ITDogChain

概要设计白皮书

ITDogChain 团队

BlockChainHackathon

2018 年 6 月 9 日

目录

第一章 项目背景

1.1 ITDogChain 从前辈说起

Crypti 是一个允许在其上开发以及分发基于 JavaScript 构建的去中心化应用的平台，它致力于构建一个易于使用，功能完备的生态系统，通过 Crypti，开发者可以利用这个由加密货币驱动的系统，来开发，发布，分发去中心化的应用，并从中赢利，该系统提供了定制区块链，智能合约，云存储，以及节点运算，等一体化的行业解决方案。尽管 Crypti 不靠资金靠社区驱动运行了很长一段时间但不幸的是，它终究还是没人维护了，但是它在国内还是已经生根发芽。

亿书，英文名 Ebook，是一个去中心化的出版平台，由新一代加密货币驱动，具备版权签名与认证、 协同创作、一键发布等功能，将促进人们更加主动地积累知识、分享经验，为人类创作注入新动力。对于出版社等企业用户和第三方开发者，它提供了侧链功能，可以基于亿书强大的网络和市场， 使用亿书侧链、智能合约、云存储和计算节点，构建、发布个性化的去中心化软件，货币化一切有 形或无形资产，并从中盈利。

1.2 ITDogChain 的诞生

久坐不起面容憔悴，脸上一抹压抑已久的闷骚，格子衬衫质朴中散发着苦味，间歇性情绪不稳，永久性眼圈发黑。神秘而沉默，这就

是纯正的 IT 狗，时间久了身边的人就会由衷的问上一句是不是还没找男/女朋友了？其实究其原因就一个字：穷！是真的穷！

好在还有一个词叫做“狗屎运”，为了可以屌丝逆袭，ITDogChain 就这样诞生了！

第二章 项目阐述

2.1 什么是 ITDogChain

ITDogChain 是一个去中心化的面向开源及私有软件项目的源代码交易平台，由新一代加密货币 IDC 驱动并具备源代码签名与认证、一键发布、一键安装等功能并可融合社交、去中心化自媒体、去中心化存储，使 ITDog 们在分享自己知识成果的过程中实现价值传递并从中盈利。

2.2 ITDogChain 的愿景

终极目标是让屌丝逆袭；首先让 ITDog 们在分享自己知识成果的过程中实现价值传递并从中盈利，然后融合现有 DHT 网络为海量共享的磁力链接资源进行权属管理和有偿流通，成为下一代互联网下的优质 P2P 资源的交易平台。

2.3 ITDogChain 的目标用户

开发者用户：对开发者来说，ITDogChain 是你中心化 github 或者

去中心化 Sia 上源码的变现平台，而且是优质代码的分享平台，更是你源码版权的维护平台。

普通用户:对于普通用户，身为屌丝的你还在找番号吗？ITDogChain 能让你找到你想找到的，你懂得....不光可以找到还可以实现权属管理，在有偿流通的过程中还能盈利。

2.4 ITDogChain 的技术选择

ITDogChain 基于 Node.js 研发，后端使用 Express.js 框架，前端使用 Ember.js 框架，客户端使用 Electron 框架，数据库使用 SQLite3，前后端统一使用 Javascript 脚本语言，Dashboard 使用 HTML5 及 CSS3。

2.5 ITDogChain 的优势

技术优势：Nodejs 是一款服务器开发处理平台，其天生的异步处理机制和强大的网络开发能力，非常适合基于事件的、实时交互的加密货币应用，为狗链高性能的即时通讯提供了坚实的技术保障。

