



TRZ

— TronCandy —

项目白皮书



目录

摘要	3
1. 项目背景	4
• 1.1 移动支付市场现状	4
• 1.2 市场痛点	6
1.2.1 对于商户	6
1.2.2 对于支付平台	6
1.2.3 对于推广人员	7
2. 解决方案	8
• 2.1 平台与区块链技术的结合	8
• 2.2 TRZ Token介绍及平台产品说明	9
2.2.1 众包推广者	10
2.2.2 商户	11
2.2.3 支付机构	12
• 2.3 系统架构	12
2.3.1 模块实现	14
2.3.2 身份识别机制	15
2.3.3 信息加密	15
2.3.4 报警处理	16
2.3.5 分布式记账原理图	16



• 2.4 平台优势	19
• 2.5 团队及发展介绍	14
3. 代币发行计划	22
• 3.1 代币发行目的	22
• 3.2 代币分配	22
• 3.3 回购机制	23
• 3.4 回购销毁的周期	23
4. 时间轴	24
5. 团队介绍	24
6. 免责声明	26



摘要

目前，随着智能手机的不断普及，全球移动支付也迎来了爆发，尤其是中国，大规模的移动网络基础建设已经完善，线下新开的商户逐年增多，移动支付市场日益壮大。线下商铺为应对消费者需求，也纷纷支持了移动支付。

但是目前全球范围内，线下移动支付服务商众多，支付宝、微信支付、银联钱包、ApplePay、GooglePay等纷纷发力，竞争激烈。多样化的支付方式不仅给商户带来了接入时的工作量，也带来了接入后的财务管理不便，同时给消费者增加了要下载多个应用进行频繁选择的烦恼。

另外，相比于淘宝、京东、亚马逊等线上电商的成熟而丰富的运营管理、营销活动，线下商户的运营、营销堪比简陋，甚至有些商户基于纸质账本的手动记录，原始而低效。

TRZ (TronCandy) 闪电营销推广平台，意于搭建推广型消费者、商户、与移动支付服务商三者的交流桥梁，不仅实现多种支付方式一码 / 机通用，并且运用区块链技术，将线下商户推广拓展这一耗时耗力高成本的传统模式进行了优化，通过形成公平、透明、信任的推广及消费的返利机制，建立一个去中心化的移动支付闪电营销生态圈。



一.项目背景

1.1 移动支付市场现状

受益于基础网络服务商、手机设备厂商、以及支付行业巨头在移动支付上的巨大技术投入及市场培养，中国的移动支付在技术和用户体验上受到了全世界的广泛认可，移动网络的建设和应用走到了世界前列，线下移动支付的市场也在前所未有的扩张中。在中国，无论一、二线城市还是中小县城，越来越多的商铺都支持手机支付，甚至于街边早点摊都挂上了手机支付二维码。

移动支付最显著的特点，是交易效率和速度大幅提升。一项测算表明，在使用现金交易的停车场，一辆车从进入收费口到开出，人工找现金平均要用10秒钟，而采用手机支付，则平均只要2秒钟，这是一种效率成数倍的提升。

