在信息系统安全等级保障、身份识别、反洗钱等业务上进行合作。同时在冷热钱包隔离上，交易平台也采取最严格的手段，最大程度降低风险。

3.2.1 架构规划

在安全架构设计方面，设计了如下架构：



在架构中进行了办公环境、中转环境和生产环境的划分。对涉及敏感数据的冷钱包、后

台核心数据库等进行了隔离，采用物理或者纯加密 API 的方式来进行通信，保证用户环境不可见，甚至内部非核心团队人员都不可以接触。借此有效地保证了用户资产的安全。具体包括：

- 办公环境：日常测试服务、VPN Server 及物理隔离冷钱包等
- 中转环境：办公与线上环境的中转功能，包括：堡垒机、DMS、BOPS、ConfigServer 等操作审计类服务；Monitor、logs 等监控类服务
- 生产环境：核心 GSLB、WAF、WEB 及其他需要外部访问服务有可联通外部网络，其他 APP、MQ、DB、Cache，中间件等均与外部网络隔离统一由中转环境各个 Server 通过内部网络访问。

总体上，通过高防 IP 与 WAF 来防御可能存在的 DDOS、CC 及各种潜在漏洞攻击，非隔离区 Server 主机部署主动防御 agent 监控可能出现的攻击渗透篡改等。

而在具体的产品实现上，我们制定完善的安全测试检查表。比如：短信、邮件、谷歌二次验证这三者的使用，在不同的场景下，使用的规则不同。如原则上所有敏感行为都需要提供短信验证码，在提现、更改绑定手机等操作中需要进行邮件确认，出现异地登录则通过邮件和短信通知。谷歌二次验证是短信验证码安全补充，用户可以根据自己的需求设置谷歌验证码。

3.2.2 规范建立

安全除了在技术层面的防御，还有很大一部分需要依赖管理流程的约束，我们将严格遵

循以下规范：

- 建立常规安全审计制度，除了工作周报之外，每半月发布安全周报，报告安全相关研发、研究与实施进展。
- 线上核心操作服务 JumperServer、Bops、DMS 等所有操作记录均会永久保存并进行异地抗灾备份。
- 所有敏感信息均进行二次加密，并进行物理隔离。
- 数据类修改操作均需至少一人及以上审核，甚至有相应的审批流程。
- 内部安全团队负责每次线上代码发布的安全 review 及不定期线上漏洞的扫描，并跟进内部使用框架跟进，测试团队在功能及性能测试同时以防操作及逻辑漏洞。
- 社区漏洞情况及时预警及修补，建立 7x24 小时响应和修复制度。
- 内部严格按照安全规范制定安全巡检审计标准，并不定期员工安全培训。

只有对安全有足够的重视，有足够的投入，有足够的规范，与实施到位，才能将安全风险降到最低，同时，在安全事故上，保持积极的应对，才能将损失降到最低，真正把 Zbc.com (Zbc 数字资产交易平台) 打造成为让用户放心的数字资产交易平台。

