

以去中心化之力、重塑生产关系

区块链行业报告

孔德云
36氪研究院
2018年2月

报告摘要

2017年，比特币投资回报率达181%，全品类数字货币合计回报率更是高达448%。

- 区块链是分布式账本的一种，它既具备了多节点完全冗余的分布式数据库即“去中心化”的特点，又具备了“环环相扣”的特色，最终解决的是价值传输的问题。**而数字货币则是区块链进行价值传输、发挥去中心作用的有力工具。**
- 在以点对点交易为主角的区块链1.0时代，回报率为王，鲜有人关注数字货币的应用价值。从比特币历史价格来看，我们预测，随块产生的比特币第三次减少即2021年时，比特币价格很有可能迎来第三次大幅上涨。此外，比特币交易手续费在经历了2009-2012年不理智的大涨大跌之后，**2018年将是手续费持续稳定攀升的一年，目前已初现端倪。**

区块链的发展可以划分为三个阶段：点对点交易、智能合约和泛区块链应用生态（Token经济）。

- 在区块链1.0时代，数字货币的买入卖出是人们参与区块链最主要的形式，该阶段鲜有人关注数字货币的应用价值，更多地关注点在于数字货币的回报率。该阶段，数字货币交易平台成为最大获利者。
- 在区块链2.0时代，区块链依据可追溯、不可篡改等特性形成了信任基础，为智能合约提供了可信任的执行环境，使得合约实现自动化、智能化成为可能。该阶段，数字身份的构建是重点。
- 在区块链3.0时代，Token是区块链网络上的价值传输载体，其以流通效率为衡量基准，更深一层则是以影响力为衡量基准。该阶段，**Token的生态建设是重点，首先是要有落地场景。**虽然目前“区块链+”热情高涨，但真正适用于做“区块链+”的场景我们认为至少要符合三点：**场景中需要一个账本存在（不局限于记录价值）；有真实性诉求；需要形成大规模共识。**

目录 Contents

一. 区块链行业概述

- 区块链发展历程及简介

二. 基于POW共识的典型交易流程

- 哈希值计算详解
- 全球算力分布情况
- 全球节点分布情况
- 奖励分配
- 不对称加密技术
- 交易手续费未来走势
- 隔离验证
- BTC与BCH的算力之争
- 其他币种信息一览

三. 区块链行业发展三部曲

- 区块链1.0：点对点交易
 - 数字货币与其他品类投资回报情况对比
 - 比特币财富榜
 - 全球主要数字货币交易平台一览
- 区块链2.0：智能合约
 - 智能合约概述
 - 数字身份概述
- 区块链3.0：Token经济
 - 全球及中国区块链项目分布情况
 - 全球区块链项目全景图
 - 典型跨境支付项目介绍—Circle
 - 典型物联网项目介绍——Filament

四. 区块链行业未来展望

- 未来展望

CHAPTER I

区块链行业概述

- 区块链发展历程及简介

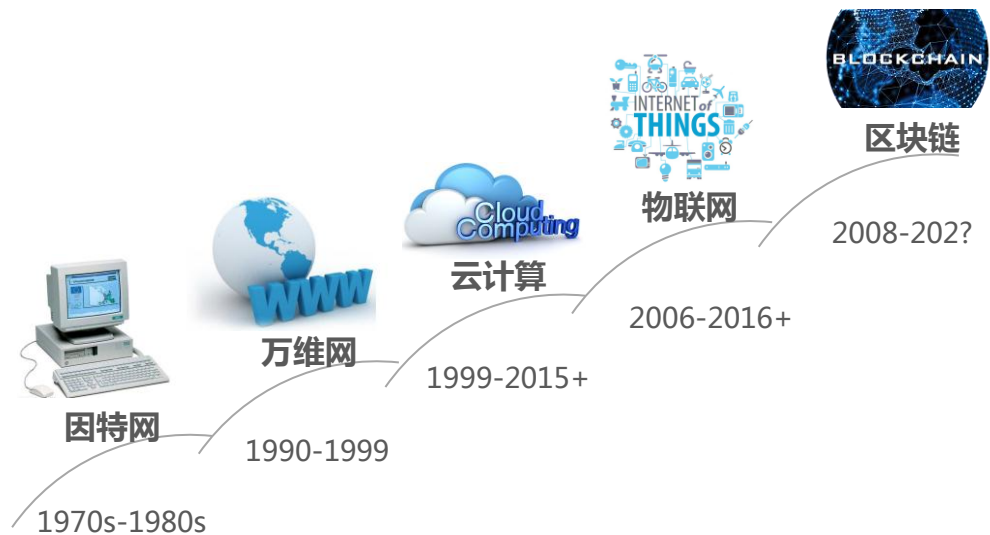
1. 区块链行业概述

1.1 区块链发展历程及简介

区块链行业概述

区块链是对过往技术的重新组合，是现阶段信息科技创新的高潮

- 从信息科技创新的角度来看，20世纪70、80年代第一次萌生了因特网，即我们当前网络架构的“第一层”；1990年开始，Tim Berners-Lee等人推动了万维网的发展，使得信息的传输和共享成为可能；1999年，Salesforce.com的形成标志着信息科技创新已进入第三阶段即云计算时代；21世纪开始，随着智能设备的普及和带宽成本的降低，我们开始体验到“物联网”的便捷；2008年，中本聪第一次提出了区块链的概念，其在密码学、分布式存储等技术的基础上，即将创造第五次信息科技创新的高潮。



来源：MIT connection science

- 谈到区块链，我们先解释一下数据库的类别。当前，数据库主要以三种形式呈现：中心式、分散式和分布式。在中心式体系中，所有数据都统一存储在一台计算机上，管理方便但易遭到破坏且信息透明度较低，类似传统的IDC机房。

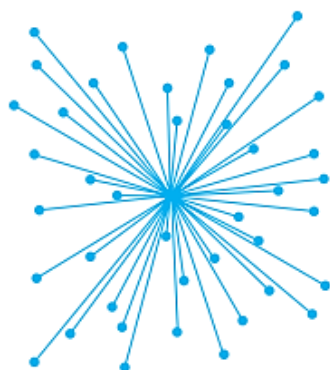
1. 区块链行业概述

1.1 区块链发展历程及简介

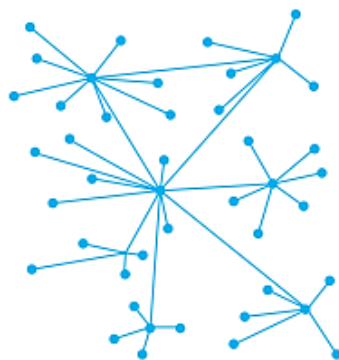
区块链行业概述

作为分布式账本的一种，区块链兼具去中心化和环环相扣的特点

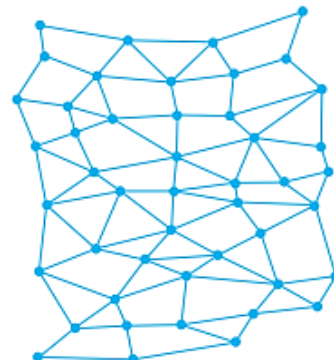
- 分散式体系中，没有中央存储，存在多个“小中心”服务器向用户提供服务，具备较强的可扩展性，类似云计算时代的CDN；分布式体系中，每个节点都存储同一份数据，并且实时更新，其特点是所有节点都拥有平等的权利，且节点越多，整个分布式系统安全性越高。



中心式



分散式



分布式

- 区块链是分布式账本的一种，它既具备了多节点完全冗余的分布式数据库即“去中心化”的特点，又具备了“环环相扣”即“最长链共识”的特色，最终解决的是价值传输的问题（“最长链共识”即长链覆盖短链，每个新区块优先以最长的链尾作为新区块头部，因此区块链得以从最长端不断延续）。

数据库

分布式
数据库

区块链

CHAPTER II

基于POW共识的典型交易流程

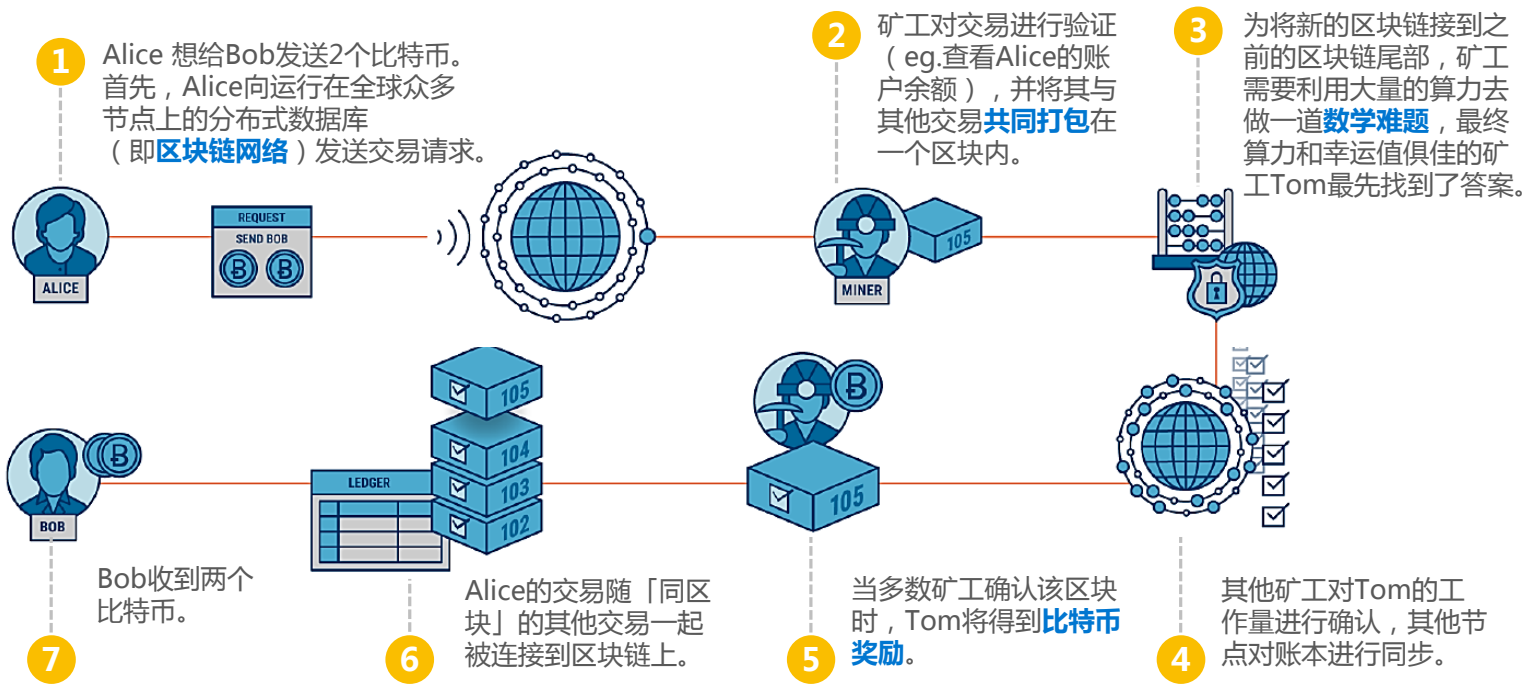
- 哈希值计算详解
- 全球算力分布情况
- 全球节点分布情况
- 奖励分配
- 不对称加密技术
- 交易手续费未来走势
- 隔离验证
- BTC与BCH的算力之争
- 其他币种信息一览

2. 基于POW共识的典型交易流程

基于POW共识的典型交易流程

交易流程包括：交易请求、交易打包、哈希值计算等七个步骤

以比特币为代表的数字货币是目前基于区块链技术最成功的应用，区块链技术也得益于比特币得到了更深层次的拓展。以Alice向Bob发送比特币为例，基于POW共识的典型交易流程大致如下：



