用未来金融赚未来财富

X-DeFi
项目白皮书

2020 年 6 月 1 日

目录

前言

随着区块链产业在社会中的共识人群和产业种类越来越多，各行各界的产业“上链”也发展成了一种趋势。

区块链技术不断的更新迭代，它的安全性、去中心化和无国界的特点受到了传统的金融业关注。如我们所知，传统的金融行业主要是指只具备存款、贷款和结算、保险业务的金融活动，例如银行和保险公司等。此类机构均是完全中心化的运作机制，只要是中心化的机制，就会存在人为干扰因素，导致利益受损的可能。例如：你将钱存进银行或者购买银行理财产品，每年获取0.3%-1%机构给到的收益，在此期间，若是因为人为和不可抗力等因素导致银行破产，或者人为操作失误导致投资的理财产品亏损，因为是完全中心化的运作机制，你的资产就会因为其他人人为的操作失误而造成损失。这种案例在现实中发生过很多，例如：韦格林银行成立于 1741 年，总部设在瑞士东北部圣加仑，有大约 10 家分行，均在瑞士国内。作为瑞士最古老的私营银行，韦格林银行倒闭的导火索就与其帮助美国富人借助秘密账户逃税有关。在 10 年时间内帮助至少 100 名美国客户逃税至少 12 亿美元，在承认帮助美国富人借助秘密账户逃税的罪名并向美国支付 5780 万美元补偿和罚金后，韦格林银行声誉受到严重影响。最终，韦格林银行设在瑞士圣加伦的总部宣布永久关闭。因为这 100 多名美国人，韦格林银行的其它用户资产受到清算的损害。

现在人们愈发的看重自己资产的安全和收益，对传统金融的信任和选择大幅降低。传统金融巨头们为了挽回客户以及寻求未来的发展，也都在尝试着业务模式的升级和转型。在这样的行业背景下，X-DeFi 应运而生；X-DeFi（X-Decentralized Finance）基于 Tezos 技术和生态能够完全消除用户和传统金融行业之间的壁垒。

1 背景介绍

1.1 市场背景——夺回资产控制权

DeFi 之所以备受广大金融用户青睐，在于它正在颠覆影响了人类金融领域数百年的中心集权规则，试图帮用户重新夺回资产控制权。也许你会问：我自己的钱难道我没有控制权吗，为什么还要夺回？是的，他并不完全受你控制。

假如你在银行有 100 万美元存款，你今天急需取出这 100 万美元使用，你认为你今天能够从银行所谓“自己的账户”中提取出这 100 万美元吗?

按照美国相关反洗钱法和联邦政府规定，在 ATM 上单日取款限额 1000 美元，柜台取款不超过 1 万美元，大额取款需提前预约且填写申请表，通过审核后才可取款。

“存钱没限制，取钱各种条条框框”。有过大额取款经历的朋友，对此应该深有感触，钱还是你的，只是绝对控制权不在你手上。如果说需要你配合调查，你的账户资产还会被冻结。如此一来，你还认为你对你的钱拥有绝对的控制权么?

同样，现代金融领域大部分金融产品都有最低准入额，例如你想购买某个银行理财产品或者资产托管，未能达到相应机构设置的最低准入额，你都没有资格进行托管和理财。即使你达到了最低准入额，你投入的资产可能会因为银行或者机构破产，人为投资失败等因素导致财产损失。

例如：英国巴林银行

巴林银行（Barings Bank） 创建于 1763 年，是英国历史最悠久的银行之一，在全球范围内掌管 270 多英镑资产。世界上最富有的女人——伊丽莎白女王非常信赖它的理财水准，曾是它的长期客户。

巴林银行曾创造了无数令人瞠目的业绩，在世界证券史上具有特殊的地位，被誉为“金融市场上的一座耀眼辉煌的金字塔”。1995 年 2 月 27 日，英国中央银行突然宣布：巴林银行不得继续从事交易活动并将申请资产清理，这意味着具有 232 年历史、在全球范围内掌管 270 多亿英镑的英国巴林银行宣告破产。

巴林银行倒闭的原因说起来既可笑又具有讽刺性：一位年轻人——年仅 28 岁的巴林银行交易员尼克·里森将的渎职将已有 233 年历史的英国巴林银行赔了个精光。

1995 年，时任巴林银行新加坡期货公司执行经理的尼克·里森一人身兼首席交易员和清算主管两职。有一次，他手下的一个交易员，因操作失误亏损了 6 万英镑，当里森知道后，因为害怕事情暴露便启动了 88888“错误帐户”（该账号是银行对代理客户交易过程中可能发生的经纪业务错误进行核算的帐户的备用账户）。随着时间的推移，备用帐户使用后的恶性循环使公司的损失越来越大。

为挽回损失，1994 年下半年，里森认为，日本经济开始走出衰退，股市将会大涨。于是大量买进日经 225 指数期货合约和看涨期权。然而 1995 年 1 月 16 日，日本关西大地震，股市暴跌，里森所持多头头寸遭受重创。为反败为胜，里森再次大量补仓日经 225 期货合约和利率期货合约，2 月 24 日，当日经指数再次加速暴跌后，里森所在的巴林期货公司的头寸损失，可以称是巴林银行全部资本及储备金的 1.2 倍，于是尼克·里森畏罪潜逃。233 年历史的老店就这样顷刻瓦解了，最后只得被荷兰某集团以一英镑象征性地收购了。

以上案例，都是因为有中心化控制机构在介入，由于中心化机构的控制，稀释了我们对资产的绝对控制权，也为我们参与金融市场设置了门槛，也因为中心化的机构，导致我们的资产随时可能面临人为的失误所带来的亏损风险。

根据这个市场痛点来反观 DeFi，DeFi 的意义才越发凸显。DeFi 即 Decentralized Finance，分布式金融（也可以称之为“开放式金融”），它相对于传统金融而言，具有如下特点：

1．无中心控制权，任何人在任何时间都可访问

2．个人资金管理有绝对控制权

3．每个人都有机会在相关协议上构建开放式金融产品，打破传统中心化金融垄断，“取消”了最低准入额的概念，近乎于人人都可参与。

1.2 DeFi 发展前景

1.2.1 从概念到落地

2018 年 8 月 Dharma Labs 联合创始人和首席运营官 Brendan Forster 一篇《Announcing De.Fi,A Community for Decentralized Finance Platforms》宣告了 DeFi（Decentralized Finance，翻译为分散式金融或开放式金融）的诞生。

