

Blockchain

区块链是什么？

从1.0到3.0行业发展窥探

谢洪波Bony

2018-2-3

第一部分 区块链1.0 比特币的发明和发展

第二部分 区块链2.0 区块链代币经济的发展

第三部分 区块链3.0 区块链技术的应用和普及

第一部分 区块链1.0

比特币的发明和发展

第一章：比特币的简介及区块链入门

第二章：比特币的有什么价值？

第三章：比特币行业发展情况

第四章：比特币的一些行业数据

第一章：比特币的简介及区块链入门

1.1 比特币的诞生

➤ 2008年11月1日

一个化名中本聪 (Satoshi Nakamoto) 的人，在密码学论坛的邮件组中贴出了一篇研究论文：

《Bitcoin: A Peer-to-Peer Electronic Cash System》

(比特币：一种点对点的电子现金系统)

➤ 2009年1月3日

中本聪在自己的服务器上挖出了比特币第一个创世区块，并在第一个区块中写入这样一句话：

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

“财政大臣站在第二次救助银行的边缘” ，

——这句话正是泰晤士报当天的头版文章标题。



1.2 比特币的诞生理论基础

- 亚当·贝克 (Adam Back) 是一位英国的密码学家，1997年，他发明了**哈希现金** (hashcash)，其中用到了**工作量证明机制** (proof of work)。这个机制的原型是用于解决互联网垃圾信息问题的。工作量证明机制后来成为比特币的核心要素之一。
- 哈伯和斯托尼塔 (Haber and Stornetta) 在1997年提出了一个用**时间戳的方法**保证数字文件安全的协议，这个协议成为比特币区块链协议的原型。
- 戴伟 (W Dai) 是一位兴趣广泛的密码学专家，他在1998年发明了B-money，B-money强调**点对点的交易**和**不可更改的交易记录**。不过在B-money中，每台计算机各自单独书写交易记录，这很容易造成系统被账本的不一致。戴伟为此设计了复杂的奖惩机制以防止作弊，但是并没有能从根本上解决问题。中本聪发明比特币的时候，借鉴了很多戴伟的设计，并和戴伟有很多邮件交流。
- 哈尔·芬尼 (Hal Finney) 是PGP公司的一位顶级开发人员，也是密码朋克运动早期和重要的成员。2004年，芬尼推出了自己版本的**电子货币**，在其中采用了可重复使用的**工作量证明机制 (RPOW)**。哈尔·芬尼是第一笔比特币转账的接受者，在比特币发展的早期与中本聪有大量互动与交流。由于身患绝症，哈尔·芬尼已于2014年去世。
- 弗里德里希·冯·哈耶克 (Hayek)，20世纪最伟大的经济学家之一，1974年诺贝尔经济学奖获得者。以坚持自由市场资本主义、反对社会主义、凯恩斯主义和集体主义而著称，哈耶克宣称：货币非国家化是货币发行制度改革根本方向，由私营银行发行竞争性的货币（即**自由货币**）来取代国家发行垄断性的货币是理想的货币发行制度。因此，他的这一主张称之为“货币非国家化”或“自由货币说”。

1.3 中本聪的贡献

- 发明比特币，代码完善，运行至今无漏洞。
- 开源比特币，让大家接受并形成共识。
- 成名后隐身，使得比特币真正去中心化。
- 手握巨额比特币，从未卖出过比特币，从未从市场中获利。



