

从一到N，掘金区块  
——区块链行业研究报告

36氪研究院

2016年6月

# 目录 Contents

## 一、区块链的概念解析

- 1.1 热度概况
- 1.2 基本概念及工作原理
- 1.3 核心技术
  - 区块和链
  - 数学加密
  - 分布式结构
  - 证明机制

## 二、区块链技术的行业应用

- 2.1 应用基础：核心优势
- 2.2 应用基础：智能合约
- 2.3 主要行业应用介绍
  - 金融业
  - 网络安全
  - 身份信息管理
  - 公证
  - 投票
  - 供应链

## 三、区块链领域投资与典型案例介绍

- 3.1 全球区块链投资概况
- 3.2 典型案例介绍
  - Shocard：保护身份信息的“骑士”
  - ABRA：跨境支付so easy
  - Agora Voting：为投票保驾护航
  - OpenBazaar：去中心化的ebay

## 附录

- 区块链金融服务领域应用公司全景图
- 金融机构参与区块链的应用及合作领域

## CHAPTER 1

# 区块链的概念解析

---

- 热度概况
- 基本概念及工作原理
- 区块链的核心技术

区块和链

数学加密

分布式结构

证明机制

## 概述

## 引言：区块链是何时火热起来的

区块链是何时火热起来的？

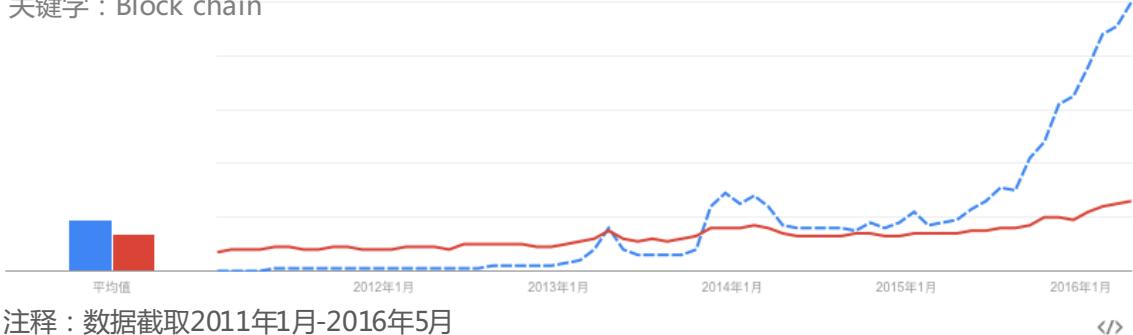
- ✓ 2015年10月，《Economics》杂志刊登了一篇名为《The Great Chain of Being Sure about Things》，文中描述了艾女士因为房产登记权纠纷而失去房子的实事；
- ✓ 2015年10月，上海召开《区块链-新经济蓝图》全球区块链峰会；
- ✓ 2015年12月，麦肯锡发布关于“区块链技术”研究报告；
- ✓ 2016年1月，中国中央银行召开数字货币研讨会，有消息称央行有推出数字货币意图。

从Google Trend和百度指数上来看，以美国为首的国外科技从2013年便开始关注区块链技术，关注度在2015年下半年取得了爆发性的增长。相比之下，国内从2015年下半年才开始关注区块链技术，今年关注热度有所提高，但并不显著。

可见，区块链技术的发展及应用，国外的成熟度远远高于国内。国内的热情还尚未开发，相关应用企业还比较少。

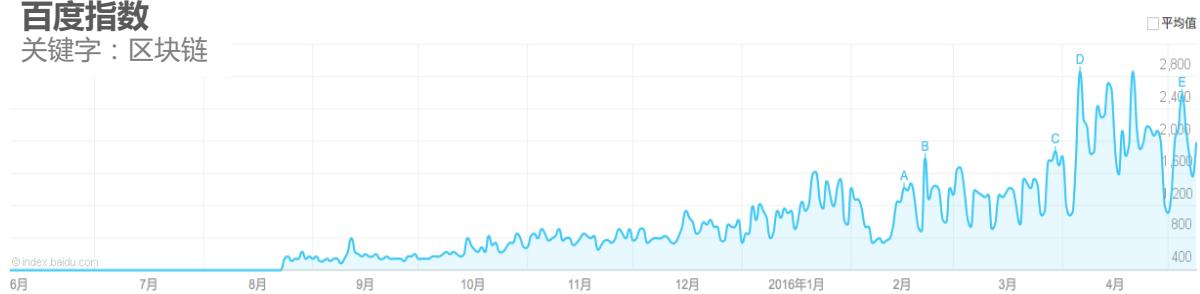
## Google Trend

关键字：Block chain



## 百度指数

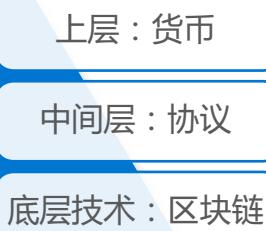
关键字：区块链



## 概述

### 区块链的基本介绍

谈到区块链，必然先想到比特币。从技术角度来看，比特币的系统包括三层：底层技术——区块链；中层链接——协议；上层——货币。



- **上层是货币**，在这里指的是比特币。
- **中间层是协议**，也就是基于区块链的资金转账系统；
- **底层技术是区块链**，去中心化、分布式记录的公开透明的交易记录总账，其交易数据全网节点共享。矿工负责记录，全网监督；

**区块链（Blockchain）** 是一种分布式共享数据库（数据分布式储存和记录），利用去中心化和去信任方式集体维护一本数据簿的可靠性的技术方案。该方案要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（即区块，block），每个数据块中都包含了一定时间内的系统全部信息交流的数据，并生成数据“密码”用于验证其信息的有效性和链接下一个数据库块。