DeFi 概念历经迭代，已从最初的“金融的改良者”逐渐向“金融的革命者”演化，区块链技术开始从应用程序服务于金融转变为对金融的重塑，催化其快速落地。

2019 年后，受惠于区块链行业生态的不断完善，业内对 DeFi 的内涵和外延进行了拓展：利用开源软件和分散式网络将传统金融产品转变为不需要信任且透明的协议的运动。据此，DeFi 不仅包括基于 ETH 网络的应用程序服务于金融行业（或提供金融应用程序服务）的开源区块链项目，也包含发行通证并用于支付结算的 Bitcoin、Stellar 等。Tezos 生态内的 VIAZ 作为我们最初的 DeFi 尝试，现如今也做得不错。

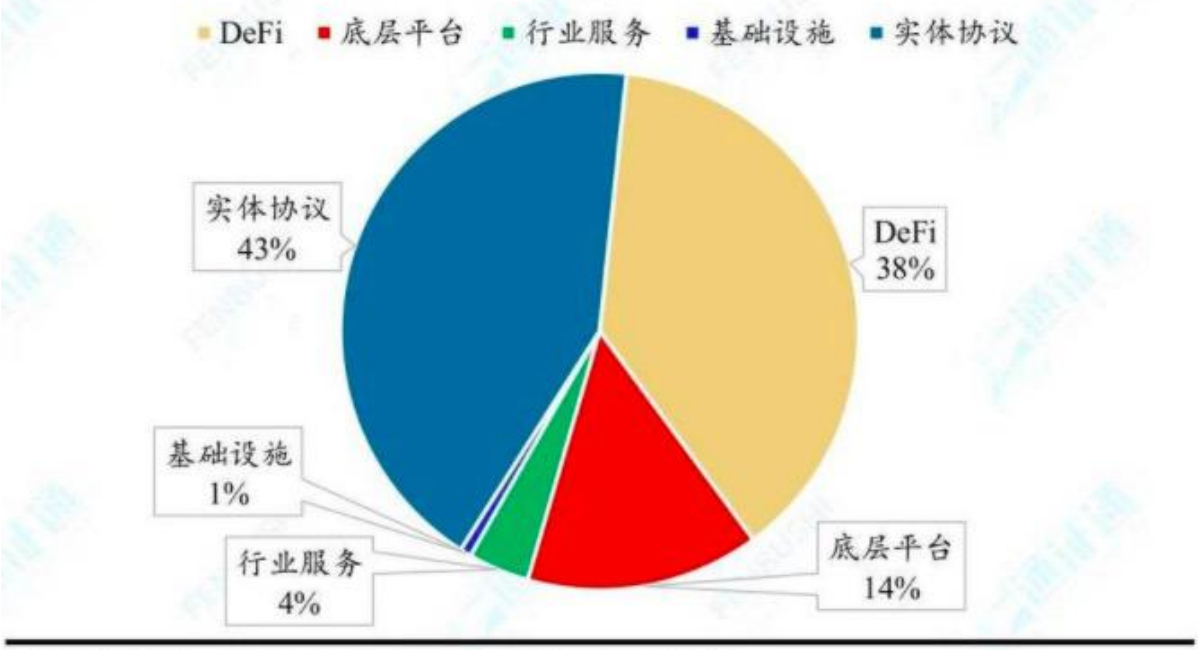
1.2.2 DeFi 受到更多人的关注

区块链或成为类“DeFi”等新概念产生的本体。

Bitcoin 产生不过十多年，区块链一词的提出时间则要更为靠后。就如当时“互联网”概念产生后不久，诸多基于互联网基础设施或应用的概念、词汇喷涌而出，互联网相应产业和工作、类目逐渐完善。“区块链”概念，在未来一定会成为该领域“新生概念”的本体。前有 Decentralized Finance、Decentralized Storage （分布式存储），同理若未来出现 Decentralized Education （分布式教育）、Decentralized Communication （分布式通讯）等新概念也不足为奇。

金融业是区块链技术应用的重点发展方向，有超过三分之一的区块链项目可归类为 **DeFi**。以学界对金融的定义为准，并根据 BICS （Blockchain Industry Classification Standard）分类，在目前市值前 1000 名的通证中，至少有 38% 的区块链项目直接应用程序服务于金融行业，包括非银金融、钱包 & 交易、通证资管、稳定通证、银行应用程序服务和支付结算。