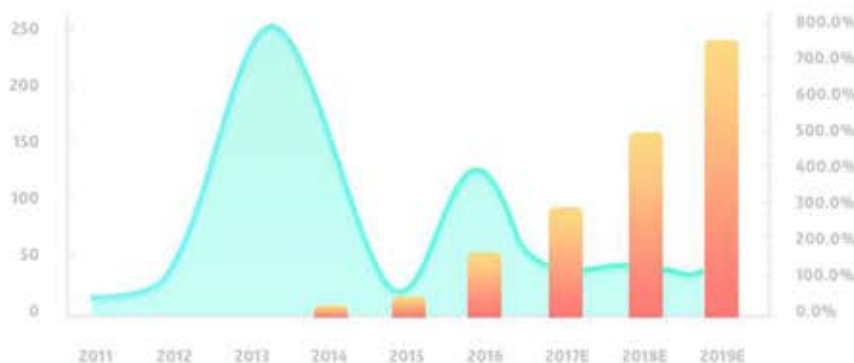




据艾瑞咨询统计数据，2013年至2016年，中国第三方移动支付市场交易规模从1.2万亿元增长至58.8万亿元，平均年化增速均达到366%。

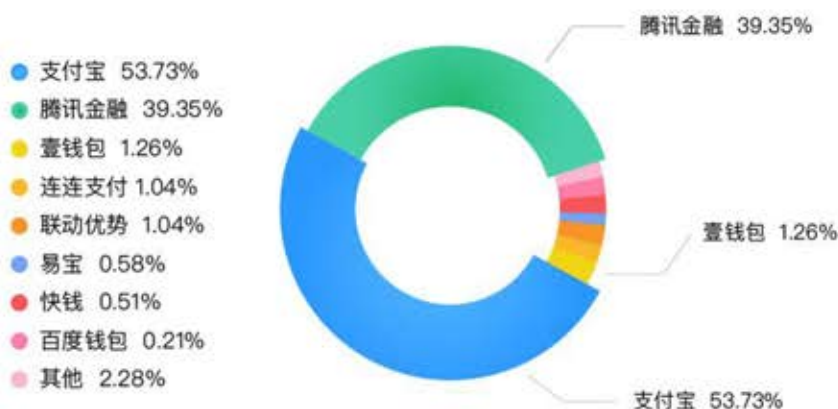
据全球知名咨询公司麦肯锡统计数据，中国已成为全球最大移动支付市场，2016年移动支付交易额相当于美国的11倍。刚刚过去的2017年，移动支付进入集中爆发期，仅在第三季度，中国第三方移动支付交易规模约达29.5万亿元，环比增长28.02%，同比则增长226.2%，移动支付的市场发展迅猛。

2011-2019年中国第三方移动支付交易



据易观数据显示，2017年第三季度，支付宝以53.73%的移动支付市场占有率遥遥领先，第二名是以微信支付为主体的腾讯，市场占有率达到39.35%，以壹钱包、连连支付、联动优势为代表的其它多种支付通道分享了剩余市场份额。

2017年第3季度中国第三方移动支付市场交易额





从移动支付的发展趋势来看，消费者已经从线上的红包、手机银行转账、APP及网站在线支付等标准化支付，向线下的基于各类场景的多元化支付快速扩展。目前线下移动支付已经从零售、餐饮、商超、物流等传统小额高频场景，逐步扩展到医院、票务、娱乐、交通等更多场景，移动支付成了不可抵挡的趋势。

线下移动支付场景不断丰富



1.2 市场痛点

移动支付发展迅猛，但也仍存在着很多问题，对行业参与者提出了更高的要求。

1.2.1 对于商户

接入成本高：

市场上众多支付渠道，如果想要全部支持，需要在不同平台开通账户，申请并购置支付码。

费率高：

主动接入支付宝、微信的商户费率均为6‰，对于本身利润不高的线下商户来说，费率并不低。



账务管理麻烦：

不同支付平台，账务来往查询、对账麻烦，较难做精细化财务管理。

交易数据：

在消费支付中产生的交易数据，被支付机构获取甚至交易，而真正数据源所有者的商家却获取不到应有的权益。

1.2.2 对于支付平台

地推耗时长成本高效率低：

自建团队成本太高，见效慢，容易错过推广黄金期而被竞争对手超越；大量的地、县级市的市场还存在空白，自有团队无精力去覆盖；不同地方各具特点，需要在当地有一定的社会资源才能事半功倍。

新市场拓展耗时耗力：

小的支付机构难以支撑巨大的市场营销推广成本，当前只能专注于个别城市或者细分市场；为了避免逐渐被淘汰的命运，小支付机构也有拓展市场，推广业务的强烈需求。

用户拓展及留存管理成本巨大：

用户需要在手机中先安装各种支付渠道的APP并且完成注册、实名、绑卡等环节，体验不好；如果不再对用户进行消费补贴，用户就会很快流失。

1.2.3 对于推广人员

积极性不高，需要有更好的激励机制：

大部分移动支付平台对推广者给予一次性奖励，商家之后无论使用推广者推荐的移动支付平台收款多久，收款多少，都与推广者无关。

和支付机构或商户间缺乏足够信任度，需要透明公平的环境：

个别移动支付平台尝试将推广者接入商户的交易额，按比例分成给推广者作为奖励的模式，但受限于传统中心化平台的计算和统计方式，无法实现商户、平台和推广者之间的数据透明化，以致于产生信任问题。



二.解决方案

TRZ闪电营销推广平台基于区块链技术，解决移动支付的线下市场拓展中存在的各种问题，为支付机构、商户、推广者等移动支付参与者提供一个的透明、公平、可信任的移动支付生态环境，促进行业发展和社会的进步。

平台通过技术手段，将不同支付通道嵌入到一个有商户代码的SDK或集成二维码提供给商户，并向商户提供统一的软硬件平台作为服务支撑，帮助商户降低接入成本，提高运营效率，具有中立性、灵活性、便捷性等特点。

资金层面,平台不参与具体的资金结算，只是完成支付环节的相关信息流转和商户操作的承载，并且运用区块链的去中心化分布式账本，去除交易记账的不透明，解决参与者间的信任问题。

