

ReciprocateLink

Based on the Autonomous Information Asset of Clumsiest Information Inc., the Blockchain technology is used to develop the daily application.

License using MIT Open Source protocol  
©2018 Clumsiest Information Inc.

『阿灵』互惠链项目推荐书

上海拙真信息技术有限公司  
北京大成律师事务所贵阳分所

2018. 3. 18

Hello, everyone:

经过一段时间的准备和思考，想给项目起个名字。

因为是坚持去中心化的分布式思想，来实现基于“自主信息资产”的区块链应用，所以点对点的、对等的、互惠互助的应用模式是我们的基础选择。

在互联互通的今天，网络和信息技术，以及铺天盖地的电子设备，已经彻底地改变了这个世界，人类从没有像今天一样地彼此相连。

正是在这样的前提和背景情况下，我们想从根本上尝试一种全新的可能，即隐私被严格保护的，信息以产权形式被确权的，个体或法人完全自主地可以开始：

① 一边工作、生活着，一边就极为便利地生成、采集和加工出自己的“自主信息资产”来；

② 与此同时，各类身边的事务也在一种全新的劳作中，互惠互助地得到了极低耗费和顺畅的处理；

③ 假以时日，随着你拥有的“自主信息资产”越来越丰富，其价值，和因将其与海量信息不断碰撞迭代而产生的新型价值，将得到持续的非线性提升。

从某个角度讲，启动这个项目是我们自身的生存需要；从另一角度讲，也许有说不清楚的使命使然；再一个角度讲，是真的好玩！

所以，义无反顾地就投身其中了。

既然这样，总得起个名吧？于是，就想到了“阿灵”互惠链（Reciprocate Link）这个名字。

各位 Collaborators，意下如何？

要不，大家就先叫起，项目中再随时 Commit Update ！

Regard,

Jeephy Ji    2018/03/20    17:18

# 第一部分

从中本聪 (Satoshi Nakamoto) 说起

为什么要“去中心化”?

“去中心化”能带来什么

区块链技术的“共享”实现

区块链技术的定义

区块链技术的应用的现状

对区块链技术应用的理解

“信用”驱动和“共享”实现

## 从中本聪 (Satoshi Nakamoto) 说起



The Times 03/Jan/09: Chancellor on brink of second bailout for banks

《泰晤士报》2009 年 1 月 3 日：财政大臣濒临第二次解救银行危机。

2009 年 1 月 3 日 18:15:05，编号信息为：Bitcoin Block #0，哈希值为：000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f 的世界上的第一批 50(BTC)比特币在芬兰赫尔辛基的一个小型服务器上诞生了。从那时候开始，没有任何中心化组织背书的纯电子数字串开始了它神奇的演化。

2010 年，比特币第一次在现实世界获得价格——美国的程序员拉斯勒·豪涅茨 (Laszlo Hanyecz) 用 1 万枚比特币交换了两块价值 25 美金的披萨。在短短的七八年时间里，比特币就曾经创造了每币 15,300 美元的峰值价格；到北京时间 2018 年 3 月 21 日 19:32 分，比特币的交易价格依然高达每币 9,084.50 美元。

剔除虚拟货币在投机市场的疯狂，我们不仅要想，原本“一文不值”的电子数字串凭什么搅起了经济社会的巨大波澜，在它的背后究竟是什么蕴含了非凡的可能或价值？

从 2014 年开始，我们因为关注“共享模式”，关注“去中心化”应用的技术实现，开始研究区块链技术。也是从那个时候知道，全分布式的、去中心化的技术应用将在未来对人们的生活、工作等方方面面带来彻底的改变。但是，我们认为技术毕竟是技术，比特币、区块链技术所实现的全分布式共识替代人们习以为常的中心认定、权威价值，恐怕还远不是时候，甚至可能是永远都不会实现的幻影。

感谢隐身的中本聪，感谢他（她）去中心化的消失，正是他（她）发布的《比特币：一种点对点的电子现金系统》(Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 年 10 月 31 日)白皮书及以此创生的比特币，唤起了世人对区块链技术的迅速认识并逐步认同，特别是要感谢他（她）在中心、权威、权力和金钱如此强盛的社会，投下了最重磅的“去中心化”种子，从此为全人类开辟了重塑社会信用体系的新纪元。

## 为什么要“去中心化”？

世界今日之现代化，全有赖于为达成某一功能、效用而人为选择或建立的结构来实现。借助科学技术的发现、发明以及相应的实施手段，人类社会已经发展到了一个高度发达的阶段。

这个阶段的典型特征是：人类几千年的文明发展史，已经从生产力制约生产关系逆转成了生产关系制约生产力的状况。

社会再继续以自我为中心，再一代复一代地通过竭力建立所谓的“不断创新”结构，来企图达成可持续发展，已经不现实了。这个不现实已经显著体现在当代东西方思想发展脉络的核心认识上，即：人类社会不能再仰赖不断累进的过度繁复的秩序、规范、习惯、原则（包括美学、力学、建筑、组织、功能等等）来实现长久健康的发展了。这个认识比较有代表性的思想有二十世纪 60 年代起源于法国的“解构主义”，有近来我国学者王东岳先生于 2002 年提出的“递弱代偿原理”等。

人首先是“以食为天”的，那么我们今天解决生存的本领（生产力水平）有多大呢？2017 年，美国有 3.22 亿人，其中住在农村地区的人仅占约 2%，从事农业生产的人只有 1%，大约 350 万的农业劳动力养活了全美国人，还是全球谷物出口的大国。中国的情况是：2014 年人口总量 13.6 亿，虽然有 6.74 亿的农业人口，却只有 1.79 亿的农业劳动力从事农业生产；到 2005 年前，中国就用不足世界 10% 的耕地养活了占世界 20% 的人口，并完全摆脱了多少代人都难以忘怀的“饥荒岁月”。

人类社会生产力水平达到如此的高度，当然仰赖于科学技术和市场经济的充分发展，也完全依靠了英雄、权威以及财富、权力这些往往以中心化模式存在的

各种力量的不歇推动和贡献。但是，当生产力水平已经发展到可以远远解决人类的基本生存的时候，严重的问题也就不期而至了。

我们知道任何中心都是有其天然的弊端的，其主要弊端表现在以下方面：

### 1. 结构脆弱

依赖中心化运行的体系，一旦中心产生阻滞，就会导致整个体系的瘫痪，风险极大；一旦中心出现错误，错误就可能在被中心所依赖的整个体系中几何级数地放大。

### 2. 缺乏良性竞争和监督

中心形成后，除了其自身的能量和能力之外，一般都伴随着事实上的权力条件。这就必然妨碍了良性的竞争，也无法对其实施有效的监督。

### 3. 管理困难、维护成本高昂

任何中心经过一段时间的发展之后，为了其自身的发展和生存，往往结构都会越来越复杂，机构都会越来越臃肿。这将导致管理渐次困难，维护成本持续高涨，并最终产生不能回避的官僚，滋生难以剔除的各式腐败。

### 4. 导向极权

中心的权力运行，因其能快速聚集人才、技术、资金、物资等资源，形成运营优势。所以就极容易走上权力至上、实力为尊和利益唯己的极权道路。极权中心的存在，其实已经是人类未来实现真正的公平和民主，实现共同文明、共同繁荣的根本羁绊。

### 5. 隐私难以得到保护

历来的中心化体系，在为大众提供服务、进行管理的时候，都无一例外地让人们典让了或多或少的信息。得到这些信息的中心化体系又都无一例外地或多或少剽取了人们的隐私。随着信息化高速发展的进程，信息及信息隐私不能够得到根本的保护，已经是极其严重且不能容忍的问题了。

