Tezos- 风险等级「C+」 - 标准共识投资风险评级

微信标题：Tezos 无法从根本上解决硬分叉问题

Tezos 无法从根本上解决硬分叉问题

北京时间 2018 年 8 月 31 日，标准共识发布针对区块链项目「Tezos」（ Token 符号：XTZ ）的一般投资风险评级报告。以下为报告的主要内容。

## Overview 概述

报告将 Tezos 风险等级定义为「C+」，该项目属于「一般风险」水平，需要投资者注意。

该项目投资风险较高，投资者应该密切跟进观察和监督项目进展。

依据「标准共识一般项目投资风险评级标准（初创期）」 Tezos 获得「C+」评级的主要原因是：**Tezos 针对目前区块链的问题提出了原创的技术解决方案，创新度高；代码质量较高，有望支持技术目标实现；通过协议的「自我修正」可解决分叉问题，但可能并不是最优方案；目前流通性风险高，用户基础薄弱，用户迁出较为明显。**

基于标准共识分析师团队调查和研究，项目主要风险及优势在于：

**项目主要风险**

风险点一：通过协议的「自我修正」可解决分叉问题，但可能并不是最优方案。

Tezos 利用投票机制实现协议和节点的共识，遵从大多数参与者的意志，避免了区块链的分叉。但是这种机制并没有从本质上解决争议，因为**多数原则**最终会造成持反对意见的人因无法接受新技术或功能而离开系统。

其次，区块链的技术方向本身具有很强的探索性，多数原则通过的方案不一定是正确的，少数人的意见可能探索出更广阔的发展空间。因此，Tezos 的投票机制可能会遏制新技术的发展，相比于「硬分叉」，Tezos 消灭了探索其他技术的空间。 以一个理性和长远的这个角度去看，「分叉」可能不是一件糟糕的事情，它固然可能导致社区出现分裂，甚至有可能对生态发展造成阻碍，但这一过程，同时也会使得社区间有更多的沟通，自由地探索更多的技术发展方向，造就更坚实的共识。

风险点二：项目采用 Ocaml 与 Michelson 作为技术编程语言，语言比较小众化，技术门槛较高，且目前未有智能合约的应用实例。

Tezos 采用 Ocaml 作为底层技术语言，利用 Michelson 语言编写智能合约。这两种语言比较小众化，对于技术人员来说存在一定的学习成本，因此技术门槛较高。且目前并未在该系统中看到有智能合约的应用实例。

风险点三：流通性风险高，用户基础薄弱，存在大批量被禁地址，用户迁出较为明显。

近一个月的全市场平均换手率为 0.29%，换手率低，流通性风险高。持仓地址为 21,615，用户基础薄弱，并且存在大批量的被禁止账户，根据白皮书介绍一年内没有任何动作的地址将被禁止行使各种权利，表明用户迁出较为明显。

**项目主要优势**

优势一：针对目前区块链的硬分叉、算力浪费和中心化、智能合约功能不完善和安全问题，Tezos 提出了原创的技术解决方案，创新度高。

Tezos 为了实现协议的「自我进化」，搭建了一个基于 OCaml 语言的协议框架，采用改进的 PoS 共识机制，并且可通过自我修正代码进化协议；Tezos 采用 Michelson 语言编写智能合约，运用形式化验证技术检验，不仅可减少智能合约编写过程中可能出现的漏洞，同时可根据持币者需求来投票决定协议的修正。

优势二：链上治理设计了投票修改机制，以实现协议的不断进化。

Tezos 的链上治理部分设计了投票修改机制，所有 Token 持有人都可以参与系统规则的修改，是一种分布式的治理机制。构想有很高的创新性，但目前项目刚上线了第二版测试网，还没有发生过投票修改事件，投票规则在实际运行中的效果尚未可知。

优势三：项目架构设计创新性较高，代码质量较高，有望支持技术目标实现。

为了便于实现「自我进化」，Tezos 将三个协议层分离，架构设计创新性较高；代码书写规范，更新频率较高，文档详细，整体来说代码质量较高。  
Tezos 基于 Ocaml 语言开发协议，利用 Michelson 语言部署智能合约，其优点是简洁、编译速度快、功能强大。但编程语言技术门槛较高、比较小众化，目前并未看到智能合约的应用实例。  
Tezos 采用形式化验证技术检验智能合约，但此技术在区块链应用还不成熟，因此目前应用还较少。

以上为项目主要风险点和优势，以下为完整报告。

如果任何项目方对标准共识的评级结果有疑问，或对相关数据提出申诉（包括但不限于项目运营数字、重要团队成员变更原因、代码更新和最新交易表现等），标准共识分析师团队会根据材料的真实性重新评估。

如果标准共识分析师团队在调查过程中使用了错误材料而影响评级结果，或任何项目变动可能导致评级等级变动时，标准共识也会重新调查和评估风险等级。

任何项目方、利益相关方和投资者可直接通过微信公众号（「标准共识」ID：SNCrating）后台与我们联系，也可以发送邮件至：contact@sncrating.com。

## Rationale 依据

### **产品和技术模块**

#### 

#### 市场及产品分析

Tezos 项目从 2014 年发布白皮书，从 2017 年 7 月 进行首次公开募集。Tezos 希望打造一个全新的智能合约平台，并提出了**「自我进化的加密账本」**设想：让持币人决定协议如何进化，通过投票达成共识，实现账本状态、协议和节点的升级、改造方式的共识。

Tezos 项目以 Bitcoin 举例，认为区块链项目存在以下 4 个问题：

1） 「硬分叉」问题，即 Bitcoin 因为共识而产生的不能够动态创新的问题；

2） 成本和中心化问题，这个问题产生的主要原因是 Bitcoin 的工作量证明机制；

3） Bitcoin 交易语言表达有限问题，无法部署智能合约；

4） 加密货币的安全隐患问题。

针对以上问题，Tezos 分别提出了技术解决方案。同时， Tezos 在协议层、共识机制、安全问题等方面与 Bitcoin 进行对比，从这些方面提出了改进方案，形成了一个可被广泛应用且能自我修正的、并可保证原协议有效性的区块链协议。

标准共识分析：

Tezos 为了实现协议的「自我进化」，搭建了一个基于 OCaml 语言的协议框架，采用改进的 PoS 共识机制，并且可通过自我修正代码进化协议；Tezos 采用 Michelson 语言编写智能合约，运用形式化验证技术检验，不仅可减少智能合约编写过程中可能出现的漏洞，同时可根据持币者需求来投票决定协议的修正，这一点是项目最大的创新。

然而， Tezos **为了解决白皮书中描述的分叉所带来的交易分流等问题，提出用投票机制决定协议修正与升级的解决方案可能并不是最优方案**，因为：

1）Tezos 要实现协议和节点升级的共识，使用了少数服从多数的投票机制。但这种机制会使系统发展遵从大多数投票人的意志，少数投反对票的人会因不适应系统发展模式或不支持技术迭代及功能更新而就此离开，最终也会造成用户的流失，交易的分流。

2）Tezos 项目一直想通过自治来避免分叉的产生，但是根据以太坊和 Bitcoin 的分叉结果来看，分叉是市场对不同共识的选择。

回顾以太坊与 Bitcoin 的分叉事件：

* 2016 年 7 月下旬，以太坊中的一个项目 The DAO 由于其自身漏洞，导致黑客窃取了当时价值约 6000 万美元的 ETH。以太坊开发团队为了挽回损失修改了以太坊软件的代码。然而，小部分成员认为这违背了区块链不可修改的宗旨，决定维护原有以太坊网络。于是，以太坊就分叉为两条链，形成了不同的社区共识和价值观。
* 2017 年 8 月 1 日，Bitcoin 在进行扩容升级时，在 Bitcoin 的原链上发生了硬分叉推出了 BCH。BCH 的挖矿算法和挖矿机和 Bitcoin 保持一致，但是将 Bitcoin 区块容量从原来的 1M 扩大到 8M，大区块具有较低的交易费用以及较快的确认速度。Bitcoin 的分叉是社区持有不同意见所导致的结果，不同算力提供者和用户可跟随自己所支持的区块链系统。

以太坊与 Bitcoin 分叉后的运行及产生的 Token 价值是由市场来决定的，即算力提供者与 Token 持有者可根据自己意愿跟随不同的区块链系统。**但这个选择是自由的，完全依赖于参与者基于技术、功能所形成的共识与对于 Token 的价值判断。**

由于区块链系统是由众多的节点组成的分布式网络，缺乏一个绝对的中心，因此在根本上无法保证所谓的「正统性」。缺乏所谓的「正统性」可能是一个分布式系统要面临的必然结果。而分叉就是缺乏所谓的「正统性」带来的结果之一。分叉本身不是一件糟糕的事情，它固然可能导致社区出现分裂，甚至有可能对生态发展造成阻碍，但这一过程，同时也会使得社区间有更多的沟通，造就更坚实的共识。这种与原有共识的分歧不一定是一种背离，它完全也可能是一种改进和突破。

3）现在市场中普遍存在的共识机制是基于账本状态所达成的共识，而仅将投票机制用于节点竞选与社区治理等方面。通常情况下，协议的开发与更新都由项目开发者决定，通过民主方式来达成协议的共识目前在区块链市场来说是一个具有创新性的概念和尝试，但是否能被参与者接受，还需要一定的时间来进行验证。

#### 技术分析

##### 技术介绍

Tezos 针对 Bitcoin 所出现的 4 个问题所提出了不同的技术解决方案：

**1）硬分叉**

以 Bitcoin 为例，随着 Bitcoin 的交易频次与数量越来越大，在原有的区块容量下，大量的 Bitcoin 交易导致交易速度的减慢、手续费提高等问题的出现。为了解决此问题，提出了 Bitcoin 扩容的解决方案。但由于用户对于扩容方式未达成共识，最终导致 Bitcoin 发生分叉，产生了多条不同的 Bitcoin 的分叉链。

