# 区块链的落地应用

2018-7-6

田海博

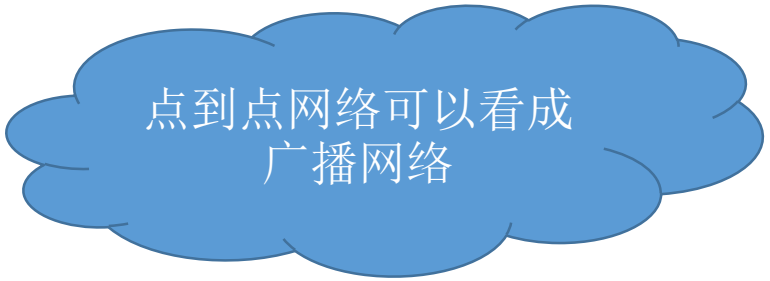
# 比特币的故事

- 2008年一篇论文，论文题目叫“点到点电子现金系统”
- 2009年出代码
- 2012年左右第一次高潮，日本交易所
- 2017年左右第二次高潮，火币，币安等交易所

# 比特币的技术特点

- 1. 需要一个点到点网络，谁都可以入网。
  - （通信能力**去中心**，节点通信能力地位均等）
- 2. 理论上网络中任意用户都可能成为领导，发布内容；网络中任意用户都是监督者，检测领导发布的内容；
  - （业务能力**去中心**，节点的业务能力均等）
- 3. 领导者需要付出代价发布内容，例如每次发布内容需要100RMB电力。领导者发的内容在几乎所有节点都有备份
  - （**不可篡改性**来源于两个方面，数据冗余和挖矿难度）
- 4. 领导者发布的内容自带可执行代码，可以指定所有人
  - （**智能合约**本身就是程序）

- 去中心，不可篡改，自动执行



# 比特币的社会特点

- 现金系统没人用就是数字
- 比特币发展过程中自然吸引了一批早期玩家，这些玩家只是花电费挖比特币，有比特币之后就好像游戏里面挣了金币一样，看着好玩，其实没什么用
- 然后，这些玩家发现比特币不是游戏，没有游戏道具，更加没有用！
- 所以，两个玩家，有一个喜欢做披萨的，有一个喜欢吃披萨的，就用比特币交换了真实物品
- 基本的逻辑是：
- XX比特币在当时的社会生产力之下=YY电力(换算为法币)=ZZ披萨

# 比特币的社会特点

- 比特币->电力->实物 这套逻辑仅在喜欢比特币的社区有效，对于不喜欢比特币的人，这套说辞毫无效果，例如在某个游戏中有XX金币，去菜市场买一个黄瓜，除非卖菜的跟他玩同一个游戏，否则基本没戏
- 所以比特币的社会特点就是**社区**、**粉丝**
- 根子上，目前比特币依旧是粉丝经济。所以搜索量越大，价格越高，关注人越多，价格越高。

- 明星要有吸引力，才不会掉粉；明星行为要检点，受公众监督。
- 粉丝对明星有需求，可以给粉丝精神、物质上的满足

# 比特币的社会特点

- 比特币满足的用户的需求在于：
- 转移资产【洗钱】（随着监管趋严，通过交易所购买比特币，转移资产越来越难；开矿场，自己铸造比特币，同样是转移资产的不二之选）
- 全球购物【丝路，暗网，病毒，黑产】（比特币的全球死忠粉形成了法币兑换比特币的**天然资金池**，比特币可以兑换为任意法币，完成全球购物的快速支付）
- 比特币的设计目标是现金，现金的基本功能就是价值存储和价值交换。通过死忠粉的培养，目前比特币已经具有了价值交换和价值存储的能力，因此实现了其设计目标。

- 倒推比特币出现之前的需求：**全球购物支付不便，资产全球流动慢。**

# 比特币的启示

- 1. 要形成资金池
- 【或者自己成为**资金池**，或者找银行形成资金池，或者找合作伙伴形成资金池】
- 2. 维护粉丝群
- 【需要满足粉丝的**真实需求**，要有用！】
- 3. 要吸引粉丝
- 【发行的积分、令牌、数字货币等粉丝**福利**要能储值，能够通过资金池兑换】