（碰巧的是，就在编写本文的时间里，国际上又爆出了一起重大的数据泄密事件：



事情起因于 2018 年 3 月 17 日的媒体曝光—Facebook 上 5000 万名用户个人信息数据遭一家名为剑桥分析公司的泄露，背后还牵扯到更为吊诡的政治密谋，2016 年美国总统大选、英国“退欧”事件。）

## 6. 终究不可信任

英雄和中心推动了人类几千年的文明发展，却在生产力高度发达，信息化、网络化迅速普及的今天，成为了终究不可信任的主体对象。道理其实非常的简单，本来对于任何的人或事物，我们都得先假定是不可信的，因为哪怕是曾经可信，都不代表其下一刻可信。

当世界的发展速度已经一日千里，信息的传递和普及已经几达光速之时，原本可相对稳定地承载众人的托付和信任的英雄或中心们，也就再没有往昔那般的必然存在价值了。

这些中心化的弊端并不是未来的产物，它们已经给人类、人类文明的发展形成了莫大的影响，导致了非常可怕的恶果。

整个人类社会，很多的问题我们真的无法回避。

比如：曾经在生产力不发达的年代，战争成为了争夺资源的最主要方式。可我们今天，如果只是要解决温饱问题，大体利用社会 30%的劳动生产力就足够了。却为什么这个世界还是战争不断？今世的战争究竟在“争”些什么？那些富裕的生产力都到哪儿去了？是消耗到战争或准备战争中去了吗？还是去满足少数人抑或大多数人的贪婪去了？而这般的贪婪又从何而来？

诚然，这些个问题是很难不好回答的。除非，您看清了现今的社会是生产关系严重地制约着生产力的发展。这个制约阻碍着人类的文明进步，妨碍着普通民众享有生产力发达后的美好幸福生活。

再比如：我们生存的环境问题？

人就是靠食物、水和空气生存的，可您在餐桌上吃的哪一样食物没有污染？您喜爱的水果哪一样没含有激素和农药？

记忆里的泉水，是不是都只是记忆了？课堂上给孩子们讲甘甜的泉水时，他们还能体会那份甘甜吗？

气候变暖、辐射、雾霾，连呼吸离不开的空气也都越来越被污染了，除了满眼的“舒适”和“奢华”外，生活的空间哪里还有一块大自然赐予的净土？

... ..

追寻这些问题的答案，不难发现，整个人类社会已经到了必须要重新思考文明，重新理顺生产力和生产关系的关系的时候啦！

如果，人们不即刻行动起来，反省发展历程，并从中找到全新的发展思路和生存样式，然后迅疾地做出改变，厄运自是不言而喻的。

何况，我们自身发展出来的人工智能，还极可能孕化出一种超级物种，TA可是在那儿等着我们嘞！人类要是自甘毁灭，TA是不是正好可以代劳呢？(^\_^)

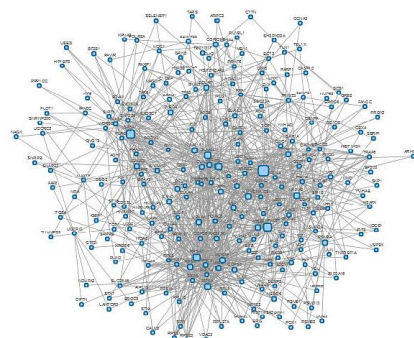
再次感谢 Satoshi Nakamoto，感谢像他（她）这样一些人类份子，为我们开辟新的未来，提供了可能的选择，比如：基于区块链技术，运用共享模式，去中心化实现的全新生存样式。



## “去中心化”能带来什么

“去中心化”（Recentralization）是指在一个开放的系统中，每个存在的单元或节点彼此协同、相互服务，并不再依赖某个单元或节点为众多的单元或节点进行统筹、管理和提供服务；单元或节点都是自治的，彼此之间的协同或服务是自洽的；系统层面淡化结构，重视连接，并能在单元或节点之间的连接并不可靠的前提下，实现全局连接的可靠、高效、成本低廉和强容错。具备这些要素的系统，我们把它称作“去中心化”的系统。

“去中心化”并不是排斥中心，它只是放弃了全局化的、固化的中心，转而强调对等地、扁平地、动态地将每一个单元或节点都可视为中心，必要的时候全局反而可以围绕某个单元或节点展开行动，提供服务或被它服务。



关于“去中心化”的定义繁多、众说纷纭，为了本文的表达以及和大家的交流不产生歧义，我们先给出上述“去中心化”的描述，也可算作是一种定义。

参照我们的定义不难发现，“去中心化”的系统很好地跨过了“中心化”系统的诸多弊端。

“去中心化”系统是强连接、多路径的，任何一个单元或节点的故障或失效都不会影响整个系统的继续运行，这就规避了中心式结构的脆弱性，换来了整体系统的强容错能力。系统的单元或节点都是通过连接实现自洽的协同，不再强调竞争机制的作用。系统的运行和进化完全基于独立单元或节点的自治和彼此自洽，不再为中心化的存在付出额外成本、支付过度代价；同时在信息技术和互联网技术的支持下，边际成本还将迅速地趋零逼近，所以其系统的成本和顺滑优势还将越来越强。

因为组成“去中心化”系统的单元或节点都是要求自治的，如果是在社会之中施行“去中心化”模式，那么每个人的信息都将被严格确权，隐私将得到充分的尊重和保护。（目前，世界上的主流国家，包括中国，都已经有了保护个体和法人单位信息及隐私的相关立法）

另一个有趣的方面是，前面我们讲了任何的人或事物都得先假定其是不可信的。那么，“去中心化”的系统又将如何解决协同所必需的信任问题呢？

其实，“去中心化”是一个描述概念，而要实现“去中心化”的系统却需要许多的条件、技术和手段。如何解决协同的信任问题，区块链技术中的“共识机制（Consensus Mechanism）”就提供了一套符合“去中心化”要求的有效解决办法。比如，在任何人都可以匿名接入的网络中，基于区块链技术实现的比特币系统，就使用了一种叫做工作量证明（Proof of Work，缩写：PoW）的共识机制，以此来证明“挖矿”的矿工付出了必要的工作量，其最终依靠算力获得的 nonce 在网络的广播中通过了合法性验证，挖矿成功。

（nonce，Number used once 或 Number once 的缩写，在密码学中 nonce 是一个只被使用一次的任意或非重复的随机数值）

这样，区块链就从本质上解决了：在开放的系统中为达成交易或者共识原本要依赖于第三方的问题。区块链的技术和安全过程使得陌生人之间在没有被信任的第三方时产生了信任。

看到了吗？

假定谁都不可信的环境中，也不用再依赖任何的中心机构，只是运用“去中心化”的思维，通过区块链技术，就实现了完全可信的交易或共识。

从社会学的角度来讲，这也将是我们未来构筑新型生产关系的基石。

## 区块链技术的“共享”实现

我们从中本聪、比特币，讲到中心化社会的弊端，再讲到去中心化的意义和区块链技术的价值，其最终还是要去推动全新的社会信用体系的到来，去践行全新的社会生产关系。

可是，真的像应景似的：“忽如一夜春风来，千树万树梨花开”，区块链技术和项目眨眼间竟充斥了世界！这不是一项单一的技术啊，也不可能以某项单纯的产品就能产生出其该有的极大价值。更何况其对中心化的颠覆，实质上是对几千年来人类习惯的一次重大变革！

感叹之余，还是要认真地拿出我们的理解，提出我们的具体方案，毕竟区块链技术的应用价值是非凡的，其可能展示的未来也是足够吸引我们的。



## 区块链技术的定义

关于区块链技术也是存在多种定义的，我们较认同的定义是：**区块链技术**（**Blockchain**）是利用块链式自引用数据结构、利用分布式节点间的共识算法来生成和更新数据，利用密码学的方式保证数据传输和访问的安全，利用由自动化代码设定的智能合约来编程和操作数据的一种基础架构，其实现了数据层面的透明、可追溯和不可篡改。