来自CBInsights；36氪研究院

- 第一步：Alice向区块链网络广播交易请求；
- 第二步：矿工通过查看Alice的账户余额等易进行真实性验证，并将这笔交易同其他**未确认交易**一同打包，形成一个区块，进行集体确认。

36588笔未确认交易



总手续费 721.58184331 BTC
总容量 613253.837 KB

图示：比特币交易情况实时图

时间截至2018.1.30 pm 14:13；数据来源：Blockchain，36氪研究院

2. 基于POW共识的典型交易流程

2.1 哈希值计算详解

2.2 全球算力分布情况

2.3 全球节点分布情况

2.4 奖励分配



3

第三步

基于POW共识的典型交易流程

哈希算法的本身特性使得区块链的「环环相扣」成为可能

- 第三步：矿工利用大量算力，通过解公式：

$$h_N = \text{Hash}(A \parallel h_{N-1} \parallel \text{Nonce})$$
 找到所要的哈希值 h_N 。其中， h_{N-1} 为父哈希值即上一次最新产生的区块（以下简称「次最新」区块）的哈希值， h_N 为本次区块的哈希值。每一个最新区块之所以能链接到「次最新」区块而非其他区块，主要原因就是每一个「次最新」区块的哈希值也就是父哈希 h_{N-1} 都是求得最新区块哈希值的 h_N 的必要已知条件，这就是“最长链共识”。对于矿工来说，当最新的哈希值被其他矿工播报并确认后，就没有必要再纠结于此区块，而是尽快以此区块产生的最新哈希值 h_N 作为已知条件，求取下一个区块哈希值 h_{N+1} 。

块高度：507751

块哈希：00000000000000000004...f1

父哈希：00000000000000000004...31

时间戳：2018-02-05 17:07:00

难度：61.96 T / 2.60 T

目标值(The Target)：0x176c2146

随机数(The Nonce)：0xd892fbba

Merkle Root：47b03...241

区块主体：此区块中所有交易信息

块高度：507752

块哈希：00000000000000000005...66

父哈希：00000000000000000004...f1

时间戳：2018-02-05 17:18:04

难度：3.49 T / 2.60 T

目标值(The Target)：0x176c2146

随机数(The Nonce)：0x0b09df45

Merkle Root：eaf53...804

区块主体：此区块中所有交易信息

块高度：507753

块哈希：00000000000000000003...c3

父哈希：00000000000000000005...66

时间戳：2018-02-05 17:19:34

难度：5.84 T / 2.60 T

目标值(The Target)：0x176c2146

随机数(The Nonce)：0x1b3be024

Merkle Root：c3556...efd

区块主体：此区块中所有交易信息

数据来源：btc.com

- 从上表中，块高度507751的块哈希值是块高度507752的父哈希值。此外，时间戳即每块产生的实时时间，产生速度基本可维持在10分钟左右（上下浮动在10分钟内）。

2. 基于POW共识的典型交易流程

2.1 哈希值计算详解

2.2 全球算力分布情况

2.3 全球节点分布情况

2.4 奖励分配

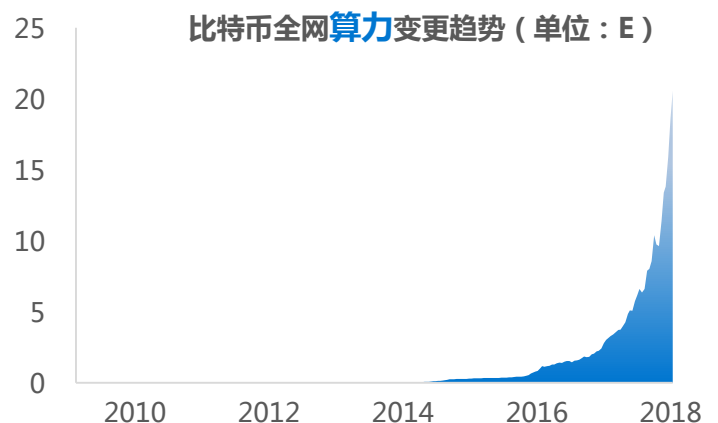
基于POW共识的典型交易流程

算力构成了基于POW共识交易网络的安全基石

- 难度值将随全网算力变化而不断优化，每出2016块进行一次难度调整（以10分钟每块为基准，若块产生速度过快，则难度提升；反之，则难度下调）。区块链协议规定，使用一个常量除以难度值，可得到目标值(The Target)。显然，难度越大，目标值就越小，则找到该值的概率越低（目标值是该区块哈希值的最大值，可用哈希值 \leq 目标值即可）。
- 整体来说，公式 $h_N = \text{Hash}(A \parallel h_{N-1} \parallel \text{Nonce})$ 中，A、 h_{N-1} 为已知值，通过不断的尝试随机数Nonce，使得 h_N 小于目标值(The Target)，即可得到该区块可用的哈希值 h_N 。
- 从全网比特币区块挖掘难度和算力变更趋势来看，两者呈正相关关系。矿机芯片也逐步由CPU/GPU，更迭到如今挖矿专用的ASIC芯片。**全网算力伴随挖矿难度的提升而不断提升的过程中，虽会造成算力资源的“浪费”，但算力整理也构成了基于POW共识交易网络的安全屏障。**



数据来源：BTC.com；36氪研究院



数据来源：BTC.com；36氪研究院

2. 基于POW共识的典型交易流程

2.1 哈希值计算详解

2.2 全球算力分布情况

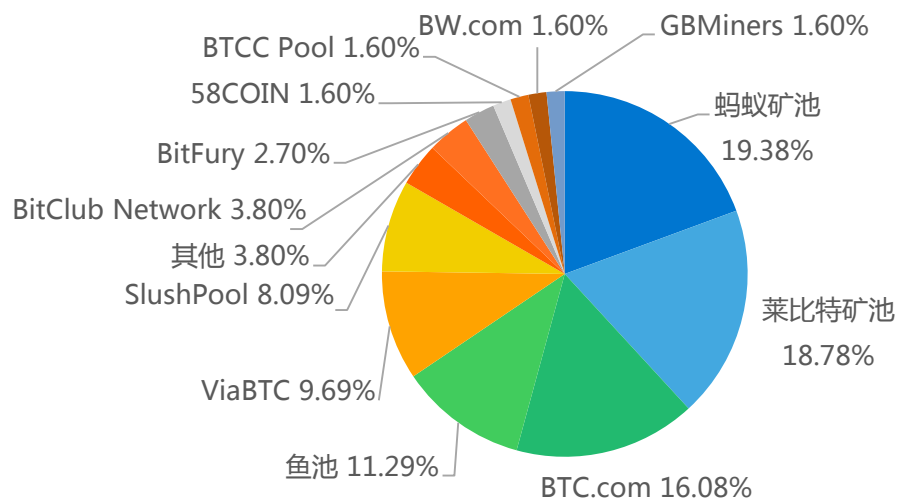
2.3 全球节点分布情况

2.4 奖励分配

基于POW共识的典型交易流程

我国矿池占据全网75%算力，成为算力领域第一大强国

- 通常情况下，算力越大的矿池最先得到可用哈希值的概率也越大。在「强者通吃」机制下，各大矿池算力争夺激烈、竞争白热化。作为一个重资产的环节，挖矿领域已不再为新进入者提供更多发展空间。目前，更多的选择是通过购买云算力来参与到挖矿环节中。
- 当前，全球排名前五的矿池：蚂蚁矿池、莱比特矿池、BTC.com、鱼池、ViaBTC都是中国矿池，中国矿池已占据全网75%以上的算力。世界上首台挖矿专用芯片—ASIC由我国芯片企业—阿瓦隆于2012年研发、制造，目前已更迭到第四代。



图示：全球矿池算力份额分布

数据来源：Blockchain.info
数据截至2017.12.13

2. 基于POW共识的典型交易流程

- 2.1 哈希值计算详解
- 2.2 全球算力分布情况
- 2.3 全球节点分布情况
- 2.4 奖励分配



基于POW共识的典型交易流程

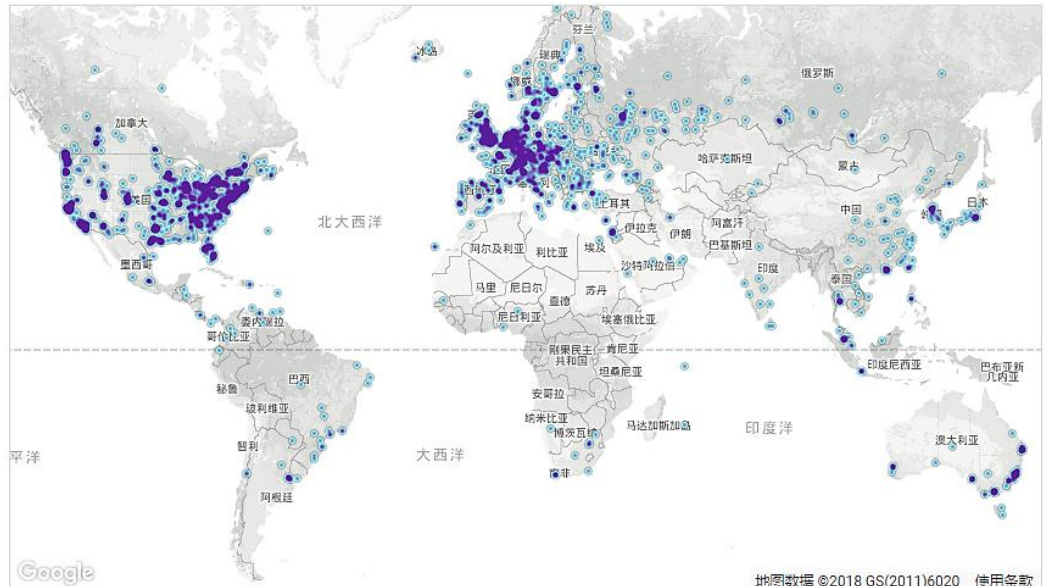
我国节点数占全网7.03%，处全球第三，发展迅速

- 第四步：基于POW (Proof of Work) 即工作量证明共识机制，其他矿工对第一个计算出可用哈希值的矿工工作量进行确认。工作量证明是所有需要挖矿的币种通用的共识机制，其要求出示一定的证明来表明工作量，对于由小概率事件累计的工作来说，出示结果就等同于证明了工作量。以比特币网络为例，当一个矿工找到合适的哈希值时，其他所有矿工就默认其付出了算力成本。
 - 同一时间，其他节点会对账本进行同步。此步骤的动力来自于新的区块在某一节点产生之后，其他节点同步越快，就能越快地开展下一个区块的挖掘。
- 截至2018.1.30，全球比特币网络节点已达11783个，中国828个，占比7.03%，处全球第三。**
- (注：2016年时，未排进前十)**

共11783节点

节点数分国家TOP10

排名	国家	节点
1	美国	3259 (27.66%)
2	德国	2027 (17.20%)
3	中国	828 (7.03%)
4	法国	780 (6.62%)
5	荷兰	537 (4.56%)
6	加拿大	473 (4.01%)
7	英国	424 (3.60%)
8	俄罗斯	350 (2.97%)
9	N/A	300 (2.55%)
10	新加坡	262 (2.22%)



图示：全球比特币节点分布

2. 基于POW共识的典型交易流程

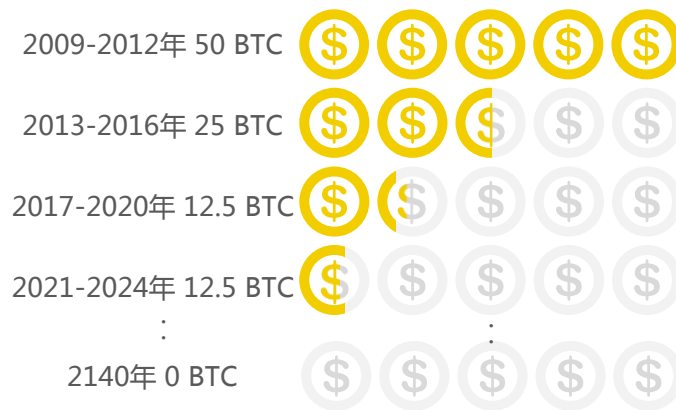
- 2.1 哈希值计算详解
- 2.2 全球算力分布情况
- 2.3 全球节点分布情况
- 2.4 奖励分配