2.1 基于区块链技术

区块链技术通过全网节点为交易、营销记录进行公证记账，加盖时间戳，保证了账本的唯一。历史数据不可撤销，不可抵赖，防止虚假、重复行为，从而不依赖任何中心化第三方建立起全网的信用，减少了建立信任所需要的大量隐形成本支出。

区块链的交易记录全网透明公开，可追溯，利用密码学的方式保证数据传输和访问的安全，利于审计和监管。不需要有第三方的担保和背书。

基于区块链的智能合约包括事务处理和保存的机制，用于接受和处理交易、营销等各种智能合约，任务的保存和状态处理都在区块链上完成，使得围绕FP平台的工作可以自动执行。



智能合约程序不仅仅只是一个可以自动执行的计算机程序，它更像是一个系统的参与者，可以把它想象成一个绝对可信的人，他负责临时保管你的资产，并且严格按照事先商定好的规则执行操作。

平台利用区块链技术优化了中心化的数字劳动力市场，解决市场中的信任问题，保障了参与者的报酬获取，激励更多有能力的参与者加入，提升了众包任务的达成效率，促进生态体系的完善。

2.2 TRZ Token与平台产品说明

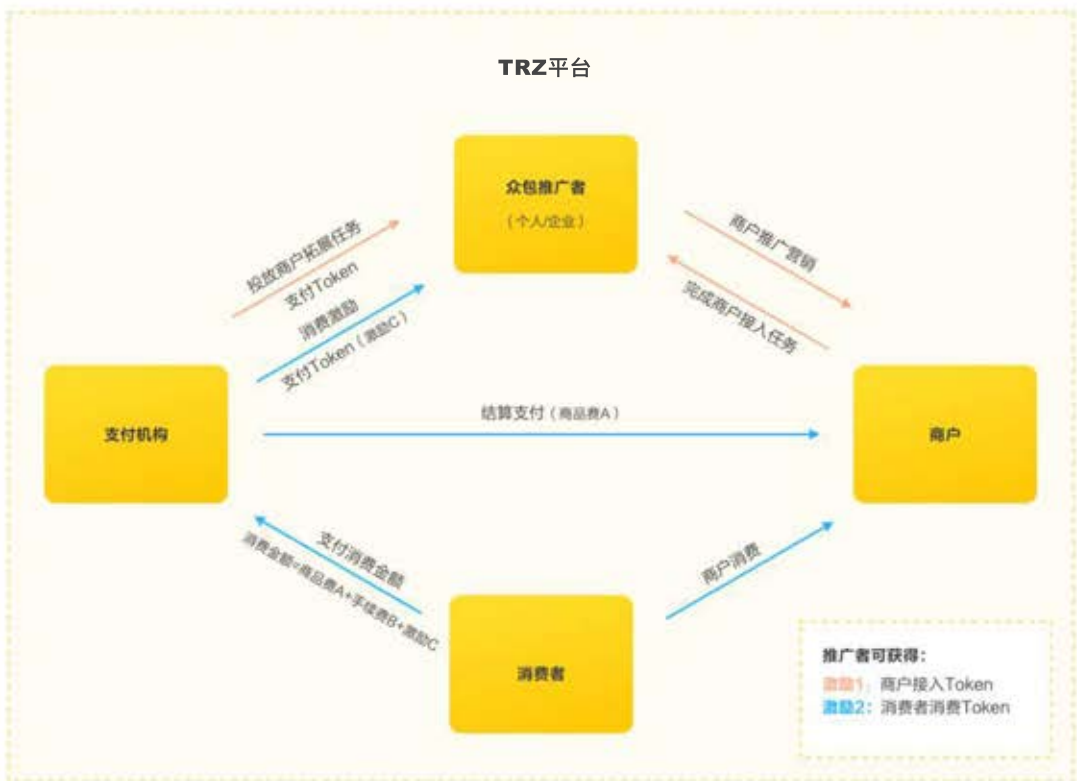
TronCandy Token (TRZ) 是平台上发行一种可流通的加密数字权益证明，也代表了对平台服务的使用及相关权益，众包个人的返佣和营销回报，商户的营销费用，都将使用TRZ结算。TRZ平台将定期回收部分TRZ并销毁，因数量的减少，TRZ也会给持有者带来投资价值。

平台场景描述：

- 支付机构、众包推广者、商户跟TRZ平台签署合作协议，并完成账号注册，及完成相关认证；
- 支付机构购买TRZ，通过智能合约建立投放推广任务；
- 众包推广者在平台领取推广任务，线下向商户推广，拓展商户接入成功获取约定数量的TRZ。
- 未来，推广者仍会持续获得所拓展商户的每次交易金额的对应比例的TRZ作为奖励；