图表1：市值前 1000 名中 DeFi 类项目占比

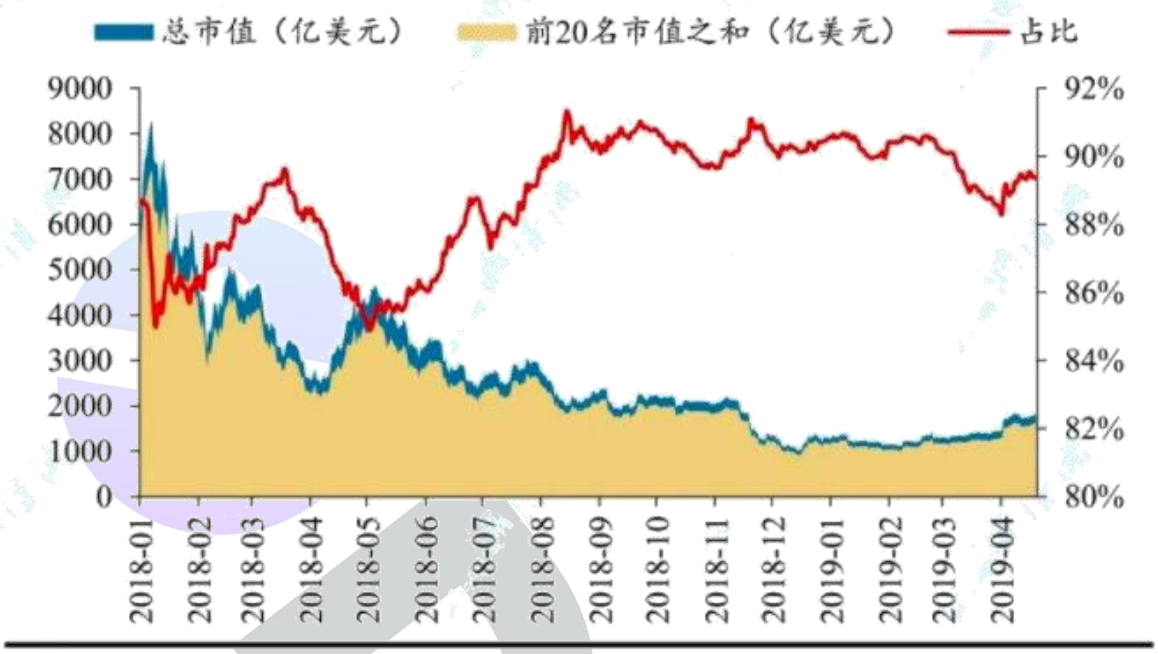


资料来源：CoinMarketcap，通证通研究院

整个区块链生态内的通证市场格局已基本形成，相比与头部区块链项目的直接竞争，基于现有格局的创新是一条更容易的“赛道”。

BTC 和区块链概念的产生，是跌宕起伏的十余年，目前为止，以 BTC 为代表的前 20 名主流通证的市值长期占市场总量的 88%-90%，并且排名比较稳固。这些通证所代表的区块链项目分布于支付结算、操作平台、银行应用程序服务、钱包 & 交易、稳定通证和通证应用程序服务等领域，值得注意的是，Tezos 的业务生态囊括了以上领域，其中支付结算以及银行业务也正在拓展和完善中。基于现有市场格局的创新，Tezos 深入研发 DeFi 不仅可以避开与这些头部项目的直接竞争，而且能够享受到原生用户沉淀，并且完善自身的生态技术构架，不失为一种“双赢”的选择。

图表3：头部通证市值占总市值的比例



资料来源：CoinMarketcap，通证通研究院

1.2.3 DeFi 类目繁多，市场空白份额大

DeFi 概念产生以来，目前符合条件的区块链项目已有上千个。据 Github，DeFi 可分为分散交换协议、稳定通证、贷款协议、衍生协议 / 预测市场等。据金融业的划分标准，可将 DeFi 重新分为：货币银行应用程序服务（如发行稳定通证）、非货币银行应用程序服务（如贷款协议）、证券业金融应用程序服务（如分类交换协议、衍生协议 / 预测市场、捆绑协议、基金协议），其他未包括的金融应用程序服务（如标记化协议、KYC/AML/ 身份认证、应用 / 工具、分析、其他）。现目前市场上的项目重心大多集中在货币银行应用程序服务和非货币银行应用程序服务，X-DeFi 也是基于 Tezos 的 XTZ 和对标 USDTZ 来发展这两项应用程序服务，未来 X-DeFi 将容纳和开发更多业务类型。

1.2.4 DeFi 发展前景

DeFi 采用的区块链技术具有可溯源、不可篡改和高透明度的特性，是对目前金融行业的有益补充。后期随着 DeFi 的日渐成熟与区块链技术的迭代，DeFi 将扮演更多、更重要的角色，甚至主导未来“代码世界”的金融体系也未可知。

DeFi 无需准入的优势将会助力金融业拓展应用程序服务内容和覆盖范围，利用较低的信任成本使得应用程序服务对象多元化。区块链技术在金融的领域的应用将会带来相对安全、信任、效率和一定程度上商业模式的重构。

2 Tezos 亮点

2.1 Tezos 概述

Tezos 源于古希腊语，智慧的合同，即区块链智能合约的含义。

Tezos 的最大优势是可以吸收任何一种基于区块链的账本好的方面，其将常规区块链上的各种操作以单纯的功能模块的方式实现。通过网络壳（Shell）利用这些操作处理网络层任务。比特币，以太坊 Cryptonote 等等都可以在 Tezos 内通过网络层应用程序服务实现，进而被表征。

更重要的是，Tezos 支持元数据升级：即可以通过自我修正代码进化协议。为此，Tezos 从一个种子协议开始定义一整套流程来让持币的用户来对代码进行修正，以及修正这套流程所必须的投票体系本身。这和哲学家 Peter Suber 的 Nomic 博弈观点不谋而和，该观点的博弈构建主要围绕一整套内省规则。

除此之外，Tezos 的种子协议被放在一个纯粹的股权证明系统（POS）上，支持图灵完备的智能合约。Tezos 通过 OCaml 语言进行实现，该语言是一套功能强大的函数式编程语言，提供高速，非歧义语义和语法以及整个生态系统。所有的这一切让 Tezos 成为一个形式化正确性证明的很好的候选者。

2.2 Shell 网络

Tezos 连接 Gossip 网络和协议的网络 Shell 通过维护客户端所知的最优链进而运作。它将从三种对象那里接受信息。前两个分别是交易和区块，确认有效后广播。第三个是协议，即用来修改现有协议的 OCaml 模块。网络 Shell 最艰巨的部分是保护节点免于遭受 DOS 攻击。Shell

还具备防御性。它尝试连接不同 IP 端的对等节点，发现掉线的节点以及禁止恶意节点。为防御某些 DOS 攻击，协议可提供 Shell 依赖区块大小和交易限制的环境。

2.3 自我修正能力

Tezos 最强大的特性是它的协议自我修正能力，主要通过暴露给协议两个过程函数实现：

1.set_test_protocol 函数，使用新协议替代测试网络中使用的协议 (通常是持币者投票决定的协议)。

2.promote_test_protocol 函数，用当前通过测试的协议替代目前正在运行的协议。

这些函数通过改变目前相关联的协议来转换 Context 对象。当下一个区块在链上产生，新的协议开始生效。

```
module Context = sig

type t

(* ... *)

val set_test_protocol : t -> Protocol_hash . t Lwt . t

val promote_test_protocol : t -> Protocol_hash . t -> t Lwt . t

end
```

protocol_hash 函数是.ml 和.mli 文件 sha256 哈希的 tarball 打包。这些文件在运行中编译，有获取较少的标准函数库权限，但被装在沙箱内， 可能无法调用系统函数。

这些函数通过协议的 apply 函数调用，返回新的 Context 对象。

很多条件可能会触发协议的修改。在最初的简单版本上，持币者可以通过直接投票进行协议修改, 而之后更复杂的协议可以通过逐步投票而获得接受。例如，当一个持币者希望一个修改案被通过，他会被要求提供计算机可以验证的证据来证明他的提案将会尊重协议的某些特性。这是对协议修改合规性在算法上的有效检测。