疑似中本聪照片

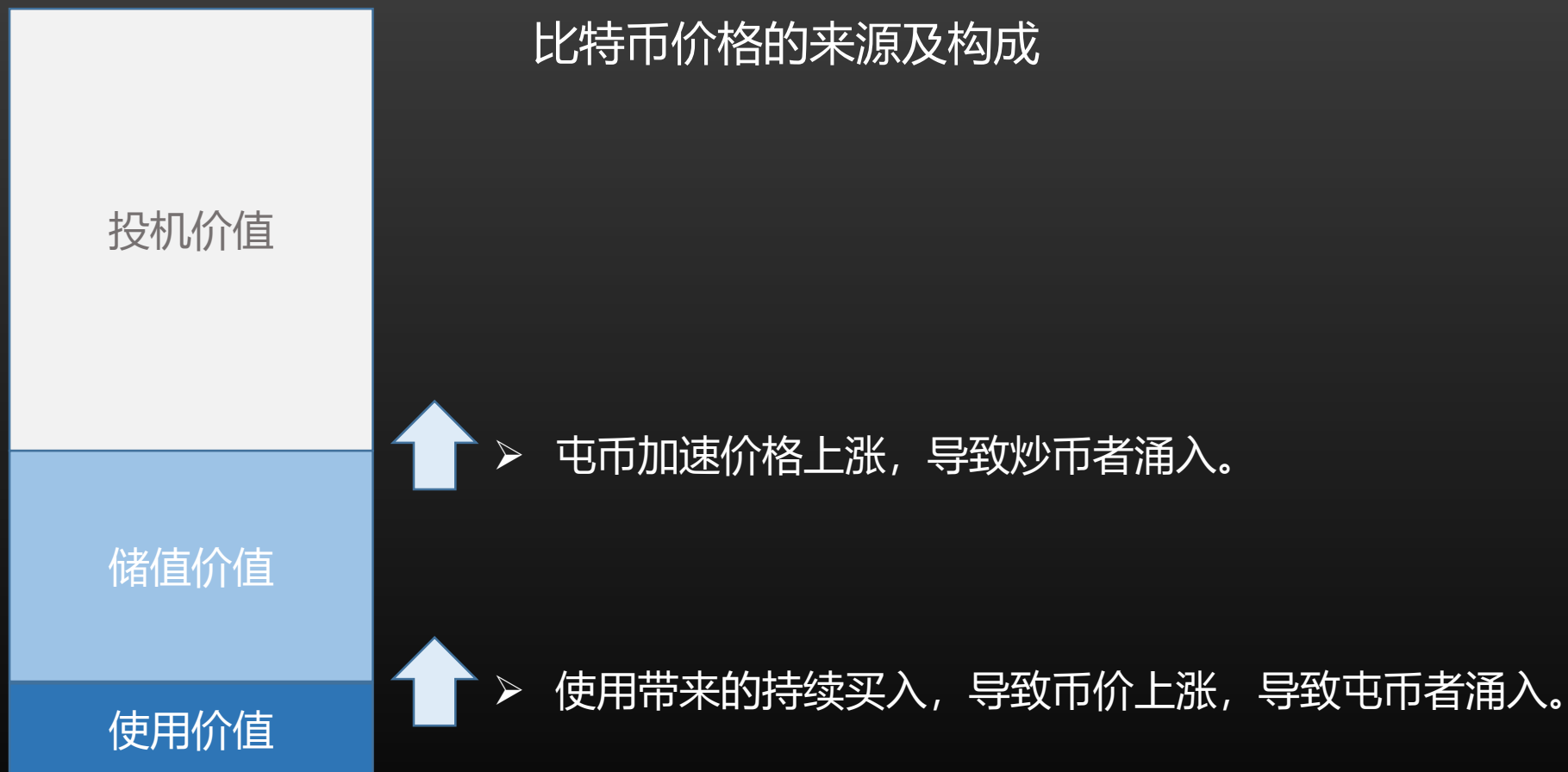
1.4 比特币是如何运行的？

八个问题理解 比特币 运行和交易

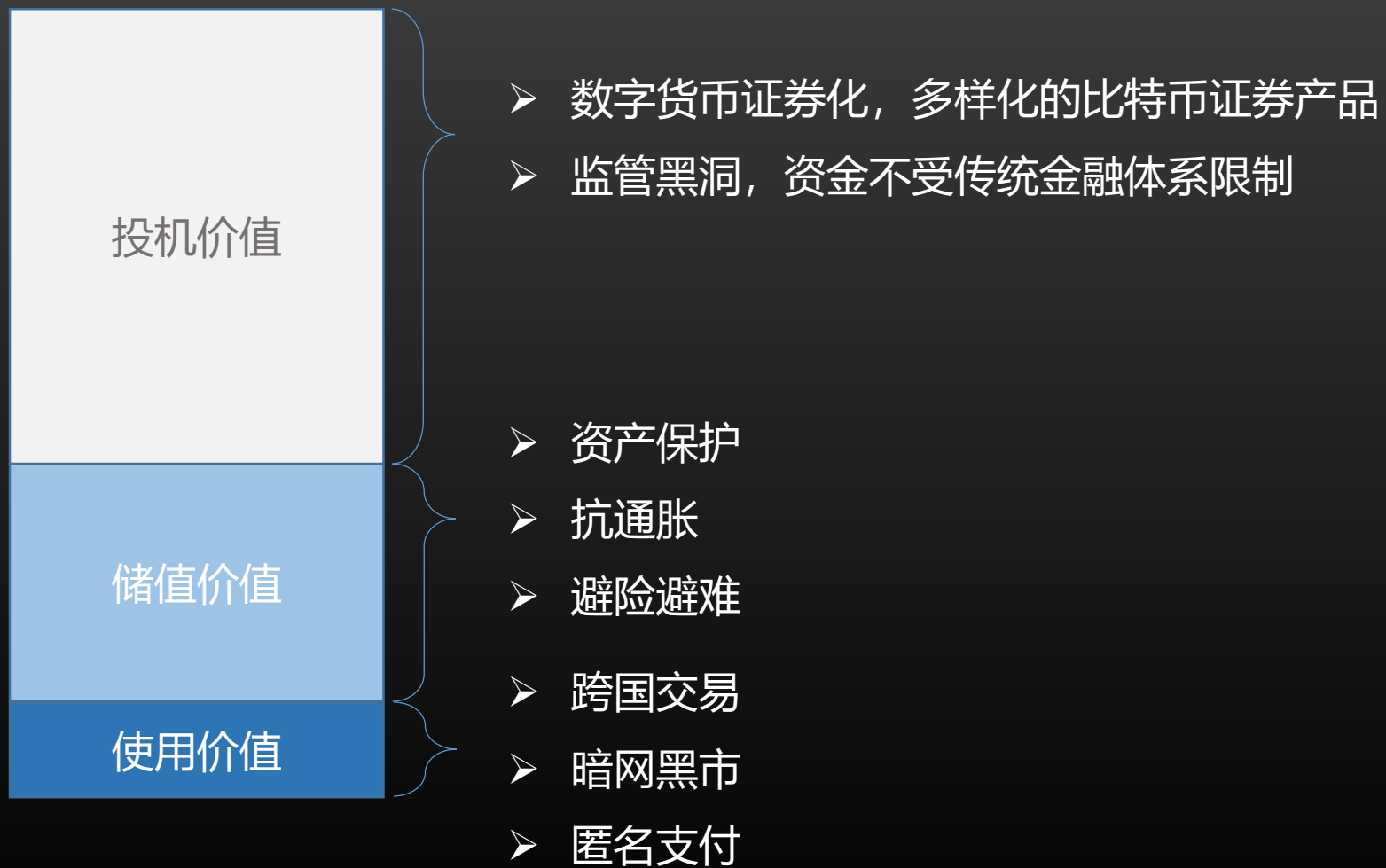
1. 身份问题：公钥（地址）--私钥（密码）
2. 认账问题：代码开源，交易共识
3. 账本保管问题：去中心化节点，新区块实时同步
4. 不可复制问题：只存在一条所有人都认可的主链
5. 确认交易问题：记账需6个节点确认
6. 记账激励问题：通过工作量证明POW，获得比特币区块奖励
7. 通胀问题：总量恒定2100万，每四年奖励减半
8. 51%攻击问题：挖矿难度调整机制

第二章：比特币的有什么价值？

2.1 比特币价值构成



2.2 比特币有什么价值？



2.3 政商学对比特币的看法

加密货币存在着严重的风险，包括洗钱，逃税和资助恐怖主义。

——俄罗斯总统普京

没有结论 - 不赞成/不拒绝。要知道当纸币代替黄金时，人们也对此持怀疑态度。

——高盛集团CEO 劳埃德·布兰克费恩

比特币的火热与近期媒体反复推断全球经济将不景气有关，而它的价值又比传统金融产品更容易被炒作。炒比特币虽然风险巨大，但我们从来不缺投机者。作为一个新兴的金融投机工具，比特币会长时间与我们相伴。