**比特币是一种可全球范围内可交易的电子货币，是目前区块链技术最成功的应用。**当前银行等机构更多关注的也是正是比特币背后的区块链技术。**从比特币的工作原理可以清楚的了解区块链的定义及创新之处。**

**如果说比特币完成了技术“从零到一”的华丽诞生，那么区块链则是“从一到N”的日益丰富。**

#### 应用

##### 比特币 Bitcoin

- 全球数字货币
- 比特币交易波动性大、流动性高，受高频交易及对冲基金的喜爱

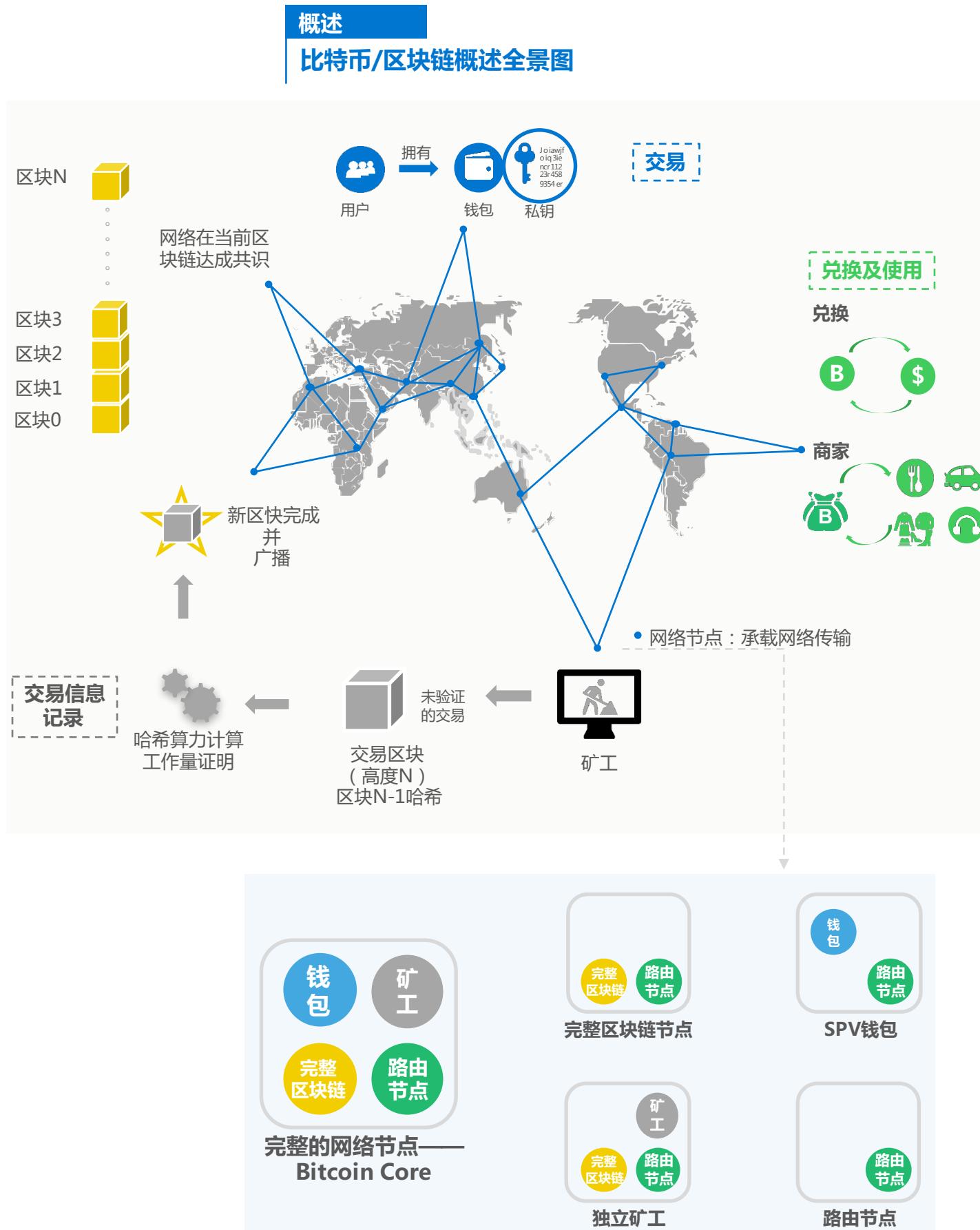


#### 技术基础

##### 区块链 Blockchain



- 经密码加密的完备分布式总账
- 在需要第三方监管的中介网络及清算系统中发挥潜力
- 向其他需要较高信任机制的应用领域延伸

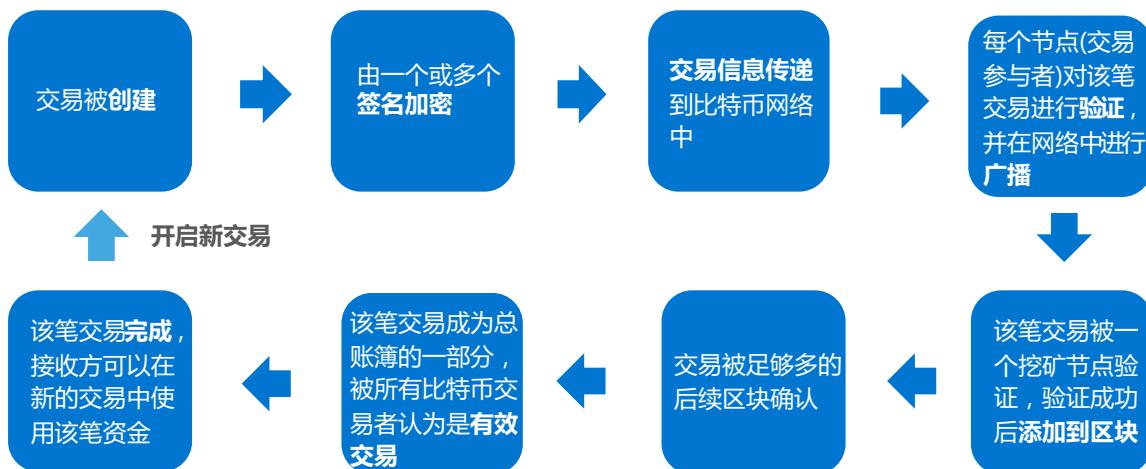


## 概述 · 交易

### 比特币交易及交易过程

通过区块链的工作原理可以看到，**比特币交易本质是一种数据结构**，该数据结构是包含交易信息的区块从后向前有序连接起来的。比特币区块链是全球复试记账的总账簿，每一笔比特币交易都是比特币区块链上的一个公开记录。

#### 比特币的交易过程

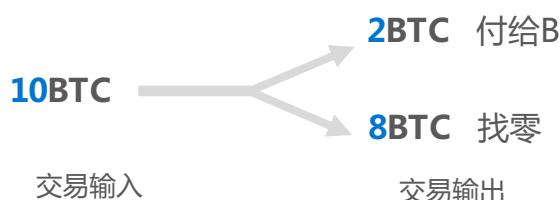


#### 交易的输出和输入

比特币交易的基本单位是**未使用的交易输出 (unspent transaction output, UTXO)**。UTXO是可以被网络识别成货币单位的一定量的比特币货币，可以是任意值，但不可分割。

实际交易环节中，通常出现的情况是**UTXO大于所需支付的金额值**，那么该UTXO在交易中将会被整体消耗，同时产生零头。

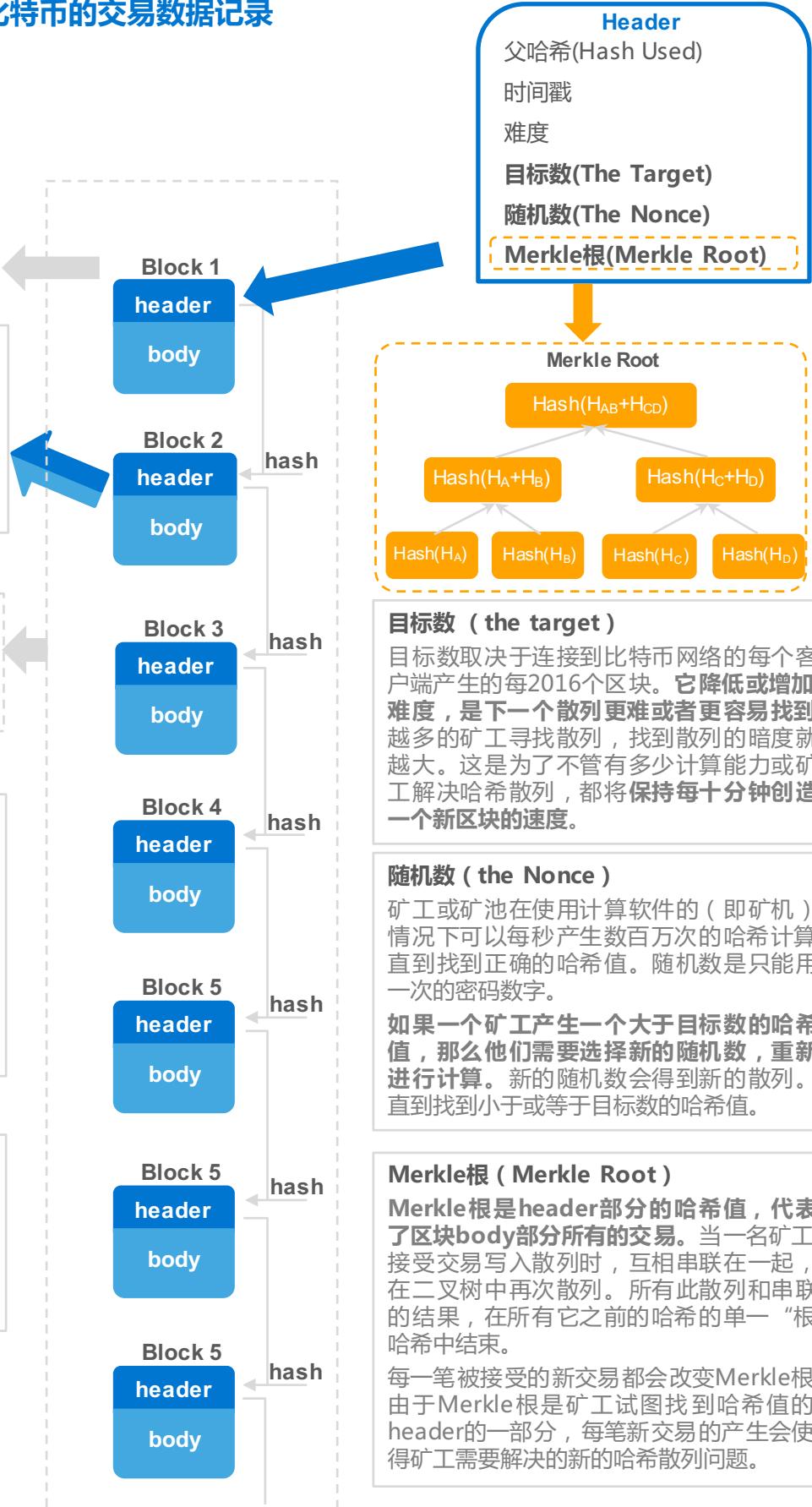
比如，A拥有一个10比特币的UTXO，他需要向B支付2比特币，那么交易中，交易输入为该10比特币，会被整体消耗，同时产生两个输出：2比特币支付给B，以及8比特币的零头返回A的钱包。