社区优势：前后端统一的技术架构，大大降低了狗链及其侧链开发难度，任何熟悉 JavaScript 和 Node.js 的开发者，都可以快速参与进来。

第三章 技术原理

3.1 数据层

1、加密和验证

ITDogChain 采用 sha256 加密算法、该算法是经过长久快来验证的有效、安全的算法之一

2、地址

ITDogChain 提供了类似比特币的 HASH 地址，并在此基础上添加了扩展功能、比如“用户名”。添加扩展功能的理由如下：

(1)用户需要：复杂的字符串地址不适合人类脑记，很多人在最初接触比特币的时候，非常不习惯，经常弄混、忘记自己的比特币地址就是很好的证明。

(2)产品需要：说到交互功能，比特币除了交易之外，是没有什么

交互的，交互功能被摆在突出位置，充满个性化的用户名是必须的。

(3)签名和多重签名

随着区块链等相关技术的创新和突破，很多有形或无形资产都将实现去中心化，数字资产将无处不在。无论数字资产，还是程序源码，都是有明确所有权的，而多重签名是对签名的扩展使用，给数字资产转移提供了安全保障和技术手段。

一个多重签名钱包就是指一个钱包有多个持有人共同持有并管理。多重签名钱包的交易必须是由数位，或者是全部持有人共同签署才会有效。多重签名基于 M/N 架构，其中，多重签名钱包的所有者数量 N 最多不超过 16 个，当签署交易时，至少要有 M 个所有者进行签名。M 必须大于 1 且小于等于 N 的数量。一旦你从多重签名钱包发起一笔交易，所有钱包拥有者都会看到该条待处理的交易，并可决定是否要同意或者拒绝，一旦达到需要的签名数量，那钱包就会允许该交易被提交到网络，并广播全网，打包进下一个区块中。多重签名钱包的所有者可以在获得 M 个所有者同意的情况下，随时更改多重签名的规则交易共识

3.2 网络层

P2P 网络去中心化的基础，其作用和地位不言而喻，无可替代。ITDogChain 采用了一个建立在 HTTP 协议之上的标准对等网络(P2P)架构，P2P 模块包含了版本、系统、IP、端口号几项数据。该架构具有以下特点:

1、产品提供初始节点列表，保障了初始化节点快速完成，不至于成为孤立节点;

2、节点具备跨域访问能力，任何节点之间都可以自由访问;

3、节点具备自我更新能力，定期查询和更新死掉的节点，保障网络始终畅通;

3.3 共识层

共识机制是分布式应用软件特有的算法机制。在分布式软件开发中，节点间的互操作，节点行为的统一管理，没有算法理论作为支撑，根本无法实现。所以，要想开发基于分布式网络的加密货币，共识机制无法回避。

ITDogChain 采用 DPOS(授权股权证明)机制。由受托人来创建区块，受托人来自于普通用户节点，需要首先进行注册，然后通过宣传推广，寻求社区信任并投票，获得足够排行到前 101 名的时候，才可以被系统接纳为真正可以处理区块的节点，并获得铸币奖励。比特币是通过计算机算力来投票，算力高的自然得票较多，容易获胜。DPOS 机制是通过资产占比（股权）来投票，更多的加入了社区人的力量，人们为了自身利益的最大化会投票选择相对可靠的节点，相比更加安全和去中心化。整个机制需要完成如下过程：

(1)注册受托人，接受投票（得票数排行前 101 位）;

(2)维持循环，调整受托人

块周期：也称为时段周期（Slot），每个块需要 10 秒，为一个

时段（Slot）；

受托人周期：或叫循环周期（Round），每 101 个区块为一个循环周期（Round）。这些块均由 101 个代表随机生成，每个代表生成 1 个块。一个完整循环周期大概需要 1010 秒(101x10)，约 16 分钟；每个周期结束，前 101 名的代表都要重新调整一次；