# 以太坊的故事

- 比特币出现之后，激励了一批山寨币的出现，包括莱特币，点点币，名字币等系列的数字货币
  - 【一个大明星出现了，千万个小明星会出现，类似娱乐圈】
- 这些山寨币都跟比特币类似，做个小整容，换个不同的风格，用自己的方式吸引不同的粉丝，打造自己的社区
- 以太坊的创始人觉得自己要搞一个大社区，抢过来所有不同小社区的粉丝。这个大社区是一个平台，可以让任意用户在这个平台中构造任意的山寨币。
- 以太坊创始人深谙明星效应，所以在比特币社区兜售自己的想法，引人关注，从比特币社区引流量。
- 比特币社区有很多人有很多比特币，实在没什么用，突然发现有个人有新的拉群的方法，而且只需要给些比特币就可以进新群，何乐而不为？于是第一个ICO成功了。

# 以太坊的技术特点

- 1. 继承了比特币的特点，去中心，不可篡改，智能合约
- 2. 突破了比特币只记录每个公钥多少钱这种模式
  - 【明确了账户地址的概念，可以记录每个账户多少钱】
  - 【突破了记录的内容，可以在账户地址中记录任意数据】
  - 【突破了账户地址的拥有者模式，除了人，程序也可以拥有账户地址】
- 3. 部分实现了“可信第三方”，条件是这个第三方不需要密钥，例如不能指望这个第三方给你解密
- 例如，可以部分的取代“中介模式”。
  - 任意买卖双方 都可以在这个可信第三方发布需求信息，程序自动完成匹配，公开透明
  - 需求信息的真实性需要“有根”，所以“中介”难以完全避免
  - “中介”升级为“纪检委”。中介行为受监督

# 以太坊的社会特点

- 首先依旧是粉丝经济
- 其次以太坊是平台，可以容纳各行各业的各种需求，而不仅仅是现金的需求
- 从而可以各行各业发币圈粉，而不仅仅是全球购物和资产转移。

# 以太坊的启示

- 倒推以太坊的需求：
  - 发币【成为明星的需求】

- 人人都是淘金者，偏做路旁卖水人！

# 超级账本的故事

- 比特币和以太坊的成功引起了企业家的关注
- 有一个基金会，IBM在该基金会下公布了自己的代码Fabric
- Fabric基本上代表了超级账本，所以两者往往不做区分（尽管超级账本之下有很多其它项目）
- IBM主推Fabric，通过Fabric培训，协助启动Fabric项目赚钱
  - 【回想在云计算时代，IBM主要通过云服务器赚钱】
- Fabric是IBM的利润增长点之一，技术于其不过是个噱头，赚钱才是核心
- IBM要自己赚钱，不发币！
- 比特币是应用，以太坊是平台，Fabric定位自己为联盟（小平台，高端俱乐部）

# Fabric的技术特点

- 不是去中心，而是多中心联盟
- 不可篡改不依赖挖矿，而是单纯依赖数据冗余
- 重点突出智能合约
  - 智能合约是与账本交互的唯一通道
  - 智能合约在多个节点预运行以检查请求的合法性
  - 智能合约运行后的结果，在多个节点确认之后，依次写入账本
- 分开一般客户端和联盟节点
  - 客户端通过与多个联盟节点同时通信修改和访问账本数据
  - 比特币和以太坊的客户端严格意义上是需要跟节点在一起的，否则需要通过“可信的”中间服务器完成中转。

# Fabric的社会特点

- Fabric跟以太坊一样，也是卖水的，以太坊卖水给草根，Fabric卖水给企业
- Fabric出身名门，无需努力便是明星，自带圈粉能力，所以不需要ICO，不需要发币

# Fabric的启示

- Fabric我们自己并做不了，出身太高
- Fabric圈粉的思路可以借鉴，做联盟
- 联盟即生态
- 联盟有目标，赚钱或者公益
- 联盟需要满足联盟成员的利益诉求，最好能够增值保值，带来利润

