互联现金

一种正在改变世界的去中心化生态环境

成都家驰科技有限公司

二零一七年九月

目录

第 1 章 概述

1.1 背景

2009 年的比特币横空出世，仿佛为我们打开了一扇新世界的门。这种去中心化，不可篡改，永久保存的特性，让不同的合作伙伴可以建立起分布式的信任机制。

但是在今天，提到将在未来改变世界的技术中，人工智能，基因编辑，量子计算机等往往为大众所知，而区块链技术虽然具备着极低的开发门槛，但一直没有借此征服普通民众。让我们做一个简单对比，从 09 年至今，比特币的价格一度达到 30000RMB/1BTC，实际使用用户约为 580 万到 1180 万**注 1**，而 08 年创办美图秀秀，至今月活跃用户已经达到 4 亿，11 年创办的微信，月活跃用户逼近 10 亿。有人说，他们不能一起对比，但实际情况是，比特币的价值是由目前 1000 万左右的用户撑起的，并且整个数字货币市场市值还未达到一家世界级企业的估值，我们找到了如下的几个原因:

1.数字货币脱离了普通人的生活。比特币与其他数字货币确实有真实的价值，但是一个普通的一个白领，一个菜农，一个商贩，他们过着普通的生活，对目前市面上所有的发行数字货币是不会有任何交集的。

2.鱼龙混杂的数字货币市场成为了庄家与投资投机者的博弈，赌徒的狂欢。目前除了少数几个经过了数年时间发展的数字货币，如比特币，具备着真实的交易量，其余大多是无监管的类二级市场，买入与卖出是以法币盈利为目的。

3.比特币的初衷是提供一种去中心化的自由交易方式，今天它已经成为了一种金融衍生品，而目前狂热的 ICO 市场，提出着一个一个的创新点，开发着一种一种代币，击鼓传花。

结论：数字货币市场需要一个能追赶甚至超越微信的生态系统，而我们正在进行着这样的一个新实验。

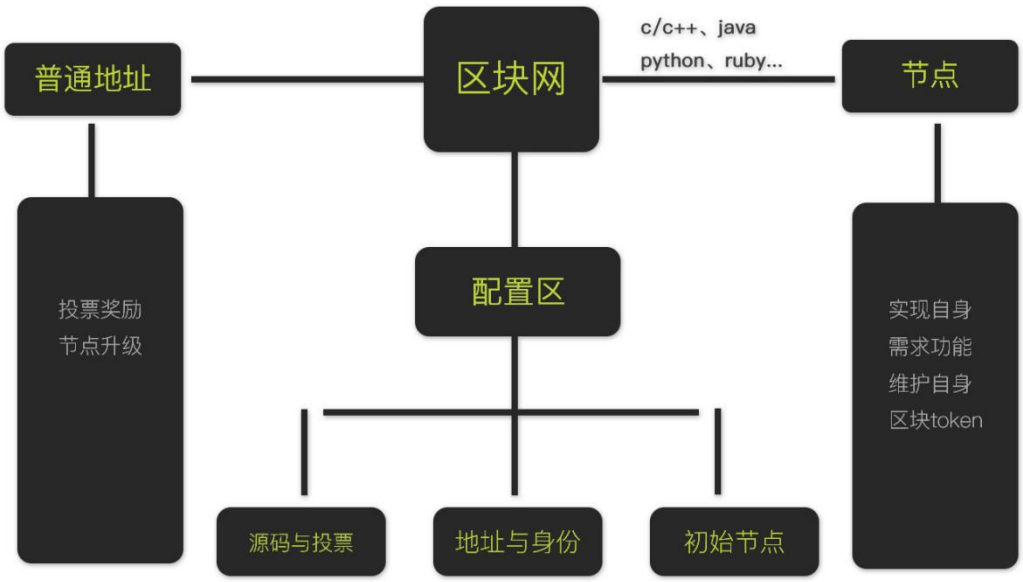
互联现金以区块链等多种技术为基础，搭建了一个全新的国内自主的底层平台，通过 POA 算法实现绝对公平的代币分配，在互联现金的区块网上，迁移或复制在去中心化上存在优势的现有成熟节点，进而推动区块链技术在中国的发展。