2.4 DPOS

我们认为任何一个去中心化的货币要保证安全性都需要给予参与者金钱上的奖励。正如在我们的定位白皮书中提到的，仅仅依赖于交易费进行激励会受到公共地悲剧影响。在 Tezos 中，我们提供一个“债券”和现金奖励的二元激励体系。

“债券”是烘焙人所需要购买的一单段时间的安全存款。当出现双重签名的情况下，这些“债券”将会被收回。

一段时间后，烘焙人除了“债券”以外还将获得另外的奖励，作为他们投资成本的补偿。债券和奖励的价值是系统安全的最主要保证，而它们的价值将仅占全部价值的一小部分。债券的真正目的是减少奖励的总量，并利用人对损失的普遍抗拒心理来提高网络的安全。

根据种子协议，每挖一个块将获得 512Tezos 币现金奖励以及需要 1536 币的债券。而每个区块签名将获得 32ΔT (−1)(注：-1 为右上角标) 个 tez 的奖励。这里 ΔT 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，但签名不需要持有债券。

假设出块率为每分钟一个区块，那么有 8% 的最初货币供应量在第一年 后应该以安全债券的形式被持有。

我们的奖励的计划被设定为 5.4% 的通货膨胀率。这个名义上的通货膨 胀应该是中性的，它不会让有的人变富，而让其他人变穷（与之相比, 比特币的挖矿的通货膨胀让比特币的持有者整体变穷，而中央银行又让金融界变得有钱，而让储户变穷）。

这个奖励机制将给矿工 33% 的债券回报 。这个回报在初期必须要足够高，因为矿工和签名者需要共同持有一段时间易波动的债券资产。但是，随着 Tezos 的成熟，这个回报可以被逐渐降低到一个同期的主流利率水平，并长期维持低于 1% 的形式通胀率。

2.5 智能合约

比特币确实允许智能合约，但其历史上，大多数 opcodes 已被 disabled ，可能性是有限的。以太坊引入智能合约系统，有一些关键区别：它们的脚本语言是图灵完备的，他们用状态账户（ 其包括一个余额，一个合约代码，一个数据存储；一个账户，其存储状态可通过转向此账户的一笔交易进行更改；交易指定传递给合约代码的一个数额及参数）代替比特币的未花费输出。

对于合约而言，一个图灵完备脚本语言的缺点是，执行一个脚本所需步数，可能是无限的，一个通常而言，无法计算的特性。

为解决这个问题，以太坊设计了这样一个系统，通过这个系统，验证交易的矿工，要求收取费用，此费用正比于复杂性及执行合约所需步数。

但是，为了确保区块链的安全，所有活动节点都需验证交易。一个恶意矿工可能在其区块中包含一笔这样的交易：他特意制作此笔交易，以进入一个无限循环，并自付一笔高昂费用以验证此笔交易。其他矿工可能会浪费很长时间验证此笔交易。更糟糕的是，他们可能会懈怠且无法验证此交易。但实际上，大多数有趣的智能合约，都可以非常简单的商业逻辑进行实现，不需要执行复杂计算。

我们的解决方案是，在一单笔交易中，限制一个程序所被允许运行的最大步数。由于区块有一个大小限制，每一个区块有一个交易量上限，每一个区块也有一个计算步数上限。此速率限制，挫败了 CPU-usage denial-of-service 攻击。同时，合法用户可发出多笔交易，以计算多于一单笔交易所允许的步数，尽管速率仍有限。矿工可能会决定排除一个太长的执行，如果他们觉得，其所包含费用太小。由于 Tezos 协议可修订，在未来修订版中，随着需求发展，这个上限可提升，一个新的加密原语可包含入脚本语言中。

我们认为，我们已经构建一个较大吸引力的种子协议。当然，Tezos 的真正的潜力存在于：让持币者掌控最优质应用程序服务协议的选择权利。

3 X-DeFi 介绍

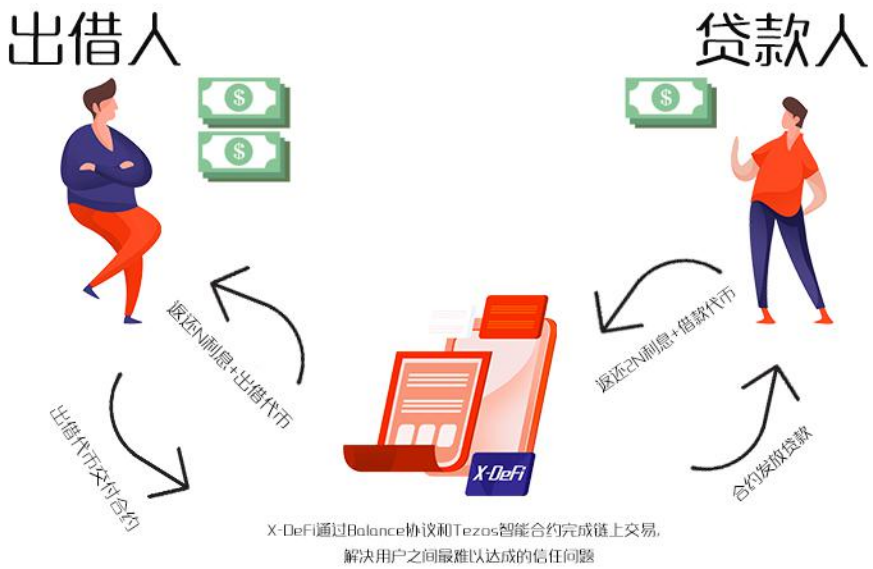
3.1 X-DeFi 概述

X-DeFi 中的核心是基于 Tezos 网络编写的 Balance 协议，Balance 协议是一个 DeFi 平衡收益协议。它的特点是收益最大化、流动性挖矿，且用于建立基于用户资产的供求变化，以算法计算得出利率的资金池。资产的供应方和借款人直接与协议进行交互，从而赚取或支付利率。