3.3 高便利性

3.3.1 优质用户体验

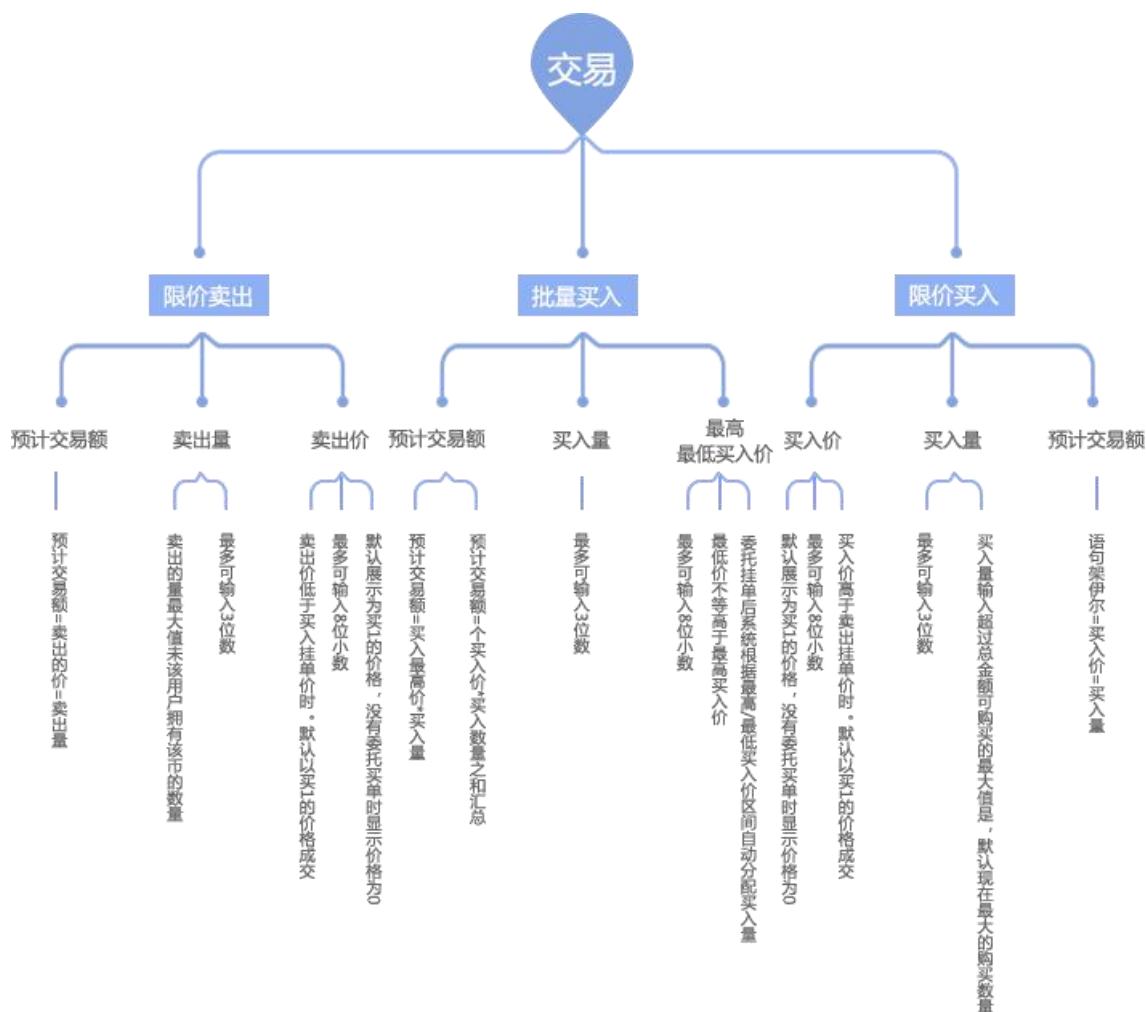
我们对于用户体验极度重视，阿里巴巴、腾讯背景的产品设计负责人，加上国际知名金融和交易平台背景专业人士，组成了强大的产品团队。为了让我们的交易平台操作体验做到

最好，将大量借鉴来自于互联网一线的产品体验，在具体的实施上，在产品的研发过程中，我们将每一个细节与体验写成相应需求说明，并在产品上线前进行需求验证与测试，并形成如下测试报告（示例）：

模块名称	开始时间	结束时间	测试用例 (个)	用例通过 (个)	问题数 (个)	通过率 (%)
用户注册	2018.1.30	2018.1.30	10	8	2	80
用户登录	2018.1.30	2018.1.30	14	12	2	85.7
用户交易	2018.1.30	2018.2.28	6	6	0	100
用户认证	2018.1.30	2018.1.30	15	14	1	90
找回密码	2018.1.30	2018.1.30	5	5	0	100
安全设置	2018.1.30	2018.2.11	10	9	1	90
操作日志	2018.1.30	2018.1.30	2	2	0	100
用户充值	2018.2.01	2018.2.15	5	5	0	100
用户提币	2018.2.01	2018.2.01	10	9	1	90
委托订单	2018.2.15	2018.2.25	12	10	2	83.3
K钱交易	2018.2.15	2018.2.25	10	8	2	80
用户资产	2018.2.25	2018.2.28	5	5	0	100
官网公告	2018.2.26	2018.2.26	3	3	0	100
充值明细	2018.2.27	2018.2.27	5	5	0	100
账户管理	2018.2.27	2018.2.28	8	7	1	87.5
合并深度	2018.2.27	2018.2.28	2	2	0	100

同时设计更为细致的需求体验测试对照表单，确保设计的每一个细节与体验实施到位。示

意图如下（部分示例）



3.3.2 多语种支持

作为全球性国际化交易平台，我们服务于大部分支持数字资产交易的国家的用户，尤其是面向日本、韩国、俄罗斯和东南亚的用户，在上线初始将支持日文、英文和中文，在半年之内，再完成对俄语、韩语和阿拉伯语的支持。在产品和技术设计时，我们就做好了多语种的准备，在设计实现时，将语言资源文件做成可配置的版本。比如管理后台、下单、撮合、用户系统、提存等都是支持可配置的，保证了快速扩展与扩容。

3.3.3 客户关系管理

用户的服务与响应是交易平台业务本身的客户服务，在交易平台上采用客户关系管理

(CRM)API 来支持对用户问题的及时处理 , 比如使用 InterCom 即时消息 API 来建立用户与交易平台客服之间的实时对话 , 使用 Zendesk 建立交易平台消息的统一发布通道。这样就高效地解决了交易平台客户本身对于交易平台的需求和反馈问题。