互联现金旨在跨越数字货币与现实生活中无数场景的鸿沟，帮助更多的个人与企业，简便地使用区块链技术，实现自身需求、企业目标。

1.2 基本介绍

互联现金建立在区块链和加密货币的概念之上，如果你对此不熟悉，很值得花时间先去读一下《比特币基础介绍》和《区块链技术基础介绍》。以下这篇文章会假设读者对比特币的工作原理有已经有基本认识。

互联现金运行着一个无法停止，抗审查，不可篡改的区块网络，其中存在大量的功能节点与普通用户，同时存在一个保存着网络配置的独立区域，网络中类似生物学中的生产消费者与太阳，除了存在一个与交易账本并存的 configuration block 外，分别存在三种权限角色，未激活钱包地址、已激活钱包地址、节点地址，如下图所示:



互联现金是什么？

互联现金是一个存在于互联网上由大量区块链集合的组成，具备了绝对公平、不可篡改、抗审查、无法停止等特性的去中心化计算机网络。互联现金起始于现有区块链技术但又不止于此，它具备独立创新的 POA 算法，同时以区块网的概念改良了单一区块链的大量数据等问题。

如何运行互联现金钱包？

互联现金钱包适用于 PC 端、IOS、Android 端及其他智能设备。

目前，我们关于客户端的开发计划主要集中在移动端下的 IOS&Android，以及个人 PC 下的 windows/linux 系统，MAC、BSD 及其余 hardware 在计划中。

运行互联现金的钱包软件，即可与网络中其他同样运行的用户进行连通，钱包地址的数量是无限的任意申请的，但互联现金网络中存在激活地址的配置区，只有激活后的钱包地址，才会获得区块网奖励分配的权利及发送接收互联现金。

互联现金客户端可以做什么？

- 获取一个未激活的钱包地址
- 查看当前所有功能节点与已激活钱包地址
- 申请激活钱包地址

- 申请成为一个功能节点
- 获得区块奖励
- 享受所有功能节点提供的服务

互联现金与比特币有哪些相似之处与不同之处？

相似之处在于互联现金借鉴了比特币等数字货币智能合约，区块链等底层技术。区别在于互联现金不具备特别的金融属性，而是着重强调将传统的互联网企业，在去中心化占据优势的情况下，将其迁移成为互联现金区块网的一个功能节点，从而将传统互联网企业进行“更新换代”。

1.3 核心目标

“我们的使命是将传统企业的功能引导或复制到一个去中心化网络，实现一个绝对意义上公平的去中心化生态环境”。

互联网发展到今天，绝大多数用户需求早已挖掘殆尽，这也恰恰也是后来者的机会，可以站在无数巨人的肩膀上更好的眺望整个世界，清晰地看到所有人日常生活所需要的方方面面，互联现金的核心目标是将目前在去中心化上具备优势的传统企业的功能进行同等复制，迁移到互联现金的去中心化网络，将固定的中心利益节点打破，重新进行平等利益分配，以功能节点留存用户，以区块奖励推动整个生态网络的发展。

我们将举两个简单的例子来具体说明：

1. 以百度公司而言，其最大的搜索引擎业务为用户提供互联网所有网页的索引和指向，其市值约 800 亿美元。百度公司主要盈利方式是受人诟病的百度推广，竞价排名，这个盈利模式的本质是用户在使用搜索引擎功能，用户提供了自己的注意力价值，为百度的推广竞价提供了基础。

2.以智联招聘/前程无忧等招聘平台而言，其搭建了一个具备，用户上传简历、公司挑选简历等招聘功能的网站，智联招聘一方面发布广告吸引了大量的求职者，同时对企业进行费用收取，才让其进行正常招聘，但是企业付出的这部分费用的价值，其实是一个又一个求职者提供的，而非平台本身。