## 概述 · 数据记录

**比特币的交易记录均保存在区块的Body中。**

## 比特币的交易数据记录

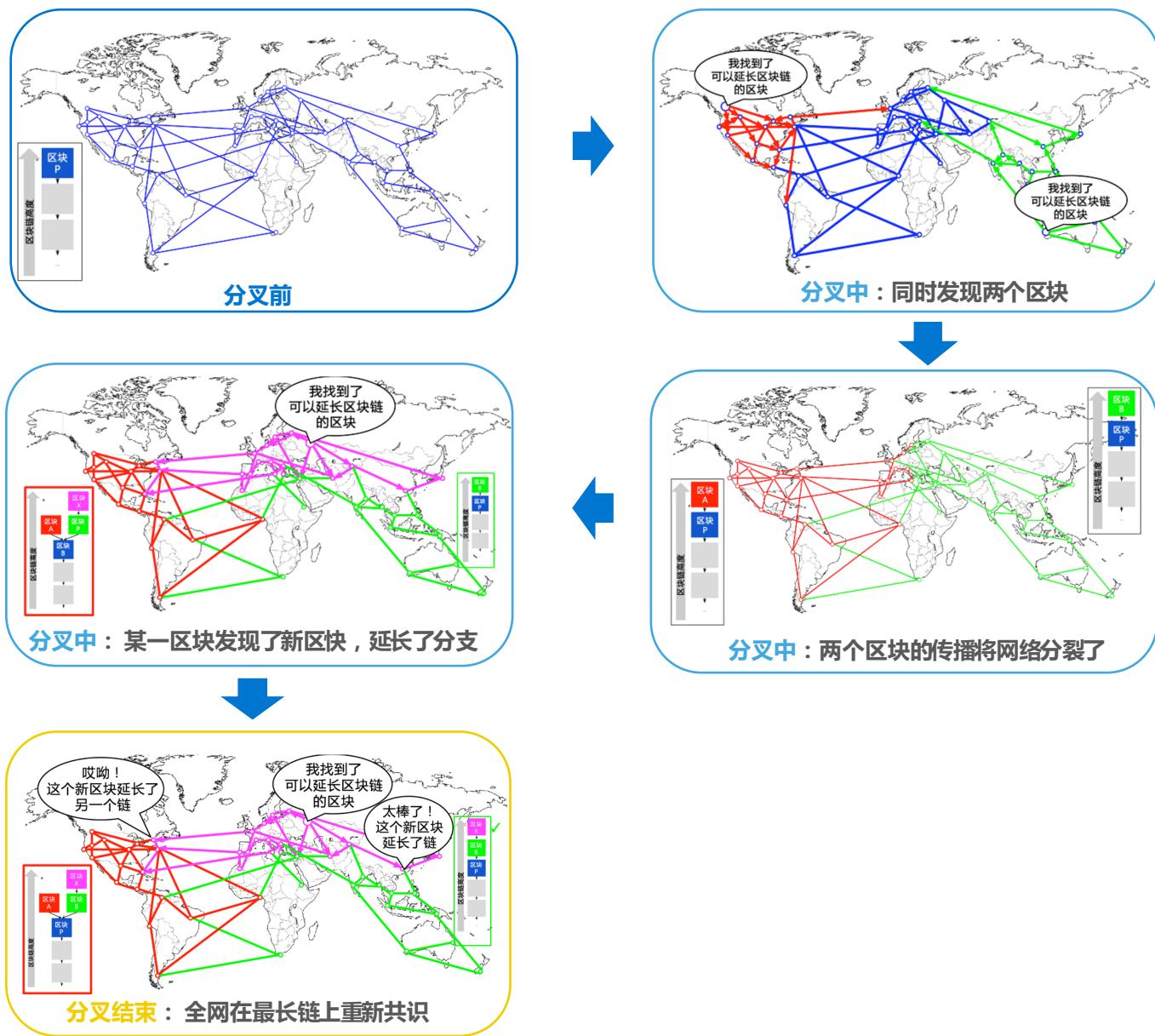


## 概述·数据记录

## 比特币的交易数据记录 — 分叉处理

在区块链中，每一个子区块只有一个父区块；然而当不同的矿工同时发现不同的区块时，会出现一个父区块暂时拥有很多子区块的情况，这种情况被称为**区块链的分叉**。

区块链的解决方法是，**每个节点选择并延长拥有最大工作量证明（或最长、最大难度）的区块链**。



来源：《精通比特币》，36氪研究院

## 概述 · 区块链

## 区块链的核心技术：区块和链

**区块+链=历史+验证**

区块结构有两个非常重要的特点：

- 每个区块的块头包含了前一区块的交易信息的压缩值，因此从创始块到当前区块形成了链条；
- 每个区块主体上的交易记录是前一区块创建后、该区块创建前发生的所有价值交换活动；

绝大多数情况下，新区快创建成功被加入到链中，该区块的数据记录则不可被改变或更改。



以上结构也保证了交易信息的不可伪造、不可虚构和不可篡改。

**不可伪造**

区块链的记录原理需要所有参与记录的节点，来共同验证交易记录的正确性。由于所有节点都在记录全网的每一笔交易，因此，一旦出现某节点记录的信息与其他节点的不符，其他节点就不会承认该记录，该记录也就不会写入区块。

**不可虚构**

当发送者广播交易信息时，区块链中参与记录的节点需要做的是通过历史记录验证发送者是否有能力履行该交易，而不是验证广播的交易消息是否为真。通过历史数据的校验功能，区块链建立了信任的基础，也保证了信息的不可虚构。

**不可篡改**

改变某一区块及区块内的交易信息几乎是不可能的。如果该区块被改变，那么之后的每一个区块都将被改变。因此试图篡改数据的人必须同时入侵至少全球参与记录51%的节点并篡改数据。从技术上来讲，这几乎是不可能的。

## 概述 · 区块链

### 区块链的核心技术：区块和链

区块链上可能出现的信息安全与不信任问题体现在两方面：

- 一、试图更改之前某个区块上的交易信息
- 二、试图控制新区块的生成

解决这两个问题的关键都在于**解数学题背后所代表的巨大计算能力的保证。**

#### 1. 更改某区块的交易信息



因此，恶意节点若想成功更改该交易信息，**只有重新计算被更改区块后续所有区块，并且追上网络中合法区块链的进度后，把这个长的区块链分叉被提交给网络中的其它节点，才有可能被认可**(请参考“分叉处理”内容)。在当前全网巨大计算能力的背景下，一个恶意节点想重新计算多个区块并且追上全网的情况很难出现。

#### 2. 控制新区块的生成

**试图控制新区块的生成，则需要恶意节点率先得出数学题的解得到认可。**由于区块中的交易由该节点决定，因此恶意节点可以永远不让某个交易得到认可。

理论上控制新区块的生成是可能的实现的：当恶意节点的计算能力高于网络中所有其它节点的计算能力的总和时，也就是恶意节点占据了全网 51% 的计算能力，恶意节点就可以控制新区块的生成，这种攻击被称为 **51% 攻击**。然而，在现实当中，一个节点的计算能力超过其它所有节点的总和是非常困难的。

## 概述 · 区块链

### 区块链的核心技术：数学加密

**比特币的所有权通过数字密钥、比特币地址和数字签名来确定。**其中，数字密钥由用户生成并存储在文件或数据库中，成为“钱包”。**钱包中不包含比特币，只包含密钥。**一个用户的数字密钥是完全独立于比特币协议的，由用户的钱包生成并自行管理，无需区块链或网络连接。

**每笔交易需要一个有效签名才会被存储在区块中。**只有有效的数字密钥才能生成有效签名，因此拥有了密钥就相当于拥有了对账户中比特币的控制权。

密钥是成对出现的，由一个私钥和一个公钥组成。其中，**公钥**是公开的，相当于传统货币交易场景中的银行账号，用来接收币特比；**私钥**仅限拥有者可见并使用，用于支付时的交易签名，以证明所有权。

#### 私钥、公钥及比特币地址之间的关系



私钥是一个随机选出的数字，通过不可逆的加密函数（椭圆曲线运算）产生一个公钥；再通过公钥，使用哈希函数生成一个比特币地址。比特币地址是由数字与字母构成的字符串，可以与任何人分享。

Transactions	
954cba57b9337acafe65ca6567f6031d68826541444ff052250c5dc1439b6e	比特币地址
No Inputs (Newly Generated Coins)	2016-05-17 06:27:53
	1KFHE7w8BnaENAswwryaooccDb6qcT6DbYY
	25.65854471 BTC
	25.65854471 BTC
717b34f7bd8f02b0989a13be55ce82bd48617acdd9b0b60f5992e8e33a95bea9	2016-05-17 06:15:23
1KjnLgQDf2X4YPVFSAYFVCXDulM6yfymYv	
	15WFx2BxYzOXfdwPQ9uDGZmHFCGIM9WEwd
	3CygFxBXIC59jHjWzhqjQxFcOp7VIDdku
	93.734 BTC
	22.265 BTC
	115.999 BTC

来源：blockchain.info，36氪研究院

## 概述·区块链

## 区块链的核心技术：分布式结构

区块链的分布式结构使得数据并不是记录和存储在中心化的电脑或主机上，而是让每一个参与数据交易的节点都记录并存储下所有的数据信息。为此，区块链系统采用了开源的、去中心化的协议来保证数据的完备记录和存储。

传播

区块链中每一笔交易信息由单个节点发送给全网所有节点。因此，信息拦截者无法通过拦截某个信息传播路径而成功拦截信息，因为每个节点均收到了该信息。另外采用非对称加密的数学原理，只有拥有该交易信息私钥才能打开信息读取内容，保证了信息安全性。

记录

区块链构建了一整套协议机制，让全网络的每个节点在参与记录数据的同时，也参与验证其他节点记录结果的正确性。只有当全网大部分节点（甚至所有节点）都确认记录的正确性时，该数据才会被写入区块。

存储

在区块链的分布式结构的网络系统中，参与记录的网络节点会时时更新并存放全网系统中的所有数据。因此，即使部分节点遭到攻击或被破坏，也不会影响这个数据系统的数据更新和存储。

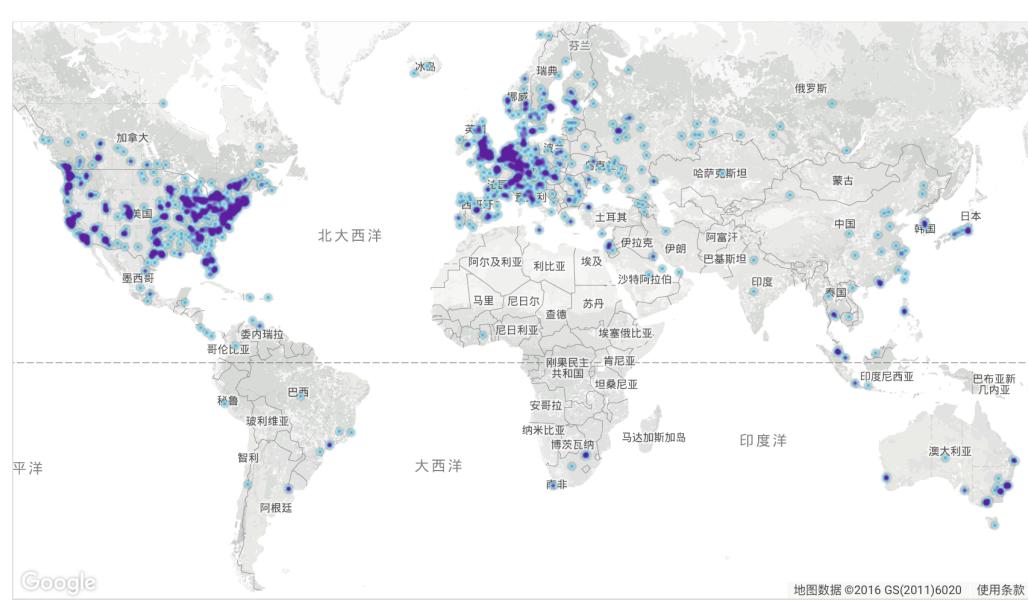
GLOBAL BITCOIN NODES  
DISTRIBUTION  
Reachable nodes as of Wed May 11 2016  
17:39:05 GMT+0800 (CST).