奖励周期：根据区块链高度，设置里程碑时间（Milestone），在某个时间点调整区块奖励。

上述循环，块周期最小（10 秒钟），受托人周期其次（16 分钟），奖励周期最大（347 天）。

(3)循环产生新区块，广播产生新区块和处理分叉等内容。

3.4 激励层

该层主要针对块奖励进行设置，与比特币的块奖励每 4 年减半类似，ITDogChain 的块奖励也会遵循一定规则。大致的情况是这样的，第一阶段（大概 1 年）奖励 5 IDC（IT 狗币）/块，第二年奖励 4IDC（IT 狗币）/块，4 年之后降到 1 IDC(IT 狗币)/块，以后永远保持 1 IDC/块，所以总量始终在少量增发。

具体增发量很容易计算，第一阶段时间长度 = rewards.distance 10 秒 /（24 60 60）= 347.2 天，增发量 = rewards.distance 5 = 3000000 * 5 = 1500 万。第二阶段 1200 万，第三阶段 900 万，第四阶段 600 万，以后每阶段 300 万。这种适当通胀的情况是 DPoS 机制的一个特点，也是为了给节点提供奖励，争取更多用户为网络做贡献。

3.4 应用层

1、ITDogChain 应用层作为 ITDogChain 架构的最上层，将直接为 ITDogChain 生态圈的用户提供具体服务。所提供的服务场景包括但不限于挂载 Sia、github 上传 Dapp 等。各 ITDogChain 的开发者也可以基于 ITDogChain 应用层的可视化开发环境或开放 API 接口自行开发去中心化应用。

2、交易是 ITDogChain 的核心,加密货币的整个系统，都是为了确保正确地生成交易、快速地传播和验证交易，并最终写入全球交易总账簿——区块链而设计。因此，从开发设计角度考虑，一笔交易必须包括下列过程：生成一笔交易。这里是指一条包含交易双方加密货币地址、数量、时间戳和有效签名等信息，而且不含任何私密信息的合法交易数据;广播到网络。几乎每个节点都会获得这笔交易数据。验证交易合法性。生成交易的节点和其他节点都要验证，没有得到验证的交易，是不能进入加密货币网络的。写入区块链,加密解密、P2P 网络、区块链等一系列技术都是围绕交易展开的。ITDogChain 目前包含如下交易类型：

类型	注释
SEND	转账交易
SIGNATURE	“签名”交易
DELEGATE	注册为受托人
VOTE	投票

USERNAME	注册用户别名地址
FOLLOW	添加联系人
MULTI	注册多重签名帐号
DAPP	侧链应用
IN_TRANSFER	转入 Dapp 资金
OUT_TRANSFER	转出 Dapp 资金
ARTICALE	发布文章
BUY	购买
READ	付费阅读

3、社交功能、ITDogChain 允许用户维护一个联系人列表，该功能可用来存储一些常用帐户，包括合作者、客户、读者或朋友。这是一项社交功能，是 ITDogChain 协作功能的基础，它类似于社交网站的关注功能。一个用户被添加到某人的联系人列表，那在该用户的客户端里面，会显示一个待处理的联系人请求，不管该用户是否接受该请求，他都会显示在别人的联系人列表上，而如果该用户接受该请求，那他们双方都会添加对方到自己的联系人列表里。每一个用户都会优先看到在线联系人的各类公开状态，并可直接访问该用户博客页面，阅读或购买该用户的书籍，向该用户直接发送消息等。用户的动态会推送给联系人列表里的所有人，增强用户互动性。

4、去中心化自媒体、ITDogChain 客户端集成了一个内容管理系统 WCM，可以简单的展示用户撰写的博客文章，用户能够方便的改变页面主题，控制文章或程序源码发布状态。其他用户能够通过用户名

直接进行访问，阅读和评论。用户可以在服务器上安装全客户端，绑定域名，供全世界用户访问浏览。同时，在本地使用轻客户端进行管理，将本地客户端与远程节点同步，从而实现远程控制，大大减少博客维护难度。

5、去中心化存储、用户在使用 ITDogChain 过程中，会产生大量数据，包括各类文本，聚合的各类电子书，及其导出的 PDF 等格式的文档，图片，视频等，还有第三方开发的去中心化的应用数据，这些文件需要安全存储，快速分发。ITDogChain 可外挂 Sia，可以让用户的数据分布存储于网络的各个节点。