——哈佛大学公共政策与经济发展教授 Chris Robert

比特币易于储存、难于盗窃、难于造假的特性赋予其巨大价值，但由于比特币的供给量有限而且已知，所以它注定无法成为货币的有效替代物。另外，它显然没有任何使用价值，这一切将使之彻底覆灭。

——美国联邦贸易委员会前经济学家 Robert McMillan

比特币的火热和黄金走俏一样，都是我们在量化宽松时代对法定货币信任度降低的表现。比特币最大风险在于，政府可能会采取干预措施，摧毁这种法定货币的替代品。但假如一个主权国家也发行这种基于算法的货币呢？是否会把法定货币逐出市场？

——《经济学人》杂志资深编辑 Matthew Bishop

比特币有可能会崩塌，但只要是货币就必须接受考验，所有的货币都在经历存在危机。真正的问题不在于比特币是否会经历坎坷、暴跌，以及人们的疯狂，而是它能否在这场不可避免的考验中生存下去。如果能，即使以非常低的价值生存下来，它也将改变我们对价值储存手段、金融，乃至虚拟经济独立性的看法。

——弗吉尼亚大学达登商学院教授 Peter Rodriguez

2.3 政商学对比特币的看法

怀疑者	姓名	职位	评价	时间	价格	支持者	姓名	职位	评价	时间	价格
	Jamie Dimon	摩根大通总裁 CEO, JPMorgan	“它是个骗局 It's a fraud”	2017.9.12	\$ 4,148		Christine Lagarde	国际货币基金组织总裁 Managing director, IMF	“我觉得反对虚拟货币是不明智的 I think it may not be wise to dismiss virtual currencies.”	2017.9.28	\$ 4,185
	Robert Shiller	耶鲁大学金融教授， 诺贝尔奖经济学家 professor, Yale	“最好的泡沫案例就是比特币 The best example [of a bubble] right now is bitcoin”	2017.9.5	\$ 4,422		Mark Carney	英格兰银行行长 Governor, Bank of England	“让金融系统变得更加抗风险 Potential to enhance resilience”	2016.6.17	\$ 748
	Warren Buffett	伯克希尔哈撒韦公司 总裁 CEO, Berkshire Hathaway	“比特币不是货币 Bitcoin is not a currency”	2014.5.3	\$ 437		James Gorman	摩根斯坦利总裁 CEO, Morgan Stanley	“不单单是一个噱头 More than just a fad”	2017.9.27	\$ 4,209
	Ben Bernanke	前美联储主席 former chairman, US Federal Reserve	“比特币有严重的问题 Bitcoin has serious problems”	2015.11.19	\$ 326		Arthur Levitt	前任美国证监会主席 Former commissioner, SEC	“我不知道是比特币还是以太坊，但他们一定会存在 I don't know whether it will be bitcoin or ethereum ... But it's here to stay”	2017.9.14	\$ 3,226
	Vitor Constancio	欧盟央行副行长 vice president, European Central Bank	“比特币类似郁金香泡沫 Bitcoin is a sort of tulip”	2017.9.22	\$ 3,603		Larry Summers	前美国财政部长 former US Secretary of the Treasury	“一个非常重要的想法 A very important kind of idea”	2015.2.12	\$ 222
	Ray Dalio	桥水对冲基金创始人 founder, Bridgewater Associates	“比特币是一个泡沫 Bitcoin is a bubble”	2017.9.19	\$ 3,897		Vikram Pandit	前花旗银行总裁 former CEO, Citi	“有改变世界的潜力 Have the promise to change the world”	2014.11.17	\$ 386
	Howard Marks	橡树基金共同主席 co-chairman, Oaktree	“他们不是真实的事物...一个毫无原由的热潮 They are not real..Nothing but an unfounded fad”	2017.7.26	\$ 2,550		Haruhiko Kuroda	日本央行行长 governor, Bank of Japan	“有潜力极大改变整个金融服务的体系 May have the potential of significantly changing the structure of financial services”	2016.8.23	\$ 581
	Paul Krugman	纽约市大学教授 professor, City University of New York	“比特币是恶魔 Bitcoin is evil”	2013.12.28	\$ 730		Aswath Damodaran	纽约大学金融教授，金融估值的权威 Professor, New York University,	“加密货币替代了黄金 Cryptocurrencies have taken the role of gold”	2017.7.18	\$ 2,328
							Ravi Menon	新加坡金融管理局局长 MD, Monetary Authority of Singapore	“很有可能是颠覆性的变革 Potentially transformative”	2015.6.29	\$ 256
							Abby Johnson	Fidelity 总裁， 全球最大共同基金 CEO, Fidelity	“我相信比特币 I'm a believer”	2017.5.23	\$ 2,291
							Blythe Masters	数字资产总裁 CEO, Digital Asset Holdings	“就像钱变成电子邮件 It's analogous to email for money”	2015.8.31	\$ 230

