电话会议纪要

2016 年 03 月 29 日

# 详解区块链—颠覆式创新技术

## ——电话会议纪要





**相关研究**

《区块链技术：颠覆式创新—区块链和数字货币系列报告之一：入门指南（上）》

**证券分析师**
谢伟玉 A0230512070007
xiewy@swsresearch.com
王胜 A0230511060001
wangsheng@swsresearch.com
**联系人**
王洋阳
(8621)23297818×7386
wangyy2@swsresearch.com

**会议时间：2015 年 3 月 25 日**

**主讲：**申万宏源策略研究部 王洋阳

**嘉宾：**多年银行银联支付从业经验、上海国际金融研究中心特约研究员、区块链比特币专家陶荣祺先生

**会议纪要整理：**申万宏源策略研究部 王洋阳

**主要内容：**

- **区块链技术开始独立于比特币获得更大产业应用空间。**区块链本质上为去中心化的分布式账本数据库，作为比特币底层技术起初和比特币相伴相生。比特币区块链拥有去中心化分布化、系统无须中心信任、不可篡改和加密安全性的优点。随着比特币区块链的扩容，交易费用开始升高、价格波动性强、容量限制、确认时间变长等缺点开始显露。但例如私有链、联盟链等各种创新部署区块链在信息公开程度和中心控制力度上实现变通，让例如银行、审计事务所、政府等机构的应用变成可能。同时例如以太坊等竞争型开元区块链的出现和崛起，结合智能合约技术，将基于区块链底层协议的智能资产交换执行变成可能，打开例如证券、投票、众筹协议、金融衍生品、公司管理应用、审计等众多应用可能空间。

- **区块链本身为基于底层去中心化的新信用机制，符合经济学原理未来发展可期。**相比中央机构背书的基于信任的运作机制，区块链的出现代表的是一种低成本的信用机制诞生，并慢慢地茁壮成长。由其设计机制保证，区块链运行时间越久，篡改的难度越高。从此纬度看，区块链必然会得到持续关注和推广。

- **关注以太坊、小蚁等基于区块链技术上的智能资产应用开发项目，以及 A 股内数据储存和专业交易软件公司相关动态。**如果某些领域的信用成本很高或者缺乏信任，则区块链存在大量机会。这样的机会包括跨国支付、股权发行、证券交易、公证等等。结合智能合约的植入效应，区块链在物联网和网络安全等方面也存在大量机会。海外产业发展和投资趋势已跨越传统支付领域，向私有股权发行、交易所内证券交易、物联网等领域进军，同时商业发展模式逐渐多元成熟化。其中，区块链 2.0 代表以太坊是否可以发展出不同类型领域智能合约之间兼容并互相交流的 token 标准为关键，若成功建立，则区块链各种互联空间被打开。国内前期投资发展领域偏硬件挖矿，目前也开始呈现出发达国家内产业发展趋势，但仍缺乏大型机构支持，万向集团产业基金投资发展方向值得关注。创业项目小蚁同样值得关注。小蚁口号是做证券市场的 Uber。目前证券市场内大量资金集中在一级市场，二级市场门槛较高，存在政府租值，而小蚁提供的解决方案可将门槛降低，利用其产品技术可以发行数字资产。若交易所愿意流通，其发行数字资产交易可运行。建议密切关注产业内动态。同时，A 股公司方面，建议关注相关数据存储和专业交易软件公司相关发展动态。