区块链技术的要素包括：

- 块链式自引用数据结构
- 分布式存储
- 对等网络通讯（**Peer-to-Peer Network**）
- 共识机制
- 强加解密算法
- 全民账簿
- 智能合约（**Smart Contract**）

区块链技术应用具备许多新的特性：

- 匿名接入/隐私保护
- 节点自治
- 规则可编程
- 任何数据均可追溯
- 任何数据不可篡改
- 集体维护

区块链技术作为一种数据处理的基础架构，可以应用在非常广阔的领域。目前的应用开发比较集中在：转账支付、资金结算、智能合约、身份认证、电子商务、版权保护、证券交易、贸易金融、物联网和大数据这些领域。





## 区块链技术的应用的现状

盘点 2017 年，比特币价格全年涨幅超过 1500%，币圈黑马瑞波币涨幅超过 36000%，以太坊涨幅为 9162%；就是一些并不为大众熟知的新经币、Stellar 和达世币，价格上涨幅度都分别达到 29842%、14441%和 9265%。

区块链技术似乎除了在虚拟货币领域不断缔造“造富神话”之外，却鲜有实际领域的成熟应用落地。

目前虚拟货币的疯狂，基本上是彻头彻尾的投机行为使然。待巨大的泡沫过后，尘埃终会落地。

而我们却必须要审视的是：在如此疯狂的虚拟货币神话刺激之下，为什么没有诞生真正具有重大实用价值的区块链技术应用？

普遍的报道、分析和认识有这些：

... ..

数字货币分析师肖磊称，受制于场景应用、技术配套以及缺乏第三方来翻译“区块链语言”，区块链落地成为一大难点。

业内多位人士称，其“颠覆”意义不仅是对现有互联网技术的改进，长远来看是对社会组织协作方式、商业运作模式的颠覆。不过短期来看，受投机氛围、技术因素等限制，谈“颠覆”尚早。

区块链并不是不能去除代币的机制，只不过失去代币机制区块链的价值将大打折扣。“失去了代币这种通证，区块链就变成了一种升级版的企业数据库，意义就缩减了 99%，其改造社会的能力就会大大降低。”中文 IT 社区 CSDN 副总裁孟岩告诉新京报记者。

这项技术的处理速度太慢，无法大规模应用。以太坊每秒只能处理大约 15 笔交易。相较之下，Visa 每秒可处理 2000 笔交易。

类似中本聪的无政府自由意志论者或许会为区块链辩护：它的好处在于可以规避国家干涉，但杰勒德认为传统企业没必要采用这一技术。

“区块链应用的场景应该是共享、共建、共监督，既要对区块链技术有很深



的研究，又要对应用领域的痛点了如指掌。现在很多人是拿着锤子找钉子，拿着技术去试场景，这是错的。”布比区块链 C00 李军说。

“目前从我们掌握的情况看，区块链在大金融的支付、P2P、票据、供应链，以及公证、医疗、社交等领域存在应用基础。”一不愿具名的投资人称。

挖矿十分耗电，现在爱尔兰用在挖比特币的电力比全国日常家庭电耗还多。

区块链投资基金 Outlier Ventures 的 CEO 和创始人杰米·巴尔克（Jamie Burke）表示：“我认为至少两三年内区块链还无法发展出任何有意义的用途。但第一代技术往往无法带来轰动性的变革，要等到第二代或第三代技术。技术被采纳常常要经历这样的过程。但区块链的唯一不同之处在于它的迭代过程受到了大量关注，原因来自对虚拟货币的热捧。”

... ..

这些报道、分析和认识，基本上从各个方面客观反映了区块链技术应用的现状和困难。

不过，序幕既然已经拉开，前奏已然喧嚣，故事的主旋律总要登台。



## 对区块链技术应用的理解

要运用去中心化思维和区块链技术，开辟全新的社会信用体系，创新新型的社会生产关系，为普通民众提供全新的生存样式，使他们能充分地享有生产力发达后的美好幸福生活，就必须对事物的本质有着更深的理解和把握。

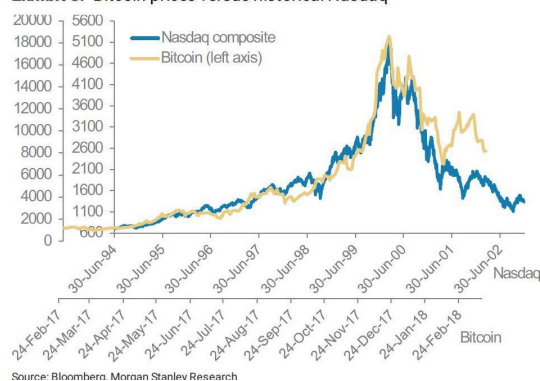
冷静地分析比特币的火爆成功，我们将会发现：虚拟货币一开始先回避了与现实世界的直接对话，那些神奇的电子数字串并没有和任何实物、交易相关联。这就为它突破强悍的现实世界的束缚，充分地展示“不依赖于任何的中心机构，就能实现或达成完全可信的交易或共识”的社会实验创造了条件。

这项社会实验取得成功的价值是非凡的。比特币网络自 2009 年上线以来，在无人管理的情况下，全球范围 7 x 24 小时运行已达 9 年，单日最高处理过 255,000 笔交易，最高单笔交易金额到达 1.5 亿美元，迄今未出现过重大的系统故障。比特币真正从实践意义上实现了安全可靠的去中心化机制。



但是，比特币依然是根植于经济利益驱动的，“矿工”们依靠公平的“工作量”付出而获取收益，这也就很容易地演化出完全投机的虚拟货币交易市场。近年来，明目繁多的虚拟货币交易的兴起，伴随着人们对可信的未来的真切期许，对虚拟货币可实现非凡价值的展望，也就迅疾地产生了极其夸张的“比特币泡沫”。

Exhibit 3: Bitcoin prices versus historical Nasdaq



摩根士丹利：比特币像纳斯达克泡沫

同时，我们还需要关注区块链技术应用的一些关键问题。

应用首先要注重的是去中心化的架构。这要求，应用项目的主要资源是分散化的、群体化的，项目运营的模式是自洽式的，项目的发展是迭代式的。这些道理看起来挺简单，觉得实现起来会很容易。但事实证明，因为人们都习惯了的中心化的思维和做法，往往喜欢规划路径、设计细则，热衷于集中资源办大事，习惯于管理和被管理，于是就总在项目的成形和运营中，把项目最终又导入了中心化的困局。

区块链技术的应用有赖于去中心化的思维，它就必然是轻结构、重连接的。不再基于搭建复杂而强大的结构来实现项目的核心功能，而是依赖于交互各方完成连接后的自洽来实现，或是交由信息的代码化来透明地实现。

区块链技术的应用项目，还比较容易进入误区。比如：如果我们建设一个交互平台为客户群体提供了大量的有价值服务，就常会以为自己占据了一个流量的必经通道，就会以此衍生不当的高额收益，甚至会滥用客户信息，触犯信息隐私，打造竞争垄断等。这些误区的形成，其实都是源于中心化思维和习惯的必然结果，只不过是觉得顺理成章而不自知罢了，甚而还会很可笑地当成是理所当然。

区块链技术虽然涉及的技术分项繁多，但基本没有任何一项是源于区块链自身发展出来的。所以说，区块链技术本质上是一种应用技术、一种聚合技术，那就要求在具体的项目中尤其要注重对实际应用场景的深度贴合，并以此为基础来激发项目的创新价值，保障项目的健康发展；另外，动态地掌握所涉及的各项技术的发展规律和特质演化也是非常必要的，也还需要时刻关注相关新兴技术与区块链技术的碰撞与融合。