X-DeFi 是由 Tezos 官方核心技术团队成员和特佐斯基金会（Tezos Foundation）共同出资研发的生态类项目，X-DeFi 项目中包含 DeFi 银行货币业务和 Tezos 超级节点定期投资理财，未来我们将提供 ETH 和 BTC 等主网数字货币支持，实现 Tezos 和其它主网在协议内的交互（可关注官网 BTCTZ 和 USDTZ 项目进展）。X-DeFi 将不断完善业务生态内种类，将包含货币银行应用程序服务、非货币银行应用程序服务、证券业金融应用程序服务、金融应用程序服务等四大类服务。

3.2 商业模式

X-DeFi 通过超级节点的建立，早期提供给矿工高额的额外收益，期限为固定 20 个周期（cycle），通过初期高额的收益以及市场营销吸引和留住用户，利用 DeFi 之间的利率差、平台交易手续费（非链上 Gas）、Balance 协议所提高的超额挖矿产能等来消抵支出，超级节点将在一段时间内无限趋近于 Tezos 正常挖矿收益，补贴 XTZ 也将逐步减少，直至发展激励金为零。



3.3 DeFi 服务

3.3.1 借入 XTZ

允许用户以 USDT 作为抵押（未来我们将开放更多种类的可抵押数字货币），毫不费力地从协议中借用 XTZ，以用于 Tezos 生态系统中的任何地方。并给定一个由市场力量决定的固定利率，固定利率会根据市场浮动进行变化，该利率决定了每种资产的借贷成本。因为超级节点理财收益很高，所以我们的固定利率都略高于市场利率，以规避掉公司可能面临的损失。

3.3.2 抵押品价值

协议持有的资产都有一个价值评估，以 USDT 抵押举例：

抵押时 USDT 价格/抵押时 XTZ 价值*抵押 USDT 数量=用户可借贷 XTZ 数量

3.3.3 风险与赎回

如果某个账户发生了借贷，那么他的账户将被锁定，直到他赎回了他全部的抵押借贷订单，他的账户才会解锁。

如果在借贷到期当天截止，借贷订单未被赎回，系统将自动冻结账户并进行清算，以消除平台协议风险。

3.3.4 出借与收益

用户可以将自己生产或购买的 XTZ 放在 X-DeFi 平台进行出借，出借后系统会生成订单，并开始计算利率收益。利率收益方式为 T+15 的 14 天固定收益，出借订单生成当天为第 T1 天，第 T14 天理财周期结束，周期收益完整获得，第 T15 天将发放收益至现金钱包。收益发放过后，本金将自动加入下一个周期的固定理财，直至用户手动取消理财，取消理财后本金 T+1 发放至现金钱包。注意：理财天数不满 14 天则不能获得利率收益。

3.3.5 出借与抵押、赎回资产本位计算

出借：初期我们将仅支持 XTZ 的出借，资产本位按照数字货币本位进行计算，利率收益按照 XTZ 数字货币本位发放。

抵押：初期支持 USDT（后续将支持其它数字货币的抵押）的抵押，资产本位按照资产资金本位进行计算，获得资产等金额价值的 XTZ 货币借贷。

赎回：赎回抵押资产需支付借贷利息，利息以借出数字货币种类进行支付，赎回时将一并扣除借贷本金和利息，赎回完成后抵押资产将在 T+1 天释放至现金钱包。

3.3.6 主要用例

用户可以使用其现有投资组合（USDT）作为抵押，通过借入 XTZ 为超级节点投资筹集资金。

用户可以将闲置资金出借以获得利率收益，其本金随时可取出支配。

3.4 Tezos 超级节点

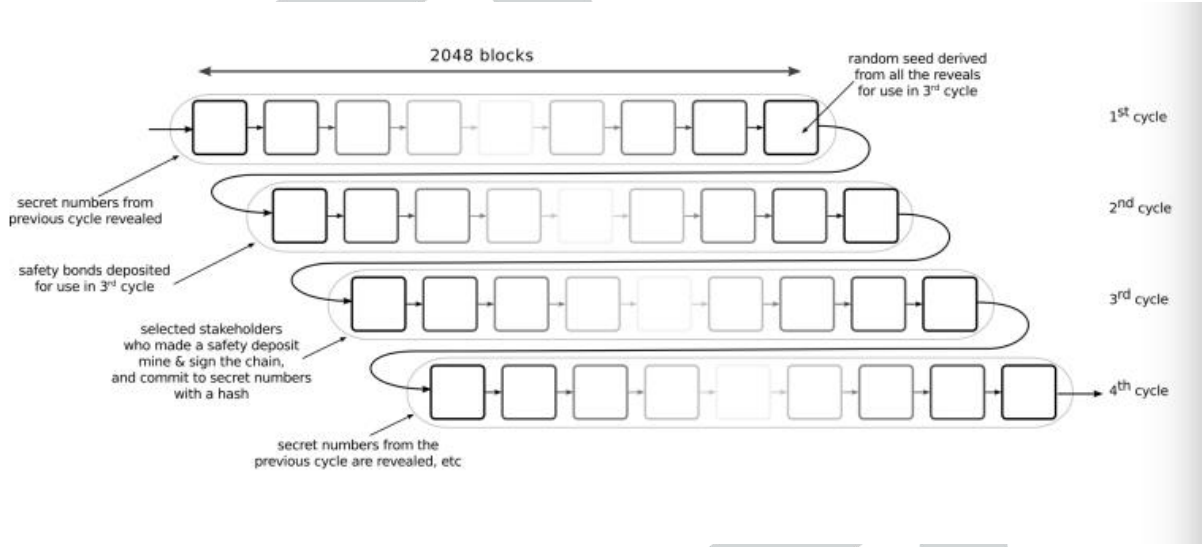
X-DeFi 里面的 Tezos 超级节点，是属于 Tezos 社区节点中的超级节点（试运行），由 Tezos 官方核心技术团队成员 Mukul Sharma 和其团队历时 3 个月开发完成，其出块方式以及运行周期等均和 Tezos 现有节点相同，但令人兴奋的是其奖励大大提高，通过 Balance 协议将流动性挖矿和质押挖矿两者进行协议内的互补，以达到收益在模型内的最大化，高额收益除了挖矿获得，X-DeFi 还将通过 X-DeFi 提现手续费、奖金池以及 DeFi 利率等平台收益在早期对矿工进行补贴。Balance 协议会根据平台出借和借币用户订单数量，以及现阶段特有的奖金池，自动进行动态调整超级节点的收益和 DeFi 利率，预计项目早期我们将拿出一部分创始 XTZ 补贴到市场，这部分资金由特佐斯基金会（Tezos Foundation）提供，补贴资金逐步递减，直至恢复正常 5%通胀水平。