➤ 支持者VS怀疑者

其中最著名的反对者郎教授

“比特币是炒作泡沫，比特币有价格无价值”

——郎咸平



2.4 比特币的价值来源

1776年《国富论》（亚当·斯密）

尊敬的先生，你号称经济学能让我们的国家变得更富裕。

可是纺织女工织布，农夫耕作。

你一不织布、二不耕地，请问你创造的财富，从何而来？

陛下，财富来自交易

经济学第1定律：交易创造财富

交易越多，社会的财富越多

电报有价值：把 **信息** 从一处运到另一处

银行有价值：把 **资金** 从一处运到另一处

互联网有价值：把 **信息** 从一处运到另一处

比特币有价值：把 **资金** 从一处运到另一处

互联网: **信息** 全球自由流动
比特币: **货币** 全球自由流动

信息+货币=交易

求帮助--关于比特币的问题

只看楼主

已收藏

回复



楼主

红尘恋星

BTC小黑

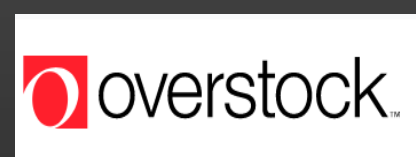


我公司是不接受比特币的。但是今天美国老客户再次问我能不能用比特币交易，差的钱他会在下次不过来。西联和速汇金的限制都太多了。。。

- 1.他怎么将比特币给我？代码吗？
- 2.在中国不管多少都能马上卖出并且体现人民币么？

谢谢！

目前接受比特币支付的网络服务商



在香港、美国、加拿大、澳大利亚出现的比特币ATM机：



在日本有近5000家超市，商店接收比特币支付，预计在2018年超过27万家。



经济学第0定律：自由创造交易

限制越少，交易越多

法币是政府垄断的一种商品

垄断导致资源错配与低效

政府难以抑制放水的冲动

凯恩斯主义

不愿被收通货膨胀税怎么办？

哈耶克：货币自由竞争

1974年诺贝尔经济学奖得主：《货币的非国家化》

奥派经济学

于是就有了比特币

去中心化的，总量恒定的数字加密货币

那是什么承载着他的价值？

其实是**共识**

当社会认同一个物体能够承载多少价值时，这个物体就承载了相应的价值。

关于比特币的两句广告语

1

比特币在人类历史上第一次用技术手段保证了私有财产神圣不可侵犯。

2

Long bitcoin, Short the world.