针对此类问题，Tozes 提出由持币者共同投票来决定系统发展的方式及方向，同时将采纳被多数人投票的结果，即实现无需硬分叉就可完成升级。

**2）算力浪费和中心化**

Bitcoin 采用的是 PoW 机制，在此机制下，可能会出现以下问题：

* 挖矿算力集中化：包括 51% 攻击、中心化矿池占据了大部分的市场份额以及转账费用的定价权等弊端。
* 动机：PoW 的挖矿利润包括矿工费用与股东利润，因此无法使矿工利益与股东利益保持一致。
* 成本：虽然在 PoW 机制下，算力攻击所花费的成本较高，但是 PoW 机制在挖矿过程中消耗了大量的资源，为生态带来了负面的影响。
* 控制权：PoW 机制下，矿工并不一定是 Token 的持有者。一旦发生分叉，矿工存在利用其控制权作恶的情况。

因此 Tezos 使用了改良后的 PoS 机制，集成了 Slasher ，chainof-activity 和 proof-of-burn 。在 PoS 机制中，若想发动攻击必须掌握大量的 Token，可在不浪费资源的情况下，也有较高的安全保障；其次，矿工必须持有 Token，即生态系统的安全性与矿工的利益紧密相关。

**3）智能合约不完善**

Tezos 认为：「Bitcoin 系统功能有限，目前还无法部署智能合约。而像以太坊此类图灵完备的区块链系统又可能面临着走入死循环的问题。由于以太坊矿工费用与执行合约的复杂性和步数成比例，因此若矿工通过执行一个死循环的交易来提高其矿工费用，同时其他矿工也需要浪费大量时间来验证此笔交易。」

**但这一认识并不符合以太坊的实际执行情况。**以太坊支持图灵完备的智能合约，只是此类智能合约需要使用以太坊的虚拟机 EVM 去运行。为了避免出现死循环的问题，EVM 上的程序的每条指令都要消耗不同的 Gas 费用，如果 Gas 费用被消耗完，无论程序执行完没有，都会被强行终止。其中运算越复杂，需要消耗的 Gas 越多。因此以太坊通过给程序加上一个消耗 Gas 的上限，就可以防止程序出现死循环而不能停止的情况了。

**同时，以太坊还给每个区块的程序需要消耗的总 Gas 设定了上限，以免区块中包含的程序过多，从而影响其他节点。每个区块能消耗的 Gas 上限也是可以调整的，由矿工们进行投票决定。**

Tezos 提供了 Michelson 语言/语法框架来编写智能合约。这套语言没有限定智能合约的具体写法。Tezos 提议用户利用 Michelson 的一些特性，在写合约时加上一些限制，以防止安全问题。譬如，通过对单个交易中程序允许执行的最大步数、区块的大小设定一个上限，可以避免恶意用户提供大量参数，导致交易在 Gas limit 以内无法完成，进而导致合约 deadlock（锁死）。

**4）安全**

Bitcoin 在 2010 年 8 月 6 日被发现了协议的漏洞：交易的信息在没有经过正确验证之前，就被列入交易记录里面。在这一次交易中生成了超过 1840 亿枚 Bitcoin，并被发送到两个 Bitcoin 地址上。即此次漏洞的发生是由于 Bitcoin 的编写语言 C++ 无法对其执行的代码进行检查。

因此，为了解决此类安全问题，Tezos 采用 Ocaml 语言作为程序语言，并利用 Michelson 语言编写智能合约。Caml 是函数式编程语言，它的扩展语言还有基于微软.net 平台的 f# (fsharp)语言。OCaml 将 Caml 语言在面向对象方面做了延展。

相对 C++ 语言来说，Ocaml 与 Michelson 语言虽然语法简洁，编译速度快，形式化验证功能比较强大，但是语言应用范围较小，且编写难度较大。而因其技术门槛较高，在一定程度上限制了开发者的使用。

##### **自我修正的加密账簿**

1）协议层

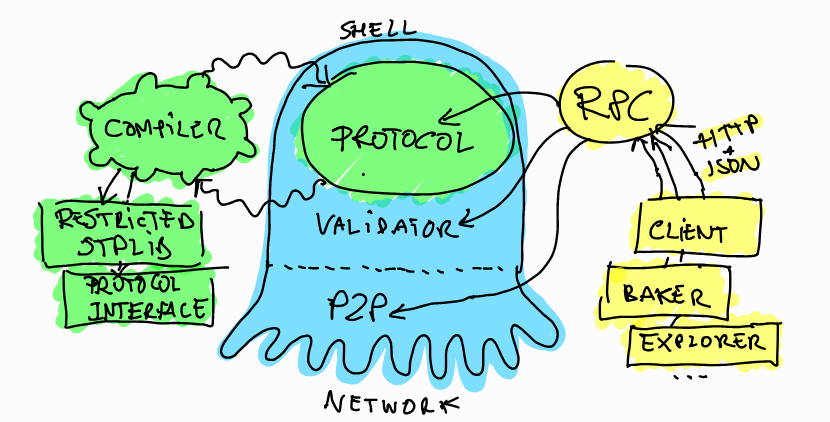
Tezos 区块链协议层与 Bitcoin 协议层类似，包括以下三层：

* 网络协议层：发现并广播交易
* 交易协议层：定义有效交易
* 共识协议层：形成针对主链的共识

2）网络 shell

Tezos 将这三个协议层进行了分离。交易协议层和共识协议层被置入一个负责维护区块链的通用的网络 shell 内。对三个协议层进行分离的原因是为了便于实现协议的自我修正与升级功能。

Tezos 总体技术架构如图：



整个蓝色部分表示一个节点。其中的绿色部分是所谓的经济协议（economic protocal），简称协议。该协议会根据社区投票决策机制来决定自我修复，这是 Tezos 的一个主要特性。

##### **Tezos 种子协议**

Tezos 的种子协议是一种可以被广泛应用和修改的区块链协议，即可以通过修改其种子协议来支持多种基于区块链的算法，实现快速迭代代码以及升级算法，从而自我修正成为一套新的区块链协议。

Tezos 采用 Michelson 语言编写智能合约。Michelon 是一种比较高级的语言，目前采用此语言进行智能合约编写的项目较少。通常情况下，程序员会采用 Liquidity 语言编写智能合约，然后再编译为 Michelson。Tezos 在安全方面提出了一个「 formal verification」的概念，并通过 Michelson 来执行。但此技术在区块链应用还不成熟，因此目前应用还较少。

「 formal verification」即形式化验证，是根据某个或某些形式规范或属性，使用数学的方法证明其正确性或非正确性。这是一个系统性地验证过程，将逻辑形式与功能进行一致性比较。此验证方法主要用于对误差要求极高的行业，譬如核电站、航天和医疗设备等。

功能评测

Tezos 是一个分布式的「共识平台」，不仅能如 Bitcoin 或者以太坊一样就账本状态达成共识，而且能就协议和节点的升级、改造方式也达成共识。

Tezos 目前有三个网络：

* Betanet：这是目前 Tezos 区块链的主要实验网络。它使用 XTZ 运行，是 Tezos 主网正式发布之前的最后一步。该实验网络于 2018 年 6 月 30 日启用；
* Alphanet：Tezos 区块链的测试网络，运行与 Betanet 相同的代码，很少重启，适用于想要在 Beta 之前测试软件的开发人员或者希望在使用真正 XTZ（Tezos Token）之前熟悉网络的用户；
* Zeronet：Tezos 的最新开发网络，可能会随时重启，主要由 Tezos 内部开发人员使用。

可以使用 Docker image（容器镜像）或本地编译运行 Tezos Betanet，因为本地编译仅限于 Linux 环境，这里使用镜像方式搭建其网络节点。

首先，下载 DOCKER 环境，然后运行下列命令，就可以获得最新的 docker image，运行 Betanet 节点：

wget -O betanet.sh https://gitlab.com/tezos/tezos/raw/master/scripts/alphanet.sh

chmod +x betanet.sh

这时，可以使用下列程序：

* tezos-node：Tezos 节点后台程序；
* tezos-client：Tezos 命令行客户端和钱包；
* tezos-admin-client：节点管理工具；
* tezos-{baker,endorser,accuser}-alpha：在 Tezos 网络上执行烘培（bake）、背书（endorse）和归责（accuse）的后台程序。（在 Betanet 上，后台程序的名称必须包含序号和所绑定的协议的部分哈希值，例如tezos-{baker,endorser,accuser}-002-PsYLVpVv）；
* tezos-signer：从远程对操作或者区块签名的客户端。

通过调用这些程序，就可以运行 Tezos 网络上的所有功能。

# **TEZOS 节点的使用**

节点实际上就是 Tezos 区块链的各个组成部分，其功能主要用两个：运行通信网络和更新环境信息，构成了一个 P2P 网络。

Tezos 网络中有两种账户，一种是隐式账户，即普通账户；一种是发源账户，用于委托 Token或者执行 Michelson 代码，即智能合约。

节点在「定义智能合约」部分实现如下例所示：

tezos-client originate contract id for alice \

transferring 1 from alice \

running ./src/bin\_client/test/contracts/id.tz \

--init '"hello"'

Id.tz 这个文件就代表了一个智能合约，上述语句就是对其内容的初步设定。

声明该合约时，不光显示 alice 要向 id.tz 这个智能合约账户支付1 Token，而且还需要支付一定的费用（Gas fee）。这个费用取决于合约和初始化内容（“hello”）的存储需求。如果用户觉得可以接受这样的费用，就可以执行下列命令，真正执行该交易：

tezos-client transfer 0 from alice to id --arg '"world"' \

--Gas-limit 1475 \

--storage-limit 46

其中对费用和存储空间都设置了最高值。如果实际消耗超过该最高值，交易将会失效。烘焙方（baker）会更倾向于采用 Gas 和存储限值较低的交易，因为这样成本较低，所以用户需要尽可能挑选接近实际的限值。