3.4.1 股权证明机制

我们的 DPOS 机制集成了几个不同的观念，其中包括 Slasher，Balance，chainof-activity 以及 proof-of-burn。以下的是对算法的简要概览。

区块由随机的持币人（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奖励，但是也要求存一笔一段时间的押金，如果期间出现双挖或者双签，那么这笔押金将被没收，挖出的奖励将由 X-DeFi 通过 balance 协议进行分配，分配数量将展示在对应节点收益上。

这个协议以 2048 个区块为周期运行。在每个周期的开始，矿工选择数字做成随机种子，提交至倒数第二个周期，并在最后一个周期展现出来。通过使用随机种子，“跟随币”策略分配给指定地址的下一个周期的挖矿权以及签名权。



3.4.2 时钟

协议在区块之间增加了最小延迟。原则上，任何一个持币人都可能挖出块。但是，就一个特定的块而言，每个持币者都将受到一个随机的最低延期的制约。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。这将保证在一个分叉中持有股权较少的持币人拥有较低的出块率。否则，一个针对 CPU 的 DDos 攻击将可能欺骗节点，导致其确认一个较长的自称高得分的链。通过 balance 协议进行资源处理和分配，出块效率更高，挖矿产能比最大化。

3.4.3 随机种子生成

事实上，在一个 N = 2048 周期内，某个参与节点中一小部分 f 的人 将会获得平均值为 fN 的挖矿权，一旦接收到这个有效的部分，那么 f0 的 标准差将为：

$$\sqrt{\frac{1}{N}}\sqrt{\frac{1-f}{f}}$$

如果一个攻击者通过 W 个不同种子进行穷举式搜索，那么他的攻击的优势至多是：

$$\left(\sqrt{\frac{2\log(W)}{N}}\sqrt{\frac{1-f}{f}}\right)fN$$

个区块。（这是在 W 正态分布变量的最大期望上的标准界限）举个例子，一个控制了总量 f = 10% 币卷的攻击者，他可以预期 在每个周期挖大约 205 个区块。假设他在试图控制种子的秘密分叉上有超 过一万亿个哈希的算力，那么其可以分配给自己占总量区块 14.7% 的 302 个块。值得注意的是：

1.产生种子的哈希是通过一个复杂的密钥生成函数产生的，这让穷举式 搜索变得不现实。

2.要想在挖矿中取得线性收益，攻击者将花费平方指数级增长的资源。

这就是 X-DeFi 的魔力，集最大的产能进行挖矿和按出质量进行收益配比，恶意攻击者也不能轻易捣乱和攻击。

3.4.4 公开谴责机制

为了避免一个区块上的双挖以及双签问题, 一个矿工可以在他的区块中加入一个公开谴责机制。

该公开谴责机制采取双签名的形式。每一个造币的签名或者块的签名都签入区块高度，构成恶意行为的证据，这让不良行为很难隐藏。

尽管我们可以允许任何人来谴责不良行为，但没有人比矿工更适合来 这样做。事实上，一个矿工可以简单地复制不良行为的证据并将其作为自己 的发现转达给其他人（零知识证明允许任何人从谴责不良行为获益，但获益多少并不十分明确）。

而一旦发现有双挖或者双签，那么其债券将被没收。

3.4.5 超级节点收益

有意思的是这一套用于 Tezos 的公共 DPOS 协议挖矿同样适用于 X-DeFi 的超级节点，区别在于集中的分配对于矿工来说收益是最大化的，并且 Balance 协议可以将不同抵押数量的矿工自动进行收益配比，这也和我们接下来准备取消零散用户（单独个体且非托管账户）投票和 DPOS 的权利相契合。

3.5 Balance 协议

Balance 协议是 X-DeFi.com 基于 Tezos 网络编写并发布的 DeFi 平衡收益协议。它的特点是收益最大化、流动性挖矿，它的治理代币采用 Tezos 的 XTZ。X-DeFi 采用 XTZ 作为自理代币，它最大的“好处”是共识高、稳定，对于 X-DeFi 的借贷和挖矿业务带来更多曝光。

Balance 协议是借贷和挖矿收益的最大化助力，所以它和预言机一样，是 X-DeFi 平台必需的平衡性工具，既让用户收益最大化，又能通过协议让平台得以运转。

3.5.1 借贷收益平衡优化

用户将 XTZ 经过 Balance 协议存入 X-DeFi 平台，Balance 协议帮助用户在 Compound、Aave、bZx、dYdx 等协议中进行调整，并在 X-DeFi 给到的奖金池中进行比对和领取奖励，最终以帮助用户获得更高的收益。

3.5.2 挖矿收益平衡优化

本质上依然是帮助投资者通过不同矿池中 XTZ 挖矿策略进行调整，获得更高收益。

3.5.3 超级节点挖矿收益平衡升级

在挖矿收益平衡优化的基础上，开放既定投资组合，并设定投资策略，协议策略机制在各大矿池中不间断寻找最佳收益组合，有用户投资便自动投入找寻到的最佳收益组合位置。此次超级节点挖矿收益平衡协议升级中加入了 X-DeFi 的奖金池，既用户参与超级节点挖矿同时可享受奖金池补贴，直至奖金池金额为零。

3.5.4 链间交互

未来，Balance 协议将进行协议链间升级，支持除 Tezos 外的 ETH、BTC 和 EOS 网络。支持 ETH 的映射币 ETHtz 和 BTC 的映射币 BTCtz 等多币种组合资产服务。并且将发布新型代币化保险的测试协议，我们认为保险将是 DeFi 的必经之路。

Balance 协议的每一次更新迭代，都有可能带来新的利好消息和币价上涨，大家多多关注。

3.6 团队成员

Ryan Sean Adams：X-DeFi 首席执行官。毕业于英国剑桥大学数学系，在校期间开始关注 Tezos 并参与了 Tezos 的 ICO。毕业后成立工作室，研究 Tezos 技术和生态环境的建设，并于 2016 年开始运作 VIAZ 项目。

Mukul Sharma：X-DeFi 首席技术官。Tezos 创始技术团队八个核心技术之一，毕业于纽约大学数学硕士，曾担任 Gemini 交易所 CTO，后担任 Tezos 的技术 VP，深耕 Tezos 协议研究和开发。