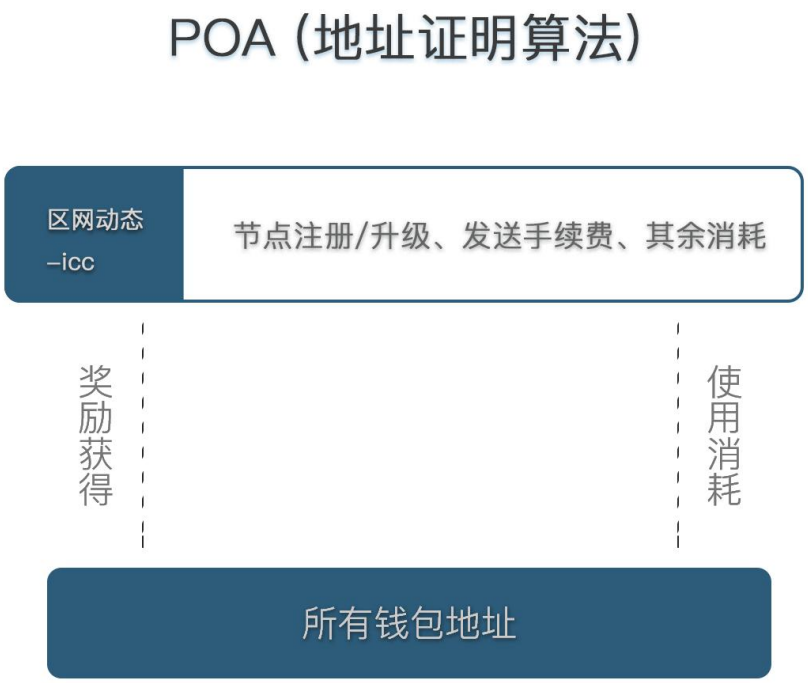
我们每次打开浏览器，进行了一次价值提供，一小部分是给导航栏 url 后面尾部的会员号，一部分是给该会员所在推广平台，剩下部分则是贡献给该导航站；我们走在路上看到的广告牌，进行了一次价值提供给承包该牌的广告商；我们使用着或正版或盗版的操作系统，为微软或雨林木风等公司。我们生活中的每一分每一秒，都在创造着价值，不属于自己的价值。

互联现金则是一个试图改变这种现状的数字货币。

第 2 章 创新技术

2.1 POA 共识机制

为保证整个区块链的安全性和正常运转，记账权所有者与区块的生成需要遵守一定的共识机制，09 年比特币的横空出世带来了 POW 算法，而 NXT 和 PPC 的 POS 算法与 bts 的 DPOS 也为数字货币带来了新的活力。而互联现金的共识机制是全新的 POA(Proof of address)共识机制**注 2**，其包括以下属性：



（1）记账权：全网活跃节点根据节点激活顺序依次获得记账权，由于 POA 的代币分配性质，记账权的竞争性消失，性质变为交易信息的发布体。其余节点和地址拥有对分配总量、分配地址的审核权，通过则同步该区块。

（2）正常区块奖励：首选每个区块奖励将会分配动态数量的代币，每一次区块生成将会自动调整区块奖励，保证本次奖励为四年剩余分配代币总额减半的平均数。计算公式如下：

$$\mathrm{Re}\,wards = \frac{\mathrm{Re}\,main}{2} \bullet \frac{1}{210240}$$

$$\mathrm{Re}\,ward = \frac{\mathrm{Re}\,main}{2} \bullet \frac{1}{210240} \bullet \frac{1}{Actives}$$