# **TEZOS 区块链的运行**

在参与 TEZOS 区块链网络运行时，可以采取两种方式：把 Token 委托给别人，或者自己充当委托人。

1. 把 Token 委托给矿工

执行下列命令，就可以把 alice 的 1000 个 Token 委托给 bob：

tezos-client originate account alice\_del for alice \

transfering 1000 from alice \

--delegate bob

其中alice\_del实际上是一个中间合约，alice 先把 1000 委托给它，再尤其交给 bob。

1. 自己充当矿工

矿工负责烘培区块（即挖矿，Tezos 称之为 Baking ）、担保（endorse）区块，以及对其他试图双重烘培或者双重担保的委托人进行追责。

在网络中，烘培和担保权会按照与每个委托人所获得的卷数（1 卷是一万个 Token）成正比的方式，随机地分配给委托人。一卷就是一万个 Token，所有计算都会取最近整数，譬如 1.6 万个 Token 会取为 1 卷。

1. 保证金（deposit）

如果某个委托人想要烘焙或者担保一个区块，委托人就需要冻结一笔保证金（也叫 bond，债券）一段时间（由 preserved\_cycles 参数指定）。因此，委托人必须要拥有足够的资金，支付它在preserved\_cycles 时间内可能烘培/担保的所有区块的保证金。目前要求的保证金是，烘培一个区块需要缴纳 512 XTZ，担保一个区块需要 64 个。

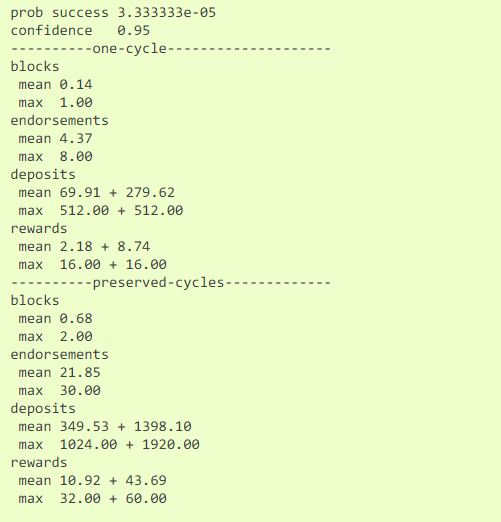
对于其他人委托来的 Token，委托人并不能使用这些 Token，而是只是将其添加到卷中，用以获得烘培或者担保的机会。所有保证金都必须要委托人自行支付。

1. 预测获得烘培/担保的机会、保证金和奖励

假设用户拥有一券币（roll），需要预估烘培或者担保的机会，以便准备相应的保证金。这个几率取决于网络上当前有效的卷数，这样我们就可以知道在一个周期内可以烘培或者担保多少个区块。要获得当前有效的卷数，需要这两个数据：

1. 当前有效委托人数：delegates?active
2. 每个委托人的余额：stacking\_balance

将其加和之后，再除以10k（每卷10k 个 Token），就得到卷数。目前，在 betanet 上有效卷数为 30k 个。这意味着有一卷的用户，获得烘培权的机会是 1/30k，担保权是这个机会的 32倍。因为每次抽签都是离散的，所以被选中的概率符合二项分布：p=1/30k。另外一个参数是抽签次数。在一个周期中，烘培的抽签次数是 n\_b = 4096，担保的抽签次数是 n\_e = 4096 \* 32。这样 p \* n 就是获得选中的几率（平均值）。每个周期中，实际的几率将会围绕这个值波动。Tezos 提供了一个 Python 脚本用以计算一个周期和多个周期内烘培、保证区块的平均和最大几率，以及保证金和回报的平均值和最大值，运行结果如下：



1. 烘培

烘培后台程序会在链接一个帐号以后，计算该账户的烘培权，搜集交易和烘培区块。调用命令如下：tezos-baker-alpha run with local node ~/.tezos-node bob

6. 担保

担保后台程序会在连接到一个帐号之后，计算该账户的担保权，然后在接收到一个区块之后，验证区块的有效性，执行一个担保操作。调用命令如下：tezos-endorser-alpha run

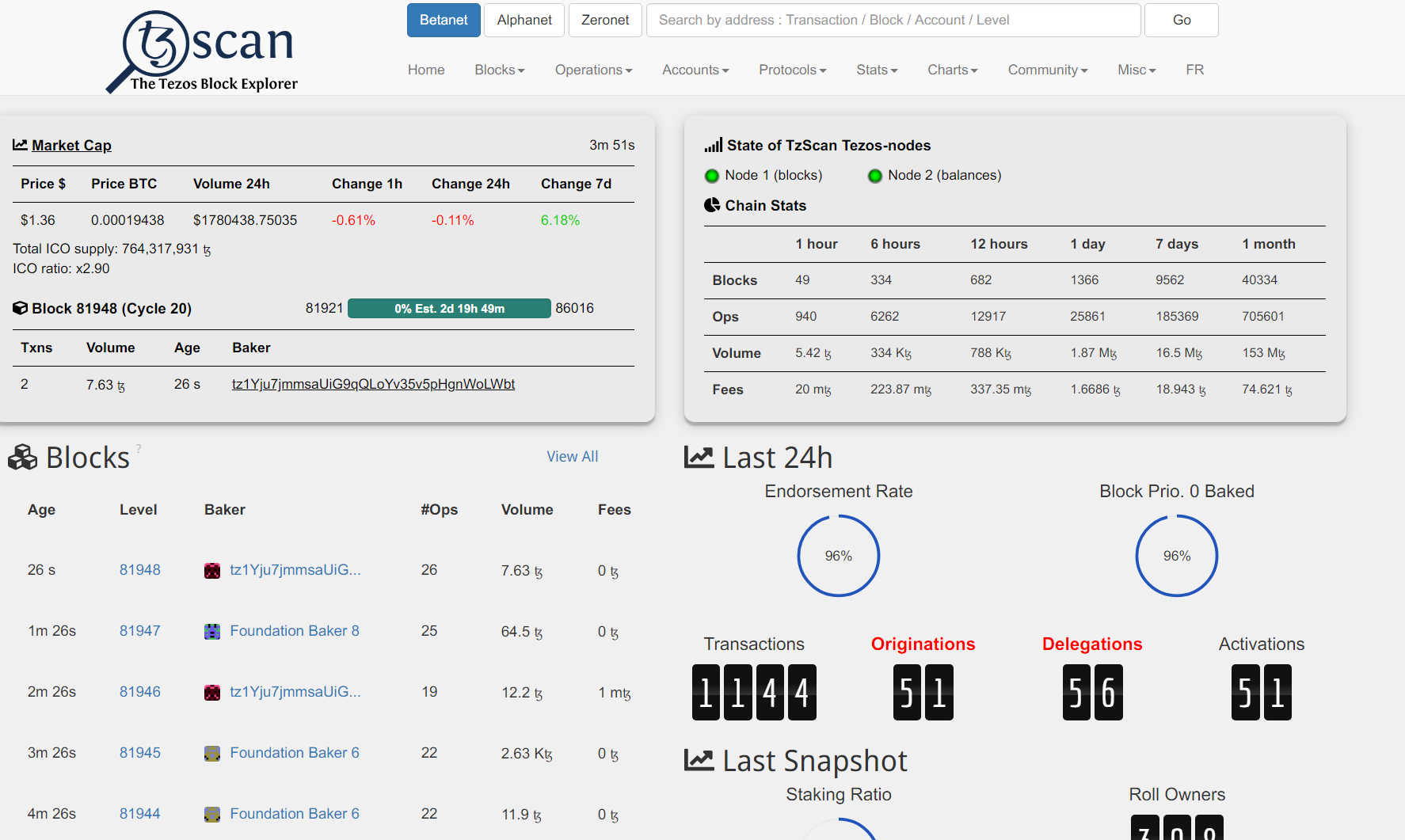
7. 指责（Accuser）

指责后台程序会在监控所有链上的所有区块，寻找：

* 在同一层级上对两个区块进行签名的烘培方；
* 对同一个烘培槽，进行超过两次担保操作的担保方。

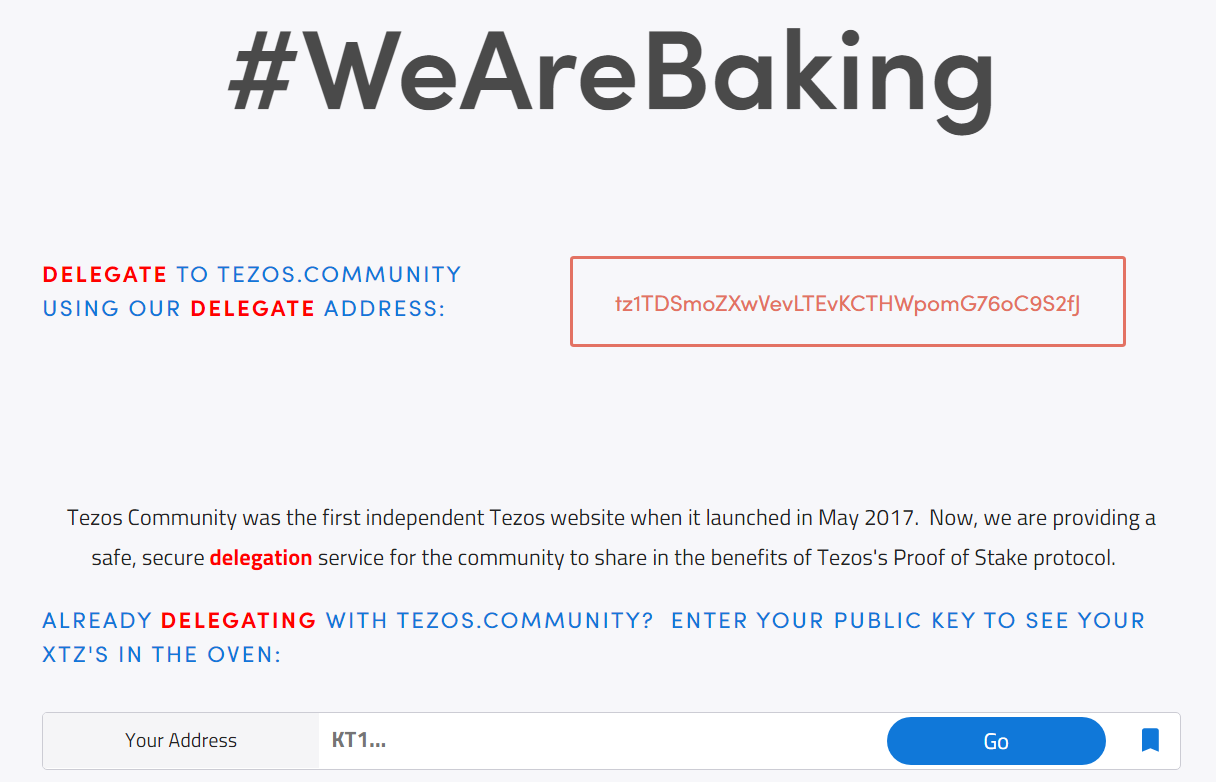
一旦发现这些情况，该程序就会执行双重烘培或者双重担保指责操作，导致犯规者失去保证金。调用命令为：tezos-accuser-alpha run。