Jason Lee：X-DeFi 首席运营官。熟知美国和中国大陆社区运营模式，曾负责 Tezos 东南亚地区社区负责人。

David Williams：X-DeFi 设计主管。毕业于纽约视觉设计艺术学院，曾任职于亚马逊，并担任 Department of Design 一级助理一职。

Paul Razvan Berg：X-DeFi 高级后端工程师。毕业于麻省理工学院数学硕士学位，拥有十年区块链技术开发经验。

4 X-DeFi 应用程序服务条款

欢迎使用 X-DeFi，这是由 Tezos（“我们”，“我们的”或“我们”）提供的应用程序服务托管的用户界面（“应用程序服务”或“应用程序”）。该应用程序服务提供对 Tezos 和 ETH 区块链上分散式协议的访问，该协议允许某些数字资产的供应商和借款人参与自主利率市场（“协议”）。

本应用程序服务条款协议（以下简称“协议”）解释了您可以访问和使用界面的条款和条件。您必须仔细阅读本协议。通过访问或使用该界面，即表示您已阅读，理解并同意接受本协议的全部约束。如果您不同意，则无权访问或使用该应用程序服务。

4.1 修改本协议

我们保留自行决定修改本协议的权利。如果我们进行任何修改，我们将通过让您重新阅读的方式来通知您。所有修改将在发布后生效，并且您对应用程序服务的继续使用将确认您接受这些修改。如果您不同意对本协议的任何修改，则必须立即停止访问和使用该应用程序服务。

4.2 资格

要访问或使用该应用程序服务，您必须能够与我们签订具有法律约束力的合同。因此，您表示您已经年满 18 岁，并拥有代表您自己以及您可能会接触到的任何公司或法人实体并遵守本协议的条款和条件的全部权利、权力或使用界面。您进一步声明，您不是受美国经济制裁的任何管辖区或团体的公民，居民或成员，或者您对应用程序服务的使用属于非法或以其他方式违反任何适用法律的地方。您进一步声明，您对应用程序服务的访问和使用将完全遵守所有适用的法律和法规，并且您不会访问或使用该应用程序服务进行宣传。

4.3 专有权

我们拥有应用程序服务及其内容的所有知识产权和其他权利，包括（但不限于）软件，文本，图像，商标，应用程序服务标记，版权，专利和设计。除非得到我们的明确授权，否则您不得复制，修改，改编，出租，许可，出售，发布，分发或以其他方式允许任何第三方访问或使用该应用程序服务或其任何内容。只有您有资格，就在此授予您访问和使用该界面的单个个人有限许可。本许可证是排他性的，不可转让的，并且我们可以在不另行通知的情况下随时免费撤销。严格禁止将应用程序服务或其内容用于本协议未明确允许的任何目的。

4.4 隐私权

我们关心您的隐私。尽管我们会遵守所有有效的传票请求，但我们会仔细考虑每个请求，以确保其符合法律的精神和法律条文，我们会毫不犹豫地对无效，过分或违反宪法的请求提出质疑。我们使用商业上合理的保护措施来维护您的个人身份信息（“ PII”）和汇总数据的完整性和安全性。但是，我们不能保证未经授权的第三方永远不会出于不正当目的获得或使用您的 PII 或汇总数据。您承认自己提供 PII 和汇总数据的风险由您自己承担。通过访问和使用该应用程序服务，您理解并同意我们收集，使用和披露您的 PII 和汇总数据。

4.5 禁止活动

您同意不参与或尝试从事与您对应用程序服务的访问和使用有关的以下任何禁止的活动类别：

知识产权侵权。侵犯任何版权，商标，应用程序服务商标，专利，公开权，隐私权或其他依法享有的所有权或知识产权的活动。

网络攻击。旨在干扰或损害任何计算机，应用程序服务器，网络，个人设备或其他信息技术系统的完整性，安全性或正常功能的活动，包括（但不限于）病毒的部署和拒绝应用程序服务攻击。

欺诈和虚假陈述。旨在欺骗我们或任何其他个人或实体的活动，包括（但不限于）提供任何虚假，不准确或误导性的信息以非法获取他人财产的行为。

市场操纵。违反任何有关交易市场完整性的适用法律，法规或法规的活动，包括（但不限于）操纵策略，通常被称为欺骗和清洗交易。

任何其他非法行为。违反美国或其他相关司法管辖区的任何适用法律，法规或规定的活动，包括（但不限于）美国法律施加的限制和法规要求。

4.6 不提供专业建议

应用程序服务提供的所有信息仅供参考，不应视为专业建议。您不应基于应用程序服务中包含的任何信息采取或避免采取任何行动。在做出有关应用程序服务的任何财务，法律或其他决定之前，您应该从适合该领域的执照和合格人员那里寻求独立的专业建议。

4.7 不承担任何责任

该应用程序服务是按“原样”和“可用”提供的。在法律允许的最大范围内，我们不承担任何形式的明示，暗示或法定陈述和保证，包括（但不限于）适销性和针对特定目的的适用性保证。您承认并同意，使用应用程序服务的风险自负。我们不代表或保证对应用程序服务的访问将是连续的，不间断的，及时的或安全的；应用程序服务中包含的信息将是准确，可靠，完整或最新的；或者该应用程序服务将没有错误，缺陷，病毒或其他有害元素。我们提供的任何建议，信息或声明均不应被视为对应用程序服务进行任何保证。对于第三方关于应用程序服务的任何广告，报价或声明，我们不认可，保证或承担任何责任。

4.8 没有信托义务

本协议并非旨在也不会在我们身上建立或施加任何信托义务。在法律允许的最大范围内，您承认并同意，我们对您或任何其他方不负任何信托义务或责任，并且在法律或权益中可能存在任

何此类义务或责任的情况下，在此不可撤销地否认，放弃和消除。您进一步同意，我们唯一应承担的义务和义务是本协议中明确规定的义务和义务。

4.9 合规义务

该应用程序服务是从美国境内的设施操作的。该应用程序服务可能在其他司法管辖区不可用或不适合使用。通过访问或使用该界面，您同意您对遵守可能适用于您的所有法律和法规承担全部责任。如果您是受美国经济制裁的公民，居民或任何司法管辖区或组织的成员，或者您对应用程序服务的使用将是非法的或以其他方式违反任何适用法律，则您不得使用该应用程序服务。应用程序服务及其所有内容仅针对位于美国的个人，公司和其他实体。