第四章 项目团队

4.1 ITDogChain 团队成员

谭祎同学勇敢的承担了前端、后端以及设计的岗位

刘青亮同学勇敢的承担了前端、后端以及产品的岗位

王钰森同学勇敢的承担了前端的岗位

4.2 ITDogChain 团队成员招募

需要逆袭的 ITDog 拥有健康的身体，一颗不老的心，对新事物、新技术、新观点有好奇心，尊重不同观点和思想。

第五章 ITDogChain 的价值分析

5.1 狗链与以太坊(一)

以太坊，毫无疑问地，开发者可以访问一个强大的去中心化的底层系统，然而，它缺少了内置的前端以及开始时就没有内置一些存储方案，这迫使开发者不得不依靠一些第三方的中心化存储，这远称不上最佳解决方式。

狗链就完全不一样了，开发者可以访问一个去中心化的系统，提供了一个真正的去中心化应用的前端，底层以及存储的全套解决方案，另外，做为额外的奖励，每个 Dapp 能是通过我们自己的 Dapp 商店来提供，用户可以通过极其简便的界面来下载，安装并运行。

5.2 狗链与以太坊(二)

在**以太坊**，所有的智能合约都直接嵌入了以太坊的主链内，而全网用单片的方式一起执行；这是一个比较严重的问题，如果有一天，有几十万个智能合约在以太坊的网络上运行的话，那它将无法有效地扩展，到时让上万个节点同时执行一个智能合约将是完全不可行的，更何况以太坊的区块链大小可能增涨至 TB 级别。目前 Mist 全节点下载大约两百多 G，耗时大约一周左右。

狗链则是建立在 HTTP 协议之上的点对点网络，基于 DPOS（授权股权证明机制）共识算法，无需挖矿，大约 1 亿枚币子。每个块的时间为 10 秒，每个周期的 101 个区块均由 101 个代表随机生成，广播

并添加到区块链里，在得到 6-10 个确认后，交易完成，一个完整的 101 个块的周期大概需要 16 分钟。很多人担心这种通胀，会降低代币的价值，影响代币的价格。事实上，对于拥有大量侧链应用的平台产品来说，一定要保证有足够代币供各侧链产品使用，不然会造成主链和侧链绑定紧密，互相掣肘，对整个生态系统都不是好事情。这种情况可以通过以太坊的运行情况体会出来，特别是侧链应用使用主链代币众筹时更不必说，此消彼长，价格波动剧烈。

第六章 项目总结

在这里借用朱志文老师在《Node.js 区块链开发》中写到的“人活着到底是为了什么？我们每个人可能都问过自己这个问题。我们有时候踌躇满志，想要拥有一切。有时候又高尚地低下头，崇尚与世无争，无忧无虑。但在纷繁复杂的真实世界里，我们总会被某个力量牵引着，挣脱不开，欲罢不能。”

项目有了简单的落地，ITDogChain 团队也再继续努力让狗链狗币的功能更加完善顺带吹个小牛，狗链可要要改变世界的哦！

第七章 参考文献

[1] [Crypti 白皮书 v2.1]: https://crypti.me/crypti.pdf

[2] [Express.js 开发框架]: http://expressjs.com/

[3] [Ember.js 开发框架]: http://emberjs.com/

[4] [Electron 官方网站]: https://github.com/atom/electron

[5] [Sqlite 官方网站]: http://www.sqlite.org/

[6] [Bitshares DPoS.]: http://wiki.bitshares.org/index.php/BitShares

[7] [NPM 官网]: https://www.npmjs.com/

[8] [ebookchain 白皮书]: http://www.ebookchain.org/ebookchain.pdf

[9] 《Node.js 区块链开发》：朱志文