以上基本覆盖了其主要功能。在 <http://tzscan.io/> 网站，可以查看当前各个网络上的情况，以下以 Betanet 为例：

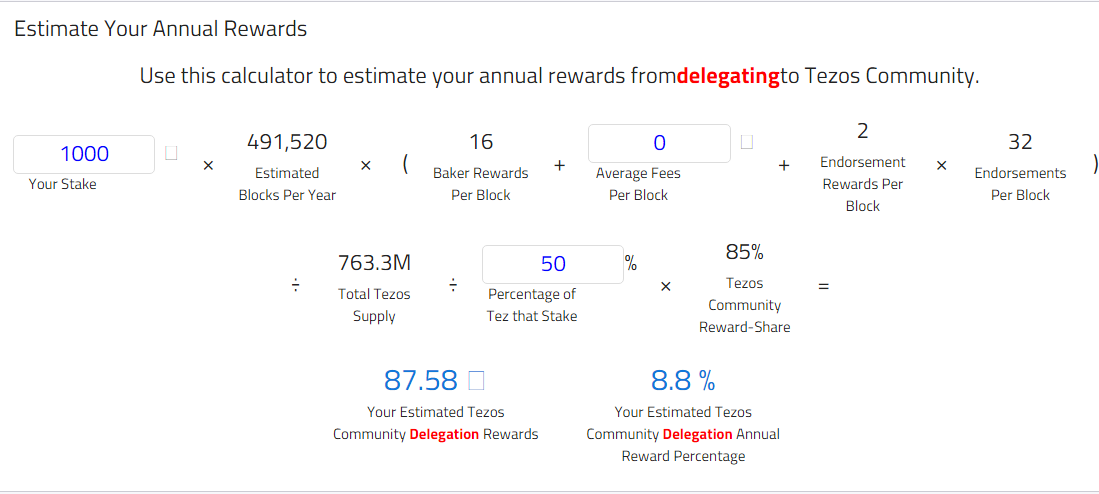


另外，Tezos 社区也提供了委托服务，即用户可以选择把自己的 Token 委托给他们进行烘培或者担保，以获得回报：

<https://www.tezos.community/delegate-home>



它们提供了预计的回报率，目前可以达到 8.8% 的年回报率。



##### GitHub 代码质量评测

Tezos的代码已经开源，发布于：<https://gitlab.com/tezos/tezos/> ，所有开发者文档位于：[http://doc.tzalpha.net](http://doc.tzalpha.net/)。

核心代码都位于：<https://gitlab.com/tezos/tezos/tree/master/src>，主要用比较小众的 OCaml语言编写。

节点负责通过 RPC 端口监听，借助 HTTP 协议，以 JSON 文件格式从网络上的烘培方（baker）获取各种链信息，选择和下载各种链信息，再提供给协议进行检查，设定一个绝对值。而后，节点将会选择绝对值最高的有效头部分析。这部分被称为验证器（validator）。节点其他部分包括 P2EP 网络、磁盘存储、账本状态和节点间通信等。

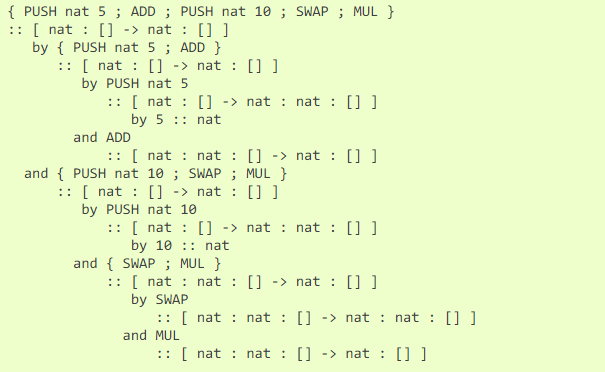
因此，其代码也主要分为以下几个部分：

* tezos-base：包含了所有和区块链网络相关的代码；
* tezos-shell：负责节点通信、P2P 网络和 PRC 的代码；
* tezos-protocol-environment: 与协议和其编译器有关的代码；
* client 库：和 client 有关的代码。

另外，Tezos还支持用其定义的 Michelson 语言构建智能合约，其代码位于 [**micheline.ml**](https://gitlab.com/tezos/tezos/blob/master/src/lib_micheline/micheline.ml) 库

并提供了详细的语法说明

下面是用 Michelson 语法计算 (x+5)\*10 的范例：



总体而言，代码结构相当严谨，注释完整，更新频繁。

##### 锁仓代码检查

虽然项目披露会锁仓 20% Token， 但是没有在代码中找到锁仓代码。

##### 总结

从代码质量分析，Tezos 项目的开发团队实力较强，代码书写较为规范，代码更新频率较高，文档也写得较为详细。通过对烘培、担保、追责等各方机制的限定，达到了效率和安全性兼备的效果。不足之处是其语言用了比较小众的 OCaml 和 Michelson，目前看到的智能合约还很有限。

标准共识分析：

为了便于实现「自我进化」，将三个协议层分离，架构设计创新性较高；代码书写规范，更新频率较高，文档详细，整体来说代码质量较高。

Tezos 基于 Ocaml 语言开发协议，利用 Michelson 语言部署智能合约，其优点是简洁、编译速度快、功能强大。但编程语言技术门槛较高、比较小众化，目前并未看到智能合约的应用实例。

Tezos 采用形式化验证技术检验智能合约，但此技术在区块链应用还不成熟，因此目前应用还较少。

#### Token 生态系统

Tezos 初始供应总量为 763,306,929.69 XTZ，按照规划分配如下：

|  |  |
| --- | --- |
| **分配** | **数量** |
| 首次公开募集支持者 | 607,489,040.89 XTZ |
| 早期支持者和项目贡献者 | 3,156,502.85 XTZ |
| Tezos 基金会和 DLS | 76,330,692.97 × 2 XTZ |

DLS ：Dynamic Ledger Solutions Inc.公司，是创始人注册的公司实体。

Tezos 基金会 和 DLS 的分配额，行权期为 4 年，每月解锁一次。也就是初始供应总量的 20％ （Tezos 基金会10% + DLS 10%）处于锁仓。

##### Token 主要用途

Tezos 的激励体系中必须持有 Token 才可以拥有以下权力：

* 部署和运行节点
* 创建和验证区块
* 对网络治理问题进行投票

具体在挖矿环节，Token 主要作为债券（ bond）和奖金（reward）两种用途。

1）债券

Tezos 中负责出块的矿工需要冻结一部分 Token 作为押金，也就是 「债券」，如果出现双花，这些押金就会被没收。Tezos 修改了第一版白皮书后补充到：**见证人也要抵押债券(endorsers will also be required to purchase bonds) ，**是一种担保（Endorsing

）机制。

2）奖金

一次周期完成，矿工和**见证人**会得到奖金。

3）增加成为下一个矿工的机率

根据 Tezos 的共识机制，最高优先级的持币人很可能会在上一个块出现后一分钟后挖出下一个。优先级第二的持币者可能在两分钟后挖到下一个块，以此类推，优先级第三的会在三分钟后挖到下一个块。

矿工每挖一个块将获得 512 个 tez作为奖励，但需要抵押 1536 个 tez。每个区块签名将获得 32∆T−1 个 tez 的奖励。这里 ∆T代表以分钟为单位的区块和先前区块之间签名的时间间隔。每个区块至多有 16 个签名，但签名不需要抵押 Tezos 。