## “信用”驱动和“共享”实现

其实区块链技术应用最难的地方，是在项目的内在驱动力方面。

对于中心化的应用，承担中心职责的中心、机构抑或是权威、英雄，通过价值实现会赢得名声、尊重和自我满足，会有利益的收获，还时常会伴有权力的攫取，如此等等就构成了项目得以发起、投资、开发、实施、运营、维护的内在驱动力。

显然的，对于区块链技术的应用项目来说，这些原本存在于中心化项目中的内在驱动力没有了，项目靠什么来驱动呢？

我们不妨这样来思考：

社会是建立在每个个体的劳动和劳动产出的成果交换之基础上的。随着社会的发展，社会化分工越来越精细，最原始的物物交换就远远不能满足人们的生存需要了。于是，商品产生，支撑商品交换的货币产生。

而货币其实承载的是劳动者的劳动成果，从保护劳动成果的本性出发，货币和商品交易必需是绝对可靠的、完全可信的，即：货币和商品交易必需要绑定“信用”。比如，各个国家发行的法定货币，如人民币、美金、英镑等，就是使用的国家信誉来承担商品交易在价值结算上“信用”保障的。

而商品交易的可靠、可信，是通过检验、鉴定、认证、测试、评估、公证、保险等第三方机构来从不同的方面提供“信用”保障的。

但是，在比特币出现之前，由于交易各方之间存在信息不对称，以及中心化机制下各自的趋利导向（最严重的是，第三方中心机构为达成利益最大化而丧失公平、公正原则），人们在劳动成果的交换中普遍存在难以克服的利益失衡，高效率的市场资源配置也难以实现。

而去中心化的区块链技术，让人们找到了一条切实可行的途径，可以不需要任何的第三方“信用”而实现可靠、可信的商品交易，以及任何需要交易的事物的交易。

既然很好地运用区块链技术可以建立全新的“信用”体系，而无需任何第三方地切实保障劳动成果和劳动成果交换，促进社会公平、公正，提高资源配置效率；那么，从本质上讲，区块链技术的应用就得是基于“信用”驱动的。



“信用”是人们可以参与社会并广泛协同的根本前提，有了区块链技术的绝佳保障，有了大数据、人工智能等的助力，重塑新型的社会生产关系，人类社会的文明就迎来了又一次重大的发展机遇。

认清了区块链技术应用的“信用”驱动本质，在实际项目的运作上还必须要仔细甄别合适的实现模式。

前面我们剖析了区块链技术的概念，分析了当前创建落地项目的现状和困难，也用很多的文字阐述了我们对于区块链技术的理解。如果以这些为基础，不妨可以从以下五个基本方面来考察区块链技术应用项目如何选择实现模式：

## 1. 价值主张

区块链技术应用本质上是为目标受众提供信用保障的价值，主张基于信用的交易或共识。

## 2. 目标受众

区块链技术应用都是运用在开放环境中的，又没有主从关系或者类似于服务与被服务等关系，所以目标受众一般都比较宽泛。

## 3. 应用渠道

区块链技术应用一般都是在 **Peer-to-Peer** 的对等网络上架构的，任何两点之间都是直接连接，是最优化的渠道布局。

## 4. 群体关系

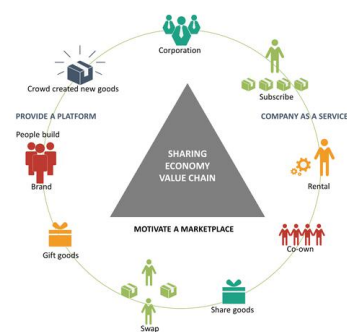
区块链技术应用中的节点都是自治的，维护群体关系的方式大都是节点自维护为主，辅助以博客(Blog)、论坛(BBS)、分享(Share)到--微博(Weibo)、微信(Wechat)、推特(Twitter)、脸书(Facebook)等。

## 5. 合作伙伴

区块链技术应用节点之间的协同都是自治式的，也可辅助以编程实现的自动化代码化来执行智能合约。

这五个基本方面一罗列出来，我们都会不约而同地想到：“共享”模式可能是最适合区块链技术应用的实现模式。

SHARING ECONOMY





“共享”模式因其启用闲置资源、消除中介、供需自洽、连接扁平等特质，与“去中心化”的区块链技术应用有着良好的契合度；同时，两者都是信息技术、计算机及网络技术充分发展的产物，是同一时代的伟大发明，相容性极好。

综合以上所述，我们可以将之总结为：**创建区块链技术的应用项目，最好是“信用”驱动、“共享”实现。**

## 第 二 部分

“阿灵”互惠链做什么

项目技术架构

技术重点和难点

项目技术重点

项目技术难点

项目的开发和实施

项目的关键着手处

## “阿灵”互惠链做什么

前面用了大量的篇幅阐述去中心化思维和区块链技术，是为了把我们要创建的区块链落地项目——“阿灵”互惠链的背景、核心理念和技术脉络说清楚。

那么，“阿灵”互惠链是个什么样的项目，它又要做什么嘞？

我们每天都在和各种各样的信息打交道，也可能知道活着的每分每秒都可以反映为数据，也程度不同地使用着许多的信息处理工具来完成各种事务。伴随着智能手机的普及，大多数人们的生活迅速“数字化”了。尤其是许多年轻人，还患上了严重的“手机病”。

这一切说明，我们已经进入了“信息化”的时代。

奴隶社会是奴隶主拥有奴隶，封建社会是封建主（地主）拥有土地，资本主义社会是资本家拥有生产资料。那么，在信息化时代，又该是什么样的呢？比较理想的是：人人拥有信息。

对于意识形态的东西，也许您不想搞得太清楚。不过，有一点您一定是想明确的，即：自己的信息该属于谁？公众信息您能否公平享用？

明确的答案其实是：谁也不能反对您完全拥有自己的信息，公众信息当然该每个人都公平享用。

可问题是：您的信息在哪儿了？您又哪来条件公平地享用浩如烟海的公众信息呢？

更为可怕的是，您大部分已经数字化了的信息，其实是在各式各样的为您提供免费或付费服务的电商手里；真正能够处理和利用公众信息的，也是那些大型的中心化机构或企业，而我们经常只有被它们“愚弄”的份。

（如果感兴趣，可以看看前述内容中提到的脸书数据泄密事件的最新报道：使用泄露用户数据的剑桥分析公司，助力了 2016 年的特朗普当选美国总统）

现在，我们有了区块链技术这样的颠覆性工具，有了“比特币社会实验”的成功验证，有了民众对“不再依赖任何的中心机构，就能实现完全可信的交易或共识”的认识，“阿灵”互惠链要实现的就是：人人公平地拥有信息！

“阿灵”互惠链（ Reciprocate Link ）是去中心化地为客户建立“自主信息资产”账户，设立客户数字化信息的所有权、使用权和可交易的运行机制；提供丰富的移动端、浏览器端工具，使客户可以便利地生成、采集和加工日常数据，不断累积各自的“自主信息资产”；通过功能扩展，支持各种以“自主信息资产”为基础的区块链技术应用模块，实现如：文书公证、供需自配、供应链追溯、智能合约、原创验证、资产价值挖掘、精准医疗、精准教育等应用。