感谢实习生黄俊杰为本文整理做出的贡献和帮助

申万宏源研究微信服务号

# 目 录

1.申万宏源策略研究部王洋阳：区块链开始脱离比特币，迎来广大应用发展潜力 ..... 3

2.区块链专家陶荣祺：区块链—基于底层去中心化的新信用机制 ..... 6

3.Q&A ..... 7

# 1.申万宏源策略研究部王洋阳：区块链开始脱离比特币，迎来广大应用发展潜力

区块链近期获得了大量的关注，小川行长公开表示央行要研究区块链技术；2015年区块链成为了美国创投中获得融资最高的板块；26岁少年Vitalik创建的开源区块链平台以太坊，2015年7月上线后市值飙升至10亿美元，成为新晋独角兽；区块链在金融、共享经济、物联网等方面存在很高的应用价值，吸引了高盛、花旗、纳斯达克、德勤、Airbnb等巨头的积极布局。那么区块链是什么？区块链技术有哪些特点？区块链的应用价值和潜力有多大？这们这次电话会议的目的就是向您解释清这四个问题。今天很荣幸能邀请到有着多年银行银联支付工作经验、上海国际金融研究中心特约研究员、区块链比特币专家陶荣祺先生，来和大家一起探讨区块链的发展潜力。

**首先，区块链是什么？**区块链本质上是一个去中心化的分布式账本数据库，是比特币的底层技术，和比特币是相伴相生的关系。区块链本身其实是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。每当有加密交易产生时，网络中有强大运算能力的矿工(Miner)就开始利用算法解密验证交易,创造出新的区块来记录最新的交易。新的区块按照时间顺序线性地被补充到原有的区块链末端,这个帐本就会不停的增长和延长。通过复杂的公共钥匙和私人钥匙的设置，区块链网络将整个金融网络的所有交易的账本实时广播，实时将交易记录分发到每一个客户端中，同时还能保证每个人只能对自己的财产进行修改。当然，账本里也有别人的交易记录，虽然你可以看到数值和对应的交易地址（基本上这是由一段冗长的乱序字母和数字组成），但是如果不借用其他技术手段你也根本无法知道交易者的真实身份。(各位投资者可以拿出手机，通过访问这个网址，blockchain.info来体验一下全球比特币交易平台的运作，对区块链技术获得一个更直观的了解。)

**区块链技术具有哪些优点？**（1）分布式去中心化：区块链中每个节点和矿工都必须遵循同一记账交易规则，而这个规则是基于密码算法而不是信用，同时每笔交易需要网络内其他用户的批准，所以不需要一套第三方中介结构或信任机构背书。在传统的中心化网络中，对一个中心节点（比如说，支付中介第三方）实行有效攻击即可破坏整个系统，而在一个去中心化的，比如说区块链网络中，攻击单独一个节点是无法控制或破坏整个网络的，掌握网内50%的节点只是获得控制权的开始而已。（2）无须信任系统：区块链网络中，通过算法的自我约束，任何恶意欺骗系统的行为都会遭到其他节点的排斥和抑制，因此，区块链系统不依赖中央权威机构支撑和信用背书。传统的信用背书网络系统中，参与人需要对于中央机构足够信任，随着参与网络人数增加，系统的安全性下降。和传统情况相反，区块链网络中，参与人不需要对任何人信任，但随着参与节点增加，系统的安全性反而增加，同时数据内容可以做到完全公开。（3）不可篡改和加密安全性：区块链采取单向哈希算法，同时每个新产生的区

块严格按照时间线形顺序推进，时间的不可逆性导致任何试图入侵篡改区块链内数据信息的行为都很容易被追溯，导致被其他节点的排斥，从而可以限制相关不法行为。

**比特币区块链目前存在哪些缺陷？**比特币在经历了 5 年的发展后，目前市值达到 70 亿美元，接近一个中小型国家的 GDP，比较大的市值提供了较好的流动性保证。但是也暴露了很多问题，例如：（1）价格呈现高波动性，比特币炒作性强，但同时又受制于监管限制，所以风险较大；（2）交易费用升高，虽然比特币交易费用很低，但随着交易变频繁，币值上涨，交易成本也大幅提高；（3）容量限制。比特币区块链设计之初人为地将一个区块容量设置为 1MB，随着交易量加大，容量开始面临限制，处理速度受到影响。（4）确认时间变长，由于容量限制和工作量证明时常挑战运算极限，目前比特币无法处理超过每秒 7 次的交易，无法和类似 Visa 等支付方式在速度这个纬度上进行抗衡。（5）比特币由于隐蔽性强，所以在贩毒、军火交易、支付绑架赎金等方面被广泛应用，同时前段时间人民币贬值期间，比特币也被用作进行外汇转移。所以大部分国家的监管层比较难接受比特币的广泛应用。