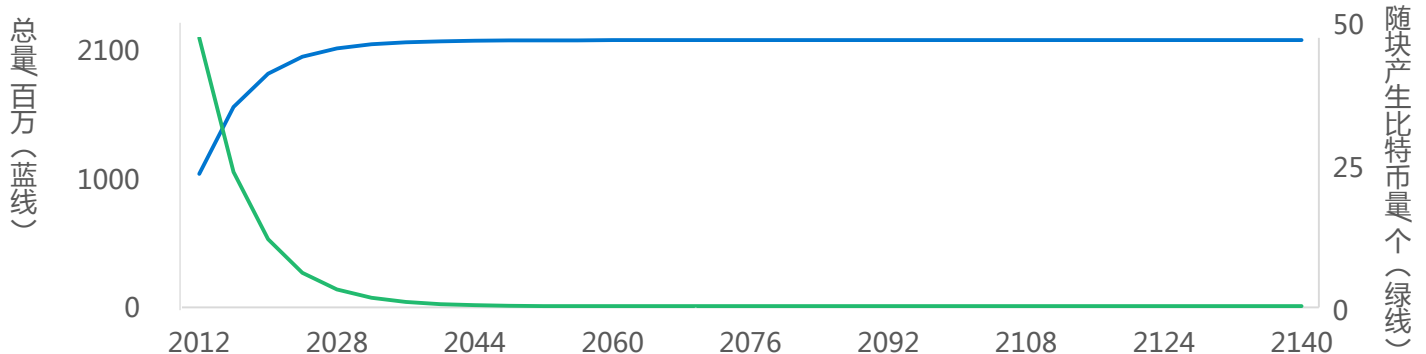
基于POW共识的典型交易流程

比特币总量增速放缓，随区块产生的比特币奖励逐步降低为零

- 第五步：当其他多个节点确认该区块时，最先找到该区块可用哈希值的矿工将得到比特币奖励。通常情况下，我们认为经过6个节点的确认即可验证比特币交易的真实性。该奖励主要包括两部分：**随区块产生的比特币+该区块包含交易的所有手续费。**
- 随区块产生的比特币以每四年减半的机制增加：2009年第一个创始块出现时，随块产生了50个比特币；2013年每个区块产生25个比特币；2017年阶段也就是当前，每个区块只产生12.5个比特币；依此类推，到2140年时，随区块产生的比特币将降为0个，总量达到约2100万个，不再增加。



比特币总量增速放缓



来源：36氪研究院 — 比特币总量/百万个 — 随块产生比特币量/个

2. 基于POW共识的典型交易流程

- 2.1 哈希值计算详解
- 2.2 全球算力分布情况
- 2.3 全球节点分布情况
- 2.4 奖励分配

基于POW共识的典型交易流程

2021年，比特币价格或将迎来第三次大幅上涨

- 从比特币历史价格来看，能够发现在2013年年末以及2017年年末，比特币与美元汇率都处于井喷式增长阶段，而2013年和2017年又都恰巧是随块产生的比特币减半的关键节点。据此，我们预测，随块产生的比特币第三次减少即2021年时，比特币价值很有可能迎来第三次大幅上涨。



数据来源：BTC.com；36氪研究院

- 除随区块产生的比特币外，矿工还会额外得到该区块所包含交易的所有手续费。由于比特币区块大小被限制1M以内，因此打包过程中通常按照手续费高低对交易进行排序，以确保能在有限的区块容量内尽可能包含多的手续费，故支付手续费更高的交易能得到更快速的确认。在交易拥堵时，为使交易被尽快确认，手续费曾高达到0.007BTC/KB*。

高度	包含交易数量	大小 (B)	块收益 (BTC)	时间
508,051	1,847	1,128,708	12.5+1.1794	2018.2.7 11:17:43
508,041	1,206	1,050,650	12.5+0.7126	2018.2.7 09:13:05
508,040	302	1,003,854	12.5+0.0638	2018.2.7 09:03:13

注：蓝字12.5为块收益中随区块自然产生的BTC；绿字为该区块中所包含交易的所有手续费

*本页数据均来自于BTC.com

2. 基于POW共识的典型交易流程

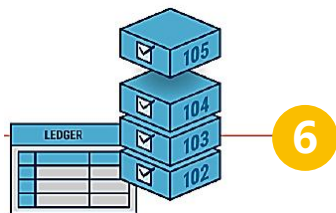
2.5 不对称加密技术

2.6 交易手续费未来走势

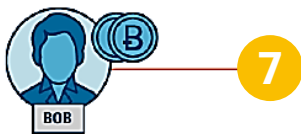
2.7 隔离验证

2.8 BTC与BCH的算力之争

2.9 其他币种信息一览



第六步

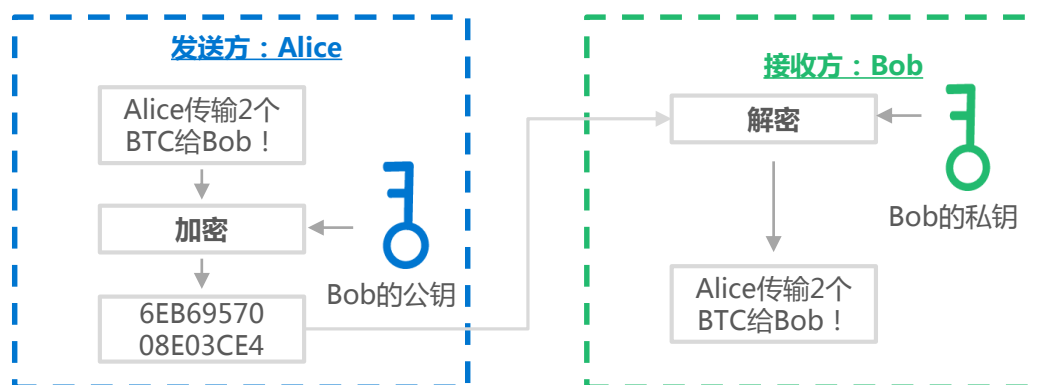


第七步

基于POW共识的典型交易流程

不对称加密技术保障了价值传输过程的安全性

- 第六步，Alice的交易随「同区块」的其他交易一起被连接到区块链上；
- 第七步，Bob收到两个比特币。其中，在第七步中涉及到了区块链交易过程中一个很重要的密码学技术——不对称加密技术。
- 在价值传输过程中，发送人Alice首先利用接收人Bob的公钥对数据进行加密，加密之后，只有Bob的私钥才能对其进行解密，大大提高了传输过程中的安全性。Bob接收到数据（比特币）后，利用私钥对数据解密，即可验证发送人身份信息。简单地说，公钥相当于Bob的银行卡账号，是公开的，而私钥相当于Bob的取款密码，而且可以验证数据发送人。



*数据来源：CoinMarketCap；36氪研究院

- 经过以上七个步骤，即完成了一次基于POW共识机制的价值传输过程。

2. 基于POW共识的典型交易流程

2.5 不对称加密技术

2.6 交易手续费未来走势

2.7 隔离验证

2.8 BTC与BCH的算力之争

2.9 其他币种信息一览

基于POW共识的典型交易流程

比特币区块容量已达上限，手续费将一路走高

- 对于交易手续费而言，我们认为，**其与实时交易并发量成正比、与区块容量增速成反比**（区块容量最大可增加到1MB）。
- 首先，从比特币交易量逐年走势来看，比特币整体交易量呈快速增加态势（2017.9.4，中国境内全面禁止数字货币交易后，比特币交易量曾出现断崖式下跌，随即迅速反弹）；从区块大小趋势来看，进入2017年后，新生的区块容量已基本达到了最大值，在当前比特币网络规则下，已无更多增长空间。

比特币**交易量**逐年走势（单位：KB）



时间截至2018.2.4；数据来源：Bitcoin.com；36氪研究院

比特币逐月**区块大小**中位数（单位：K）



截止日期：2018.1；数据来源：BTC.com；36氪研究院

2. 基于POW共识的典型交易流程

2.5 不对称加密技术

2.6 交易手续费未来走势

2.7 隔离验证

2.8 BTC与BCH的算力之争

2.9 其他币种信息一览

基于POW共识的典型交易流程

比特币区块容量已达上限，手续费将一路走高

- 基于比特币交易仍处于快速增长阶段，而区块容量已达到峰值的现状，我们判断比特币交易网络堵塞现象将逐步加剧，而交易手续费在经历了2009-2012年不理智的大涨大跌之后，**2018年将是手续费持续稳定攀升的一年，目前已初现端倪。**



- 隔离验证 (segregated witness) 技术或许是以上问题的最佳解决方案。隔离验证是对现有区块优化的一种方式，其最早提出是为了解决比特币交易的延展性问题，即其他节点对该区块见证签名进行真实性确认时留下的一系列长尾数据信息。签名过程会改变哈希交易ID(TxID)，造成的直接后果是两张具有不同TxID的汇款单同时都有效。2014年2月份，比特币交易网站Mt.Gox宣布破产——85万个比特币被盗，此事件与多重签名验证机制强相关。(接下一页)

2. 基于POW共识的典型交易流程

2.5 不对称加密技术

2.6 交易手续费未来走势

2.7 隔离验证

2.8 BTC与BCH的算力之争

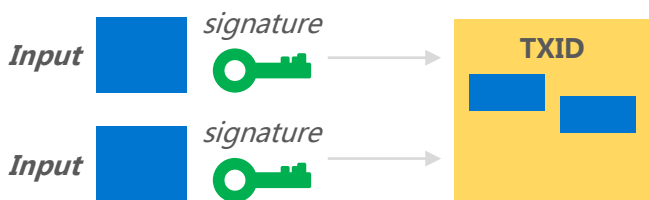
2.9 其他币种信息一览

基于POW共识的典型交易流程

隔离验证技术可暂解燃眉之急

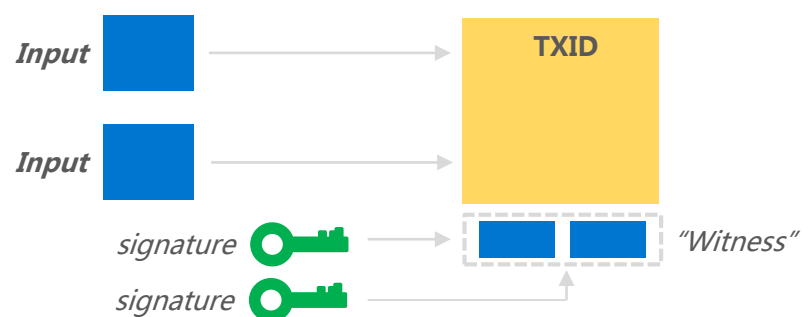
- 具体来讲，比特币交易主要是由两部分的数据构成：“基础交易数据”（主要负责记录交易比特币的来源和去处）；“见证数据”即真实性确认过程中留下的签名信息(Witness)。隔离验证是将见证数据与基础交易信息相隔离，进行单独验证。此后，只有发出交易的一方才可改变交易ID，这样可以保证一连串未确认交易的有效性，避免双重支付现象，同时也是未来发展双向支付通道或闪电网络的必要功能。
- 而隔离验证在解决以上扩展性问题的同时，带来的附加值是将见证数据隔离后，区块在计算容量时不将其计算在内，交易信息得到了很大程度的“瘦身”，1MB的区块空间便可容纳更多的交易。