4.10 风险承担

通过访问和使用应用程序服务，您表示您已了解与使用基于密码和基于区块链的系统相关的固有风险，并且您已了解数字资产（例如比特币（BTC），以太币（ETH）），特佐斯（XTZ）的用法和复杂性）和其他数字令牌，例如遵循特佐斯和以太坊令牌标准（ERC-20）的令牌。您进一步了解到，由于包括（但不限于）采用，投机，技术，安全性和法规等因素，这些数字资产的市场非常不稳定。您承认使用特佐斯、以太坊等基于加密和基于区块链的系统进行交易的成本和速度是可变的，并且随时可能急剧增加。您进一步认识到数字资产在提供给《协议》时可能会损失其部分或全部价值的风险。您进一步确认，我们对这些变量或风险不承担任何责任，也不拥有或控制协议，也不对您在访问或使用我们提供的应用程序服务时所遭受的任何损失承担责任。因此，您理解并同意对访问和使用应用程序服务以及与协议交互的所有风险承担全部责任。

4.11 第三方资源和促销

该应用程序服务可能包含对第三方资源的引用或链接，包括但不限于我们不拥有或控制的信息，材料，产品或服务。此外，第三方可能会提供与您访问和使用界面有关的促销信息。对于此类资源或促销活动，我们不承担任何责任。如果您访问任何此类资源或参与任何此类促销活动，

则后果自负，并且您了解本协议不适用于您与任何第三方的交易或关系。您明确免除我们对因使用任何此类资源或参与任何此类促销而引起的任何责任。

4.12 索赔的免责

您明确同意承担访问和使用应用程序服务以及与协议交互有关的所有风险。您进一步明确声明免除我们的责任，并免除我们因使用应用程序服务以及与协议交互而产生的或以任何方式引起的任何责任，索赔，诉讼因由或损害。

4.13 赔偿

您同意就以下各项引起的所有索赔，损害，义务，损失，负债，成本和费用对我们和我们的管理人员，董事，雇员，承包商，代理商，分支机构和子公司构成无害，免责，弥偿和赔偿：

（a）您对界面的访问和使用；

（b）您违反本协议的任何条款或条件，任何第三方的权利或任何其他适用的法律，规则或规定；

（c）在您的协助下或使用您拥有或控制的任何设备或帐户，任何其他方对应用程序服务的访问和使用。

4.14 责任范围

在任何情况下，我们或我们的任何管理人员，董事，雇员，承包商，代理商，关联公司或子公司均不对您承担任何间接，惩罚性，偶然性，特殊，结果性或示范性损害，包括（但不限于）损害赔偿因与应用程序服务的任何访问或使用有关或与之有关而导致的利润，商誉，使用，数据或其他无形财产的损失，我们也不承担因黑客，篡改，或其他未经授权的访问或使用应用程序服务或其中包含的信息。对于以下任何情况，我们不承担任何责任：

（a）错误，错误或内容不正确；

（b）由于访问或使用该应用程序服务而造成的任何性质的人身伤害或财产损失；

（c）未经授权访问或使用我们控制范围内的任何安全服务器或数据库，或使用其中存储的任何信息或数据；

（d）与该应用程序服务有关的功能的中断或停止；

（e）可能会传输到应用程序服务或通过接口传输的错误，病毒，特洛伊木马等；

（f）由于使用了通过应用程序服务提供的任何内容而导致的错误或遗漏，或者造成了损失或损坏；

（g）任何第三方的诽谤，冒犯或非法行为。在任何情况下，我们或我们的任何高级职员，董事，雇员，承包商，代理商，关联公司或子公司均不对您承担的任何索赔，诉讼，负债，义务，损害，损失或费用承担超过您的金额的责任（支付给我们以换取访问和使用该界面的费用）。无论所称责任是基于合同，侵权，疏忽，严格责任还是任何其他依据，并且即使我们已被告知可能承担这种责任，本责任限制均适用。一些司法管辖区不允许排除某些担保或限制或排除某些责任和损害。因此，本协议中阐明的某些免责声明和限制可能不适用于您。此责任限制应在法律允许的最大范围内适用。

4.15 争议解决

我们将尽最大的努力通过非正式的真诚谈判解决任何潜在的争端。如果发生潜在纠纷，您必须通过发送应用程序或其它社交软件与我们联系，以便我们能够尝试解决此纠纷，而无需诉诸正式纠纷解决方案。如果我们无法达成非正式解决方案，那么您和我们双方都同意按照以下规定的程序解决潜在的争议。

因应用程序服务，本协议或您可能认为我们应负责的任何其他作为或不作为而引起的或与之有关的任何索赔或争议，包括（但不限于）关于可仲裁性的任何索赔或争议（“争议”），应最终根据可选的美国快速仲裁程序通过仲裁解决。您了解必须通过有约束力的仲裁解决所有争议。仲裁应由一位仲裁员以保密方式在美国进行。除非您和我们双方都同意在其他地方进行仲裁，否则仲裁将在美国进行。除非我们另有协议，否则仲裁员不得将您的索赔与任何其他方的索赔合并。仲裁员作出的关于裁决的任何判决均可进入具有管辖权的任何法院。

参考文献

1.特佐斯—自我修订的加密账本白皮书（Tezos — a self-amending crypto-ledger White paper）https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf

2.特佐斯—自我修订的加密账本立场文件（Tezos: A Self-Amending Crypto-Ledger Position Paper）https://tezos.com/static/position_paper-841a0a56b573afb28da16f6650152fb4.pdf

3.特佐斯共识算法（Tezos Consensus Algorithm）https://learn.tqtezos.com/files/proofofstake.html#intro

4.VIAZ https://viaz.io/

5.compound https://compound.finance/docs/ctokens

6.瑞士最古老银行请求关闭 https://www.telegraph.co.uk/finance/financial-crime/9779615/Switzerlands-oldest-bank-Wegelin-to-close-after-pleading-guilty-to-aiding-US-tax-evasion.html

7.巴林计划对银行倒闭进行听证 https://www.thenational.ae/business/bahrain-plans-hearings-into-bank-failures-1.420443