**因为比特币区块链存在着以上我刚刚说的那些缺陷，所以现在开始出现了各种形式的区块链创新。创新式区块链技术的出现和成熟，让产业内开始将焦点放至区块链技术其本身。**首先，部署方式区块链出现创新，在比特币这种公共链（所有人都可参与）形式的基础上，目前延伸出了联盟链和私链。这些链在信息公开程度和中心控制力度方面有所限制。（1）联盟链采取多中心式，参与成员是预先根据一定特征所设定的（比如说，各券商的策略分析师）。联盟链容易进行控制权限设定，拥有更高的应用可扩展性，对于产业内（例如各券商）或跨国家同联盟机构的交易、清算、结算、审计等都有很大的应用价值。（2）私有链没有去中心，但具有分布式特点。中心控制者指定可以参与和进行交易验证成员的范围。私有链对于公司政府内部的审计和测试有很大的价值。（3）比特币的缺点开始暴露后，大量的竞争币也开始出现，拓展区块链技术应用范围。例如 Ripple，全球第一个开放的全球银行汇款和支付系统，核心是基于比特币区块链去中心化思想基础之上的 Ripple 支付协议，从而挑战传统的银行间 SWIFT 系统。在 Ripple 系统中，比特币等虚拟货币、以及美元、欧元、人民币等实体货币皆可流通并受到系统支持。Ripple 币为系统提供流动性和安全性。而作为另类区块链中的优秀改进，以太坊近日快速崛起，关键在于它将区块链和智能合约技术实现了良好的结合。智能合约就是在资产内植入一些代码，这些代码可以自动智能决定网络中相关资产运作的地点和方式。以太坊致力于打造一个提供超强图灵完备脚本语言的优秀底层协议。在该协议的基础上，区块链结合智能合约可以打开大面积商用应用空间，用户可以创建任意的高级智能合约、例如：众筹协议、货币、投票、金融衍生品、公司管理应用等。

**接下来，我们探讨一下，区块链的应用价值和潜力有多大？以目前的发展来看，区块链技术在支付、金融交易、物联网等多领域存在广大应用潜力，其中智能合约是关键。**支付方面，传统支付采用“拉式”模式（传统拉式是用户将个人信息提供给第三方，第三方利用这些信息进行支付处理），而区块链技术采用“推式”模式，直

接绕开第三方，大幅改善安全性。同时区块链自动化强降低支付成本并缩短处理时间，去中心化开放特点则有助于平台内创新。智能合约作为区块链延伸核心技术打开区块链各种领域互联智能的应用空间。在金融交易领域，区块链技术可将结算审核时间从小时级降低至秒级，自动化强大幅降低中间成本，结合智能合约将数字证券自动发行和金融衍生品交易变为可能。在审计方面，公司不需要招聘专门审计人员来公司内部审核账本，所有交易可以集中记录储存在内部区块链，由于区块链具有不可逆性和时间邮戳功能，会计事务所等外部审计人员和监管机构通过跟踪这些区块链可以实时监控公司账本，同时机构可以借此大幅减少对于审计员审核金融交易的依赖，将审计业务变得更有效率。对于物联网，智能设备呈现呈数量指数级增长，区块链技术在这些设备之间建立了低成本的互相直接沟通桥梁，同时又通过去中心化的共识机制提高系统的安全私密性。区块链叠加智能合约技术可将智能设备变成可以自我维护调节的独立个体，这些个体可在事先规定或植入的规则合约基础上执行类似和其他个体交换信息或核实身份等功能。