当前状态



来源：Hackernoon

隔离验证



- 但目前，对比特币网络的隔离验证还未得到大多数算力的认可。而在2017年8月，比特币硬分叉产生了BCH（比特币现金），BCH虽未实现隔离验证，但其通过线上扩容，区块最大可支持8MB。一定程度上，BCH的出现暂时缓解了比特币的手续费压力。

2. 基于POW共识的典型交易流程

2.5 不对称加密技术

2.6 交易手续费未来走势

2.7 隔离验证

2.8 BTC与BCH的算力之争

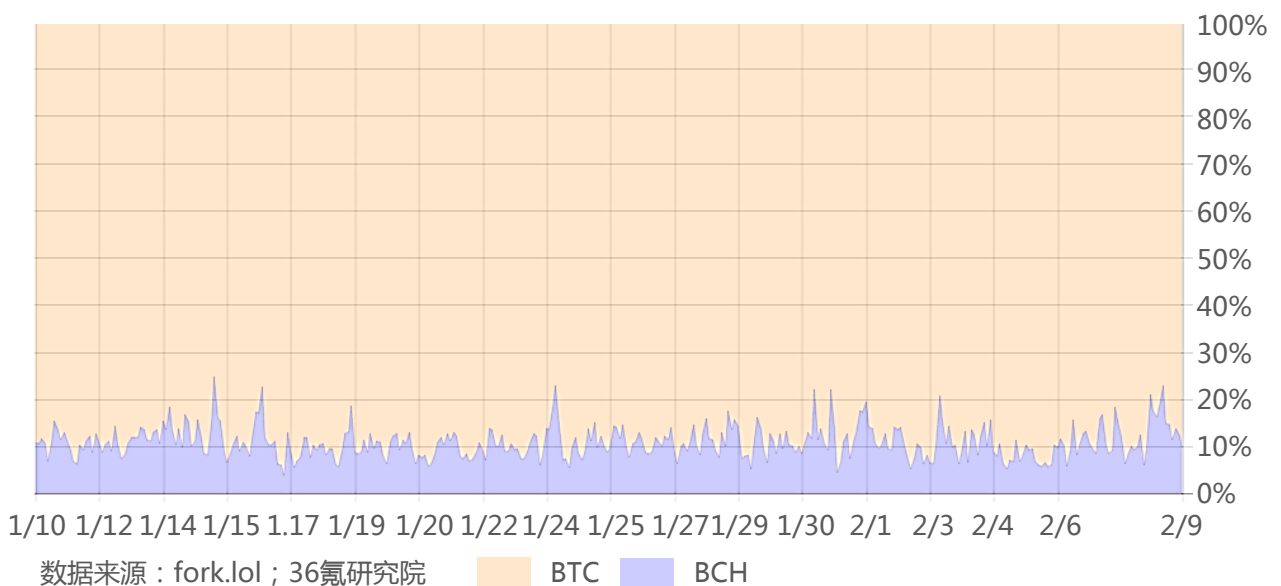
2.9 其他币种信息一览

基于POW共识的典型交易流程

未来，BCH或将得到更多的算力支持

- 上述缓解比特币手续费压力的原因主要是由于BTC与BCH共用全网算力，存在一定的竞争关系。在2018年比特币区块容量已基本饱和的态势下，比特币区块扩容之争将进一步被激化，若应用于比特币网络的隔离验证仍迟迟得不到多数算力的认可，那么**BCH很有可能在未来争取到更多的算力，价格大涨，甚至成为新一代的“比特币”。**

BTC Vs. BCH算力占比 (2018.1.10-2.9)



- 截至2018.2.10，全球公开发行交易的币种有889个，总市值逾3890亿美元*。其中市值TOP10的数字货币分别是比特币、以太币、瑞波币、比特币现金、小蚁币、恒星币、莱特币、新经币和IOTA。除比特币、比特币现金外，其他币种大多以场景应用概念脱颖而出，例如瑞波币主打跨境支付场景；IOTA主打物联网节点间小额支付场景。

*数据来源：CoinMarketCap

2. 基于POW共识的典型交易流程

2.7 隔离验证

2.8 BTC与BCH的算力之争

2.9 其他币种信息一览

基于POW共识的典型交易流程

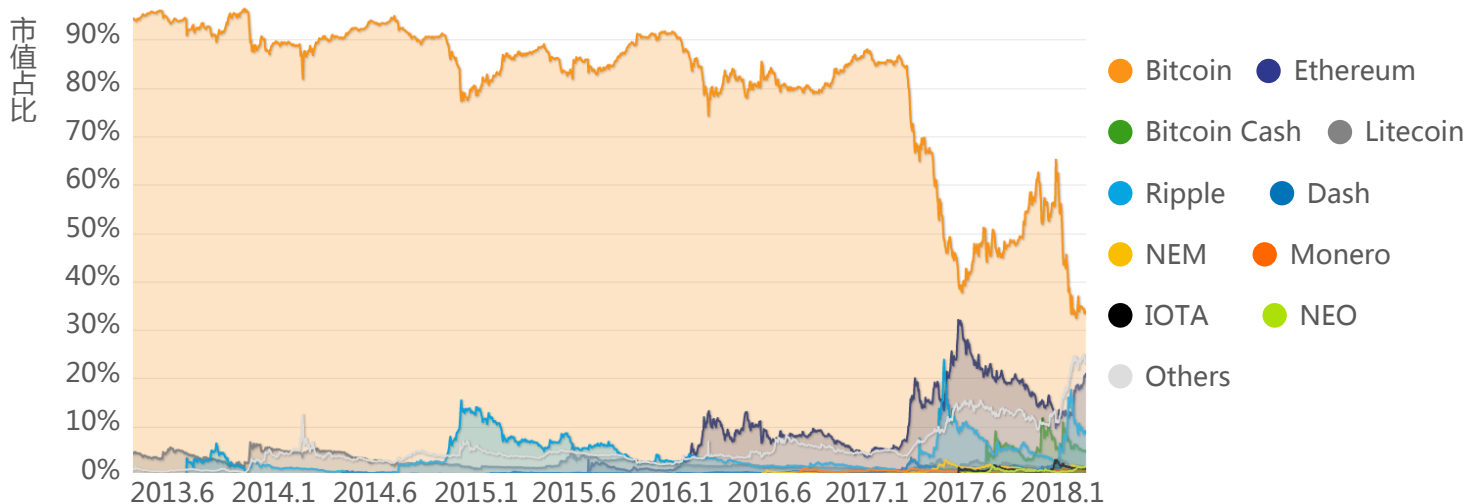
其他主要币种信息一览

排名	币种	市值	流通总量
1	Bitcoin	\$172,106,553,735	16,836,712 BTC
2	Ethereum	\$106,327,973,546	97,320,031 ETH
3	Ripple	\$43,958,854,913	38,739,142,811 XRP
4	Bitcoin Cash	\$25,336,334,554	16,941,375 BCH
5	Cardano	\$13,278,263,978	25,927,070,538 ADA
6	NEO	\$9,363,900,000	65,000,000 NEO
7	Stellar	\$9,322,564,332	17,868,698,000 XLM
8	Litecoin	\$9,041,801,627	55,002,808 LTC
9	NEM	\$6,852,338,999	8,999,999,999 XEM
10	IOTA	\$6,383,469,248	2,779,530,283 MIOTA

图示：全球数字货币之市值TOP10

数据截至 2018.1.31, AM 8:56 UTC ; 数据来源：CryptoCurrency Market Capitalizations

主要币种市值占比 (2013.4.28-2018.1.31)



注：数字货币总市值：\$447,744,763,526；

数据来源：CryptoCurrency Market Capitalizations

2. 基于POW共识的典型交易流程

2.7 隔离验证

2.8 BTC与BCH的算力之争

2.9 其他币种信息一览

基于POW共识的典型交易流程

其他主要币种信息一览

- 目前，应用于数字货币的共识机制除了POW，还存在于POS (Proof of Stake)、 DPOS (Delegated Proof of Stake)、 PoI (Proof of Interaction) 和一些混合共识。

Coin	Proof Type	Algo	Mining?	Max Hardware	Notes
Bitcoin	PoW	SHA256	Yes	ASIC	
Ethereum	PoW	Ethhash	Yes	GPU/CPU	
Bitcoin Cash	PoW	SHA256	Yes	ASIC	
Ripple	N/A		No		Proof of Correctness
DASH	PoW/PoS	X11	Yes	ASIC	
Litecoin	PoW	Scrypt	Yes	ASIC	
Open Trading Network	N/A		No		
Monero	PoW	Cryptonight	Yes	GPU/CPU	
Bitconnect	PoW/PoS	Scrypt	Yes	GPU/CPU	
NEO	N/A		No		Delegated BFT
NEM	PoI		No		Proof of Importance Vesting
IOTA	Tangle		No		
ETC	PoW	Ethhash	Yes	GPU/CPU	
EOS	DPoS		No		ERC-20Token
OmiseGO	PoS		No		ERC-20Token
Bitshares	PoS		No		
ZCash	PoW	Equihash	Yes	GPU/CPU	
USK	DPoS		No		ERC-20Token
USDT	N/A	N/A	Yes	N/A	N/A
Gnosis	N/A	N/A	No		ERC-20Token
Stellar	PoS	N/A	No		
Waves	Leased PoS		No		
Stratis	PoW/PoS	X13	No		
Vertcoin	PoW	Lyra2RE	Yes	GPU/CPU	
Decred	PoW/PoS	BLAKE256	Yes	GPU/CPU	Hybrid PoW/PoS system
Bitcoin Gold	PoW	Equihash	Yes	GPU/CPU	

数据来源：Cryptocompare

CHAPTER III

区块链行业发展三部曲

- 区块链1.0：点对点交易
- 区块链2.0：智能合约
- 区块链3.0：Token经济

3. 区块链行业发展三部曲

3.1 点对点交易

区块链行业发展三部曲

区块链1.0：回报率为王

- 回归区块链本身，我们认为区块链的发展可以划分为三个阶段：点对点交易、智能合约和泛区块链应用生态（Token经济）。点对点交易即以矿机算力为依托的去中心化的数字货币（BTC、LTC等）交易；智能合约则基于区块链可追溯、不可篡改的特性，形成了信任基础，使得合约实现自动化、智能化成为可能，其相当于20世纪90年代在因特网上萌生出的万维网、相当于2007年Google开发的开放源码的操作系统Android，都作为基础设施衍生出了多样的应用场景；泛区块链应用生态属于区块链3.0阶段，在这一时期，衍生出了Token（通证），如果区块链是一个价值传输系统，那Token则是区块链网络上的价值载体，区块链对现今商业体系实现颠覆性的最佳方式即通过发行Token并保证其流通性的形式实现各行各业的覆盖。



- 在区块链1.0时代，数字货币的买入卖出是人们参与区块链最主要的形式，该阶段鲜有人关注数字货币的应用价值，更多地关注点在于数字货币的回报率。**2017年，比特币投资回报率达181%，全品类数字货币合计回报率更是高达448%，远超房地产、黄金和股票投资。**