6318 NODES

[24-hour charts »](#)

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2177 (34.46%)
2	Germany	798 (12.63%)
3	France	455 (7.20%)
4	Netherlands	306 (4.84%)
5	Canada	274 (4.34%)
6	United Kingdom	252 (3.99%)
7	Japan	206 (3.26%)
8	Ireland	178 (2.82%)
9	Russian Federation	153 (2.42%)
10	n/a	126 (1.99%)

[More \(85\) »](#)

注释：数据截至2016年5月11日

来源：Blitnodes , 36氪研究院

## 概述 · 区块链

## 区块链的核心技术：证明机制

区块链的证明机制也就是其证明算法，通过某一种证明算法以证明区块的正确性和拥有权，以使各个节点达成共识。目前区块链的证明机制有三种：

- 工作量证明机制 Proof of work (POW)
- 权益证明机制 Proof of stake (POS)
- 股份授权证明机制 Delegated Proof-of-stake (DPOS)

其中，比特币使用的是工作量证明机制。

	POW	POS	DPOS
简介	比特币的证明机制，即通过挖矿来证明。通过与或运算，计算出一个满足规则的哈希值，即可获得本次记账权； 发出本轮需要记录的数据，全网其它节点验证后一起存储。	Pow的一种升级共识机制；根据每个节点所占代币的比例和时间，等比例的降低挖矿难度，从而加快找随机数的速度。	类似于董事会投票，持币者投票决定出一定数量的节点，代理他们进行验证和记账。
优点	完全去中心化，节点自由进出	在一定程度上缩短了共识达成的时间	大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证
缺点	目前bitcoin已经吸引全球大部分的算力，其它再用Pow共识机制的区块链应用很难获得相同的算力来保障自身的安全； 挖矿造成大量的资源浪费；共识达成的周期较长，不适合商业应用。	还是需要挖矿，本质上没有解决商业应用的痛点。	整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的。

来源：互联网，36氪研究院

可以看到，比特币使用的工作量证明机制存在几个缺陷，首先，**技术垄断和算力集导致了中心化**。因此，普通个体是不可能挖到矿，矿池则应运而生。

**其次，矿工与持币者的利益错位**。矿工不一定是比特币持有者，因此会出现“矿工利益”和“持币者利益”不同的情况。比如，“双花”的情况下，挖矿的人才会获利，而持币者利益必将受到损失。

**最后，巨大的成本消耗必将带来通胀**。目前比特币的通胀率大概为年化13%。比特币的数量是有上限的，因此随着产量减半，在价格不变的情况下，算力至少下降一半，则网络安全性就会下降。在不损害网络安全性的前提下，则有必要维持高通胀率。

## CHAPTER 2

# 区块链的行业应用

---

- 应用基础：核心优势
- 应用基础：智能合约
- 主要行业应用介绍

金融业

网络安全

身份信息管理

公证

投票

供应链

## 应用基础

### 区块链技术的核心应用优势



高效低成本  
解决中间成本问题

区块链的信任机制基于非对称密码原理，是纯数学加密方法。实现了网络中信息共享的同时，也保证了数据背后交易者的个人隐私信息。这使得区块链网络中的交易双方在陌生模式下即可进行可信任的价值交换。同时，在去中心化的网络系统中，价值交换的摩擦成本几乎为0。因此区块链技术在保证了信息安全的同时，也保证了系统运营的高效及低成本。

**应用场景：应用于传统的中心化场景中，替代原本由中介或中心机构处理的交易流程。**

**主要应用行业：金融行业，如银行、证券等。**



便于追踪和验证  
解决数据追踪及信息防伪问题

区块中包含了创始块以来所有的交易数据，且形成的交易记录不可篡改或虚构，任何网络中的数据可以追本溯源，因此交易双方之间的价值交换数据可以随时被追踪和验证。现实生活中，信息和数据在传递过程中经过多次交换会出现失真的状况，长链条的传递过程也给不法分子提供了可乘之机。利用区块链技术便可以为物品或数据简历一套不可篡改的记录。

**应用场景：数据追踪和防伪**

**主要应用行业：食品安全、奢侈品、金融及财务等**

## 应用基础

### 区块链技术的核心应用优势



数据可持续性高  
解决物联网的核心缺陷

区块链中每个参与记录和存储数据信息的节点具有相同的权利，不存在中心节点，因此在受到攻击的时候，也可以保持数据库的正常运转。同时，由于区块链技术可以使得无需信任单个节点的情况下达成这个网络的共识，使得节点与节点之间具备了能动性。此外，分布式结构也大大降低了传统中心节点设备的损耗。数据的可持续性及信息的安全性均得到了保证。

**应用场景：物联网、智慧交通、供应链等**



可编程“智能合约”模式  
有效规范市场秩序

区块链中每笔交易信息基于可编程原理，内嵌了脚本概念，使得基于区块链技术的价值交换活动升级成为可编程“智能合约”模式。因此，在市场秩序不够规范的环境下，在资产或价值转移的和合约中引入区块链的“可编程特性”，可以规定该笔交易资金日后的用途和方向。

**应用场景：各类合约**

**应用基础****智能合约：基于区块链技术的重要衍生应用**

智能合约的概念最早在1995年由多产的跨领域法律学者尼克·萨博（Nick Szabo）提出。该定义依旧适合于对区块链技术下的智能合约的理解。

**“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。”** ——尼克·萨博

**合约要素示例**

**承诺**：买家向卖家支付比特币；  
卖家向买家交付货物。

**协议**：参与方同意货款以比特币支付。选择的协议则是比特币协议，在此协议上，智能合约被实施。

**数字形式**：比特币脚本语言。

智能合约中的三个要素：

- I. **承诺**：参与方同意的权利和义务，确立合约的本质和目的。
- II. **协议**：协议是技术实现（technical implementation），在这个协议基础上，合约承诺被实现，或者合约承诺的实现被记录下来。
- III. **数字形式**：承诺写入计算机可读的代码中。只要参与方达成协定，智能合约建立的权利和义务是由一台计算机或者计算机网络执行的。

区块链技术则是提供了更好的记录及安全保障。可见，智能合约本身成为合约整个确立、管理与执行过程的参与者。

- 合约确立** ➤ 智能合约对接收到的价值和信息作出回应
- 合约管理** ➤ 智能合约临时保管价值
- 合约执行** ➤ 当满足协议的条件出现时，智能合约自动执行，输出价值和信息

**合约确立****交易**

向合约输入价值

**事件**

向合约中输入信息

**智能合约**

合约价值      合约状态

**合约执行****交易**

从合约输出价值

**事件**

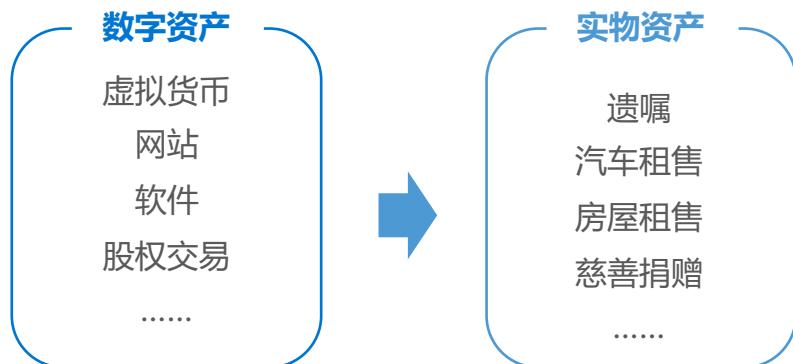
从合约中输出信息

可复制、可共享的账簿

## 应用基础

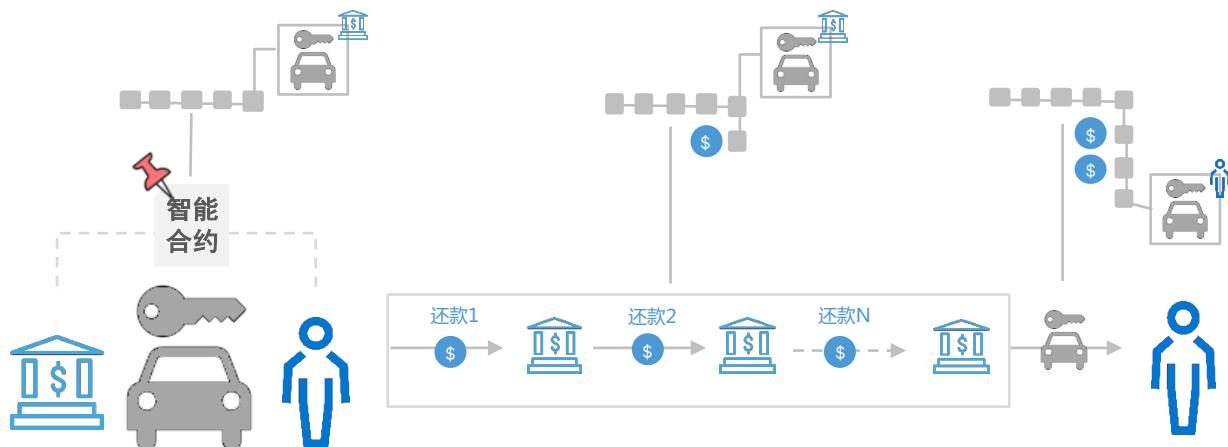
### 智能合约：从数字资产到实物资产

因为数字资产的执行容易规范、且易强制执行，因此，我们认为智能合约首先会在虚拟货币、网站、软件、云服务，以及股票交易等数字资产领域发展。随后，智能合约将向实物资产领域进行扩展。比如遗嘱执行、汽车租赁、房屋租售等。