**最后我们讨论一下，区块链产业目前处于怎样的发展阶段？发达国家积极布局区块链，各领域多点开花。**随着比特币的局限性开始显露，区块链技术结合智能合约的应用空间打开、优点开始展现，产业内投资重点已从比特币挖掘硬件转向区块链技术相关应用。目前最高融资区块链公司已超过1亿美元，而且很多初创公司目前正在雄心勃勃进行支付、交易、风控等多领域布局。金融机构例如高盛、花旗、纳斯达克等积极探索区块链在金融领域的应用，同时大力布局金融交易清算相关区块链技术公司，先行者纳斯达克已开始利用区块链技术进行私有股权发行交易；物联网和网络安全相关公司比较容易得到政府和大型机构投资者青睐；支付领域则得到银行和电商的垂青。需要注意的是，四大（德勤和普华永道）在区块链技术在审计领域的应用探索是非常积极的。

**中国相关机构产业内投资力度较小，后期有望突破。**我国过往的产业内相关投资较重视挖矿，以及报价、信息提供业务和咨询，商业模式比较简单。有深入商业模式研究、有一定规模的应用项目是比较匮乏的。目前，行业内开始呈现出向区块链商业应用和深度探索的发展和投资趋势，但体量较小并且缺乏大型金融机构政府支持。万向集团下的区块链实验室是比较少有的有大型机构支撑的研发项目，万向集团旗下还有区块链基金。其中万向集团相关负责人是肖风先生，也就是博时基金的前总经理。随着央行对区块链重视加深、来自国外最新科技进展的溢出效应、海外以太坊作为区块链技术标准的逐渐确认、伴以区块链应用的更加成熟和可投资投标的增加，区块链有望成为“互联网+”后的下一个热捧对象。这将激发创业者和应用者的热情，从而形成我国区块链发展的良性循环。产业内动态值得跟踪关注。

# 2.区块链专家陶荣祺：区块链—基于底层去中心化的新信用机制

**数字货币和区块链的发展带给我们“真实”感。**我在区块链领域从业大概两三年，目睹了类似地球生态中生物进化的过程，从无到有逐步进化。比特币从 2009 年创始到现在也就是 7 年的时间，在这 7 年时间，它一点点地成长了起来。我们把它看作一个从无到有的货币也好、现象也好、状态也好，去观察它都是非常荣幸的。能够观察到一个系统、一个生命体，说得宽泛一点，一种状态是如何从无到有发展起来的，这带给我的冲击是从无到有、完完全全、自下而上的。这样的成长是符合经济学原理的，第一个含义就是往低成本的方向去走；我理解经济学的第二个含义，就是满足人们需要的，比特币和区块链这几年来的成长就是如此。我们现在看到的很多经济社会状态，比如为什么要进行供给侧改革、共享经济，本质上就是因为满足人们需要的成本太高。区块链也能看到这样的趋势，因为它是能够搭建人与人之间信任的一座桥梁。现在人与人之间的信任活动更多地基于国家政府、文化习俗的现行体系。文化习俗的积淀是很深的，没有问题，但国家机器是有缺陷的，这个问题在于经过考验的时间不足，毕竟国家机器仅成立了几十年的时间，可能还不够完善。可以看出，文化习俗、国家机器为我们建立起来的信用体系的成本目前偏高，尤其是国家机器，因为它强制需要很多制度、很多人（可能超过总人口 10%）来维持这个体系。同时，不管是哪一代人，劳务成本是差不多的，所以不管是哪个时代，10%的人来维持体系，其成本必然过高，更何况目前的信用体系还是不够好，比如春节联欢晚会要提出建立诚信社会，本质原因还是社会不够诚信。**一种低成本的信用机制诞生，并慢慢地茁壮成长，即区块链，必然会得到关注和推广。**

**区块链的信任来自于底层技术，即用历史信息换得现行的信任。**现在我们去看财务报表时会想财务报表是否提前被修改过，同时，现在的财务报表是横截面的。而比特币区块链是 10 分钟建立一个区块，并盖好时间戳。从密码学来说，一旦盖好时间戳，这个区块就没有办法破解。从创始到现在，每 10 分钟的时间戳包含这 10 分钟全世界所有的交易信息，这意味着历史交易信息都在你的手里，并且无法篡改。区块链带来的冲击就在于用时间换取人们的信任。类似地，如果政府运行时间越长，并且每次说的都能做到，民众的信任度也会增加。**比特币的特点是，运行时间越久，篡改的难度越高，这是由它的设计机制保证的。**