第三章：比特币行业发展情况

比特币的生态圈



主要公司一览

交易所

现货交易 >

 Bithumb  Korbit  Coinone  KEX  Bitfinex  Poloniex  bitFlyer  Kraken  BITTREX

 Coincheck  Bitstamp  Yobit  Cex.io  OKCOIN  KuCoin  Quoinex  coinbase  UPbit

期货交易 >

 BitMEX  HitBTC  EtherDelta  zaif  EXX

币币交易 >

 Bibox  CoinTiger  Liqui  OKEX  ZB.COM  币安  AEX  LBANK  OEX  Gate.io

 Dragonex  币赢网  ALLcoin  币牛网  withbtc  HB.top  BigONE  Hashtoken

场外交易 >

 LinkCoin  Huobi  eBTCbank  Bit-Z  Coinbene  BitcoinWorld  Localbitcoins  itBit

 Remitano  CoinCola  BITIG比特爱鸽

主要公司一览

钱包及支付



钱包



主要公司一览

行情、资讯、数据、工具



行情



BitcoinWisdom



Bitcoincharts



Cryptowatch



AlCoin



币看



行业媒体



金色财经



CoinDesk



Cointelegraph



BTC123



Cryptocoinsnews



Newsbtc



Bitcoinist



Forklog



Abitco



Bitcoin.com



挖币网



链之家



块讯



工具



BTC



Etherechain



比特币全球流向图



CoinMarketCap



Exchange War



ETHFANS



Blockchair



IOTA



Tether



block123

浏览器 >



Etherscan



bitbank



Ripple



Dash



区块



小蚁



NEM



Qtum



Asch



井通

主要公司一览

挖矿、矿池、矿机

⚡ 矿业	
矿池	⚡ 蚂蚁矿池  BTC矿池  国池  F2Pool 鱼池  BTC.TOP  ViaBTC  SLUSHPOOL  BitClub
	 BIXIN  BitFury  GBMiners  1Hash  BATpool  Bitcoin-india  Ethermine  Nanopool
矿机	 蜂窝矿机  熊猫矿机 蚂蚁矿机 (BITMAIN) 阿瓦隆矿机 Bitfury矿机
云算力	 Hashnest  币网

挖矿行业与比特币网络

比特币怎么来的？

比特币挖矿则是在追逐账本的记账权！

矿工：比特币网络的守护神

矿工通过不断的运算，解出新区块答案的人拥有区块的记账权，并获得比特币奖励

奖励办法：工作量证明 = 空块奖励 + 交易手续费

这个奖励机制叫做工作量证明，即POW：Proof of work

比特币目前的生产情况

16,824,762枚
(截止至18年1月25日)

目前新区块奖励
12.5个BTC

下一次减半时间
2020年

矿池及全球分布

矿池实时算力

[更多](#)

				24小时变化	3天幸运值
1	BTC.com		4276.00 PH/s	2.76%	110.98%
2	AntPool		3628.18 PH/s	1.94%	104.94%
3	ViaBTC		2320.28 PH/s	-1.79%	97.95%
4	SlushPool		2010.54 PH/s	-	-
5	BTC.TOP		1515.00 PH/s	-21.34%	91.33%
6	F2Pool		910.43 PH/s	-	-
7	BTCC		562.01 PH/s	1.16%	81.02%
8	BitClub		405.94 PH/s	-5.45%	169.87%
9	BitFury		379.35 PH/s	-	-
10	GBMiners		263.00 PH/s	-4.71%	13.68%
11	BW.COM		201.44 PH/s	-1.89%	101.41%
12	58COIN		189.67 PH/s	-	-