- 商户可以在平台购买TRZ，支付TRZ新建投放营销任务；
- 众包推广者承接商户营销任务，面向消费者营销，根据营销效果获取一定TRZ；



平台参与者具体描述：

2.2.1 众包推广者

众包推广者可以是个人也可以是公司的形式，负责在平台承接任务（推广任务，营销任务等），通过完成相应的任务获取对应的TRZ奖励。

- 下载并安装TRZ Dapp客户端；
- 了解平台注册成为众包推广者，并在平台承接任务；



- 完成平台承接的任务，获取代币TRZ激励；
- 商户维护，获取持续的TRZ奖励。

2.2.2 商户

商户是指有实体经营场所的商家，以入驻的形式加入平台，接入移动支付服务消费者。同时，商户还可以在平台投放营销任务，由众包推广者承接任务，以实际营销结果支付相应的TRZ。另外，未来商家还可以将自身的交易数据在平台生态中共享和交易，获得数据交易带来的TRZ奖励。

1) 支付管理

- 接入平台，通过推广者的邀请进行注册认证；
- 享受平台提供的支付服务；
- 用TRZ代币的方式支付服务平台费；

2) 营销管理

- 购买TRZ代币，投放相应的营销任务，比如，增加商户社交媒体号关注度；
- 众包者推广承接任务；
- 完成任务后，商户根据推广效果支付相应TRZ代币给众包承接者。

3) 数据交易

- 商户在平台开通消费数据交易功能；
- 数据需求方向商家进行数据购买，支付TRZ代币；
- 扣除平台手续费后，商家获得剩余的TRZ。

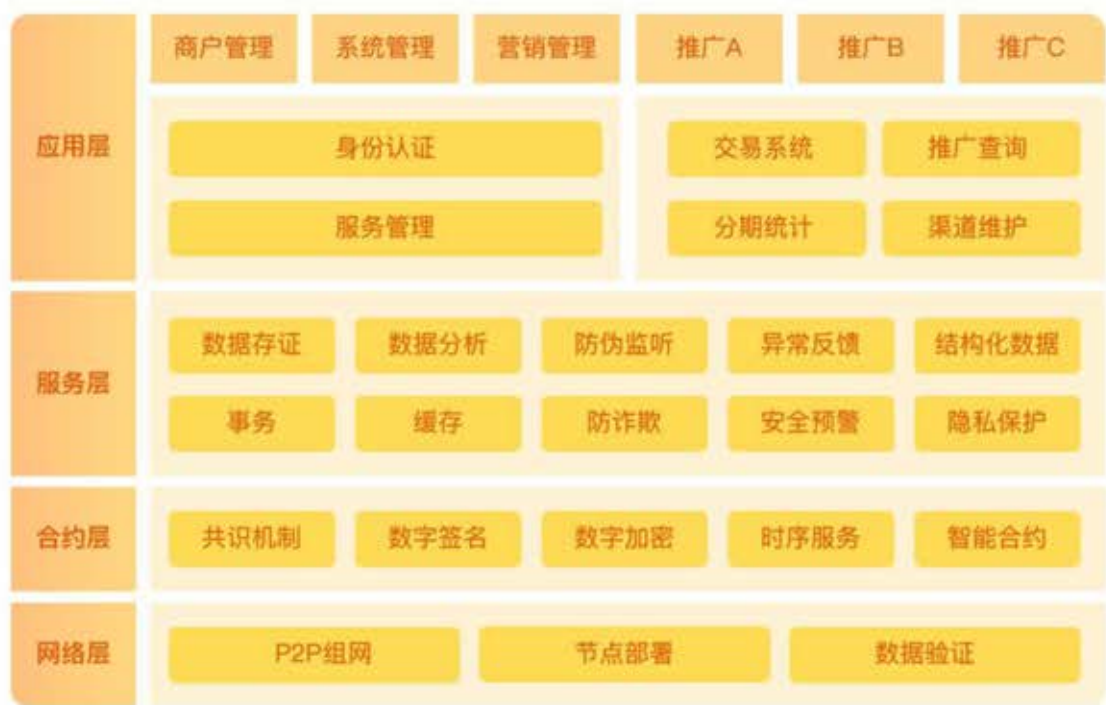


2.2.3支付机构

所有的有原市场维护、新市场推广、全球市场拓展等不同需求的持牌支付机构。在平台发布众包推广任务，由众包推广者承接任务，以实际任务达成结果支付相应的TRZ。

- 接入平台，完成认证签约及代币充值；
- 根据自身的实际情况在平台上投放相应的众包任务；
- 任务完成后，支付相应的TRZ代币给众包承接者。

2.3系统架构





TRZ是利用处理器的可信执行环境 结合 PoS 与 DAG 等方案来增强和完善网络的可信度。这种方案对移动设备非常友好，特别适合在现在最流行的 Android 和 iOS 平台开发应用