3. 区块链行业发展三部曲

3.1 点对点交易

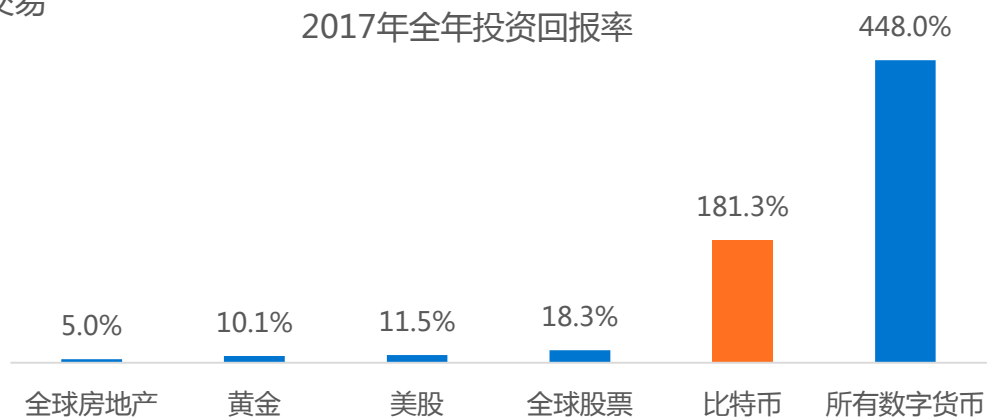
3.1.1 数字货币与其他品类投资回报情况对比

3.1.2 比特币财富榜

3.1.3 全球主要数字货币交易平台一览

区块链行业发展三部曲

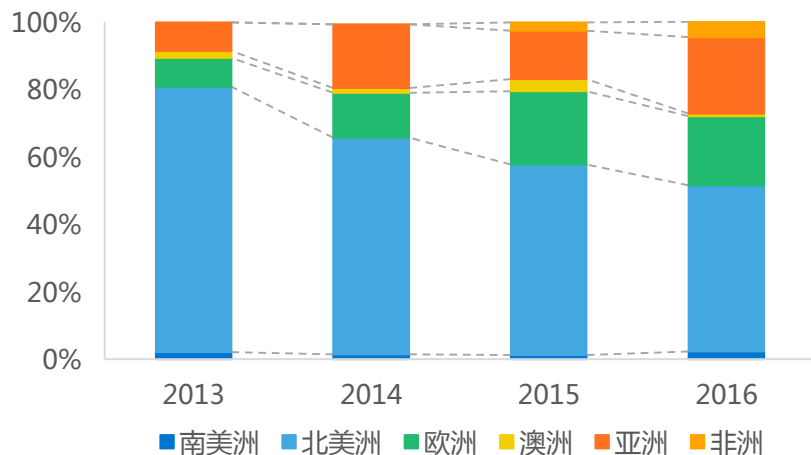
区块链1.0：回报率为王



数据来源：Coindesk

- 以比特币为例，从交易额分布情况来看，从最初2013年北美洲占据接近80%的交易份额，到2016年北美洲交易份额不足50%，其他大洲尤其是亚洲、欧洲交易量急剧增加。数字货币随着更广泛地域分布的持有者加入，逐步成为具备全球化跨境支付能力的交易货币。

五大洲比特币逐年交易额分布图



数据来源：CB Insights

3. 区块链行业发展三部曲

3.1 点对点交易

3.1.1 数字货币与其他品类投资回报情况对比

3.1.2 比特币财富榜

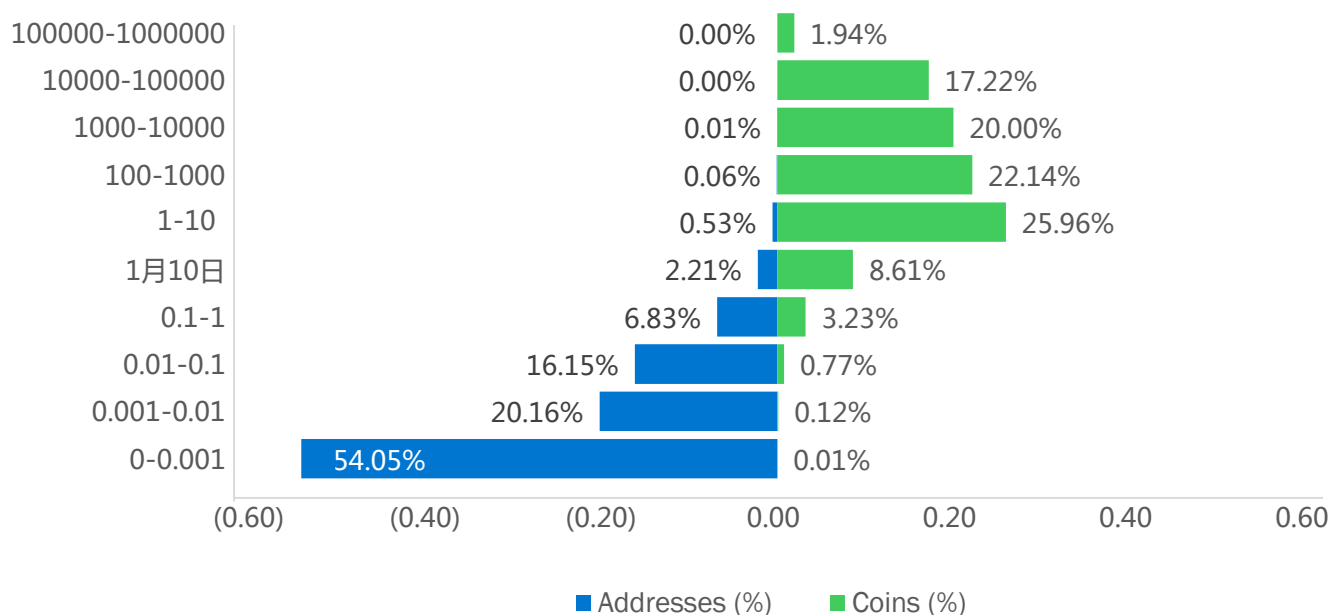
3.1.3 全球主要数字货币交易平台一览

区块链行业发展三部曲

区块链1.0：二八定律更甚，交易平台成最大获利者

- 从比特币财富榜可以看出，与现实财富世界类似，比特币同样符合二八定律甚至更两极化：0.6%的钱包地址拥有87.26%的比特币。

比特币财富榜



数据来源：bitinfocharts；36氪研究院

- 在比特币交易量不断上涨的区块链1.0时代，买入卖出双向手续费机制使得区块链行业的卖水人「数字货币交易平台」赚足红利。以交易平台币安为例，截至2018.2.23日，币安24小时交易额达125.1亿*，以0.1%交易手续费计算，币安每日仅手续费一项收入将高达1251万元。依此交易额水平，年手续费收入可期45亿。

*数据来源：非小号

3. 区块链行业发展三部曲

3.1 点对点交易

3.1.3 全球主要数字货币交易平台一览

区块链行业发展三部曲

主流数字货币交易平台一览

交易平台	坐标	支持法币	支付方式	可交易数字货币
 coinbase	美国·旧金山	AUD/USD/EUR /GBP/CAD/CNY & 50+ more	信用卡/借记卡	BTC/BCH/ETH/LTC
 eToro	英国·伦敦	USD	信用卡/借记卡 /Neteller/PayPal/Skrill/WebMoney/Yandex Money	BTC/BCH/DASH/ETC/ETH/LTC/XRP
 CEX.io	英国·伦敦	USD/EUR/RUB/GBP	信用卡/借记卡/SWIFT/SEPA/数字货币	BTC/DASH/ETH/XRP/ZEC
 CryptoGo	英国·伦敦	所有法币	信用卡/银行转账	BTC/BCH/ETH/DASH 25+ more
 Coinmama	斯洛伐克	USD/EUR	现金/信用卡/借记卡	BTC/ETH
 Bitit	法国·巴黎	EUR/USD/GBP/CNY/SEK/NOK/DKK	信用卡/借记卡/Neosurf/Cashlib/Trustpay/ePay	BTC/ETH
 LocalBitcoins.com	芬兰·赫尔辛基	AUD/USD/EUR /GBP/CAD/CNY & 50+ more	现金/信用卡/借记卡/数字货币 /BPAY/Flexepin/Neosurf/Neteller/M-PESA/PayPal/Perfect Money/WebMoney/Western Union/iDEAL/SEPA/Skrill/SWIFT	BTC
 kraken	美国·旧金山	USD/EUR/CAD/GBP/JPY	银行转账/山寨币	BTC/ETH//BCH/DASH/EOS/ETC/GNO/ICN等16种
 Changelly	捷克·布拉格	USD/EUR	信用卡/借记卡	BTC/BCH/BTG/ETH/ETC/DASH/DOG/NEO & 50+ more
 BITFINEX	中国·香港	USD	银行转账	BTC/ETC 30+more

图示：主流数字货币交易平台一览
数据来源：36氪研究院整理

3. 区块链行业发展三部曲

3.2 智能合约

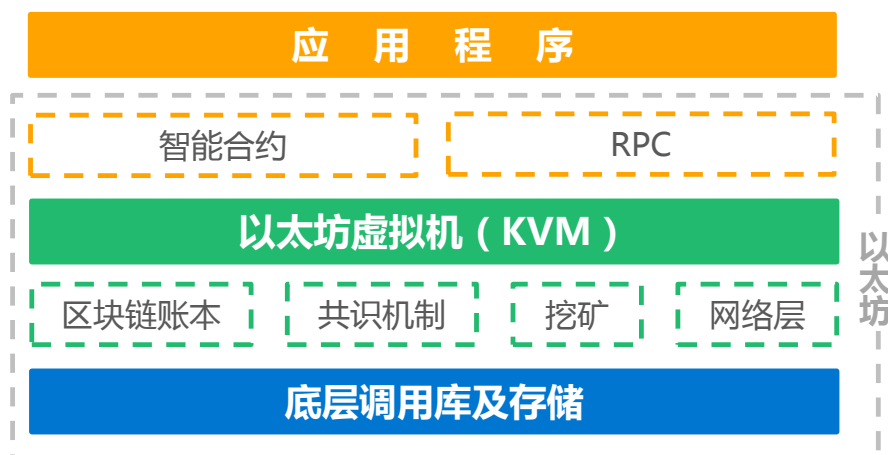
3.2.1 智能合约概述

3.2.2 数字身份概述

区块链行业发展三部曲

区块链2.0：智能合约为上层应用开发提供基础设施支持

- 在区块链2.0时代，区块链依据可追溯、不可篡改等特性形成了信任基础，为智能合约提供了可信任的执行环境，使得合约实现自动化、智能化成为可能。以太坊则是在区块链上实现智能合约的一种技术手段，支持图灵完备的脚本语言，为开发者在其设置的「操作系统」之上开发任意应用提供了必要的基础设施。



信息来自于公开资料整理

- 智能合约与传统合约最大的不同之处在于其不受现实社会法律的制约，针对于合约主体在触发合约条款后自动执行协议，而仲裁平台在智能合约中不再对执行结果进行判定而是承担执行之责。

	合同主体	合同条款	仲裁平台	仲裁对象
传统合约	甲方、乙方 (自然人/法人)	合约规定甲乙双方的权益和义务 (兼容现行法律)	判决权益和义务的归属	合约中定义的权益和义务
智能合约	甲方、乙方 (拥有数字身份)	由代码构建的加以双方的权益和义务 (不兼容现行法律)	代码自动判断并执行合约的所有条款，判决过程不需要第三方机构代理	合约中约定的数字资产

3. 区块链行业发展三部曲

3.2 智能合约

3.2.1 智能合约概述

3.2.2 数字身份概述

区块链行业发展三部曲

区块链2.0：构建数字身份是首要

- 在智能合约里，第一步是构建数字身份。数字身份是我们与社会发生泛商业关系时产生的一切数据对我们个人身份的数字化重塑。其作为数字资产与现实身份的映射证明也有着强烈的创投需求。全球范围内，数字身份正在加速落地。