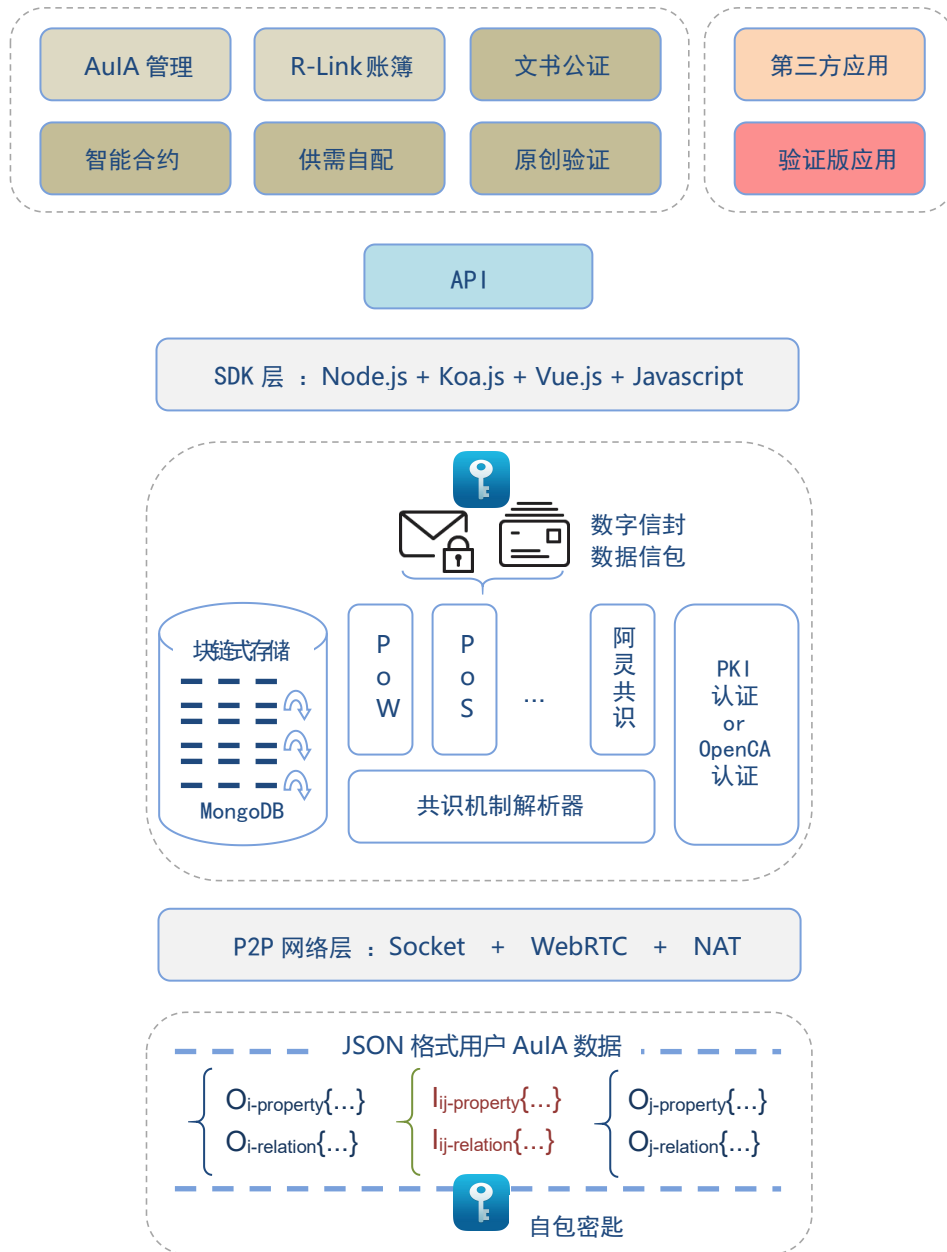
“阿灵”互惠链的主要特点：

- 信息资产化
- 严格保护隐私
- 功能模组化，可动态配置和扩展
- 操作智能化
- 资源共享接入
- 全云化



“阿灵”互惠链应用场景图

## 项目技术架构



“阿灵”互惠链技术架构图

从“阿灵”互惠链的技术架构图中，我们可以看到，整个项目建立在上海拙真信息技术有限公司的“自主信息资产”（Autonomous Information Asset，简称：AulA）框架之上。JSON 格式的用户 AulA 数据包括了用户的自有属性数

数据集  $O_{i\text{-property}}\{\dots\}$  和内部关系数据集  $O_{i\text{-relation}}\{\dots\}$ ，以及用户之间交互的数据集：关系属性数据集  $I_{ij\text{-property}}\{\dots\}$  和交互关系数据集  $I_{ij\text{-relation}}\{\dots\}$ 。所有的用户数据都必须在传输和存储前采用自包密匙进行加密。

P2P 的分布式对等网络，通过 WebRTC 开源协议可实现点对点的包括实时音视频直播的数据传输；通过 NAT 可实现在用户使用内部网络（如：公司局域网，家庭 WiFi 路由内部网）时都能完成点对点的内外网穿透，保障数据传输的畅通。

所有经过加密后的用户数据，在基于系统选择的共识机制达成后，经过安全认证，均以块链式结构写入开源的非关系型数据库 MongoDB 中。而从数据库中调出数据时，均采取数字信封或数据信包的方式提供，以保证任何人对数据的访问，要么是非对称加密保护下的访问，要么访问的是经剔除敏感元素后的可公开信息。

整体项目的开发，除需特别优化之外，均统一在前后端使用 JavaScript 语言进行开发，全部使用开源的、优选的 SDK 工具，进行项目的开发、调试、测试、部署、维护和迭代升级。其中，选用 Node.js 作为代码运行平台，服务端框架使用 Koa.js，前端框架使用 Vue.js。

技术架构上将 API 集完全独立，便于应用层的功能扩展，还支持第三方开发基于“阿灵”互惠链的应用，也支持各类应用模块的动态配置（包括对实验性质应用的支持）。

注意一点，目前区块链技术的应用，存在多种实现共识机制的算法或方法。一则是不同的用户认同或偏好不一样，二则是更多、可能更好的算法或方法还不停地产生，所以我们的技术架构中使用了共识机制解析器，来像支持插件一样地支持不同的共识机制在一个系统中共存。

## 技术重点和难点

“阿灵”互惠链项目是立足于实现落地的区块链技术应用去的，在目前全世界都还没有真正落地的好项目的背景下，其难度是可想而知的。再有，我们先瞄准的不管是哪一个具体功能实现，一旦上线成功，都是海量用户级的，对系统的健壮性、可扩展性、可维护性都是极高的挑战。

所以，我们有必要把可能设想到的技术重点和难点提前进行梳理。



## 项目技术重点

### 1. 基于开放式网络的数据访问和操作规范

信息要成为资产，就必须是在整个开放的环境中被准确识别和理解，还包括在授权许可下能够被无歧义地操作。从另一个角度讲，就是必须在开放的环境下消除“信息孤岛”，才能真正释放信息的价值。

“阿灵”互惠链项目必须在资产化信息都经过强加密的情况下，采用 RESTful（Representational State Transfer，简称 REST）规范，统一以 JSON 为基础数据格式，来进行全网络的数据访问和操作，以实现可重用性、简单性、可扩展性和组件可响应性的清晰分离，最大化地展现数据价值，并最终大幅优化全网的数据冗余。

### 2. 全程的透明与开源

区块链技术对最佳“信用”的实现，其实是依赖于公开、透明的原则来达成的。理解了这一点，就要求我们在整个项目中要做到：从数据、数据操作到业务逻辑的执行，从开发架构、开发工具到运行的源代码都要做到公开、透明。