通过强大的token 创建和交易功能实现智能积分系统，集合支付，赠送。同币交易，跨币交易的完整的功能。通过优化区块链数据结构设计，实现地推，店面上线，运营，消费，支付，评价后完整的数据上链。通过消费评价系统追溯取证，商品质量或者菜品口感，服务态度等，自动化管理，信息挖掘实时掌握消费者主观动向，并推送优质商家，用于市场营销。





平台基于终端ARP协议通过 geth 连接Ethereum区块链，通过web3.js和智能合约层进行交易。

参与者通过Wallet 管理私钥，并能在钱包上进行任务发布、转账、查询、分润等功能。

商户的消费支付数据经过加密处理后提交到链上，通过P2P去中心化的模式，使网络中的参与者处于对等地位，保证了交易过程产生的数据的真实、透明、公开及可追溯性。同时FP开放接口支持同步和异步操作两种模式。接口适配层对业务请求进行解析，鉴权和签名校验之后，通过共识算法将业务请求记录到账本存储上。接口适配模块作为共识管理模块的客户端，也会参与共识管理。接口适配模块主要负责各个共识节点返回结果的汇总和一致性判断。

2.3.1 模块实现

智能网络层：

实现点对点的去中心化数据传输，区块链是建立PBFT改进协议。客户端生成公钥和私钥，公钥用于发送和接受。以及与其他节点通信。

区块链层：

实现区块链基本功能（不可篡改，时间戳，全网记账），并使用区块链交易信息。

数据层：

结合IPFS 区块链保证数据可用，数据层通过At-rest 加密

合约层：

构建众包行业智能合约，合约层提供智能分润，智能下单的功能，并且实现复杂的业务逻辑和计算

合约注册之后，通过外部条件出发合约，支持定时、和事件触发、交易出发或者



其他合约触发方式。合约独立运行包括对合约构造镜像环境代码执行。状态修改以及异常处理

2.3.2 身份识别机制



地推&商户身份信息识别。目前较为成熟的数字身份体系是基于Public Key Infrastructure的 X.509 标准。在TRZ中,我们将实现一套兼容 X.509 的身份识别标准。除了兼容 X.509 的层级式的证书签发模式,还支持点对点证书签发模式。并通过人脸、指纹、语音、短信等多因素认证实现签发阶段和使用阶段的真实身份比对。同时,还将使用区块链取代 OCSP 协议来管理、记录 X.509 的吊销证书列表 CRL。当用户访问服务器,在线证书状态协议发送一个对于证书状态信息的请求。服务器回复一个“有效”、“过期”或“未知”的响应。协议规定了服务器和客户端应用程序的通讯语法。在线证书状态协议给了用户的到期的证书一个宽限期,这样他们就可以在更新以前的一段时间内继续访问服务器。

2.3.3 信息加密

平台运用的属性加密属于公钥加密体系的一中,特点在于用户的密钥和密文都依赖特定的属性,比如地推者信息,客户信息、商家信息交易信息。当所有属性集合经过加密与原来产生密文匹配。才能正常解密。



私钥生成过程，我们采取用户的权限和访问规则来生成。
通过次数、时间、内容等限制安全访问。

密钥生成：根据地推或商户属性各种身份信息赋值 P ，计算输出私钥 $\text{KeyGen}(p)$
 $\rightarrow \text{skp}$

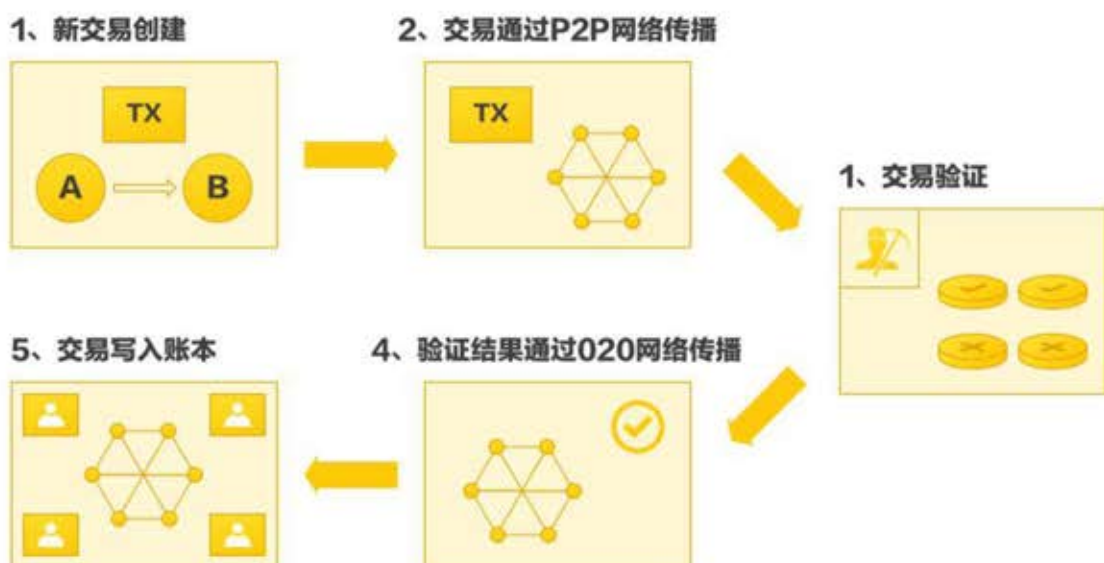
加密算法：输入公开参数秘钥 pk 以及加密方法 way ，计算会话密钥 ek 密文 m ：
 $\text{Encry}(pk, way) \rightarrow (ek, m)$