Tezos 也提供了委托服务，即用户可以选择把自己的 Token 委托给他们进行挖矿或者担保，以获得回报。

##### 共识机制

## 

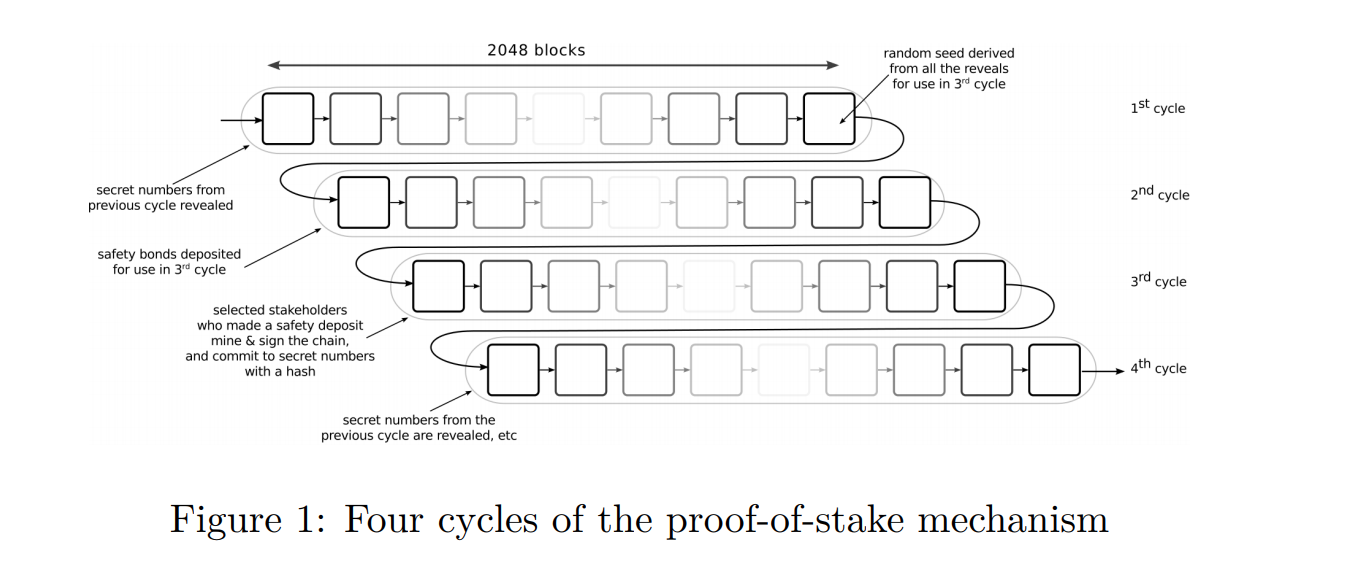
## Tezos 使用的是一种改良的集成了 Slasher ，chainof-activity 和 proof-of-burn 的 POS 机制。。

## 区块由随机的矿工挖出，并包括随机的持币人（签名人）提供的前一个块的多签。挖矿和签名都将获得一笔小奖励，但系统也要求挖矿者存一笔押金，质押期限由第一版白皮书的一年修订为一个周期。如果验证期间出现双挖或者双花，那么这笔押金将被没收。

标准共识分析：

## 1） Slasher 是由 Vitalik Buterin 提出的一种对 PoS 的改良，在 Tezos 的 PoS 机制中， Slasher 主要是以没收押金惩罚双挖或双签节点的方式；

2）chainof-activity 机制设计的目的是为了解决随机分叉问题，规定只有唯一一个权益人可以创建下一个块，并通过一个交叉机制在之前的区块中确认权益人。具体在 Tezos 的实现如下图所示：



Tezos PoS 机制的四阶段：

第一阶段：以 2048 个区块为周期运行。在每个周期的开始，上一个周期的矿工随选取下一阶段的种子，提交至第三周期，上一周期的哈希值需要在此阶段公开。

第二阶段：矿工的押金释放，用于第三阶段。

第三阶段：矿工挖矿、签名并用密钥生成哈希值提交。

chainof-activity 在此作用是决定谁将成为每一个周期的矿工的，依据「follow the coin strategy」策略，最高优先级的持币人很可能会在上一个块出现后一分钟后挖出下一个。优先级第二的持币者可能在两分钟后挖到下一个块，以此类推，优先级第三的会在三分钟后挖到下一个块。

4）Tezos 认为以 Bitcoin 为代表的 PoW 存在算力集中和 51% 攻击等问题，因此设计了一套改良的 PoS 机制。

在 Tezos 的逻辑推演中，如果有人持有多数算力，那么它必然持有多数的货币，这样的结果是如果要发动 51% 攻击的成本很高，增加了系统的安全性。

其次 chainof-activity 机制有利于鼓励 Token 持有人积极参与生态建设；

综上，Tezos 对 PoS 的改良增加了系统安全性，有利于系统生态，创新性值得肯定。

根据目前 Betanet 测试网的运行情况，差不多1分钟生成一个区块，每个区块大约15-20比交易，因此 TPS 是大约0.3笔交易/秒，PoS 机制在大量用户的情况下能否有效提高网络性能尚未可知。

**社群基础**

##### 用户社区

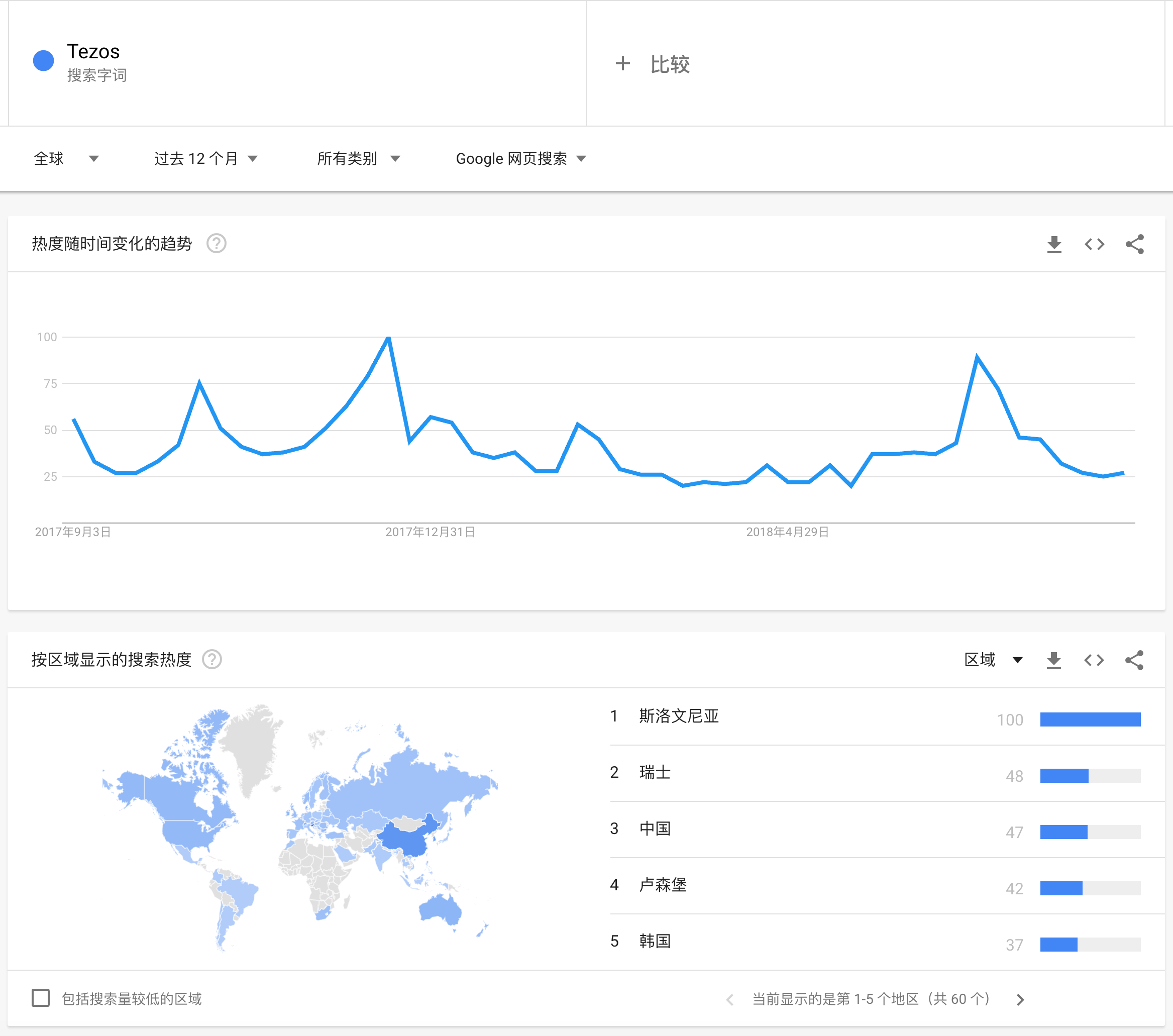
Tezos 使用了 Riot.im 作为社区沟通平台，聊天室成员有 5000 人，讨论积极、质量较高，并不只限于币价讨论，管理员维护行为积极。Tezos 开设了自己的论坛 https://forums.tezos.community/

|  |  |  |
| --- | --- | --- |
| **分类** | **地址** | **表现** |
| riot.im | https://riot.im/app/#/room/#tezos:matrix.org | 成员：5,000 |
| Facebook | <https://www.facebook.com/tezosledger/> | 关注者：3,933  点赞数：4,372 |
| Twitter | <https://twitter.com/tezos> | 关注者：37,200  点赞数：283 |
| Medium | <https://medium.com/tezos> | 粉丝数：2,000 |
| Reddit | https://www.reddit.com/r/tezos/ | 订阅者：9,700 |