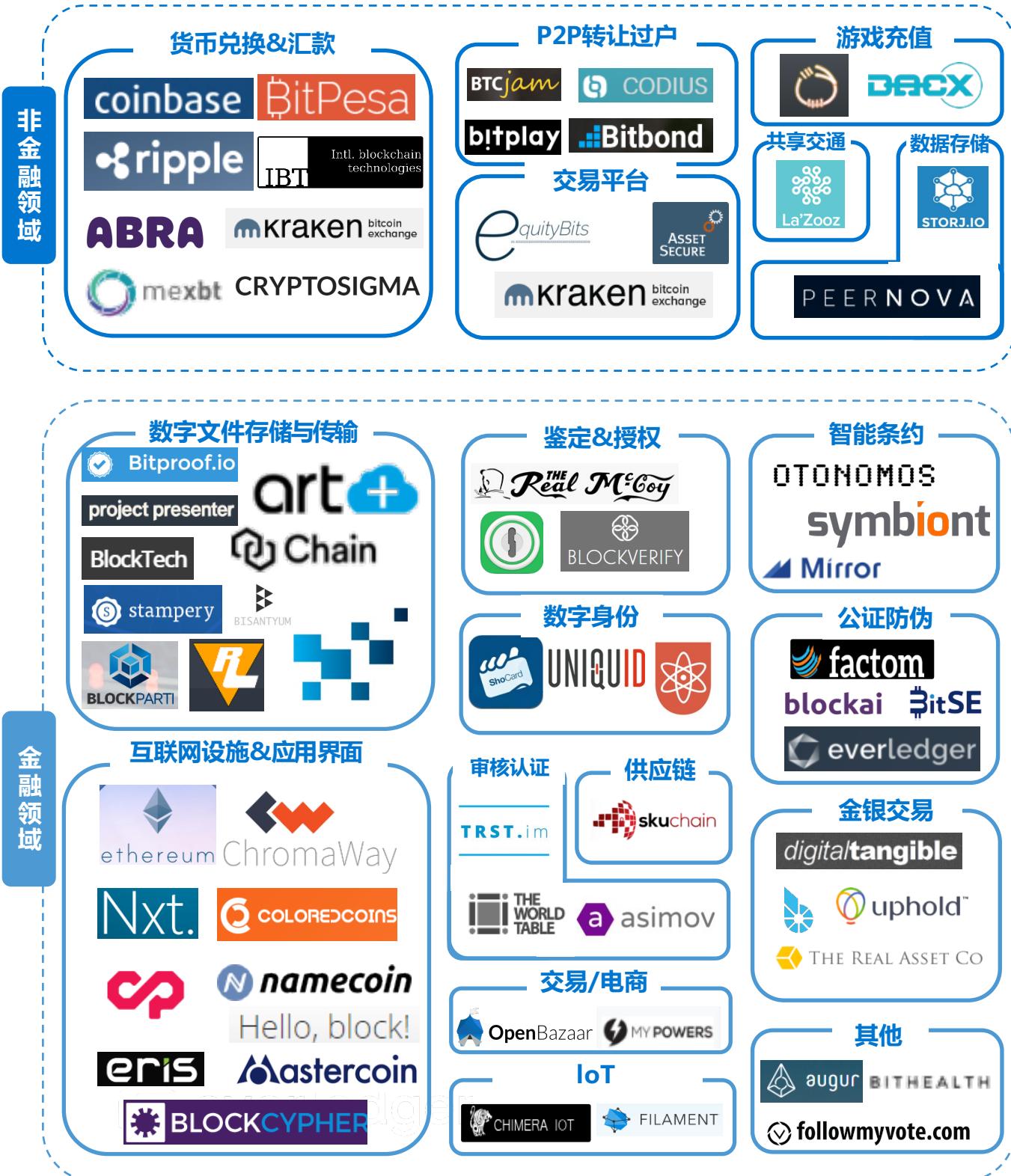
以“汽车租售”为例，简单说明智能合约的执行过程：消费者在购买汽车时，与银行或其他财务公司签订智能合约，约定消费者每月还款额及还款期限。智能合约将派发“智能钥匙”给消费者，用以启动汽车。当消费者全部偿还汽车贷款后，智能合约将自动把汽车从银行或财务公司名下转让到该消费者名下。但如果消费者不还款，智能合约将自动收回发动汽车的数字钥匙，消费者将无法启动汽车。

#### 智能合约执行流程示例



## 行业应用

### 区块链行业应用全景图 — 国外公司



注释：主要包含国外区块链/比特币相关公司，如有遗漏或错误，请联系36氪研究院；  
更多金融领域应用请查看附录

来源：公开资料，36氪研究院

## 行业应用

## 区块链行业应用全景图 — 国内公司

国内外应用类创业公司数量及类别差距较大。不同于以美国为首的国外创业、技术及监管环境，国内区块链技术应用仍处于萌芽期，应用类创业企业并不多，多数仍是比特币相关公司。区块链仍是一个“小众”的创业概念，概念虽火热，但真正试水的人却不多。

国内区块链 / 比特币公司



注释：仅包含部分国内区块链/比特币相关公司，如有遗漏或错误，请联系36氪研究院  
来源：公开资料，36氪研究院

## 行业应用

## 以去中心化、分布式存储为中心，区块链带来行业应用新前景

主要应用领域	应用前	应用后
金融业 ( 银行、支付转账、股票交易等 )	流程复杂；中心化数据存储；第三方担保	简化流程； 分布式数据存储，安全性提升； 无需第三方，降低成本
网络安全	中心服务器存储数据、转移和传递	信息传播路径改变，不可拦截
身份信息管理	银行、信用卡身份识别过程繁琐； 身份信息易被盗用	简化识别过程； 加强身份信息
公证	需要政府、公信力第三方提供背书	数学加密做信用背书，自动完成公证； 永久保存资料
投票	计票可能存在伪造； 选民身份信息保护环节较弱	过程全网公开； 选票可追溯； 选民身份保密性好
供应链	低效、产品作假、低质量风险高	供应链各环节诚信保证高； 产品信息可追溯，质量可保证

## 行业应用

### 金融业仅仅是开始，更多行业应用正在开启

#### 1. 金融业

##### • 银行

银行作为资金的安全仓库和传输枢纽，与 blockchain 作为一个数字化、安全和不可篡改的分步账簿，具备相似的功能。这意味着基于 blockchain 的颠覆式改变可能将在未来对银行产生深远的影响。据公开信息，瑞士银行和英国巴克莱银行都已经开始使用试用区块链技术，以加快后台结算功能。

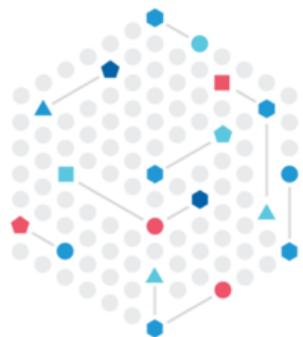
相关公司：Chain

Chain

PLATFORM ABOUT JOBS CONTACT SIGN IN

**A blockchain is more  
than a technology.  
It's a strategy.**

Chain partners with leading organizations to build blockchain networks that transform markets.