解密算法： $\text{Decry}(pk, \text{skp}, m)$ 对比 ek 如果匹配解密成功

2.3.4 报警处理

TRZ智能监控系统，会对采集用户消费方式，支付方式、支付人群、消费习惯，以及消费金额、消费时间进行全方位分析。一旦发现类似套现等行为。系统会暂时冻结该商户。平台会对其作出严厉处罚。

2.3.5 TRZ分布式记账原理图

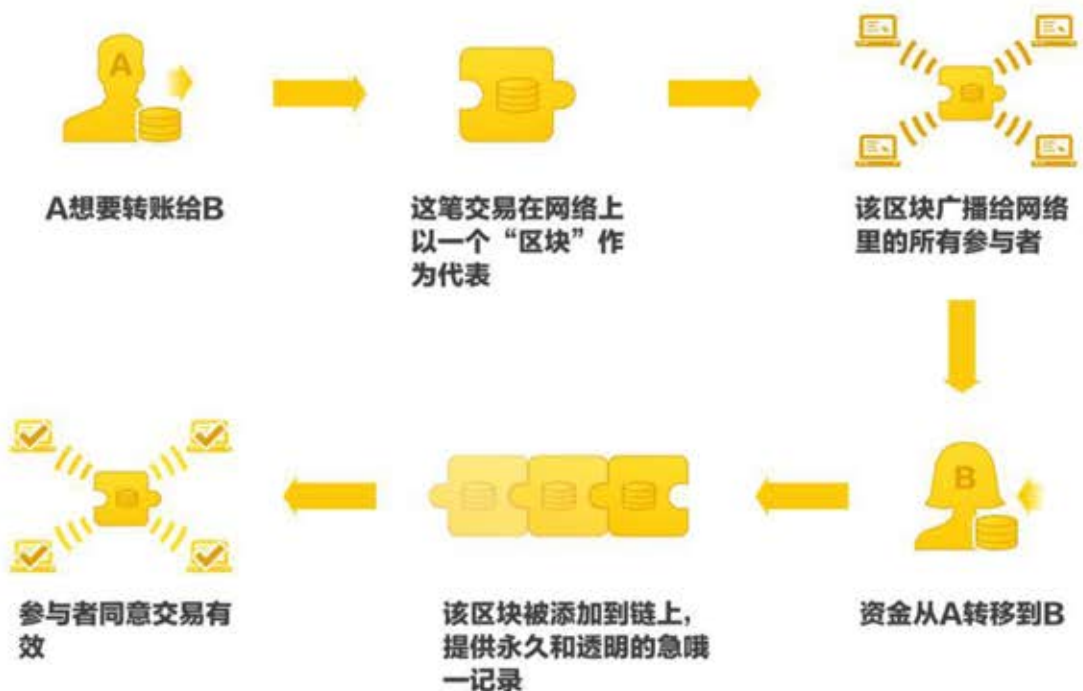




TRZ分布式记账优点：

- 1、**数据权限**——这种权限不仅说明了数据出处，还规定了数据所有权（精确性、更改、生命周期管理等的权限）以及数据最终权威版本的位置。
- 2、**数据精确性**——意味着任意对象的数据值记录都是正确的，可以代表正确的价值，形式和内容都与描述对象一致性
- 3、**数据访问控制**—— TRZ平台 可以分别跟踪商家和消费者信息，包括数据本身的详细信息、数据对应的交易等