四.会员体系

4.1 成为会员

购买 coolshield 交易手机即可成为 Zbc 数字资产交易平台 VIP 尊享会员。

4.2 会员权益与服务

购买 cool shield 交易手机即可享受：

- 免费赠送 1000 个 Zbc 平台积分，可以抵扣交易手续费。
- 免费赠送 3000 元邮轮娱乐筹码，可参与邮轮公海竞技娱乐游戏。
- 免费赠送 10000 元区块链课程，了解区块链技术。
- 免费赠送 100000 元顶级会所年卡，享受尊贵服务。

五 . Zbc 积分体系

5.1 积分概述

Zbc 积分是 Zbc.com (Zbc 数字资产交易平台) 推出的功能性积分 , 它是基于以太坊发行的 ERC20 标准的一种 TOKEN。总量发行 5 亿枚。

5.2 积分功能

5.2.1 空投糖果

持有 Zbc 积分的用户 , 交易平台将不定期按持币数占总数的比例空投项目糖果。

5.2.2 注册制投票

Zbc.com (Zbc 数字资产交易平台) 将秉持民主、自由的理念 , 对申请上线的项目实行注册制 , 每个用户都有权利对申请上线的项目进行投票 , 投票将会消耗一定数值的 Zbc 积分。消耗的 Zbc 积分将会锁定一年 , 作为其对应的注册项目的保证金 , 如一年后项目正常运营 , 则交易平台将其销毁 , 如一年内项目退市 , 则将保证金赔付给项目投资者。

5.2.3 交易专区

交易平台将设立 Zbc 积分交易区 , 对交易区的手续费实行一定的优惠政策 , 方便用户兑换积分。

5.2.4 购买服务

交易平台将以 Zbc 积分计价出售专属客户服务、专属 API 服务。

5.2.5 手续费优惠

用户可以以积分抵扣手续费的消耗。

5.3 获取 Zbc 积分

Zbc 积分不公开出售，交易平台上线后将会根据会员的交易情况，采取以赠送的方式送给会员。

六 . 风险提示及免责声明

6.1 风险提示

我们非常重视交易平台的安全，但世界上不存在绝对意义上的 100%安全，例如：由于不可抗力（包括但不限于台风、地震、洪水、政府行为、司法行为、罢工、动乱、戒严、封锁、战争及军事行动等）以及超出当前科学技术发展水平对安全防控能力造成的各种损失。我们承诺将安全性作为本交易平台运营的至高原则，从交易平台信息系统的安全性，到产品设计、交易模式的安全性，再到交易平台运维和用户交易的安全性上，均将尽最大努力确保交易平台参与者的交易行为和数字资产的安全。

Zbc.com (Zbc 数字资产交易平台) 明确表示，本交易平台秉承自愿、公开、民主原则，已向投资人和用户充分告知了相关风险，投资人和用户在此声明并确认已充分了解 Zbc.com (Zbc 数字资产交易平台) 的运维和交易模式，表示了解自愿接受参加交易平台及参与投资和交易的全部风险，并愿意自行承担一切义务、责任或后果。

Zbc.com (Zbc 数字资产交易平台) 在此明确声明，交易平台及运营者有权自主制定交易平台的各项规则，投资人和用户应充分尊重并遵守。

Zbc.com (Zbc 数字资产交易平台) 在此特别声明，概不承担任何投资人、用户参与 Zbc.com (Zbc 数字资产交易平台) 投资、交易等各项业务与活动造成的全部直接或间接损失，包括但不限于：因为用户交易操作带来的经济损失；由个人理解产生的任何错误、疏忽或者

不准确信息；个人选择各种交易行为、交易各类数字资产所带来的一切结果、损失及由此导致的任何风险、义务和责任。

6.2 免责声明

本白皮书只用于传达必要信息之用途，并不构成 Zbc.com (Zbc 数字资产交易平台) 及其运维人员的承诺和责任负担声明，也不对 Zbc.com (Zbc 数字资产交易平台) 及其运维人员发生法律约束力。

Zbc.com (Zbc 数字资产交易平台) 特别声明，交易平台会员和 Zbc 积分不是一种投资，交易平台数字资产在任何情况下均与法定货币不发生关联。 Zbc.com (Zbc 数字资产交易平台) 会员资格和数字资产交易，均充分尊重投资人和用户自愿、自主原则。

Zbc.com (Zbc 数字资产交易平台) 特别声明，交易平台无法保证 Zbc 积分一定会增值，在某种情况下，Zbc 积分也有价值下降的可能，没有正确使用其 Zbc 积分的人，有可能失去使用 Zbc 积分的权利，甚至可能失去其 Zbc 积分。 Zbc 积分在任何情况下，均不是一种所有权或控制权。控制 Zbc 积分并不代表对交易平台的所有权，Zbc 积分也并不授予任何个人有任何参与、控制交易平台。