##### • 支付与转账

通过区块链技术可以绕过传统机构复杂的流程，创造一个更加直接的付款流程。因此，区块链技术可能会改变资金转移业务的体系机构。该系统能够实现跨境、无中介、低成本，且交易可以快速完成。

相关公司：Abra



## 行业应用

### 金融业仅仅是开始，更多行业应用正在开启

#### 1. 金融业

##### • 股票投资

股票购买、销售和交易的过程存在着很大可以简化的空间。区块链技术有望实现整个流程的自动化，并提高安全性和效率。

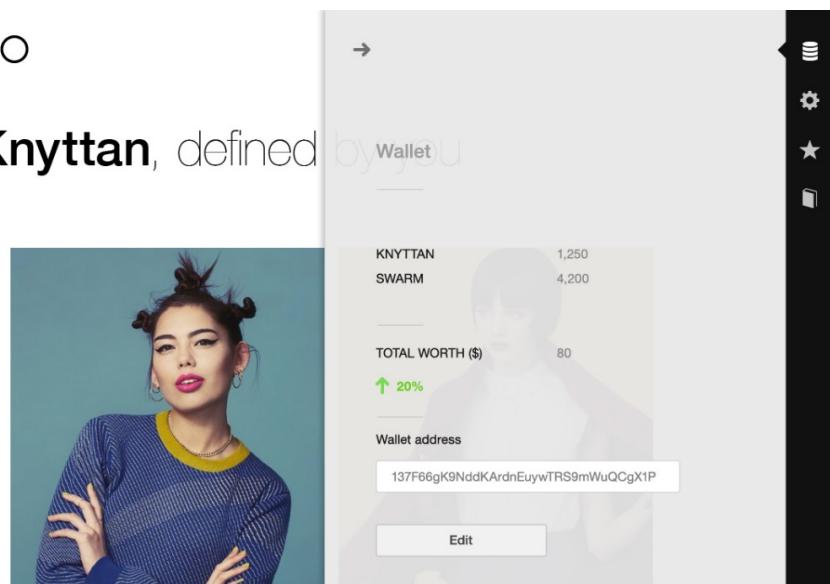
相关公司：Overstock



##### • 众筹智能合约

在股权众筹发起初期，由项目发起方、众筹平台、领投人等多方共同发起众筹智能合约，来约定各方的责任和义务。这份智能合约可以保存在区块链中，由此保证合约在履行过程中不被篡改和到期后的强力执行。

相关公司：Swarm



## 行业应用

### 金融业仅仅是开始，更多行业应用正在开启

#### 1. 金融业

- 其他

在金融服务领域，回购、债务分配及保险处理等流程均有区块链技术的相关发展。

#### 回购协议



在一个可信任的网络中，用分布式账簿替代担保品托管方及托管方制约，简化交易。

#### 债权分配



- 债权的拥有权可以追溯、保留并被监管
- 极大减少债务管理工作，增强安全性

#### 保险处理

1. 协议确认及签署
2. 自动/人工协议调整
3. 追溯丢失的文件或信息
4. 保险案件管理
5. 验证保费计算
6. 赔偿款支付流程
7. 重复付款处理

利用区块链技术保证保险处理过程的完整性，减少欺诈行为，流程化文件管理等

来源：MAGISTER Advisors, 逐鹿, 其他公开资料, 36氪研究院

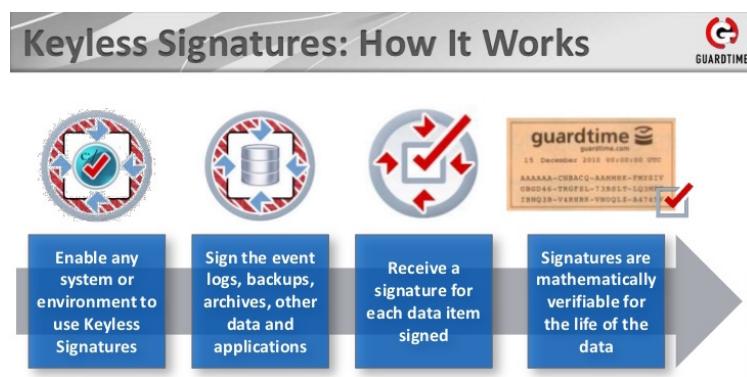
## 行业应用

### 金融业仅仅是开始，更多行业应用正在开启

#### 2. 网络安全

区块链中的分布账是公共的，并利用数学加密技术发送经过验证的数据；去中心化的方式改变了信息传播的路径，确保了数据来源的真实性，同时保证了数据的不可拦截（不可篡改或伪造）。因此，基于区块链的技术会完全改变信息的传播路径，从根本上改变信息传播路径的安全问题。

相关公司：Guardtime



#### 3. 身份信息管理

借鉴区块链非对称加密原理，可以将身份信息存储于区块链中。在需要的时候，利用密钥来证明所有者身份。用一种更安全、便捷的识别过程取代繁琐的传统银行、信用卡识别程序等。

相关公司：Shocard



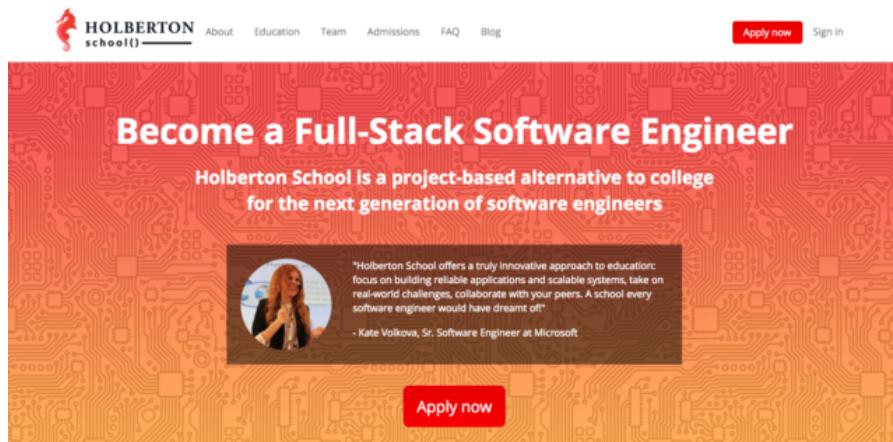
## 行业应用

### 金融业仅仅是开始，更多行业应用正在开启

#### 4. 公证

传统的公证一般是基于政府机关的信用及公信力。公证成本高、流程复杂。区块链的去中心化特征让数据资料利用数学加密来做信用背书，在没有政府机关的介入下，自动完成公证，且资料永久保留可追踪。

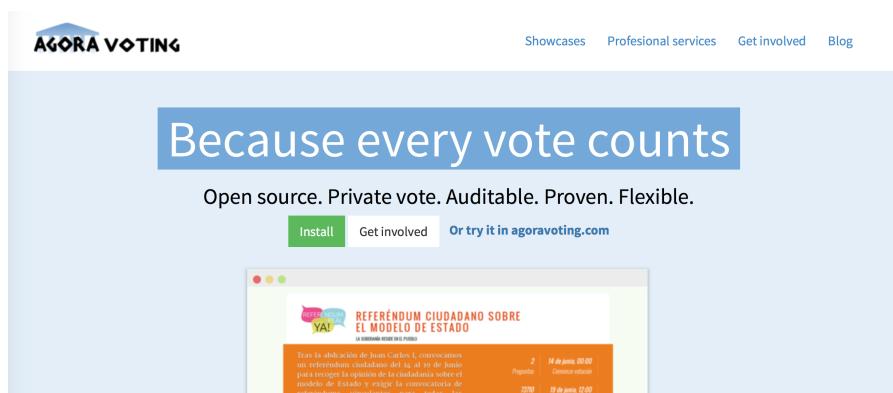
应用案例：Holberton School利用区块链技术验证学历证书



#### 5. 投票

传统的投票活动中，在计票、匿名性等环节均存在伪造和篡改的可能。基于区块链技术，则可以实时计票不间断，同时保证了投票人的身份保密。

相关案例：Agora Voting



## 行业应用

### 金融业仅仅是开始，更多行业应用正在开启

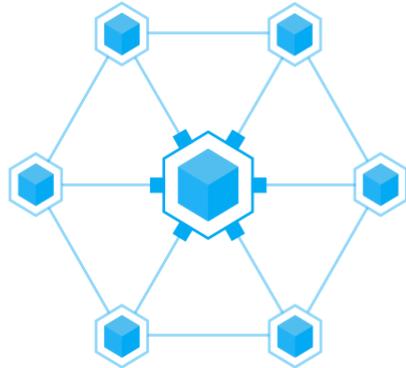
#### 6. 供应链

基于区块链技术，供应链可以通过确保产品的有效性，降低产品伪造或低质量的风险性。而通过分布式的方式来记录这些步骤，将使供应链成员变得更加诚实。

相关公司：Fluent

#### Fluent Network

Fluent is the enterprise blockchain network for financial institutions and global enterprises. Solutions and applications on the network are designed to increase efficiency, provide flexibility, and enhance collaboration across global supply chains.



## CHAPTER 3

# 区块链领域投资及典型案例介绍

---

- 全球区块链投资概况
- 典型案例介绍

Shocard : 保护身份信息的“骑士”