另外一个维度是区块链的交互。本质上说区块链是一个分布式的公开账簿，再往深层次理解，它实际是一个以太网的智能合约。中本聪在设计比特币的时候就是用智能合约的概念设计的，具体内容可以参考《区块链——新经济蓝图》的第二章。合约的甲乙双方设计一个合约，合约内容描述某个条件或状态，这个条件一旦触发就执行；传统合约的甲方乙方在条件触发时出现问题需要找国家机器、政府机关进行仲裁，这个在智能合约上是可以由区块链来做的。有人说区块链是去中心化脱媒，但实际上并没有完全脱掉，只是从国家机器、政府机关等转移到区块链本身来做。当然，普通程

序也可以设计很多合约出来，但问题在于代码是可以篡改的，因此内容无法得到完全的保证。区块链则把所有内容都公开化，并且运用时间戳的概念使得所有内容不能被篡改，因此智能合约是被强制执行的，从而可以把第三方仲裁、信任机构去掉，由区块链来执行。这实际上是从人的机构变成机器的机构，而机器的成本低于人类，所以符合经济学原理。但是，我们刚才所讲的仍然是信任，并没有做到去信任。本来信任国家机构、政府机关、文化习俗的强制执行，现在转变成区块链、机器，就真的可以相信吗？这里有两个重要问题：第一，机器会取代人类吗；第二，机器会故障吗？这些问题还有待讨论。

现在区块链有个概念叫做公开链、联盟链、私有链。公开链指，区块链的参与者是全世界所有的矿工，如比特币的公开链中，每个币址中有多少比特币完全公开，但币址指向于谁完全不知道，因此比特币是半匿名。银行希望使用区块链但并不想将信息公开的话，就可以使用私有链。这种是受到控制的区块链，可以让区块链中有些信息公开，但有些信息不公开，这个开关可以自己设置。虽然银行希望将区块链放在自己的机房里来维护，但这与普通的数据库有一定区别。因为私有链的存在，几乎所有的金融机构都在研究区块链，特别是银行业基本每家都设有一个部门研究。联盟链是指，区块链信息由多个人录入，而联盟中的对象是可以分享信息的（信息分享程度另论），联盟以外的就无法获得信息，这类似于银联卡组织。区块链解决了囚徒困境中的背叛选项，能够实现强制执行，相比于跨国之间信任度很弱的合作来说是进步的。

# 3.Q&A

**Q1：第一，区块链是颠覆人类组织模式的方式，您觉得这个过程的进展会如何？第二，区块链的展现形式会是怎样的，您刚才提到区块链的强制执行功能是由代码反映出来的吗？第三，矿工会成为区块链技术中比较核心的控制人群吗？第四，比特币是比较普及的应用，但还是有很多其他币种，那么在现实使用中，是不是还是需要国家机器来决定使用哪个币种？**

**A1：**第一，区块链不像 BAT，其实它是协议层的东西，也就是说谁都可以建立一个区块链。所以从协议层来看肯定是颠覆性的，但是在往上看，到底哪些企业能做到巨无霸级别，像以太坊这个链，其实都不好说，毕竟有自己的天花板。当然，我们认为肯定会有这样的公司出现，占据非常重要的地位。

第二，实际上，区块链还是技术层面的东西，只是说这一技术层面的东西还演化出很多变化。

第三，抛开联盟链、私有链，只看公有链。是出现过山寨币的，如狗狗币、莱特币。其实技术上是完全没有门槛的，所以就出现发行一个币种前预挖，等到做出来之后价格持续往下跌的骗局。这里面体现出竞争的态势，所谓的真实也可以从这样的竞争市场中看出，比特币一家独大后，涌现出了很多新的币种，向莱特币这样的成功了，