# 区块链的落地

- 1. 是不是必须？

- 判断一个应用是不是必须用区块链，通常可以采用替换的方法，一个投资人常用的问题是，如果不用区块链，能不能实现？

- 使用区块链做存储的，往往不用也行
- 使用区块链做支付的，有时不用也行
- 使用区块链做合约化自动支付的，通常可以被认可
- 使用区块链做信任的，有时不用也行

- 技术上判断就是，一个应用所描述的需求是不是通过云服务器可以完成？凡是通过云服务器能够完成的，都不是区块链必须应用。

# 区块链的落地

- 2. 是不是有价值？

- 比特币有现金的价值，以太币有升值的价值，联盟链在银行领域也可以加快处理速度

- 每个行业有每个行业的痛点，是不是真痛点，在于解决问题之后能不能带来价值

- 只有外在的价值存在，才有可能分一部分利润到项目本身，否则无法落地

# 区块链的落地

- 行业门槛如何？
- 每个行业都有门槛。游戏行业相对较低。中介行业相对也较低。所以这些行业较容易进入。
- 一些体制内的行业，动一动往往门槛较高

# 接触的一些项目及思考

- 1. 游戏项目
- 游戏项目的生态通常包括游戏开发商，游戏推广商，玩家。其中玩家是向生态注入现金流的，开发商和推广商是提取现金流的。
- 痛点在于：玩家不好伺候，不好挣钱，开发商资金回笼较慢
  - 【各个行业最痛的痛点就是挣钱！】
- 基本思路，搞个公链，发币，让玩家用币可以消费，玩家的游戏道具可以转化为币，道具的生成参数可以上链，让玩家可以判断道具的总量和道具的价值。随着游戏人数的增加，币甚至可以增值。
- 进化的思路：搞个游戏平台，发币，让玩家可以用币在各个平台消费

# 接触的一些项目及思考

- 游戏是真需求吗？
- Steem就是一个游戏平台，有币，可以买卖道具

- 但是没有区块链，道具的总量不可预知，道具的价值没法保证！
  - 【必须，有价值，门槛低】

# 接触的一些项目及思考

- 2. 企业管理和供应链（企业融资需求）
- 这种项目的生态通常包括原材料企业，生产性企业，零售企业，银行。企业形成一个完整的供应链，银行为供应链企业融资。

- 融资需求是企业的真需求
- 不可篡改特性很容易让人联想到可以为银行审计提供新的数据通道。

- 从企业内部管理开始，记录与最终产品相关的信息到联盟链，联盟链的信息进一步可以到公链。
- 记录信息的目的是为了银行审计，顺便可以做一些企业管理，绩效之类工作。

# 接触的一些项目及思考

- 是不是必须？

- 云服务器能否实现？
- 生产性数据记录在云端，相关信息放到公链。银行审计也可以完成！
- 企业绩效性数据可以用币的形式实现，智能合约可以加强自动化，但是私有服务器也可以实现。

- 技术上，区块链提供了一种不同的实现方式，数据在本地，隐私性等方面可能稍好。

# 接触的一些项目及思考

- 3. 房产交易平台
- 生态包括买房人，卖房人，传统中介机构

- 痛点是有的，中介机构不诚实，哄抬物价，去中介对买卖双方有利

- 问题还是存在的，如何保证卖房信息的真实性？

- 区块链是不是必须的？要去中心（中介），对区块链还是有强需求的。

# 接触的一些项目及思考

- 4.大数据项目
- 生态包括数据提供方和使用方
- 痛点在于没有数据，数据提供者处于自身安全考虑，不想把数据提交给数据中心
- 区块链可以让数据在本地，通过智能合约完成数据资产的变现，逻辑是清楚的

# 合同签署协议的思考

- 生态？
- 合同签署人，合同所定义的平台或者渠道商
- 需求？
- 中心化机构具有知晓合同内容的分享，隐私性和公平性是强需求。那么基于云服务器和密码技术能否提供保护隐私的公平合同签署呢？
- 所以为什么用区块链？“去中心”可以让合同签署人获利吗？
  - 零费率？
  - 合同币升值？
  - 自动完成合同部分条款？
  - 是否需要转变思路，把合同币转化为场景方的货币，合同签署作为一个附加功能？

# 讨论