ABRA : 跨境支付so easy

Agora Voting : 为投票保驾护航

OpenBazaar : 去中心化的ebay

## 投资

## 2015年全球十大区块链投资机构

机构	简介
国内	万向区块链实验室 万向集团出资5000万美元成立了区块链基金，用于在全球范围内投资区块链商业应用相关的各类项目。 参投项目：以太坊
	数贝投资 数贝投资基金总金额为6亿元，是全球最大的区块链投资基金总金额中，1亿为天使基金，用于孵化具有应用前景的区块链项目，以及提高区块链安全性的矿机芯片行业；5亿为产业基金，投向有明晰商业模式的中后期区块链应用项目。 目前已投区块链领域1.8亿元。
	IDG资本 IDG主要看中区块链作为分布式总账的应用类投资。 参投项目：Ripple Labs, Koinify, Coinbase, Circle, 币行, 锐波科技, 面兑
	Andressen Horowitz 投资过Airbnb、Pinterest、Jawbone等独角兽公司，区块链领域总投资额大约2.27亿美元，约占比特币及区块链领域总投资额的1/4 参投项目：Ripple Labs, Coinbase, 21Inc, TradeBlock, OpenBazaar
	Khosla Ventures 被TechCrunch称为“巨无霸风投公司”。2015年末，Khosla募集了4亿美元用于种子期项目投资，其中部分资金将用于比特币及区块链领域。 参投项目：21Inc, Blockstream, Chain, BlockScore
	AME Cloud Ventures 其早期创业基金由雅虎创始人杨致远创建，着重投资计算的移动、传感器、云计算和大数据等技术，欲在科技领域建立其投资影响力。 参投项目：BitPay、Blockstream、Ripple Labs、Blockcypher、ShoCard
	Lightspeed Venture Partners 成立于2000年，是一家全球领域的风险投资基金，重点关注美国、以色列和中国市场。虽然近年来光速减缓了对技术投资的步伐，但是其仍是比特币领域最早涉足的风投机构之一。 参投项目：blockchain、BlockScore、Melotic，以及国内的BTCChina和巴比特
	RRE Ventures 自1994年成立以来已募集了7只基金，总额达15亿美元以上，是一家重点关注快速增长市场的风投公司。RRE于2013年起便开始了在数字货币领域的投资。 参投项目：itBit、21 Inc、BitPay、Case、Gem、Ripple Labs、Mirror、Chain
	Kuala Innovations 于2015年10月以每股1美元的价格购买了Factom公司3.64%的股份，共计40万美元。目前Factom公司的估值目前为1100万美元。 参投项目：Factom
	Boost VC 成立于2013年，一直是数字货币领域最活跃的投资者之一。Boost VC曾经声明，到2017年为止，Boost VC将投资100家比特币公司。 参投项目：Align Commerce、BlockCypher、BTCPoint、BitPagos、Reveal、Mirror

## 投资

## 2015年全球十大区块链投资机构的投资标的

公司	公司类型
Ripple Lab	数字支付公司
Coinbase	数字货币交易及钱包服务提供
21 Inc	比特币挖矿公司
TradeBlock	虚拟货币数据服务提供
OpenBazaar	去中心化商品交易市场
coinbase	比特币钱包及交易所
Circle	比特币银行
锐波科技	分布清算协议与区块链研发与应用
Blockstream	比特币侧链技术公司
Chain	区块链技术提供商
BlockScore	金融服务商，身份验证服务公司
Align Commerce	跨境支付
BlockCypher	区块链网络服务公司
Mirror	区块链智能合约
ShoCard	区块链身份解决方案
blockchain	比特币钱包提供商
BTCChina	比特币交易所
巴比特	数字货币媒体
itBit	比特币交易所
Bitpay	商户付款处理器
Case	硬件钱包工商
Gem	API专家
chain	区块链技术公司
Factom	区块链记账项目的公司

注释：未包含业务已关闭的公司；如有错误或遗漏，请联系36氪研究院  
来源：巴比特，公开资料，36氪研究院

## 典型案例

## Shocard——保护身份信息的“骑士”



Shocard旨在将区块链技术应用于电子身份验证。首次于2015年5月在TechCrunch Disrupt面市。基于区块链技术，Shocard可以改变数字身份认证的传统方式，为用户提供在登陆网银及购物时保护个人信息安全的方法。

Shocard目前已获得150万美元种子轮融资，投资人包括AME云风投、数字货币集团、Enspire资本和Morado风投。公司由前雅虎高级副总裁 Armin Ebrahimi 和Coupons.com前董事Jeff Weitzman共同成立。

## Shocard 身份验证流程



## 典型案例

## ABRA——跨境支付so easy

ABRA

ABRA成立于2014年，它通过区块链技术和共享ATM网络，让用户可以随时随地存取款，或者以更便捷的方式进行跨境汇款。

ABRA建立了一个共享ATM网络作为交易对手方，称为ABRA Teller。用户通过ABRA应用找到附近ABRA Teller并与其进行面对面转账换取比特币，如需取款则以同样方式找到ABRA Teller用比特币换回现金。期间该应用会即时生成一个基于区块链的智能合同，并由分派的对手方通过套期保值等方式保证用户的资金价值在三日内不因比特币价格的变化而发生变动。ABRA Teller可以向用户收取一定比例的费用。

ABRA于2015年9月完成1200万美元的A轮投资，投资方为Arbor Ventures、Carthona Capital、First Round、RRE Ventures。

## ABRA的工作原理

## 储蓄

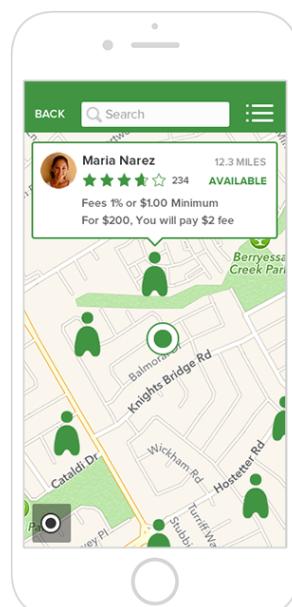
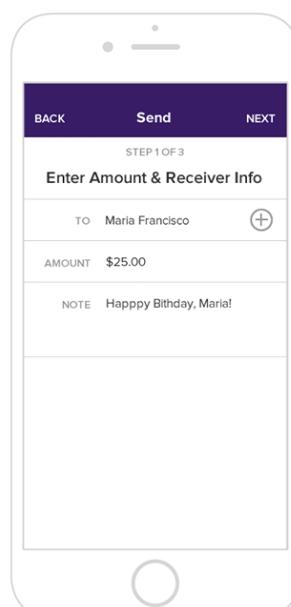
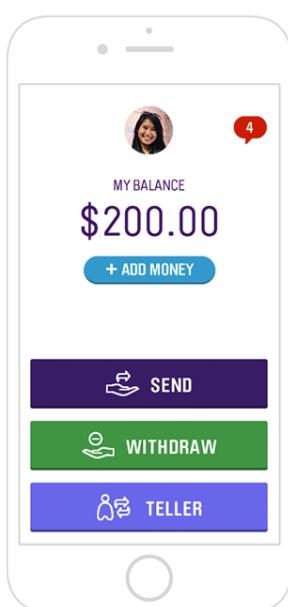
通过银行账户向ABRA钱包中充值，或通过Abra Teller用现金充值

## 支付

通过ABRA App支付或收到款项。也可以在接受Abra的商店购买商品。

## 提现

通过App寻找附近的Teller以提现，或通过银行账户提现。

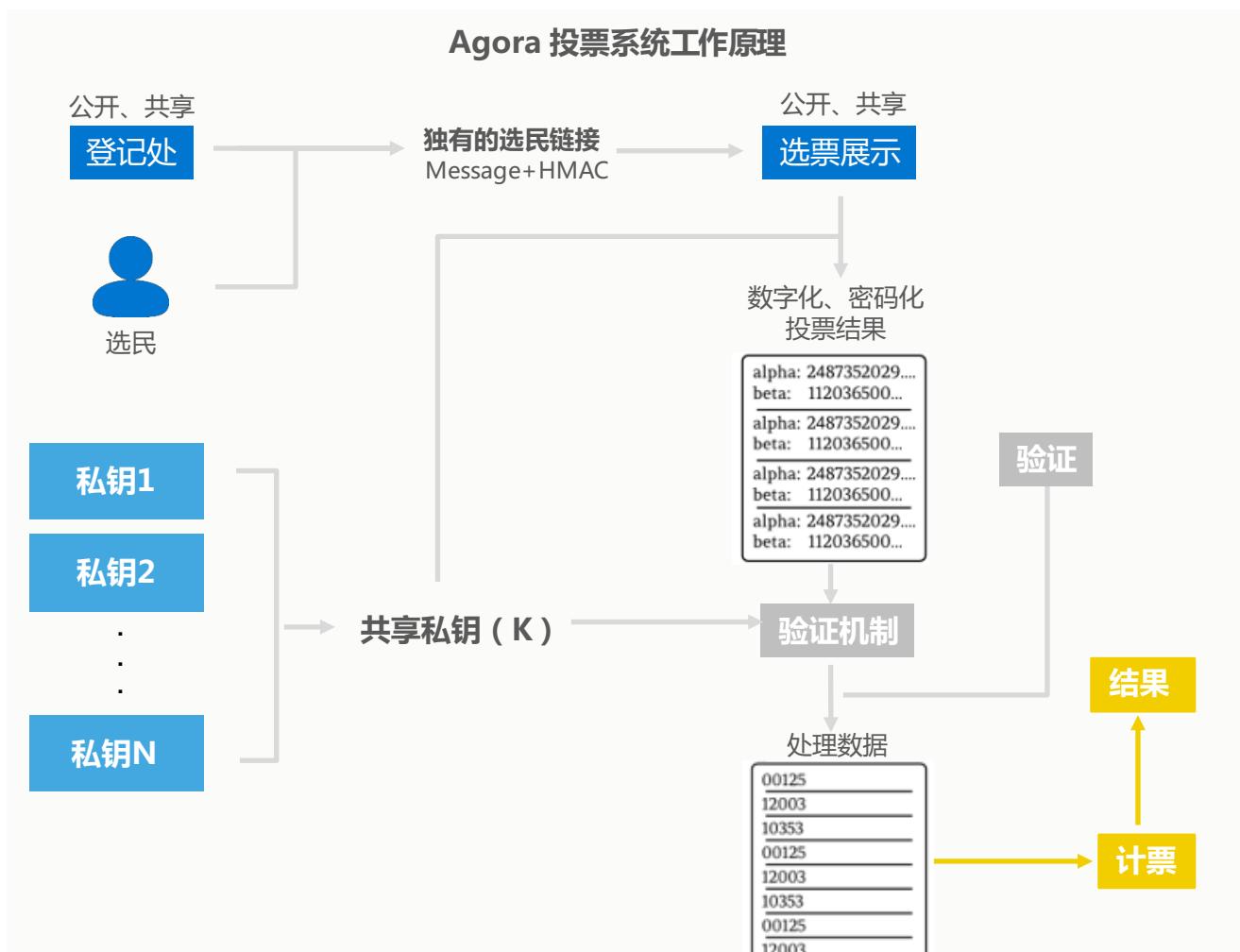




## 典型案例

## Agora Voting——为投票保驾护航

Agora Voting一家西班牙公司，提供基于区块链技术的为投票选举提供安全的解决方案。其服务涵盖整个投票过程的周期，从投票选举前的规划、到投票中的线上投票支持、最后到投票后的结果统计与报告。