但大部分失败了。作为一个币，如果背后没有附带真正的人类使用价值的话，在交易所里就只是一个炒作对象，炒完后就被抛弃，成功也仅是极少数，而且很多成功的最终也注定失败。从公有链的角度来说，模仿比特币的新币种已经很难战胜比特币了，但是从区块链和代币的角度来说不一定，比如以太坊的以太币就不能直接与比特币作比较，因为两者的应用场景是不一样的。比特币是一种商品，说大点就是数字货币，但以太币的定位类似石油，是系统中的消耗品。像比特币、瑞波币、以太币这些在未来将会有更多的应用场景，在这种场景里面，这些代币会有炒作的概念，但并不是所有都是炒作的。因此，我们可以将它理解成数字资产。我们现在的资产更多地集中在交易所里面，但未来是可以数字化的，这样的话就无所谓数字货币之间谁赢谁输了，每一个有价值的东西都可以挂上一个 token，这个情况已经有很多实现的案例了，但是许多长尾的资产还没有数字化流通。但是目前还没有做好的是，线上与线下确权的问题。

第四，矿工不会成为区块链的实际控制人，矿工的激励机制是赚快钱，他们赚的是机电费、产业化、规模化节约下的钱。实际上，矿工并不一定专业，他们与比特币的代码没有直接的关系。他们有自己的利益诉求，但与比特币本身的代码没有关系。区块链现在有很多种解决方案，哪一个会成为最终的解决方案其实无所谓，因为每一方都持有很多的比特币，不管是哪一方成功了，其他方也不会做出毁坏比特币网络之类的事情。

**Q2：区块链解决了信用机制的成本问题，但是否需要物联网发达到一定程度，促进智能合约发展，才能解决确权问题，而目前还是没有办法大规模地与物理实体进行连接？**

**A2：**物联网和区块链的应用最早是 IBM 提出来的，代表是 ADEPT 模式，但自己又认为 ADEPT 有很大的问题，主要是没有办法把区块链做得很轻。物联网和区块链合起来的话的确是可以实现物联网机器和机器之间的沟通交换，即用区块链造出 token，然后再进行资源交换，这是顺理成章的事情。目前没有推广主要还是因为现在的区块链太大、太笨重，必须通过厚重的时间维度来保证安全性。而如果做得很轻巧，就丧失了区块链自身的特性；目前国外做出了一个类似区块链但不是区块链的，叫 IOTA token，继承区块链的思路去往物联网靠拢，把区块链历史交易全部抹掉，只保留最近两笔交易。但从它自己的白皮书来看，创始人也不太确信其安全性，毕竟这类似于蒙代尔三角，不可能做到十全十美。IBM 看的是未来，根据摩尔定律来看，等未来设备的数据存量足够大，区块链的信息显得并不厚重时，那么就有应用的可能性。

**Q3：看好区块链的哪些创业方向？区块链处于哪个阶段？**

**A3：**如果某些领域的信用成本很高或者缺乏信任，那就是有机会的，如跨国贸易金融领域，两个国家之间的融资、抵押等等；又如小蚁区块链，我非常看好，它的口号是做证券市场的 Uber。现在的证券市场有个很大的问题，很多资金集中在一级市场，二级市场门槛特别高，始终有个政府租值存在，而小蚁提供一个解决方案，把门槛降得很低，即利用这一套产品就可以发行数字资产，这些数字资产都是可以被交易的，只要有交易所愿意流通它，就可以运行起来。其他的，如医疗的病例分享、审计领域、公证领域、物联网领域（物品的追溯、回溯）、供应链金融、保险（销售成本过高）等等，都有创业的案例出来。

目前区块链处于第一个泡沫阶段，它太热了，但可能还没有处于顶端；国外的资金都是几十亿地往这个领域投，但国内的资金都没有动，因此还没有达到顶端，应该是上升阶段。

**Q4：公有链这块，对于系统效率和厚重程度这一问题，现在有没有好的解决方案技术路径？大多数节点被控制时，防篡改是不是就失效了？**

**A4：**以太坊比较专注于解决这个问题，因为以太坊跑合约而比特币跑交易记录，所以以太坊的区块链增长速度比比特币还要快得多。现在快到第三阶段，等到了第四阶段，POW 会变成 POS，就能大幅减少对空间的依赖，这是以太坊 1.0，到了以太坊 2.0 还会有更多技术出来，如超级立方体等等。这些从理论上来说已经有了几年的讨论，其实一个概念的提出可能会有很多种不同的方案，提出后经过社区严密的认证，在理论上通过了才会进行测试链，如果测试链没有问题了才继续往上走。我在这方面是谨慎乐观，我认为肯定会有一个解决该问题的方案出来，但是这个东西是无法完美解决的，但是至少相比现在会好很多，毕竟公链的潜力并没有完全挖掘出来。