（3）额外区块奖励：由节点注册/升级产生、由普通用户消费产生的为全网额外区块奖励，将由参与了该行为的用户地址获得。

（4）区块奖励规则：正常区块奖励将会平均分配给所有钱包余额超过平均余额的已激活钱包地址，额外区块奖励将由参与了该行为的用户地址根据自身在该行为的贡献获得

（5）惩罚:对存在恶意欺骗，篡改交易数据等行为的节点或用户地址进行一定期限（default:1440s）的连接拒绝，根据具体情节的严重度与频率加大。

（6）不可篡改：区块生成并得到一定确认数后，通过大量的普通用户的完整账本以及记录型功能节点保证其内容的不可篡改。POA 算法仍然不可避免的会出现 51%攻击，不过相比算力集中于矿池的 POW 算法存在的 51%算力攻击，随着用户量的增加，POA 算法的 51%钱包地址攻击的可能性可以忽略不计。

2.2 XHTTP 协议

HTTP 协议是 Hyper Text Transfer Protocol（超文本传输协议）的缩写,是用于从万维网（WWW:World Wide Web ）服务器传输超文本到本地浏览器的传送协议，而互联现金采用的 XHTTP 协议是为了更好的在互联现金客户端与节点服务器之间进行数据交换，而在 HTTP 协议之上做了简单的创新和定义。

关于 HTTP 协议的具体细节请参见 The Internet Engineering Task Force (IETF)的 RFC 文档 rfc2616、rfc2617、rfc7230 三份文档，以下只列出 rfc 文档中不具备的 XHTTP 协议新定义:

The Method token indicates the method to be performed on the resource identified by the Request-URI. The method is case-sensitive.