2.3.6 TRZ代币交易功能展示



2.3.7 众包奖励算法



推广奖励

TRZ有一套完整的绩效考察地推者，通过审查任务来验证工作的有效性。地推每月提交平台商家 n ，基础奖励（每推荐一个商家奖励 x (FP)）每月获得代币总数：

$$T_m = nx(FP)$$

审核通过为 a ，其中审核通过优质客户平均为级别 w (w 表示 1-10 注：1 表示最高级别) 奖励为 $\frac{2a}{w}$ (FP) (在基础奖励上 如果客户平均级别为 w 为 1 额外获得 2 倍代币奖励)：

$$T_m = \frac{2a}{w} + nx$$

重新提交为 r ，重复提交申请次数为 $t \leq 5$ (提交由审核通过 $2x$ 每没提交一次减少 $e\%$)：

$$T_m = nx + \frac{2ax}{w} + \frac{r}{w} (2x * (1 - e\%)^t)$$

$t > 5$ 奖励代币数为 0；

$$T_m = nx + \frac{2ax}{w}$$

审核失败 f 审核失败的商户 地推者不会获得额外的代币奖励。

当 $\frac{f}{n} \leq 30\%$ 基础奖励会有 nx 变成 $nx * (1 - \frac{f}{n})$

$$T_m = nx * (1 - \frac{f}{n}) + \frac{2ax}{w} + \frac{r}{w} (2x * (1 - e\%)^t)$$

$$\frac{f}{n} \leq 30\%$$

$$T_m = nx * (\frac{1}{2} - \frac{f}{n}) + nx + \frac{2ax}{w} + \frac{r}{w} (2x * (1 - e\%)^t)$$

消费奖励算法

消费者进地推店消费金额为 m ，支付渠道费为 $y\%$ ，地推奖励为 $q\%$ 货币与代币比例为 1: d (获取交易所实时价格)

$$T_m = m * y\% * q\% * d$$



2.4 TRZ平台优势

一码（机）全渠道支持：

一个二维码（扫码枪 / POS机 / 扫码盒）支持主流支付方式。

多功能收银管理：

支持多门店、多收银员设置，统一管理各支付渠道，账目清晰，统计方便。

费率低：

通过规模效应，提升议价权，从支付渠道拿到更低的手续费率。

财务安全：

与正规支付机构 / 银行合作，专业的清算机构提供清算服务，确保资金安全。

迅速营销推广：

通过独特的众包营销推广的激励机制，将拥有线下商铺资源的推广者吸引进来，帮助支付机构闪电式的拓展市场，推广业务。

消费数据资产交易：

商家拥有自己消费交易数据的自主管理权，通过在FP平台实现数据的交易变现，产生价值。

2.5 TRZ团队及发展介绍

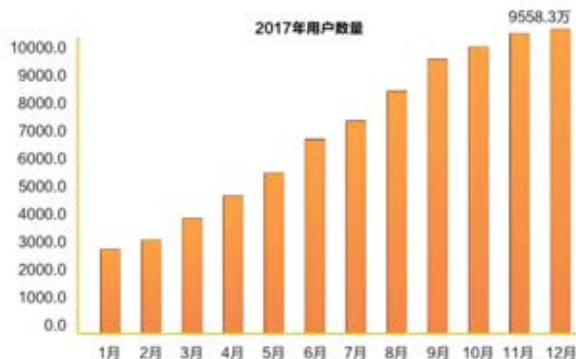
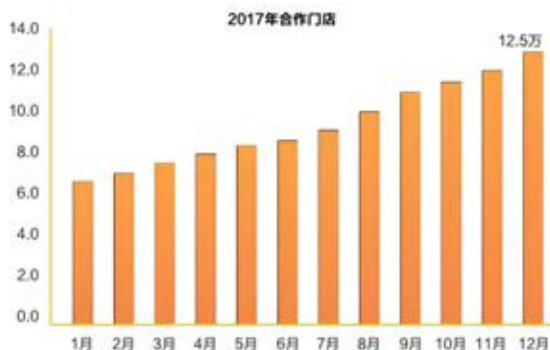
FP团队核心成员来自第三方支付机构和银行，具有丰富的聚合支付解决方案实操经验。