英国推出的GOV.UK Verify，为中央政府提供以市场为基础的身份认证服务，该系统也可用于公共和私营部门。



RealMe为新西兰居民搭建了一个简单认证、高度安全、身份可信的数字身份网站。目前，银行、邮局等第三方服务机构均与其联通。



Cryptovalley Zug

瑞士城市Zug推出数字身份认证服务，居民在等级并获得政府官员正式后，将提供城市服务的应用程序



爱沙尼亚e-Residents项目为居民建立合法数字身份，提供出生证明、结婚证明、商务合同、公证等公共服务。



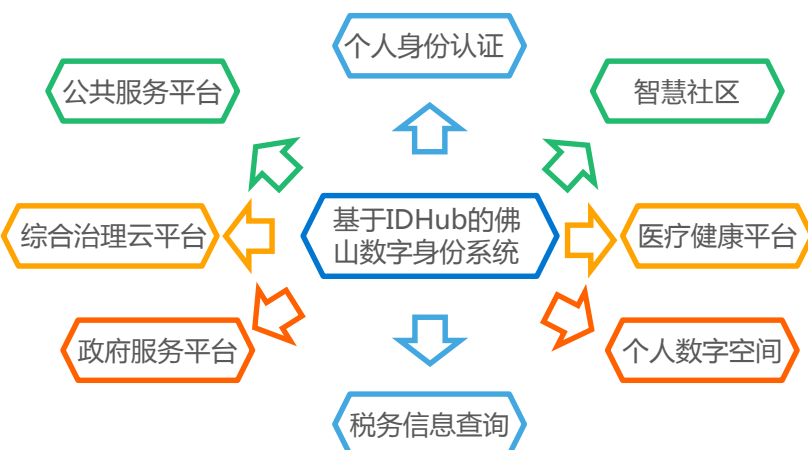
印度Aadhaar-Unique Identity Card工程旨在为公民提供唯一的身份，以此作为福利服务的基础，目前共有超过11.67亿人登记在册。



ID2020国际组织，致力于利用安全而成熟的系统实现数字身份认证，为全球11亿亿美元官方文件的人口提供合法的身份证明。

信息来自于公开资料整理

- 目前国内在数字身份领域的创业公司IDHub已在佛山正式落地。针对于整个佛山市人口数字化的计划预计将分为三期：第一期，建设自然人数字身份平台，链接民生应用、电子政务，打造一站式办公服务；第二期，建设法人数字身份平台，对接互联网应用、个人数字空间；第三期，基于区块链的立体多维信用模型体系，广泛对接线上线下的商业应用。



3. 区块链行业发展三部曲

3.3 Token经济

区块链行业发展三部曲

区块链3.0：Token经济对商业的颠覆在于其对生产关系的变革

- 区块链2.0对数字身份、智能合约等基础设施进行了构建，在此基础上，隐藏了底层技术的复杂性，应用开发者可以更多地专注在应用逻辑及商业逻辑层面。也就是进入了区块链3.0时代，标志就是出现了Token。Token是区块链网络上的价值传输载体，也可以理解为通证或代币。与传统股份制公司不同之处在于，股份制公司以利润为一切衡量基准，而Token则以流通效率为衡量基准，更深一层则是以影响力为衡量基准，影响力越大，则Token的适用生态越强大，进而保证了良好的流通效率。
- Token对人类社会最大的作用在于其对生产关系的变革，股份制公司将被替代，每一个实际参与者都成为了生产资本的拥有者。这种新型的生产关系激励着每一个参与者源源不断地贡献自己的生产力，是对生产力的一次极大解放。如果把这种商业活动映射到现实社会的通胀中，只要前者跑赢后者，随时间推移，每个Token的持有者都将获利。
- **简而言之，目前，Token最重要的是要做好生态建设，首先是要有落地场景。**虽然目前“区块链+”热情高涨，但真正适用于做“区块链+”的场景还是很局限的，**我们认为至少要符合三点：场景中需要一个账本存在（不局限于记录价值）；有真实性诉求；需要形成大规模共识。**

3. 区块链行业发展三部曲

3.3 Token经济

3.3.1 全球及中国区块链项目分布情况

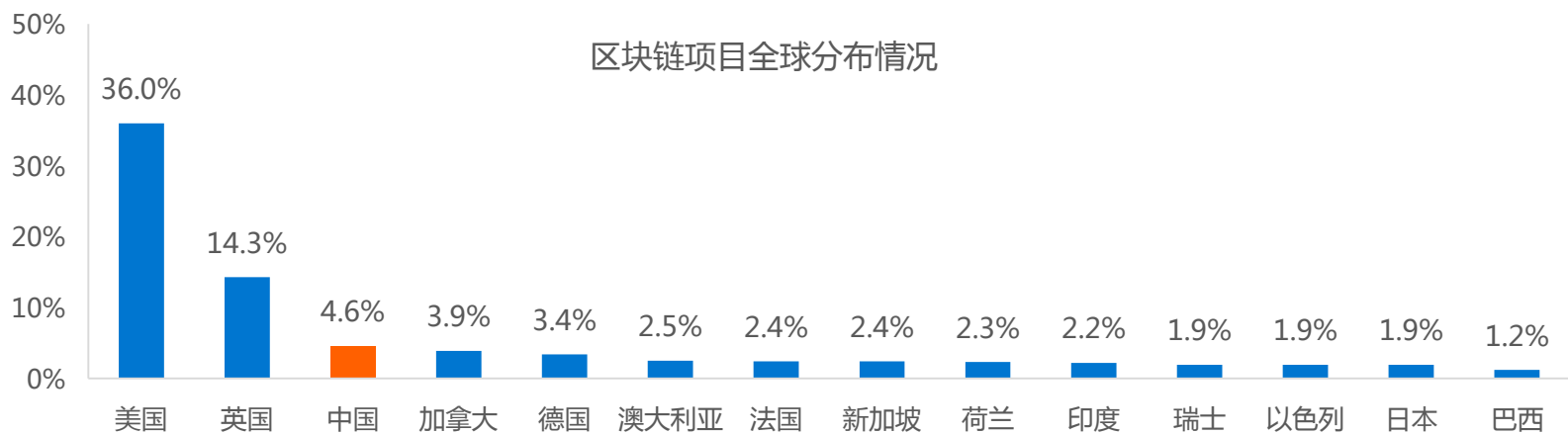
3.3.2 全球区块链项目全景图

区块链行业发展三部曲

区块链3.0：目前，区块链项目以金融和基础设施为主

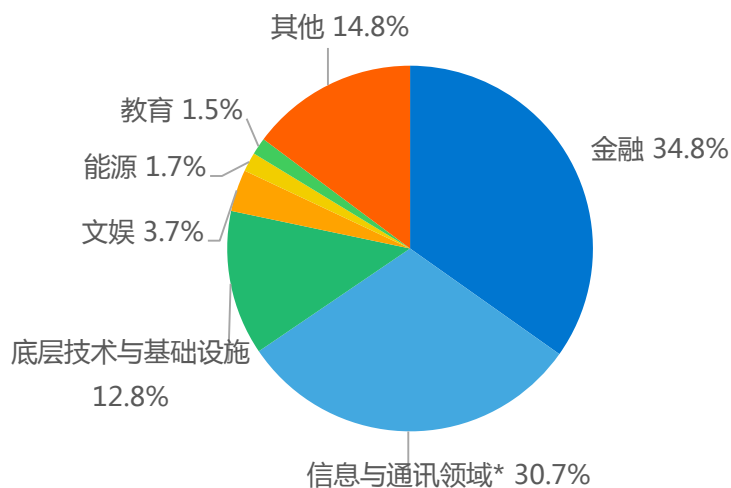
- 从全球区块链项目数量来看，截至2018.2.2，全球区块链项目合计1286个，中国仅占4.6%，居全球第三位；从项目类型分布维度来看，全球范围和中国均以金融领域居首位、底层技术和基础设施居第二位；辅以文娱、能源、教育等细分场景。

区块链项目全球分布情况



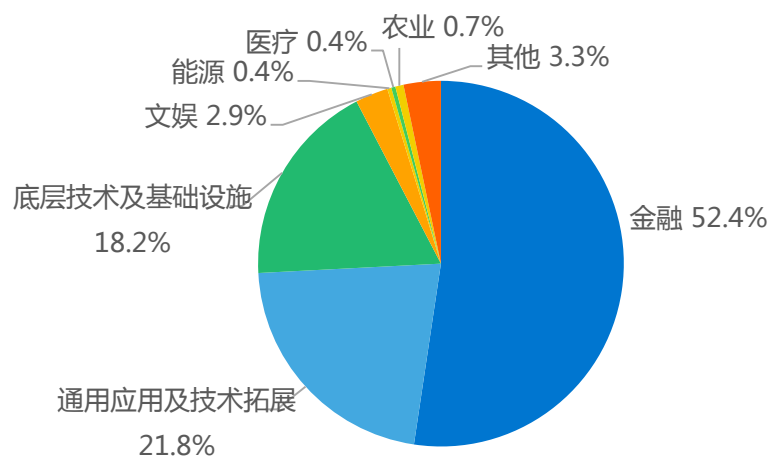
注：总项目数为1286个；数据截至2018.2.2；数据来源：Outlier Ventures

全球区块链项目类型分布



数据截至2017.2.2；数据来源：Outlier Ventures
*信息与通讯领域主要包括交易平台、钱包、支付、媒体、咨询、数据分析、数字签名、产权公证等项目

中国区区块链项目类型分布



数据截至2018.2.2；数据来源：鲸准数据

3. 区块链行业发展三部曲

3.3 Token经济

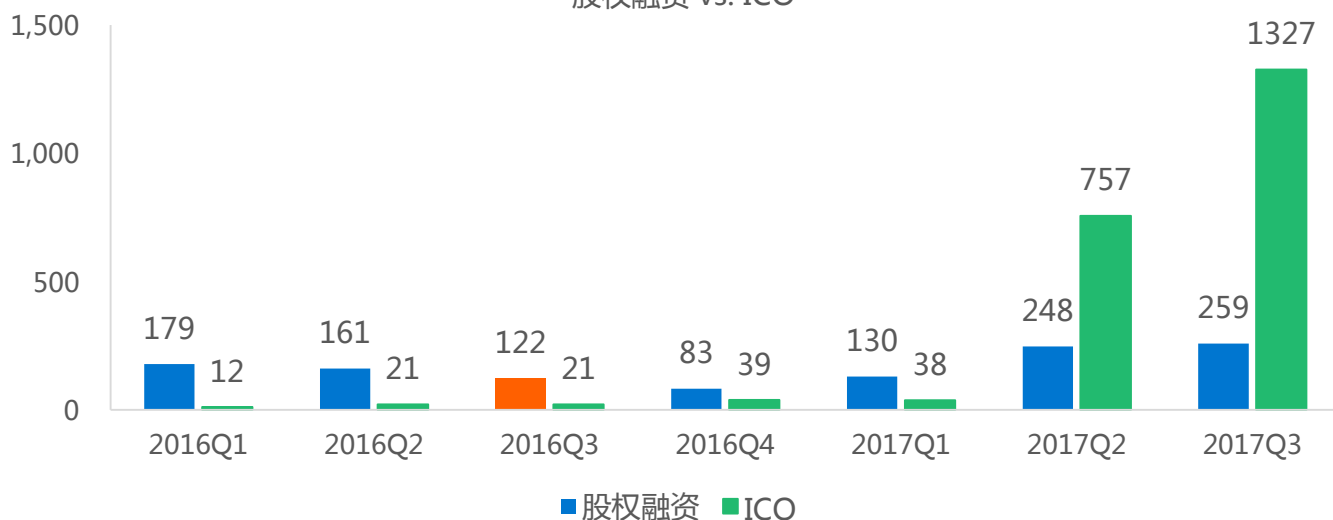
3.3.1 全球及中国区块链项目分布情况

3.3.2 全球区块链项目全景图

区块链行业发展三部曲

截至2017年Q3，区块链项目已通过ICO募集超过20亿美金

- 从全球区块链项目融资方式来看，主要存在两种：股权融资和ICO。整个2016年还是以股权融资为主，到2017年Q2，ICO爆发，截至2017年Q3，全球区块链项目已通过ICO募集超过20亿美金。并且有更多的ICO计划真正不断进行。
- 其中，通过ICO募集的大部分资金都投入到了基础设施建设和项目开发中，如Tezos（2017年Q3筹集2.3亿美元）和Bancor（2017年Q2筹集1.53亿美元）。此外，计算和存储公司也吸引了大量投资者的兴趣，如Filecoin（2017年筹集3亿美元+）、SONM（2017年Q2筹集3500万美元）和Golem（2016年Q4筹集900万美元）。