##### Google 趋势

根据 Google 趋势，目前搜索「Tezos」的热度较高的地区为斯洛文尼亚，其他地区依次为瑞士、中国、卢森堡、韩国。目前综合来看，欧洲搜索热度最高。

下图为 Google 趋势截图：

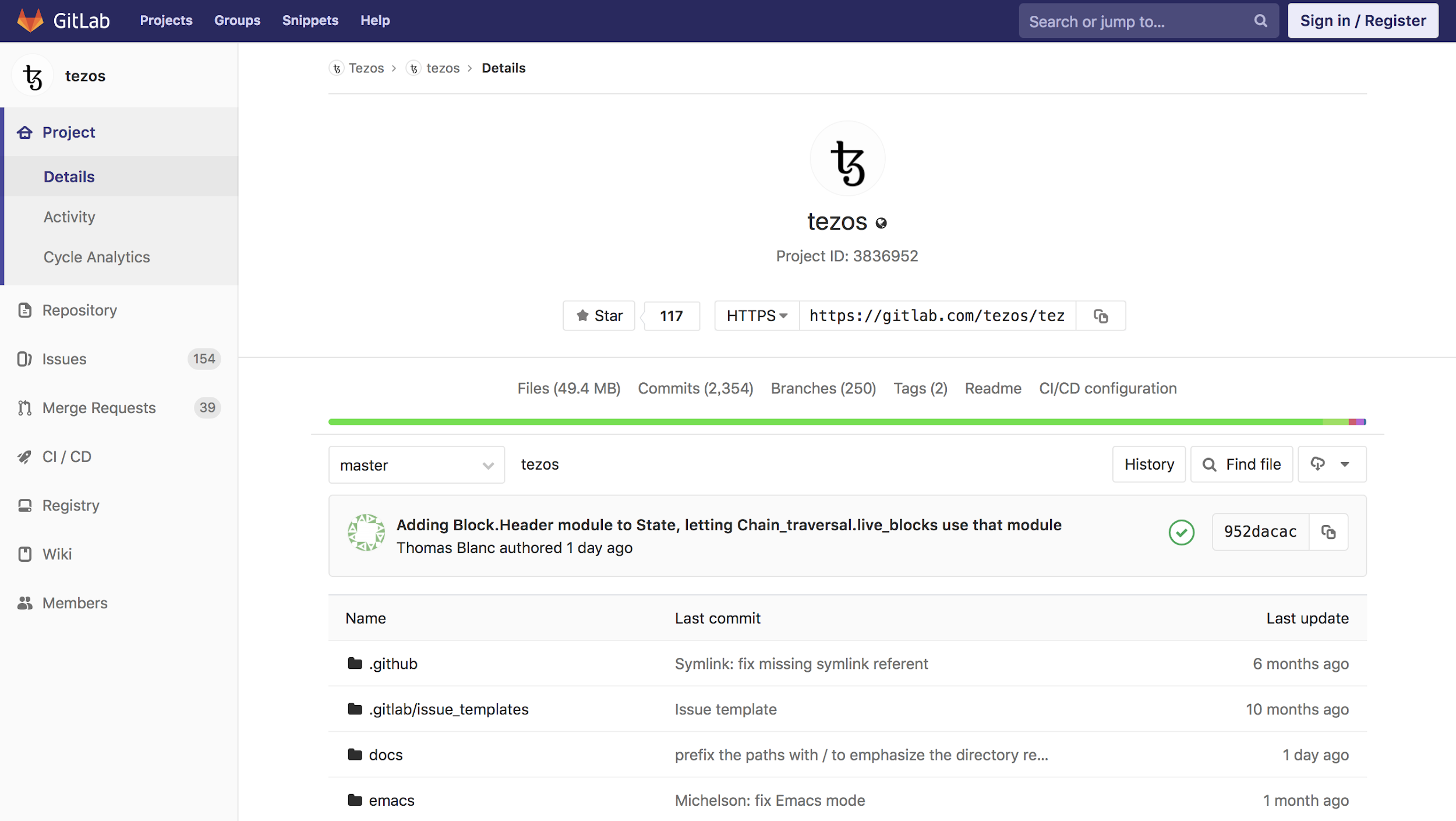


##### 开发者社群

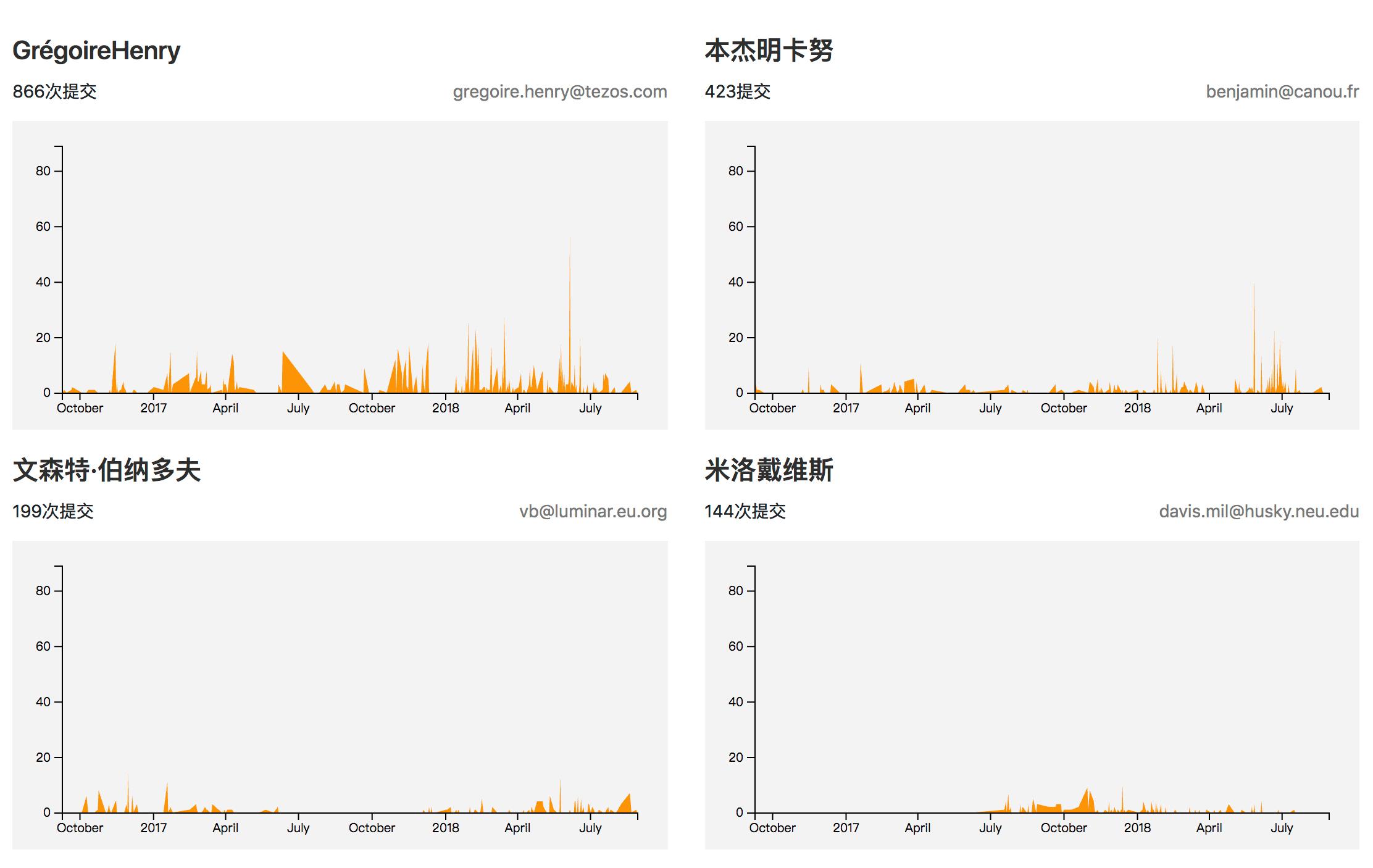
Tezos 2018 年 1 月主要开发平台由从GitHub 换成了 GitLab， 因此以 GitLab测评数据来源。

官方的 GitLab 主页有 5 个库，其核心代码库为是 tezos ，该库有 2,354 个 Commits、250 个 Branches、2 个 Tags。

下图为 Tezos 官方的 GitLab 主页：



标准共识分析：

开发者社群关注度较高，star 数为 117，主力开发者数量较多，提交 Commits 数量超过 50 的有 10 位，并且提交排名前三位的都是官方团队成员。

#### 团队分析

Tezos 官网上没有公布具体团队成员，根据 LinkedIn 和公开信息整理创始人信息如下：

|  |  |  |
| --- | --- | --- |
| **管理层** | **职位** | **背景介绍** |
| Kathleen Breitman | 联合创始人CEO | 毕业于美国纽康奈尔大学  曾在华尔街日报担任研究员  曾在 R3 CEV 担任区块链高级战略顾问 |
| Arthur Breitman | 联合创始人  CTO | 毕业于纽约大学应用数学专业。  曾担任 Google X 和 Waymo 的研究工程师  高盛和摩根士丹利的定量分析师 |
| [Bozman Çağdaş](https://www.crunchbase.com/person/bozman-cagdas) | 团队成员 | 毕业于 Denis Diderot 大学，硕士学位，主修专业计算机工程 - 语言与程序设计  毕业于理工学院，博士学位，主修电脑科学  曾在达索系统软件公司研发实习  曾担任 OCaml Pro 公司高级研发工程师 |
| Vincent Bernardoff | 团队成员 | 原 Domoco CEO 和联合创始人  巴黎大学计算机科学硕士学位 |

标准共识分析：

* 项目的 CEO Kathleen Breitman 和 CTO Arthur Breitman 是一对夫妇，Arthur Breitman 是白皮书作者，在应用数学方面有深厚的学术背景；在公开募集的介绍和其它新闻报道中公布了一些技术人员的名字，但没有相关的详细介绍; 综合公开信息，开发团队中有 OCaml 语言开发经验的程序员。
* 对项目产生重大影响的人事事件是：项目在完成成功的首次公开发售以后，创始人与Tezos Foundation 主席 Johann Gevers 发生了纠纷，在一系列争议和谈判以后「自愿退出」了董事会。Johann Gevers 拥有南非国籍，在瑞士做企业管理和咨询工作，曾经帮助以太坊发行 Token。

### **治理结构**

#### 链上治理

**协议修改**

Tezos 设计了以投票决议方式来修订协议，每一个投票周期时长为长度为2的17次方，即 131 072 个区块时间。投票结果的生效需要达到最小投票人数，满足 Q = 80%，但会为了反映平均参与度而动态适应。