所以，在我们采用的技术架构里就已经全部选用了开源实现的数据库和一系列的开源 SDK 工具；同样的，我们整个项目也将总体采用 MIT 的开源协议进行开源。

不仅如此，为充分地体现公开、透明原则，项目中还会在多个层面和必要的功能中向用户提供开放的数据查询和验证服务，也籍此强化项目“信用”驱动的本质。

另外，借助设计良好的技术架构，在全程的透明和开源条件下，项目还要为各种可能的用户共享提供便利的实现，以达到最大化推动“共享”实现的目标。

### 3. 支持多种共识机制的实现

区块链项目的开发、实现，不能违背去中心化的本质。绝不能像今天的虚拟货币一样，各自搞一套虚拟币的实现方式或标准，希望大众以后都以他的币种为



中心来完成交易，即他们都想干掉了原有世界的货币中心，自己成为未来全球唯一的中心。

果真如此的话，中本聪肯定是非跳出来不可的啦！（^\_^~^\_^）

有鉴于此，更主要的是为了支持信息尽可能无障碍地传输和交互，尽可能地实现信息价值的最大化，我们要通过底层平台实现“共识机制解析器”的方式，将不同的、各家的共识机制作为插件一样地纳入到系统中来，从而打破中心化共识机制的瓶颈。

这样实现的另一大好处是：通过“共识机制解析器”的多插件设置，利用 Node.js 的单线程、异步、非 IO 阻塞特性，就可以突破现存的区块链技术不能满足高性能应用的弊端，为每秒提供数百万次甚至更高频次的交易创造条件。

#### 4. 结合大数据和 AI

“阿灵”互惠链项目，本质上的主营业务是数据处理，而且它一旦能够成功上线，用户累积的数据量是惊人的。并且我们支持“自主信息资产”和公众信息的关联，这样就会更加放大项目的数据量规模。

但是，光有数据量并没有什么价值，项目必须要利用大数据技术，为用户挖掘海量数据形成后的关联关系价值。

在此之上，AI 人工智能才有了用武之地。我们将使用上海拙真信息技术有限公司的另一项基础技术--自主智能（Autonomous Intelligent，简称：Aul），并借助 Google 旗下的 DeepMind 公司开源的 AlphGo 和 AlphGo Zero 的成功技术，为用户的信息资产不断迭代全新的价值。



#### 5. 跨平台和跨终端的用户体验

“阿灵”互惠链项目将为用户提供不同终端的便利工具，这就包括了基于 PC 的应用软件，基于手机、Pad 等的移动 App。这些用户端的应用工具，主流的就涉及 Windows、Linux、Android、macOS、iOS 五种操作系统和众多的不同版本；同时，适合不同系统的开发语言、开发工具以及开发圈子又都完全不一样。虽然有“全栈式开发”的办法可以基本统一在一套开发体系里来完成，但在



移动端，特别是最大用户群的 **Android** 和 **iOS** 端，“全栈式开发”目前还很难为用户提供极佳的操作性能和体验。

这就迫使我们，在开发和发展上选择分步走的路线：

- ① 用户端开发分两步走：全栈式 **Web** + 原生开发；
- ② 优先解决 **Web** 的实现；
- ③ 在 **Web** 实现的基础上，用“全栈式”的工具先为移动端提供先期的应用；
- ④ 在项目发展已经蓬勃之时，再全力开发 **Android** 和 **iOS** 的原生应用。

近期，应该组织力量学习和操练 **Kotlin** 和 **Swift** 这两种新兴的语言和开发工具，未来用它们作为 **Android** 和 **iOS** 移动端开发的主流语言。



## 项目技术难点

### 1. P2P 对等网络的实现

“阿灵”互惠链项目要面对全球的用户实现分布式点对点通信，要传输的数据中还可以包括视频和音频，所有数据在传输中还必需保持密文状态；为达到高性能的要求和好的用户体验，传输的性能和质量都面临极高的要求。

项目主要参考 **BitTorrent** 和 **WebSocket** 的架构和实现方法，研究了现在多家虚拟货币的实施效果，确定以更基本的、得到大多数开发语言和平台支持的 **Socket** 为基础，使用 **Google** 开源的 **WebRTC** 来实现 **P2P** 的对等网络功能。

**WebRTC** 确实集成得很完备，性能也完全满足项目要求，但毕竟是很新的框架，开发文档不多，运用上有一定的难度。另外，**NAT** 的配置和架设需要大量的实际验证、测试和优化，才能覆盖广泛的用户群体。

所以，**P2P** 对等网络的实现是项目的一个技术难点。

### 2. 强加解密的性能和可靠性保证

目前我们可以放心使用的，不惧怕黑客攻破的加解密方案是使用非对称加解密的 **RSA2048**、对称加解密的 **AES112** 以及 **Hash** 散列值的综合方案。

就当前来讲，至少到 **2030** 年前，这个方案是稳定、可靠的。但是，我们的项目要求，任何的传输和存储中都一律使用加密后的密文，那么在大量的实时查



询中，就需要动态地执行对密文的解密计算，所以应用中的性能是一个很大的技术难题。而且，纯算法上是不具备改善条件的，只有在各种具体的功能实现上去找到理想的办法来克服大量的解密性能问题。

再有就是，量子计算离现实可用已经越来越近，所以我们设计的加解密方案还必需是可无缝过渡的。这一点，也加大了加解密方案实现好的性能和可靠性的实现难度。

### 3. 函数式编程和 ES6

其实任何的区块链技术应用项目都是一个庞杂的体系，所以我们才在技术架构和实现方案上进行了大量的统一、区隔和可扩展工作。比如说，统一开发语言为 JavaScript 就是这样。

但是，JavaScript 并不是一种强约束语言，而且它的发展历程和分歧就非常多。这就导致，我们在开发上能够更贴合项目实际的函数式编程在 JavaScript 上就不好掌握，团队在使用中会耗费很多的学习时间，也会产生很多的开发障碍；要不就会牺牲代码的开发时间或稳定性。

同样的原因，还产生了对最新的 JavaScript 标准 ES6 的支持问题上，统一一个标准，许多浏览器和第三方工具不支持；不统一又会导致工作量和可靠性的牺牲。

这些，都是我们在开发过程会面对的技术难题。需要充分重视，妥善解决。

比如，像这样的一些函数柯里化的 ES6 标准的编程方式：

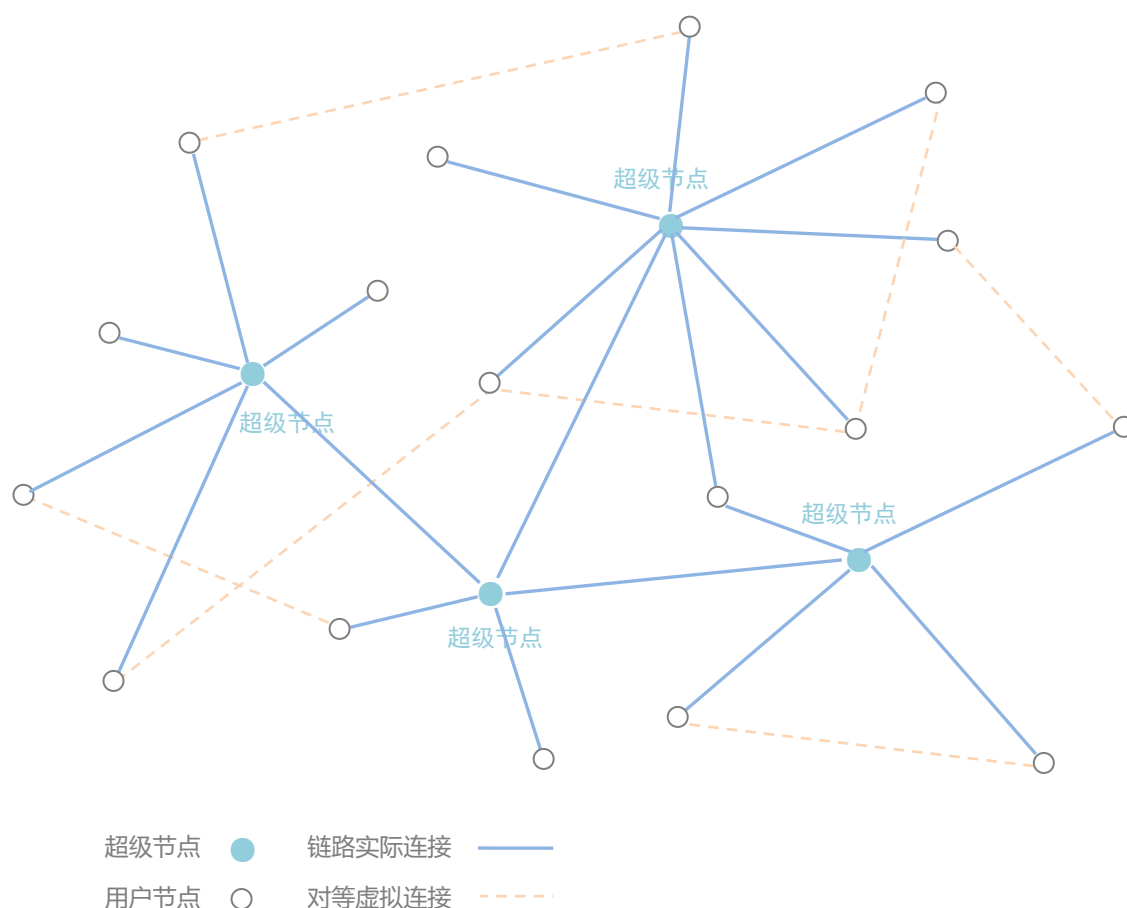
```
var compose = (f, g) => (x => f(g(x)));  
var add1 = x => x + 1;  
var mul5 = x => x * 5;  
compose(mul5, add1)(2); // =>15
```