合作支付机构包含中国境内主流支付平台，商户涵盖餐饮、超市、酒店、服装等大中型商户。

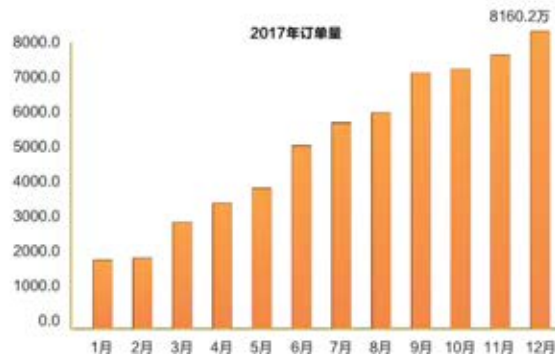
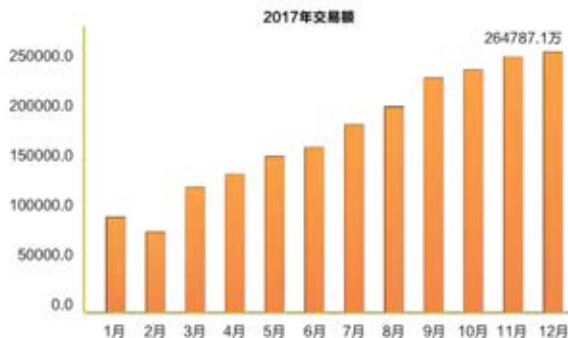


业务覆盖中国境内的北上广深等全国一百多个城市。同时，团队也在布局国外移动支付市场，计划在日本、新加坡成立分公司，拓展海外市场。





服务近12万商户，超过9235万消费者使用，微信公众号关注用户超2000万，日订单量超过260万笔，日交易额8000万人民币。





三.代币发行

3.1 发行目的

为激励及维护生态健康发展，平台将发行统一代币TRZ（TronCandy Token），TRZ代币也会用来奖励为平台带来更多交易活动的商户或个人，发行代币将按约定比例投入于产品研发，法律咨询，社区运营，市场拓展等。

TRZ Token发行总量为1000亿个，永不增发。通过私募方式募集250,000 个TRX发行完成后，代币将在最短时间内登录主流交易所。

3.2 代币分配

- (1) 基石投资人12%， $1\text{TRX} = 10 \text{ TRZ}$ ，募集100,000个TRX，锁定1年，随后每月释放锁定额度的10%。
- (2) 私募发行18%， $1\text{TRX} = 5 \text{ TRZ}$ ，募集250,000个TRX。锁定6个月，随后每月释放锁定额度的10%。
- (3) 市场运营及合作方补贴 20%。
- (4) 生态社区建设 20%。
- (5) 核心团队 15%，锁定期6个月，随后每月释放锁定额度的5%。
- (6) TRZ基金会 15%，用于项目可持续发展。



3.3 回购机制

TRZ上线后，第一年将项目收入的10%用于回购；此后每年增加10%，第5年及以后为50%。回购二级市场上发行的TRZ代币。回购的TRZ代币将转移至销毁账户进行销毁。回购记录将在第一时间公示，保证此过程公开、透明，届时用户可通过TRZ区块链浏览器查询，这个过程将持续到销毁基石、私募的TRZ代币总量（共1.5亿枚）为止。

3.4 回购销毁的周期

TRZ第一年以每6个月为周期，第一次回购将发生于2019年6月。TRZ将用佣金收入的30%回收代币销毁；第二年，以每3个月为周期，回收代币销毁；第三年，以1个月为周期回收代币销毁。TRZ总量不会增发，回购销毁后流通量会逐渐减少。



四.时间轴



五.团队介绍

核心成员



Alex

稍后公布...



顾问与投资人

稍后公布...

全球法律顾问

稍后公布...



六.免责声明

郑重提示：在您购买本平台产品前，请您仔细阅读本声明。凡以任何方式参与本平台或直接、间接使用本平台产品者，均视为自愿接受本声明。

参与TRZ则代表参与者已达到年龄标准，具备完整的民事行为能力，与 TronCandy 签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订 合同之前对 TronCandy 进行了清晰必要的了解。

TronCandy 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过 程中，平台可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调 整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参 与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的 决策。

TronCandy 明确表示，概不承担参与者因(a)依赖本文档内容、(b)本文信息不准确之处，以及(c)本文导致的任何行为而造成的损失。

团队将不遗余力实现文档中所提及的目标，然而基于不可抗力的存在，团队 不能完全做出完成承诺。

TRZ作为 TronCandy 的官方代币，是平台发生效能的重要工具，并不是一种投资品。拥有 FPT 不代表授予其拥有者对 TronCandy 平台的所有权、控制权、决策权。FPT 作为在 TronCandy 项目中使用的加密代币，均不属于以下类别：(a)任何种类的货币；(b)证券；(c)法律实体的股权；(d)股票、债券、票 据、认股权证、证书或其他授与任何权利的文书。

的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何 价值，团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。在适用法律允许的最大范围内，对因参与众筹所产生的损害及风险，包括但 不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其 它经济损失，本团队不承担责任。



TRZ平台遵守任何有利于行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查的所有信息必须完整准确。

TRZ平台明确向参与者传达了可能的风险，参与者一旦参与公开发行，代表其已确认理解并认可细则中的各项条款说明，接受本平台项目的潜在风险，后果自担。