全球区块链项目融资情况（单位：百万美元）
股权融资 vs. ICO

数据来源：CB Insights,TokenData,CoinSchedule

3. 区块链行业发展三部曲

3.3 Token经济

3.3.1 全球及中国区块链项目分布情况

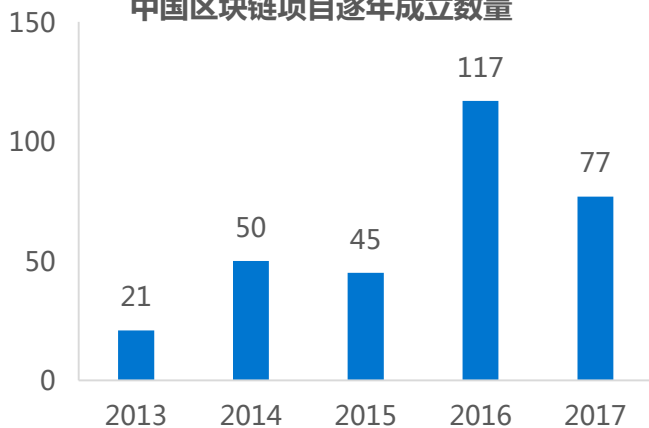
3.3.2 全球区块链项目全景图

区块链行业发展三部曲

区块链3.0：城市维度，除北、上之外，深圳和杭州尤其值得关注

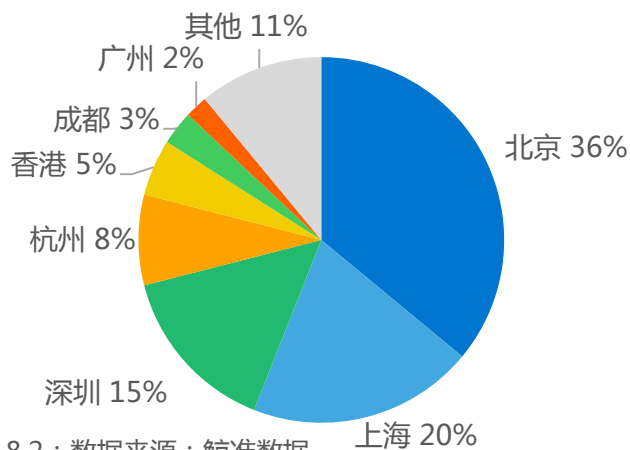
- 我国的区块链项目成立数量从2013年开始逐年走高，2017年受到政策监管等原因数量出现缩减，但获投数量和平均融资额数年走高；在地域分布方面，区块链项目仍是主要分布于北上广深等一线城市，值得关注的是深圳和杭州，其不但项目数量较多且节点数也处于我国前列；从融资轮次来看，整体仍处于早期，但大公司进行战略投资布局的占比也在逐年走高。

中国区区块链项目逐年成立数量



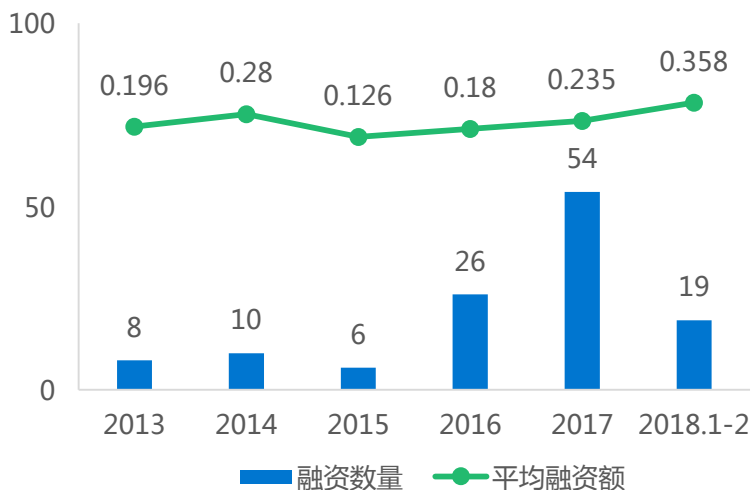
数据来源：鲸准数据

中国区区块链项目地域分布



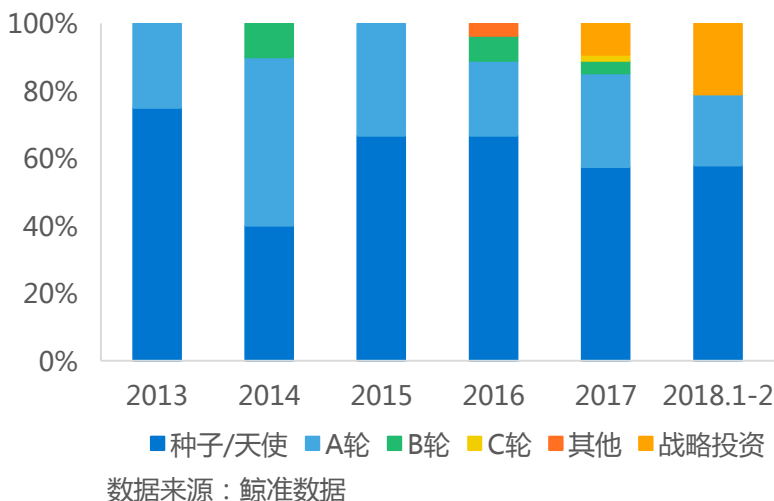
数据截至2018.2；数据来源：鲸准数据

中国区区块链项目融资数量（个）&平均融资额（亿人民币）



注：不包含ICO；数据来源：鲸准数据

中国区区块链项目融资轮次分布



数据来源：鲸准数据

3. 区块链行业发展三部曲

3.3 Token经济

3.3.2 全球区块链项目全景图

区块链行业发展三部曲

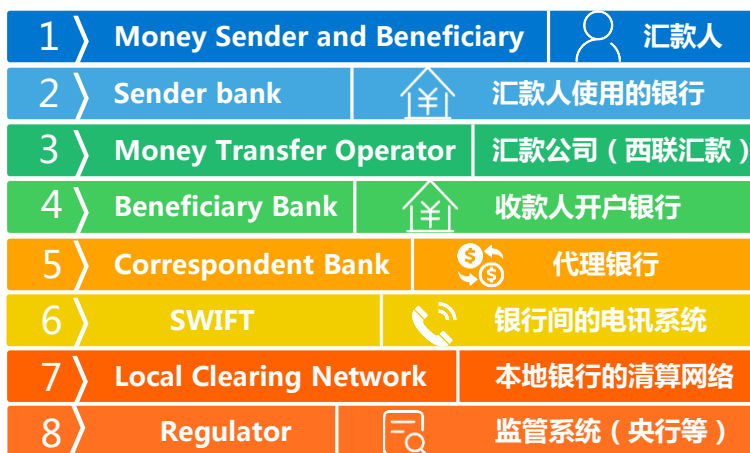
区块链应用-项目全景图



区块链落地场景 - 跨境支付

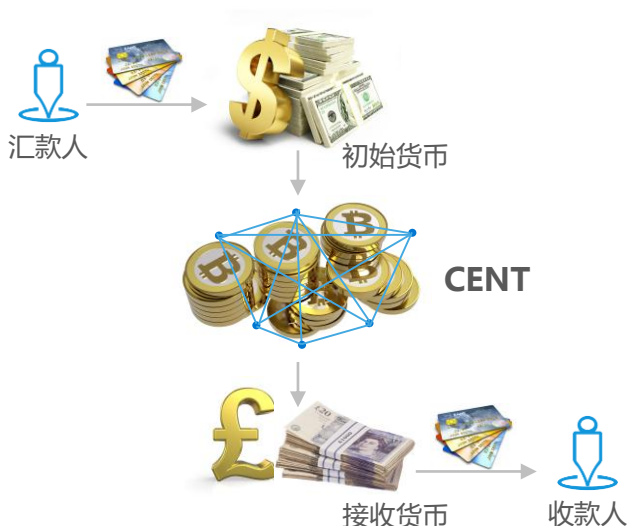
利用区块链技术在跨境支付场景实现价值的快速传输

- 基于我们上面所述的适合进行“区块链+”的分析，我们认为物联网、分享经济、跨境支付、去中心化投票都是适用场景，每个领域都将产生去中心化的巨头组织。其中在跨境支付、物联网领域已经有了不错的落地项目。



- 对于跨境支付场景来说，传统的跨境支付方式周期长、费率高*，易出错，而Circle、Veem、OKLink等企业基于区块链技术，将初始货币如美元经自身比特币池兑换为接收货币如英镑，便可实现不同国家间的货币传输任务。

图示：传统跨境支付流程图；来源：世界经济论坛

图示：Circle基于区块链技术跨境支付流程图
来源：36氪研究院绘制

- Circle Internet Financial（以下称Circle）创办于2013年，总部位于美国波士顿。Circle业务曾涉及数字货币交易、存储及支付等，2016年12月份Circle宣布其不再为消费者提供直接的比特币交易服务，业务重心转向基于以太坊支付网络的跨境支付领域。并且其旗下子公司CENTRE正在筹划推出CENT代币，目前已通过未来代币简单协议（SAFT）销售募集到2000万美元资金。在跨境支付过程中，代币CENT将成为主要的桥梁币种。

*平均每个汇款人的所承担的手续费率达7.68%，数据来自世界银行



Circle Internet Financial

创办时间：2013年

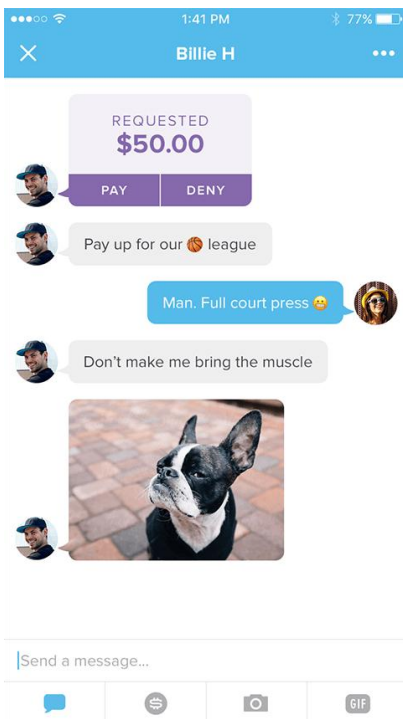
地址：美国波士顿

最新融资：D轮

获投时间：2016年6月

融资额：6000万美元

投资方：IDG资本、百度
Pantera Capital等



图示：基于社交模式的价值传输体系
来源：Circle官网

区块链跨境支付企业案例 - Circle

数字货币正在从单一的货币形式转型为其他金融服务的基石

- 并且，基于Circle的跨境汇款几乎没有时滞，此外用户也无需支付任何手续费或外汇加价费。区块链技术极大地加快了价值传输速度、降低了价值传输成本。
- 安全方面，Circle采用AES 128位对称加密技术进行加密，每层都有单独的存储机制。并且，全程在FDIC保险范围内作业，用户还可自行采用其他安全措施，例如触摸ID和PIN码等。目前，Circle已支持美元、英镑的兑换及服务。在中国市场，Circle的D轮融资顺利引入了IDG、百度、中金、光大、宜信、万向等中国财团，同时成立了世可中国（Circle China），或可期待美元、英镑和人民币的消费者无障碍连通时代的到来。
- 区块链1.0时代逐步接近尾声，创业公司作为交易平台新进场者的竞争力正在流失，但跨境支付的变革需求或将是区块链技术真正落地的蓝海，也是Token作为其他金融服务基石的重要尝试。
- 此外，瑞波币（XRP）也是一种应用于无障碍支付场景的Token，其是基于Ripple网络进行支付转账的桥梁货币。与以太坊支付网络不同的是，Ripple网络最初设计思路是基于熟人关系网和信任链，天然亲和闪电网络，有利于处理未来大并发的支付任务。