除了 51%攻击之外还有尘埃攻击，51%攻击成本太高，而尘埃攻击成本很低，因此也更危险。确实有安全性问题，目前有过攻击，但是还没有没出现被毁灭的状态。

**Q5：以太坊的盈利模式是怎样的？以太坊的矿工是由公众充当的吗？**

**A5：**以太坊不是公司制制度，而是基金会制度，也就说它是烧钱的。以太坊的基金会如果没有外来资金流入，那么钱烧光就结束了。好在以太坊基金会持有非常多的以太，而且以太最近涨了几十倍，所以现在并不缺钱，以太坊现在的资金足够开发非常多年。

以太坊的 POW 制度与比特币很类似，完全靠价格炒作促进矿工挖矿，所以矿工与应用场景没有关系。这里面有几个纳什均衡，一个就是矿工通过挖矿、卖矿实现其均衡，另一个就是使用方只需要买到以太就可以用，因此投机市场产生价格，左边连接矿工，右边是用户，但是矿工在乎价格，而用户不在乎价格，所以以太坊是双代币

制，以太本身的价格和使用者本身使用来说没有什么关系，以太坊需要把关来维护使用者的使用成本。矿工盈利点在于免费电、规模优势等等。

智能合约的开发方也有自己的盈利模式，如 Augur，自己发行代币 REP，一般收入给持有者，另一半给算力提供方，Augur 自己有持有大量 REP。

**Q6：以太坊是否已经成为发达国家区块链行业的标准？**

**A6：**以太坊刚好推出于银行想要参与区块链的时候，并且以太坊理论上来说是大部分都可以写的。银行需要的功能就可以依靠以太坊写出来，所以就慢慢将以太坊的公开链改为自己的私有链。可以理解成，以太坊是通用型的计算机，但是在某些专有领域上效率偏低，同时它最大的缺陷在于所有的计算都放在其主链上，一旦出现黑天鹅，上面所有的运算全部消失，因此有潜在的安全性问题。因此，未来很有可能是，公链成为一种标准，在公链上进行改动变成私链是解决方案，小蚁以后也可能成为国内数字资产领域的公开链标准。

## 信息披露

### 证券分析师承诺

本报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，以勤勉的职业态度、专业审慎的研究方法，使用合法合规的信息，独立、客观地出具本报告,并对本报告的内容和观点负责。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

### 与公司有关的信息披露

本公司隶属于申万宏源证券有限公司。本公司经中国证券监督管理委员会核准，取得证券投资咨询业务许可，资格证书编号为：ZX0065。本公司关联机构在法律许可情况下可能持有或交易本报告提到的投资标的，还可能为或争取为这些标的提供投资银行服务。本公司在知晓范围内依法合规地履行披露义务。客户可通过 compliance@swsresearch.com 索取有关披露资料或登录 www.swsresearch.com 信息披露栏目查询从业人员资质情况、静默期安排及其他有关的信息披露。


### 机构销售团队联系人

| | | | | |
|---|---|---|---|---|
| 上海 | 陈陶 | 021-23297221 | 18930809221 | chentao@swsresearch.com |
| 北京 | 李丹 | 010-66500610 | 18930809610 | lidan@swsresearch.com |
| 深圳 | 胡洁云 | 021-23297247 | 13916685683 | hujy@swsresearch.com |
| 海外 | 张思然 | 021-23297213 | 13636343555 | zhangsr@swsresearch.com |
| 综合 | 朱芳 | 021-23297233 | 18930809233 | zhufang@swsresearch.com |


## 法律声明