### 典型案例

## Open Bazaar——去中心化的ebay



**OpenBazaar**

OpenBazaar是为线上点对点（P2P）交易创建的去中心化网络的开源项目。OpenBazaar平台上买卖双方使用比特币进行交易，没有费用，而且不会受到政府监管机构的审查。

当前，电子商务基本是使用中心化的服务。首先，部分大型电商对卖家实施严格监管，而且收取不菲的费用。其次，电商服务需要用户的个人信息，这些信息可能被窃取或者卖给其他人，用于精准投放广告或者危害更大的滥用。

OpenBazaar则可以认为是去中心化的ebay，为电子商务提供了另一途径。它把权力归还到用户手中。OpenBazaar将卖家和买家直接联系在一起，不再需要中心化的第三方来连接买卖双方。因为在交易中不存在第三方，所以不存在交易费用，没有人能够审查交易，而且公开个人信息的决定权在用户手中。

### OpenBazaar交易流程

用户A希望出售笔记本电脑



下载客户端



在客户端内创建商品目录



商品信息发送到  
OpenBazaar的分布  
式P2P网络上

- ✓ 笔记本电脑
- ✓ 单子产品
- ✓ ...

用户B搜索相关  
关键词，则可以  
查看该商品目录

接受报价

提供新报价



交易双方签署合约，  
交易完成



OpenBazaar利用双方  
的数字签名建立合约



A和B接受报价



合约同时发送给  
第三方公证人

## 附录

### 区块链金融服务应用公司及机构全景图

---

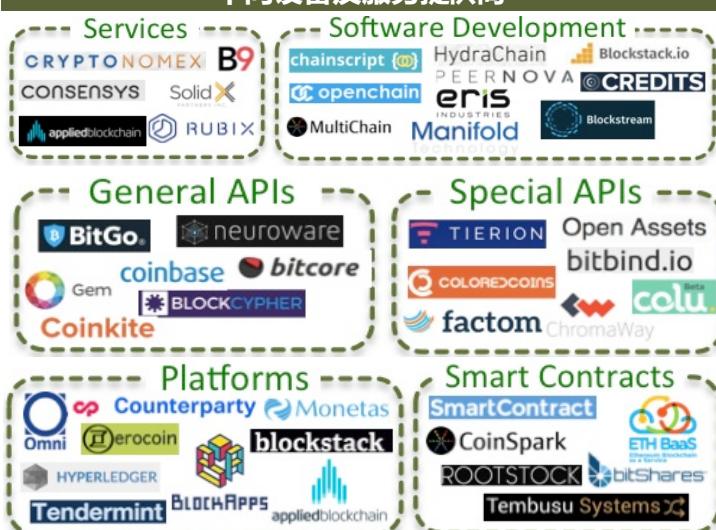
- 区块链金融服务领域应用公司全景图
- 金融机构参与区块链的应用及合作领域

## 附录

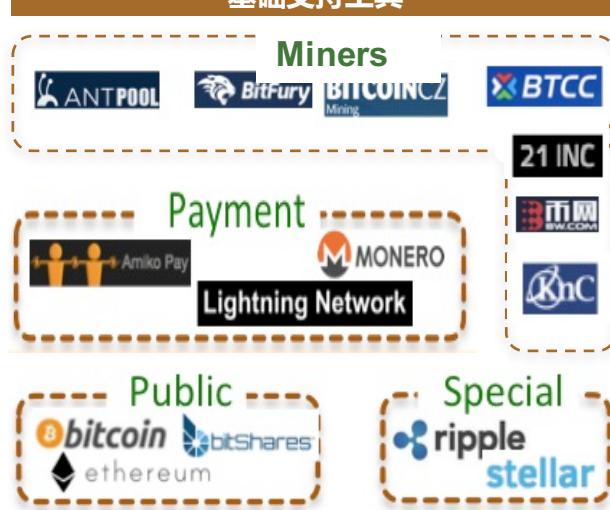
## 区块链金融服务领域应用公司全景图



## 中间设备及服务提供商

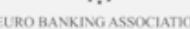
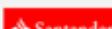


## 基础支持工具



## 附录

## 金融机构参与区块链的应用及合作领域

时间	金融机构	参与方	应用及合作领域
2013.10		  	<ul style="list-style-type: none"> <li>现金转移</li> <li>数字货币兑换</li> <li>P2P比特币交易</li> </ul>
2014.5		  	<ul style="list-style-type: none"> <li>与 Chromaway 达成 Cuber Wallet 合作关系</li> <li>现金转移服务</li> <li>数字安全</li> </ul>
2014.9			<ul style="list-style-type: none"> <li>风险管理</li> <li>跨境支付</li> </ul>
2014.10	  		<ul style="list-style-type: none"> <li>快速交易</li> <li>其他银行服务</li> </ul>
2015.1			<ul style="list-style-type: none"> <li>参与 Coinbase 的C轮融资。</li> </ul>
2015.3	 	 	<ul style="list-style-type: none"> <li><b>Barclay</b> 与 Stafello 合作运营区块链领域的创新实验室和加速器。</li> <li><b>Barclay</b> 宣布将内部进行45项实验。</li> <li><b>Federal Reserve</b> 与 IBM 合作研究数字支付系统的建立。</li> </ul>
2015.4			<ul style="list-style-type: none"> <li>建立用于全体工业产品的 “Utility Settlement” 平台。</li> <li>在 Ethereum 平台建立智能债券。</li> <li>与 BNY Mellon 合作完成某个区块链项目。</li> </ul>
2015.5	     	  	<ul style="list-style-type: none"> <li><b>USAA</b> : 追踪资产，执行实时记录</li> <li><b>Commonwealth Bank</b> : 支付确立&amp;与 ripple Labs合作。</li> <li><b>Nasdaq</b> : 建立能满足pre-IPO的支付平台&amp;与 Chain合作。</li> <li><b>DBS</b> 与 Startupbootcamp、Coin Republic 合作运行一个区块链变成系统。</li> </ul>
2015.6	  	 	<ul style="list-style-type: none"> <li><b>Santander</b> : 专注于国际支付和智能条约。</li> <li><b>Westpac &amp; ANZ</b> : 与 Ripple 合作建立低花费的跨境支付平台。</li> <li><b>Westpac</b> 参与 Coinbase 的投资。</li> </ul>

## 附录

## 金融机构参与区块链的应用项目及合作领域

时间	金融机构	参与方	应用项目及合作领域
2015.7	Deutsche Bank  SOCIETE GENERALE BNP PARIBAS Standard Chartered	-	<ul style="list-style-type: none"> <li><b>Deutsche</b>：支付、法定货币交割、资产注册、衍生品合约、监管报告支付、KYC、AML注册和交易后服务的提升。</li> <li><b>Citibank</b>：建立3个独立的Citi内部系统，部署区块链技术。建立与 Bitcoin 等价的 Citicoin。</li> <li><b>Societe Generate</b>：雇佣员工时开始参考BTC、区块链与加密电子货币领域的专家意见。</li> <li><b>BNP Paribas</b> 发现通过区块链的更快的交易方式</li> <li><b>SCB</b>：CIO表明可以利用区块链在降低成本的同时提升交易透明度。</li> </ul>
2015.9	Bank of America	R	<ul style="list-style-type: none"> <li><b>Bank of America</b>：申请了关于“运用电汇的加密电子货币的系统和方法”的专利。</li> <li>9家银行在九月中旬开始合作，依据 R3CEV 建立区块链技术的统一标准。截止9月，共计22家银行加入。</li> </ul>
2015.10	NASDAQ 	R	<ul style="list-style-type: none"> <li><b>Nasdaq</b> 披露了基于区块链的新平台，平台将有助于促进其在非公开市场上资产的转移与销售。</li> <li><b>Visa</b>：和 DocuSigh 的合作，将利用比特币区块链来记录某些合约的信息。</li> <li>3家银行加入 R3CEV 结合体，银行总数已达到25家。</li> </ul>
2015.11	Citi NASDAQ  Visa Europe Collab	chain epiphyte R	<ul style="list-style-type: none"> <li><b>Citi 和 Nasdaq</b> 投资Chain.com。</li> <li><b>Nasdaq</b> 宣布将在Estonia建立基于区块链的应用。</li> <li><b>RBC</b> 宣布将在2015年内发起一项基于区块链的可信赖型项目。</li> <li><b>Visa Europe</b> 宣布将与 Epiphyte 达成合作。Epiphyte 是即时金融交易领域的一家区块链SaaS服务供应商。</li> <li>5家银行加入 R3CEV 结合体，目前银行总数已达30家。</li> </ul>



为创业者提供最好的产品和服务