这样的编程方式非常的简洁、高效，而且运行时可以发挥异步并行的极高性能；同时还具有极好的隔离性，不会导致模块间的交叉感染和错误。可是，转换编程思维的学习曲线就很抖了。

## 项目的组织和实施

“阿灵”互惠链项目完全基于既有的技术和开源基础，又选择采用“共享”模式进行迭代式发展，所以其组织和实施也是有别于大多数传统项目的。

先来看看项目运行形态下的逻辑图：



“阿灵”互惠链项目运行形态逻辑图

我们看到，项目在运营时，实际上是面向大众的混合式对等网络状态，任何用户都可能动态地加入网络，也可能在某一时刻形成一对一的动态连接（红黄色虚线表示）。

那么，我们该怎样组织项目，并保证它很好地实施呢？

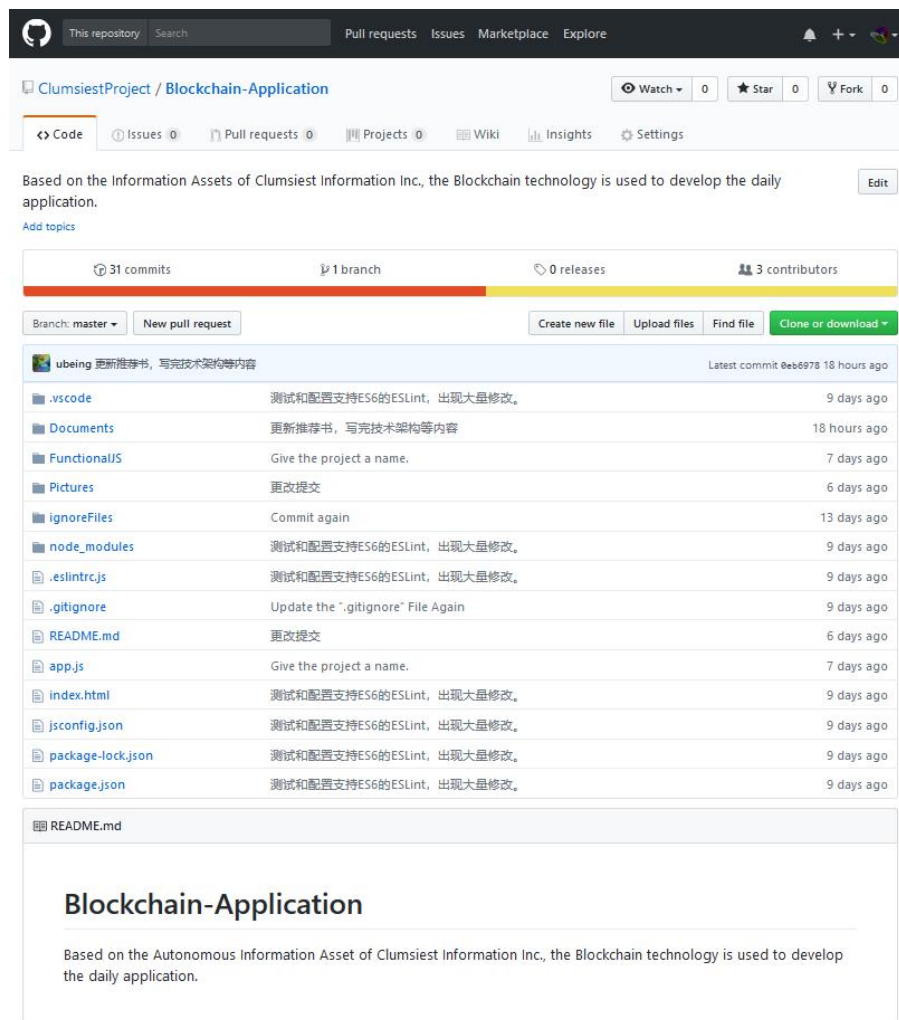
### 1. 先完成项目的大致规划，搭建开发环境

“阿灵”互惠链项目首先需要在大量调研的基础上，完成一个大致的规划。

规划可以粗也可以细，但必须把项目的核心思想说清楚，把项目想达成的目标有一个初步的确定。规划不需要面面俱到，因为我们遵循的是迭代发展的思路，在一个漫长的项目生命期中，将要面对各种各样的变化和可能，面面俱到了反而不能探寻最适合的发展道路。

有必要为项目的未来发展，先搭建开发环境。注意，这个环境一定要想到是开放、开源的；不能再困足于原来中心式的开发模式；为保证项目在开放环境下不受太多的无干扰，可使用类似 SSH 或 HTTPS 这样的一些密钥访问工具进行访问受限的协作处理。

这里，我们可以看看已经使用 Git 和 GitHub 为“阿灵”互惠链项目提供的开发环境仓库：



ClumsiestProject / Blockchain-Application

Watch 0 Star 0 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights Settings

Based on the Information Assets of Clumsiest Information Inc, the Blockchain technology is used to develop the daily application.

31 commits 1 branch 0 releases 3 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

| File              | Commit Message                     | Time         |
|-------------------|------------------------------------|--------------|
| .vscode           | 测试和配置支持ES6的ESLint, 出现大量修改。         | 9 days ago   |
| Documents         | 更新推荐书, 写完技术架构等内容                   | 18 hours ago |
| FunctionalJS      | Give the project a name.           | 7 days ago   |
| Pictures          | 更改提交                               | 6 days ago   |
| ignoreFiles       | Commit again                       | 13 days ago  |
| node_modules      | 测试和配置支持ES6的ESLint, 出现大量修改。         | 9 days ago   |
| .eslintrc.js      | 测试和配置支持ES6的ESLint, 出现大量修改。         | 9 days ago   |
| .gitignore        | Update the ".gitignore" File Again | 9 days ago   |
| README.md         | 更改提交                               | 6 days ago   |
| app.js            | Give the project a name.           | 7 days ago   |
| index.html        | 测试和配置支持ES6的ESLint, 出现大量修改。         | 9 days ago   |
| jsconfig.json     | 测试和配置支持ES6的ESLint, 出现大量修改。         | 9 days ago   |
| package-lock.json | 测试和配置支持ES6的ESLint, 出现大量修改。         | 9 days ago   |
| package.json      | 测试和配置支持ES6的ESLint, 出现大量修改。         | 9 days ago   |

README.md

## Blockchain-Application

Based on the Autonomous Information Asset of Clumsiest Information Inc, the Blockchain technology is used to develop the daily application.