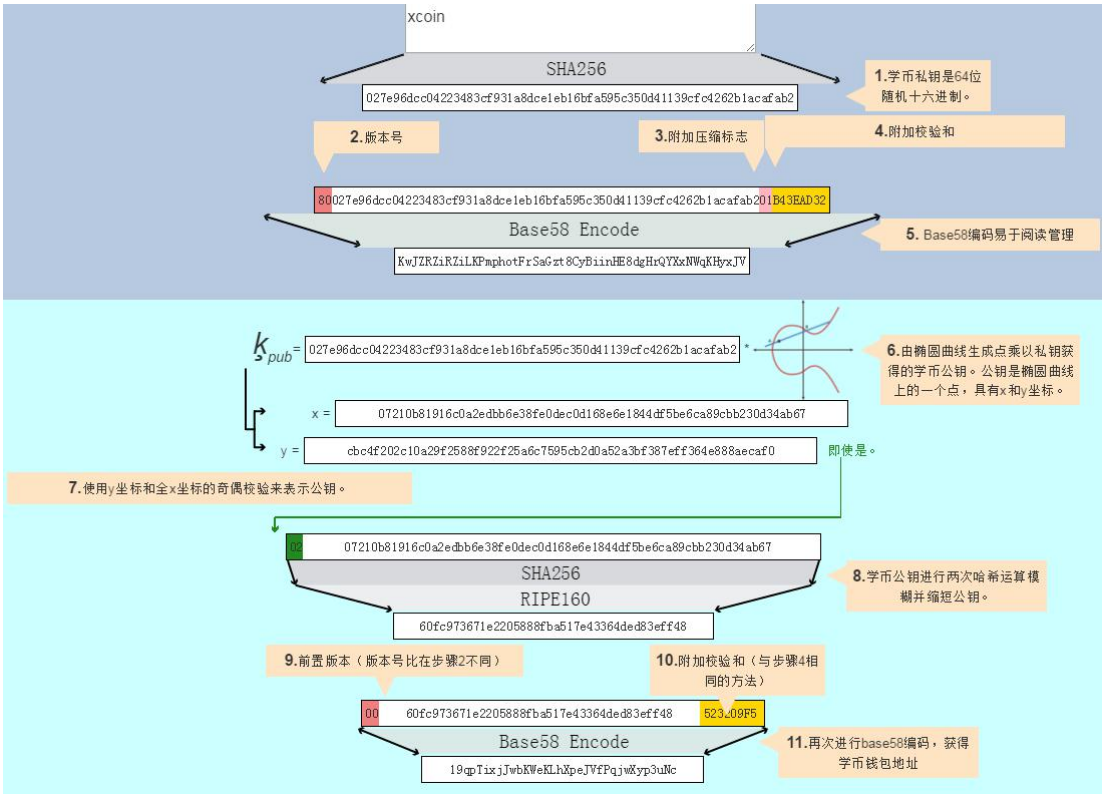
Method = "OPTIONS" ; Example

| "CHECKED" :CHECK NODE STATUS

```
                    | "STATES" :RETURN STATES ABOUT NODE
                    | "SEND"   :SEND INFORMATION ABOUT TRANS
                    ……
                    | extension-method
Status-Code    =
     "100"  ; Section 10.1.1: Continue:Example
   | "600"  ; Section 10.6.0: Command Success
   | "601"  ; Section 10.6.1: Command Reject
   | "602"  ; Section 10.6.2: Command Time-out
   | "603"  ; Section 10.6.3: Command Waiting
   | "604"  ; Section 10.6.4: Node Time-out
   ……
extension-code = 3DIGIT
Reason-Phrase  = *<TEXT, excluding CR, LF>
```

2.3 可激活地址

互联现金的钱包地址生成和格式是沿用了比特币方式，如下图所示:



未激活钱包地址:任意客户端可以生成未激活钱包地址，不具备获得区块奖励及使用功能节点的权限，可以向任意节点发送签名消息申请激活。

已激活钱包地址:由节点进行激活，该地址存储于 configuration block，节点的审核负责保证监管性，这部分团队与 EYEKEY **注 3** 达成合作意向，客户端将提供使证件，指纹，虹膜，人脸识别等多种不同级别的验证。而监管私钥会由全网所有激活地址私钥签名**注 4**,保证任何人的隐私不会泄露的同时提供法律监管，已激活地址可以享受正常的区块奖励，并且因为客户端自身的行为获得额外区块奖励，详情请参见应用场景部分。

节点地址，已激活钱包地址通过向全网上交一定的互联现金，获得全网的认可后注册成为一个节点，网络运行之初将存在一个创世节点。节点运行在一个沙盒(sandboxie)**注 5** 中，用以限制节点的权限保护客户端的安全性。节点注册的是一个服务器端口的格式化数据，也是一个类 web 界面，客户端提供包括 C/C++、java、python、php 等主流语言的开发接口，降低了节点开发者的门槛，降低了由传统程序开发向互联现金网络节点开发转变所付出的学习成本。节点的意义在

于为已激活钱包地址，即普通用户提供功能服务，节点同时可以获得额外区块奖励，详情请参见应用场景部分。

2.4 configuration block 与助记词注 6

每一个节点或普通用户的个人设备中，除了保存了公有账本，还将保存一个configuration block，其中应包含已激活地址、节点地址及服务提供地址、全网地址属性、源码区、版本号等通用属性，区块奖励、交易信息验证是通过交易账本及该 block 共同实现。

2.5 助记词与监管

我们先来以 monerod 为例简单了解一下助记种子的含义:

A 13 or 25 word phrase used to backup a monero account, available in a number of languages. This 25-word phrase (13 words in the case of MyMonero) has all the information needed to view and spend funds from a Monero account.

与互联现金团队合作的 EYEKEY(http://en.face-key.com/)，它是天诚盛业旗下人脸识别、指纹识别、虹膜识别云平台，互联现金的助记词分为多级，初级为身份证件信息流，高一级为人脸/指纹数据流，最高级为虹膜流，设置助记词可以更好的成为已激活地址，节点的激活顺序将充分考虑到未激活地址的助记级别。客户端将提供使证件，指纹，虹膜，人脸识别等多种不同级别的验证（需要移动设备硬件与 IOS&Android 软件版本支持）。更为重要的是，监管私钥会由全网所有激活地址私钥签名，保证任何人的隐私不会泄露的同时提供足够的法律监管。

2.6 投票与消费

投票与消费机制是互联现金生态系统的核心机制，它体现了“贡献”在其中贯穿的作用。

目前客户端投票消费机制拥有的功能如下:

•源码版本投票:投票达到51%时将更改所有客户端存储的configuration block中的源码来源及版本号。

• 地址惩罚:投票达到51%时将限制节点或用户的正常运行使用，惩罚时间依据发起投票人而定。

•节点排名:节点可以下一个区块产生之前，通过向全网上交互联现金的方式，以期在下一个区块产生后在所有客户端获得更前面的节点排名，获得更多的曝光使用率。

• 全网通知:节点或用户可以通过向全网上交互联现金的方式，向全网的所有地址发送通知信息，同样是在本时间段的上交互联现金数量决定了下一个区块产生后的一个区块时间内的通知发放情况。

还有更多的投票消费机制即将发布。

通过这种方式，一方面将更多的功能节点迁移到互联现金网络，另一方面将属于自身的价值给予自身，通过互联现金的额外区块奖励进行体现出来。

第 3 章 应用场景

列举产品的主要特点和特效，如可靠性、安全性、高性能等。以及有哪些优势等。

3.1 导航节点

随着自营的节点和其余节点开发者的加入，节点的数量会越来越庞大，所提供的功能也会更加多样化，导航节点为全网其他节点进行分类并整理成易搜寻和阅读的格式，具备大量的连接用户的导航节点将在区块奖励中因为贡献的连接数而获得更多的代币奖励。参照:hao123.com

3.2 记录节点

功能节点会随之带来相应的个性化数据，如自设的昵称，发表的文章，这些节点本身只能将之存储在本地，不能具备一个中心化的数据库。而记录节点则是提供数据迁移的功能，其拥有高速的上传下载带宽以及大量的闲置硬盘空间，用以存储经过了私钥加密的个性化数据，在个人隐私和网络安全问题日趋严重的今天，随着网速的不断增速，去中心化的存储也必然成为继云存储外另一项可靠的选择。参照:类 CDN 缓存节点，但具备去中心化及加密属性

3.3 舆情节点

综合目前已有的舆情平台，提供一个综合性实时数字货币价格、新闻、交易量展示平台，将舆情平台由中心化的互联网企业迁移成为一个去中心化的功能节点，通过连接数来获得全网代币奖励。参考:www.btc123.com

3.4 直播节点，主播和观众的交互不存在中心节点，主播可以收到完全的打赏奖励。但视频流产生的大量服务器带宽如何融入去中心化生态环境尚未解决。参照:www.douyu.com

3.5 场景拓展:滴滴快车/美团外卖/智联招聘/58 同城/慈善机构……，在具备大量用户以及足以进行研发算法和拓展市场的资金后，我们将优先搭建硬性需求节点，如上述节点。

第 4 章 加入我们

我们的优势

• 技术能力优秀，执行力强。

• 有完整会议及投票机制，官网会定期发布会议日志和工作进展。

• 不以金融及代币交换作为发展目标，以节点培养用户粘性，真正将互联网功能同步复制到生态网络，以突出区块链、去中心化的优越性。

• 可激活地址、可申请节点，拥有无限可能。

加入互联现金社区，了解更多

官方网站: http://www.ic.cash（建议优先阅读资源板块的路线图）

官方 QQ 群:

199920001(1 群) 199920002(2 群)

199920004(3 群) 199920005(4 群)

参考文献与注解:

注 1: 包括 Airbitz，Armory，Bitgo，Blockchain，Coinbase，Greenaddress，Ledger，Jaxx，Mycelium，Samourai 和 Xapo 在内的 26 家 btc 钱包公司，联合调查发布

注 2: 共识机制是区块链事务达成分布式共识的算法，互联现金是第一个应用 POA 算法的数字货币。

注 3: EYEKEY 是北京天诚盛业科技有限公司旗下的新型生物识别云服务平台

注 4: Fair multi-party concurrent signature scheme,叶青,2014

注 5: Design and Implementation of Linux Application Sandbox Based on Multiple Security Mechanisms，李 晨 冯圣中，2015

注 6: 是数字货币中具备全部交易权限的备份数据，参考 monerod 中的 seed