第一阶段

建议修改协议需要提交一个代表新协议的.ml 和.mli 文件的 tarball 打包的哈希。Token 持有人可能会批准任意数量的所提交协议。

第二阶段

在第一阶段获得最多批准的修改案基础上进行投票。投票人可以投票反对或者弃权。弃权票也计入总投票人数。

第三阶段

如果达到最小投票人数 (包括明确的弃权)，并且修改案达到了 80% 的支持率, 那么修改案就会被批准，并替代测试协议。否则它将被否决。假设投票人数值为 q，最小投票人数 Q，则按 Q ← 0.8Q + 0.2q 更新。

第四阶段

假定修改案被批准，则于第三阶段开始的时候在测试网络运行该修改案。Token 持有人将进行第二次投票来确认他们确实想要支持测试协议替代主协议。这也要求一定的法最小投票人数 ，以及 80% 的支持率。

#### 

#### 基金会

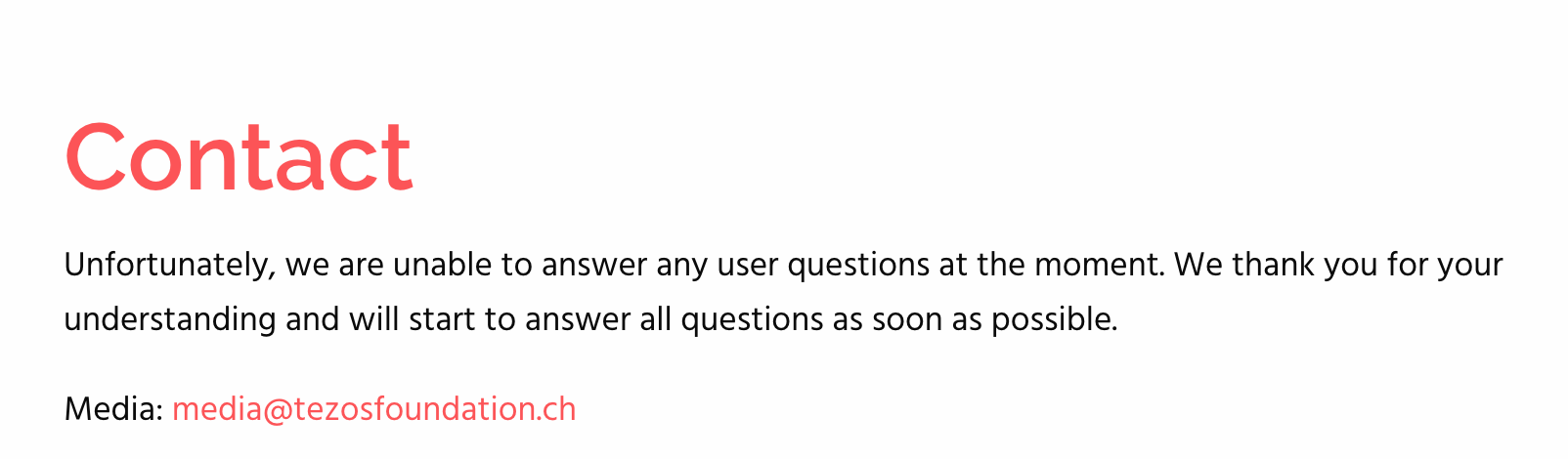
Tezos 之前成立了「Tezos Foundation」<http://tezosfoundation.ch/> ，第一任主席是 Johann Gevers，之后因为与创始人的纠纷，在一系列争议和谈判以后「自愿退出」。现任主席是 Ryan Jespersen，原为社区志愿者组建的「T2基金会」的主席。

根据基金会网页的新闻发布信息，成员还包括： Lars Haussmann、Ryan Jesperson 、Michel Mauny、Olaf Carlson-Wee、Pascal Cléré、 Marylène Micheloud 和 Hubertus Thonhauser 。但并未公布完成完整成员名单列表。

标准共识分析：

Tezos 的链上治理设计了「 修改规则」（Amendment rules），依据这一规则，所有 Token 持有人都可以参与系统规则的修改，是一种分布式的治理机制。这一构想有很高的创新性，但目前项目主网尚未上线，没有发生过投票修改事件，规则在实际运行中的效果尚未可知。

Tezos Foundation 属于链下治理机构，但并未公布完整成员名单。网站信息十分有限，连联系方式页面显示「目前不回复任何用户问题」。



**项目履约情况**

* 项目没有公布路线图。
* 根据基金会的新闻发布，Tezos 将在2018年第二季度推出Tezos betanet、第三季度发布Tezos主网络 mainnet。目前 betanet 已经上线。
* 在 2017 年 12月 Reddit 的用户提问中，项目方关于未来计划的回复中列出了一些未来计划点，但没有披露预计达成时间。主要是对现有协议的修订和优化，还包括：简化 PoS 算法 、在保证安全的前提下调整协议常量以增加吞吐量和降低成本、用于智能合约的散列存储、实现Bitcoin的 UTXO 模型、兼容 zcash、升级协议后的预测市场。原文链接：https://www.reddit.com/r/tezos/comments/7m25fo/roadmap\_for\_development/  
    
  **项目信息披露义务**
* 项目的主要信息披露渠道包括：网站、白皮书、riot.im、Reddit 等，团队能够及时回复用户问题；但没有在以上渠道公布完整的团队成员名单 、完整的基金会成员名单。
* 项目没有建立周报制度；
* 项目没有公示路线图；
* 项目的技术相关细节在 GitHub 的 和 GitLab 文档中披露得较为完善。

标准共识分析：

项目没有公布完整的团队成员尤其是技术团队履历、基金会成员名单；没有建立周报制度，信息透明度较低。

### **交易模块**

#### 价格表现

图表：XTZ 分配

|  |  |
| --- | --- |
| **项目** | **数值** |
| 价格 | $1.37 |
| 流通供给量 | 607,489,041 |
| 总供给量 | 763,306,930 |
| 流通率 | 79.59% |
| 流通市值 | $832,259,986 |
| 市值 | $1,045,730,494 |

*资料来源：Coinmarketcap，数据截止时间：2018 年 8 月 30 日，SNC 分析部*

图表：交易平台覆盖率及影响力

|  |  |  |  |
| --- | --- | --- | --- |
| **交易平台** | **交易对** | **交易对占比（%）** | **交易平台占比（%）** |
| HitBTC | XTZ/USDT | 41.63% | 50.41% |
| XTZ/ETH | 6.97% |
| XTZ/BTC | 1.81% |
| Gate.io | XTZ/BTC | 21.67% | 37.43% |
| XTZ/USDT | 13.35% |
| XTZ/ETH | 2.41% |
| Coinone | XTZ/KRW | 12.26% | 12.26% |
| 共登陆 4 家交易平台，成交主要集中于 3 家交易平台，交易平台覆盖率及市场影响力较低。 | | | |

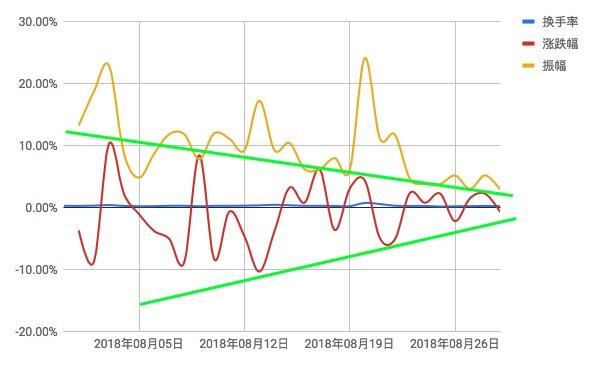
注：剩余交易平台合计占总成交量的 0%（交易量占比不足 1% 不予显示）

*资料来源：Coinmarketcap，数据截止时间：2018 年 8 月 22 日，SNC 分析部*

图表：交易对影响力

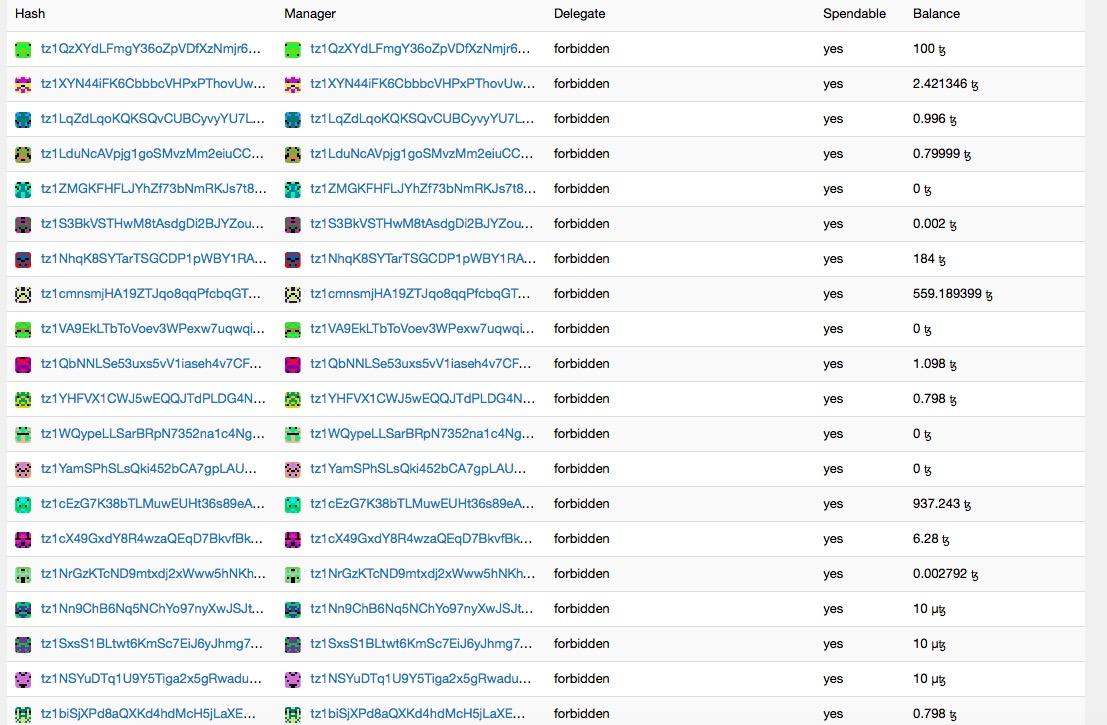
|  |  |
| --- | --- |
| **热门交易对** | **总成交量占比** |
| XTZ/USDT | 54.98% |
| XTZ/BTC | 23.48% |
| XTZ/KRW | 12.16% |
| 共有 5 种交易对，热门交易对 3 种，覆盖主流交易对，并且在韩国市场具有一定热度。 | |