访问网址：<https://github.com/ClumsiestProject/Blockchain-Application>

克隆或下载：<git@github.com:ClumsiestProject/Blockchain-Application.git>

从 Github 的网站上，我们看到“阿灵”互惠链项目已经在迭代中了，有三个 Contributors（投稿者、贡献者）分别已经 Commit（提交）了 31 次，整个项目目前只有一个 Master 分支。

我们后续将组织的开发实施人员或者是其它不知名的人员，都将在这个基础上加入进去，推动项目的发展。

## 2. 进行第一版软件的开发 (Version 0.0.1 -> Version 1.0.0)

接下来我们要做的就是，作为项目的发起人和核心参与者，尽快地提交贡献，让项目早日迭代到第一版（Version 1.0.0）系统。

这期间，应该要投入必要的资源，一方面加快开发进度；另一方面，注册域名、开通网站，创建不少于三个基于公有云的超级节点（Super Node），发动尽可能多的首批试用用户，为 Version 1.0.0 系统的投入运行创造条件。

当然，其它可以做的事情还有很多，但都可以视条件和需求而定。并不成为项目得以发展的先决条件。

## 3. 启动第一代项目的运行

当第 2 步的工作完成以后，项目就可以正式上线运行了。

这期间，项目的核心参与者应该多发动可能的参与者和用户，不断地测试和完善 Version 1.0.0 版的系统。

## 4. 改进项目的各个方面

在前面的基础上，核心参与者应根据运行的效果和反馈，以及可能已经获得的好的 Commits，分多个阶段改进、更新 Version 1.0.0 版系统。

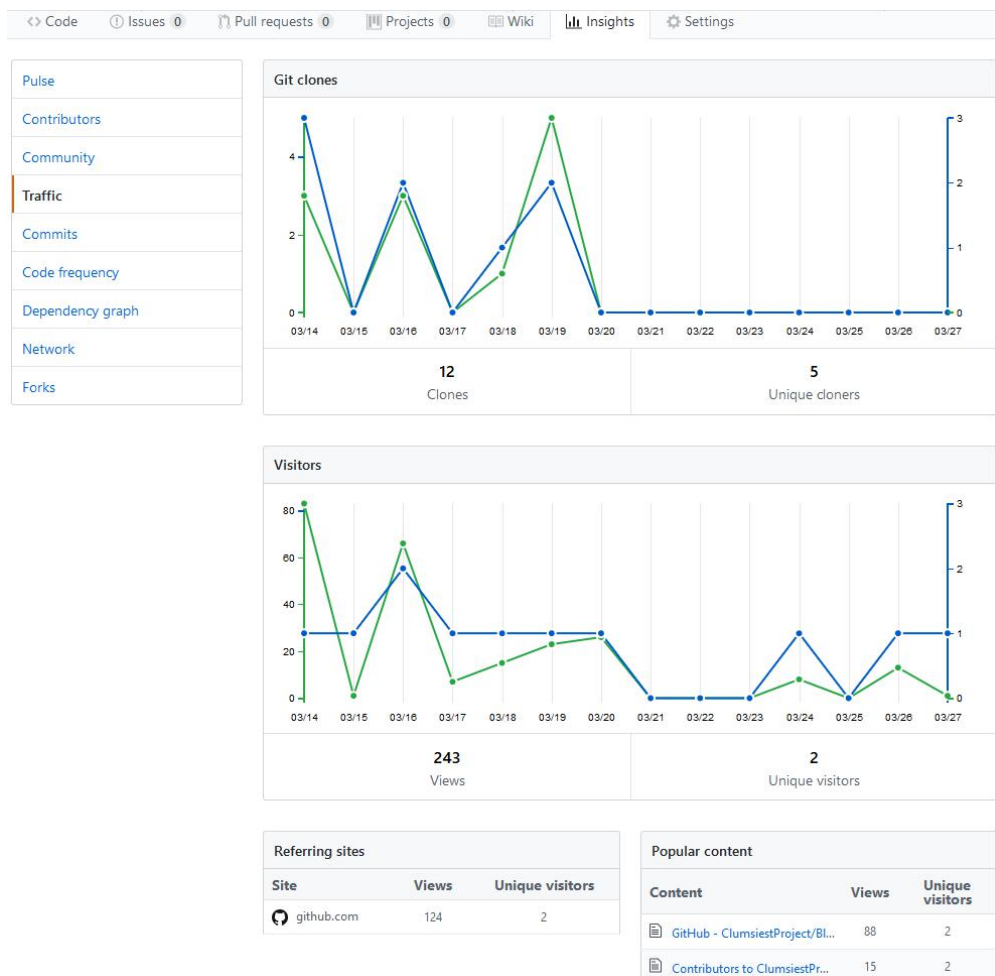
如果有重大发展异常的结果，可以在此期间终止项目的运行。

## 5. 定型重要版本的运行软件

第 4 步如果顺利，则要严格地进行重要版本（比如：Version 2.0.0 版）的定型；并选择合适的时机，将项目更新到新版的系统中运行。（如果需要，应组织好新旧版本的兼容和迁移工作，包括所有用户端的工作。）

## 6. 重复第 3 步到第 5 步

前五步完成之后，项目只要未正式终止，就一直在重复第 3 步到第 5 步的工作，这样一步步地更新和发展下去。



“阿灵”互惠链项目在 Github 上的管理视图

这就是“阿灵”互惠链项目的组织和实施方法。也是完全分布式的，基于不确定性的可能的。

## 项目的关键着手处

前面在定义和分析区块链技术的时候讲到，区块链技术本身是一种基本架构，其价值的产生在于结合了实际应用场景的需求实现。而目前应用这项技术较充分的是在虚拟货币领域，近年虚拟货币领域火爆的一个重要原因是被很多人看好：虚拟货币未来替代法定货币的前景光明。

但是，不管虚拟货币的前景怎么样，其实都不妨碍我们在现有的货币体系下，切实地用好区块链技术解决现实的市场需求，创造市场价值。唯一可能需要注意预留的是：对虚拟货币在任何时候加入到项目功能中去的支持。

还有一点很关键：

对于普通的用户来讲，去中心化再好，对他（她）们来讲都“遥远得很”；社会信用重不重要，再重要也跟他（她）们的关系不大；甚至是个人隐私的问题，按照百度创始人李彦宏在 3 月 26 日回答麦肯锡公司董事长鲍达民的话来说：“中国人对隐私问题的态度更加开放，相对来说也没那么敏感。如果他们可以用隐私换取便利、安全或者效率，在很多情况下他们就愿意这么做。”

这就是我们抱着宝了似的区块链技术，要面对的主要用户群体。

这等于是说，我们的用户是这么想的：“你不用跟我“吹”什么区块链、去中心化，你要有本事，就让我抱着手机就玩你的 xxx 应用，要玩到连打电话功能都删了，都不删你的那个什么 App，我就算服你啦！”

没有一定的用户，或者说如果我们的项目不能发展到最少维持一个合理的在线基数（比如 1,000 人在线），分布式验证、存储的基础就垮了，项目就会最终失败。所以，发起“阿灵”互惠链项目的重中之重是：我们得在项目的基本架构上，至少拿出一个“杀手级”的 App 来，让我们的潜在用户机不离手！

“人工智能”--我们的态度

结束语