3. 区块链行业发展三部曲

3.3 Token经济

3.3.3 典型跨境支付项目介绍—Circle

3.3.4 典型物联网项目介绍—Filament

区块链落地场景 - 物联网

传统物联网VS基于区块链物联网

- 物联网领域，在当前的中心化构架下，由于不同的利益主体和信任关系，物联网很难完成互通互联和自主协作，目前的物联网设备的协作和交易只能在同一信任域下进行，大大降低了物联网应用的真正商业价值和普及程度，而区块链技术能够解决非安全网络下的信任问题，解决的正是物联网缺陷的核心。相比法币，Token更适用于机器之间的小额支付场景。

痛点	痛点拆分	传统物联网	基于区块链的物联网
无法万物互联	可靠性问题	所有的设备都需要和物联网平台中心进行交互，一旦数据库崩塌，可能会造成整个物联网系统整体宕机。	基于区块链的网络结构使设备之间保持共识，无需与中心进行验证，即使一个或多个节点被攻破，整体网络体系的数据依然可靠、安全。
	安全性问题	在不同系统节点间进行数据传输，数据本身可能被非法篡改或者丢失	通过区块链的数据加密技术和P2P互连网络保证数据的不可篡改性，并且用户隐私保护也将得到进一步提升。
	利益分配	物联网服务商之间若想实现资源共享，除需达成合作协议外，还需要在架构顶层设计双方认同的结算系统。在万物互联的大环境下，这种单个服务商之间的互通所需成本非常巨大，以至于很难实现。	基于区块链上的数字货币应用，可以在全网范围内在各个不同的运营商之间按照数据流量进行直接的数字货币结算
成本逐步攀升		中心化的体系结构下，所有的数据都需要汇总到单一的中心控制系统，随着连接设备数量的几何级增长，中心化服务需要付出的计算、存储和带宽成本也会增加大无法负担的程度，设备的管理和维护将会给生产商、运营商和最终用户带来巨大的成本压力。	中心化平台的撤销，低成本的改造数亿设备，在计算力、存储容量和带宽方面都大幅度降低了要求。另外，叠加智能合约可将每个智能设备变成可以自我维护调节的独立的网络节点，省却了很多运维成本。



公司名称：Filament

创办时间：2012年

地址：美国丹佛

最新融资：A轮

获投时间：2017年4月

融资额：1500万美元

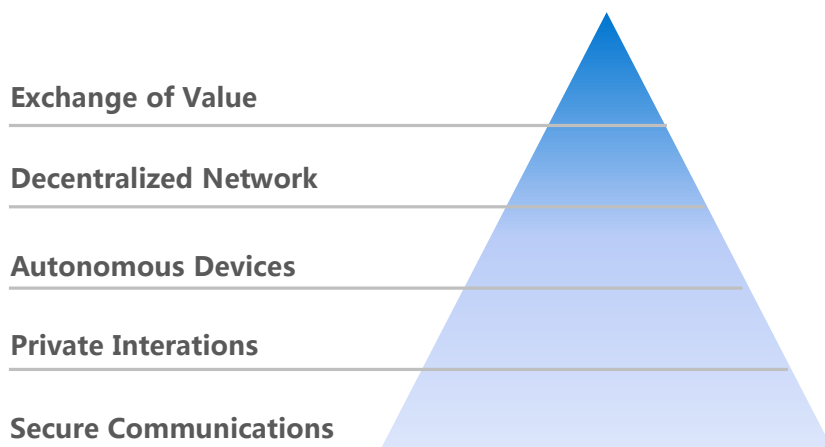
投资方：Verizon Ventures

Bullpen Capital等

区块链物联网企业案例 - Filament

区块链-物联网双技术协同发展已在小范围尝试

- 在探索区块链技术在物联网领域应用方面，巨头和创企都在行动。2015年1月，IBM联合三星推出了ADEPT项目（Autonomous Decentralized Peer-to-Peer Telemetry—去中心化的p2p自动遥测系统），ADEPT项目基于以太坊（智能合约）、Telehash（p2p信息发送系统）和BitTorrent（文件分享）三项协议，意图利用区块链技术打造一个能够自动检测、自动更新、互相通信的物联网系统，为下一代物联网构建了一个概念证明型系统。创企方面，我们将以Filament为案例阐述说明区块链-物联网双技术协同发展的现阶段水平。
- Filament 成立于2012年，其利用区块链技术为工业网络构建的软硬件解决方案，该解决方案允许工业资产安全地相互通信无线，并且可以独立在其他设备进行云连接，其不再需要一个中央系统处理即可独立执行智能协约。



图示：Filament架构图
来源：Filament官网

区块链物联网企业案例 - Filament

Filament应用技术浅析



公司名称：Filament

创办时间：2012年

地址：美国丹佛

最新融资：A轮

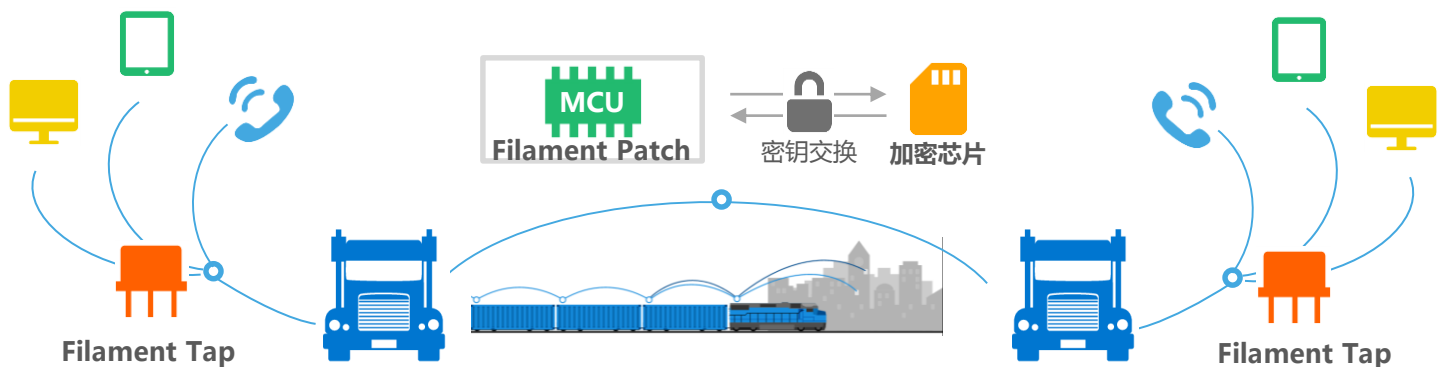
获投时间：2017年4月

融资额：1500万美元

投资方：Verizon Ventures

Bullpen Capital等

- Filament目前有两款硬件产品：Filament Tap和Filament Patch。两款硬件产品在工业设备出厂前对设备进行改造，前者作为传感器，允许该设备与周边10英里以内的电话、平板电脑和计算机进行沟通；后者则主要包括了MCU（微控制器单元），其在出厂前通过密钥与加密芯片互相配对、绑定，建立起信任的MCU只会与其配对的密码芯片通话，这种端对端的配对方式为设备间安全通讯提供了基础。目前，Filament采用的是基于Blocklet技术的JSON Web Token（JWT）作为代币进行机器之间的价值交换。软件方面，Filament将使用五层协议—Blockname、Telehash、以太坊、Pennybank和BitTorrent。Filament传感器的运行依赖于前三层协议，后两层协议供用户端自行选择*



图示：Filament硬件系统
来源：36氪研究院

- 此外，基于Tangle（缠结）网络的IOTA是专为物联网而设计的新型交易结算币种，与区块链不同的是，Tangle不是链状结构而是网状结构，可拓展性和稳定性更好，更适用于物联网这种小额高频交易场景

CHAPTER IV

区块链行业未来展望

- 未来展望

4. 区块链行业未来展望

4.1 未来展望

区块链行业未来展望

区块链行业总结 & 未来展望

- 基于比特币交易仍处于快速增长阶段，而区块容量已达到峰值的现状，比特币交易网络堵塞现象将逐步加剧，2018年将是比特币交易手续费持续稳定攀升的一年，区块扩容迫在眉睫。若扩容方案持续受阻，**BCH在未来将有机会获得更多的算力支持**。从比特币历史价格来看，在2013年年末以及2017年年末，比特币价格都处于井喷式增长阶段，而2013年和2017年又都恰巧是随块产生的比特币数量减半的关键节点，此现象与现实社会中的通货紧缩类似。据此，**我们可以预测，随块产生的比特币第三次减少即2021年，比特币价格很有可能迎来第三次大幅上涨**。
- 抛开比特币，区块链行业未来的发展将与场景紧密结合，更多的企业将会参与到Token经济中。基于Token对生产关系的变革，股份制公司将被替代，每一个实际参与者都会成为生产资本的拥有者，是对生产力的一次极大解放。目前，**Token经济中最重要的要做好生态建设，使得Token能够很好地流通起来**。虽然“区块链+”热情高涨，但真正适用的场景至少要符合三点：**场景中需要一个账本存在；有真实性诉求；需要形成大规模共识**。物联网、分享经济、跨境支付、**去中心化投票都是适用场景**，每个领域都将产生去中心化的巨头组织。去中心化组织信任度更高，但中心化组织效率更高，二者有各自的适用场景，适当情况下，也可混合搭配使用。一刀切的为上链而上链将会造成极大的资源浪费。

附录

36氪研究院介绍

- 36氪研究院依托36氪媒体与创业服务属性，拥有完善的一级市场企业数据库和强大的传播资源；配备多名深耕于各细分领域的资深分析师；研究覆盖人工智能、区块链、医疗、金融、文娱、消费、汽车、教育等多个领域；受众集中于投资者、创业者等高净值人群，兼具行业深度与影响力。目前，36氪研究院已形成行业研究报告、企业调研报告、用户数据报告等三大产品矩阵，致力于让一部分人先看到未来。

01



资源

36氪研究院依托36氪媒体与创业服务属性，拥有完善的一级市场企业数据库和强大的传播资源

02



资深

配备多名深耕于各细分领域的资深分析师

03



研究领域

研究覆盖人工智能、区块链、医疗、金融、文娱、消费、汽车、教育等多个领域

04



受众

受众集中于投资者、创业者、分析师等高净值人群，兼具行业深度与影响力

05



产出

目前，36氪研究院产出形式主要包括行业研究报告、企业调研报告、用户数据报告等三大产品

声明

报告作者

孔德云 36氪研究院 分析师

分析师声明

本报告作者具有专业胜任能力，保证报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，本报告清晰准确地反映了作者的研究观点，力求独立、客观和公正，结论不受任何第三方的授意或影响，特此声明。

免责声明

36氪不会因为接收人接受本报告而将其视为客户。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。

本报告的信息来源于已公开的资料，36氪对该等信息的准确性、完整性或可靠性不作任何保证。本报告所载的资料、意见及推测仅反映36氪于发布本报告当日的判断，本报告所指的公司或投资标的的价格、价值及投资收入可升可跌。过往表现不应作为日后的表现依据。在不同时期，36氪可发出与本报告所载资料、意见及推测不一致的报告。36氪不保证本报告所含信息保持在最新状态。同时，36氪对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。在任何情况下，36氪、36氪员工或者关联机构不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。投资者务必注意，其据此做出的任何投资决策与36氪、36氪员工或者关联机构无关。

在法律许可的情况下，36氪及其所属关联机构可能会持有报告中提到的公司的股权，也可能为这些公司提供或者争取提供筹资或财务顾问等相关服务。在法律许可的情况下，36氪的员工可能担任本报告所提到的公司的董事。

本报告版权仅为36氪所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制、发表或引用。如征得36氪同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“36氪研究院”，且不得对本报告进行任何有悖原意的引用、删节和修改。

36Kr 研究院

让一部分人先看到未来