*资料来源：Coinmarketcap，数据截止时间：2018 年 8 月 30 日，SNC 分析部*

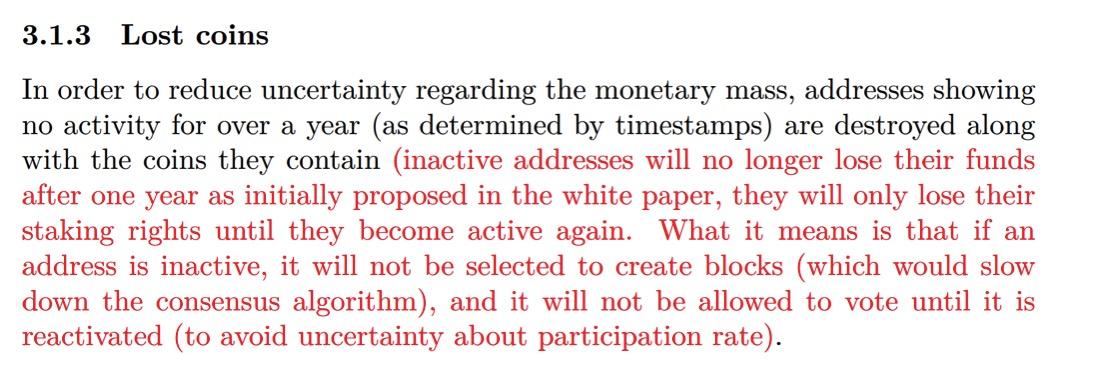
近一个月的全市场平均换手率为 0.29%，换手率低，流通性风险高，存在较大的踩踏风险。个别交易日振幅较大，而涨跌幅波动处于逐步缩窄过程，市场观望情绪浓厚。

#### 持仓分布

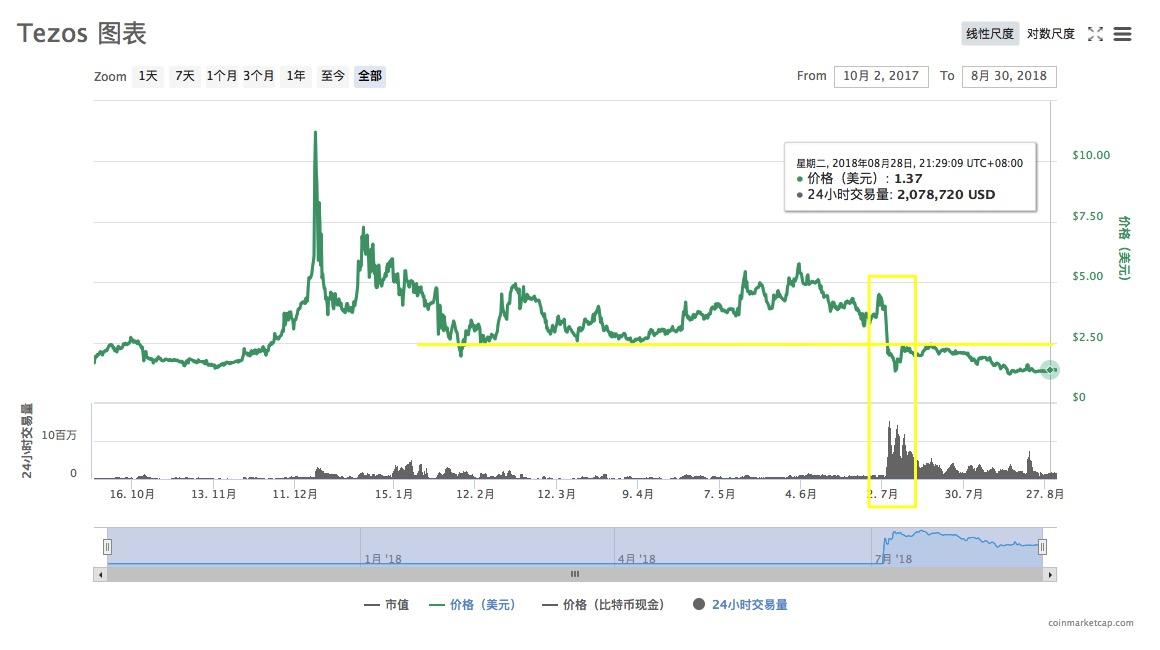
根据 Tzscan.io 数据显示，XTZ 的持仓地址数量为 21,615，但由于 XTZ 的持仓地址并非根据持仓大小排列，所以无法确定 XTZ 的持仓集中度。主网显示出 8 个 Foundation Baker 地址合计持有 20,598,781.86 个，与基金会所持 10% 具有较大差距。经追溯后 tz1RXwDDhrSKPorSPPJFy3tD9Rj341ihCvbv 地址为基金会初始转出地址，共转出近 6900 万。整体而言，XTZ 持仓地址少，用户及投资者基础较为薄弱，虽然公布了基金会地址，但存在过多次分仓，监督难度较高。

标准共识针对持仓地址进一步分析，存在大量被禁止账户，根据白皮书介绍一年内没有任何动作的地址将被禁止，表明 XTZ 用户使用意愿较低。

下图是项目对于禁止地址的说明：



#### 市场表现

从 Coinmarketcap 的全市场走势图来看，2018 年 7 月 6 日换手率峰值为 1.52%，较整体交易量有较高程度放量，此阶段大幅度下跌，跌穿支撑平台，整体流通性风险大。

具体的交易对表现上，HitBTC 交易平台的 XTZ/USDT，价格走势呈下降趋势，近期成交量有所放大，底部震荡盘整，寻求底部支撑。

最后来看 Gate.io 交易平台的 XTZ/BTC，价格波动较大，流通性差，投机风险较高。

**综上所述，流通性风险高，用户基础薄弱，存在大批量被禁止账户，用户迁出较为明显。**

#### 

## Outlook 展望

### 宏观经济展望

中国人民银行决定，从 2018 年 7 月 5 日起，再次下调国有大型商业银行、股份制商业银行、邮政储蓄银行、城市商业银行、非县域农村商业银行、外资银行人民币存款准备金率 0.5 个百分点，此次已经是央行年内第三次降准。6 月 19 日中国拟提升个税起征点至 5000 人民币，纳税总额将减少 1720 亿，国家多次缓解资金流动性。但目前商业银行大幅上调大额存单利率，及中国和中国香港银行间同业拆借利率都处于较高水平。皆表明市场整体资金流处于紧张状态。

我们预计，市场资金将由权益类投资标的向债务类和储蓄类投资标转移。数字货币市场也难在资金流趋紧的环境下独善其身。市场发展将在新生资金增长缓慢的压力下运行趋缓。6 月 14 日美联储再次加息 25 个基点，在美元持续走强的背景下，将加剧欧洲的债务危机以及新兴国家的货币波动，这些都会影响国际市场投资者的投资判断，去寻求新的投资标的。数字货币市场作为一个在不断完善过程中的金融市场，必将不断吸引新的资金进入。

另外，随着 6 月 15 日 美国将对中国 500 亿美元商品加征 25% 关税；6 月 16 日中国对美国 500 亿美元进口商品加征 25% 关税，皆 2018 年 7 月 6 日起实施。表明中美贸易战硝烟再起，国际经济形势再次紧张。

综上，目前我们对市场总体保持中性判断。

### 未来评级展望

如果 能够持续推进项目，综合二级市场最新的交易表现，我们可能调整其风险评级等级。

## Rating Action 评级结果

「」，该项目投资风险较高，投资者应该密切跟进观察和监督项目进展。主要依据是：

「」，该项目属于「一般风险」水平，需要投资者注意。主要依据是：

整个虚拟货币市场对宏观经济的波动反应还在自适应期，监管规则持续不明确。这些因素的调节作用不足以给 LRC 风险等级造成决定性影响。

感谢代码评审团成员 对本文中「技术分析」部分作出的贡献。此为 第二次参与技术评测。

免责声明：

* 标准共识提供的「风险评级」服务和其它一切相关评级产品仅是一种投资风险的提示，是标准共识根据调查和研究结果得出的结论。它并非衡量评级对象本身价值、以及其发行的 token 的价值的工具。
* 标准共识的风险评级仅是对特定风险的提示，而无法展示一个项目或一种虚拟货币的全部风险。
* 任何一个风险评级报告都仅展示某个时间范围内对项目和其 token 生态未来的投资风险预期，而非对未来某个事实确定发生的判断。
* 对任何项目的风险评级不构成投资者作出最终投资决策的全部依据。
* 标准共识仅是金融信息的提供者，评级类产品不对投资者的任何投资决策及其所导致的结果负责。
* 风险评级不是永久有效的，项目的投资风险等级可能随着时间、环境因素和项目进展等外部环境的变化作出调整。同时，评级标准调整也可能会造成项目风险等级变化。任何调整和原因都会向所有投资者公开。
* 在标准共识的评级体系下，我们按照不同的等级对评级对象的投资风险划分，用「S」「A+」「A」「B+」「B」「C+」「C」「D」等符号，由低到高依次表示其投资风险等级，展示一种相对的风险。

参考标准文档：

* 一般项目投资风险评级标准（初创期）