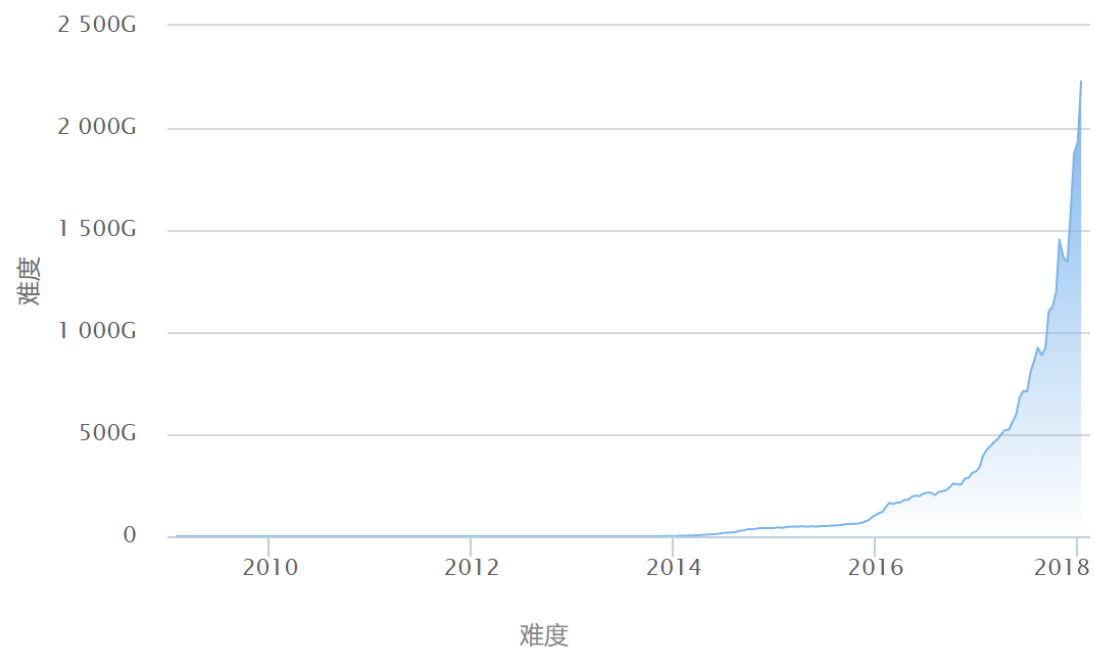
全网算力及难度数据

全网算力

19.87 EH/s

全网难度

2,227,847,638,503 - 2.23 T

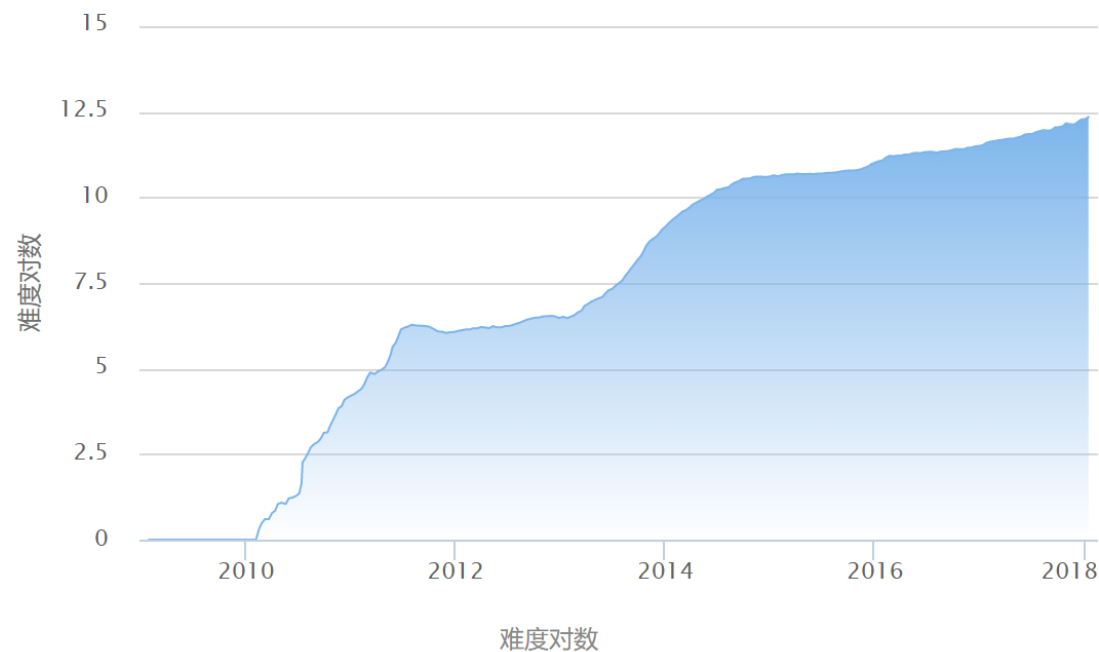


预测下次难度

2,590,196,814,964 - (+16.26%) 2.59 T

距离调整还剩

0 天 4 小时



此时此刻大约有150万台蚂蚁S9矿机正在联网挖矿 (截止至18年1月25日)

矿机和矿场



蚂蚁矿机L3+ 504M

发货时间：11月1日-11月10日

¥ 13700 CNY



蚂蚁矿机S9 14T

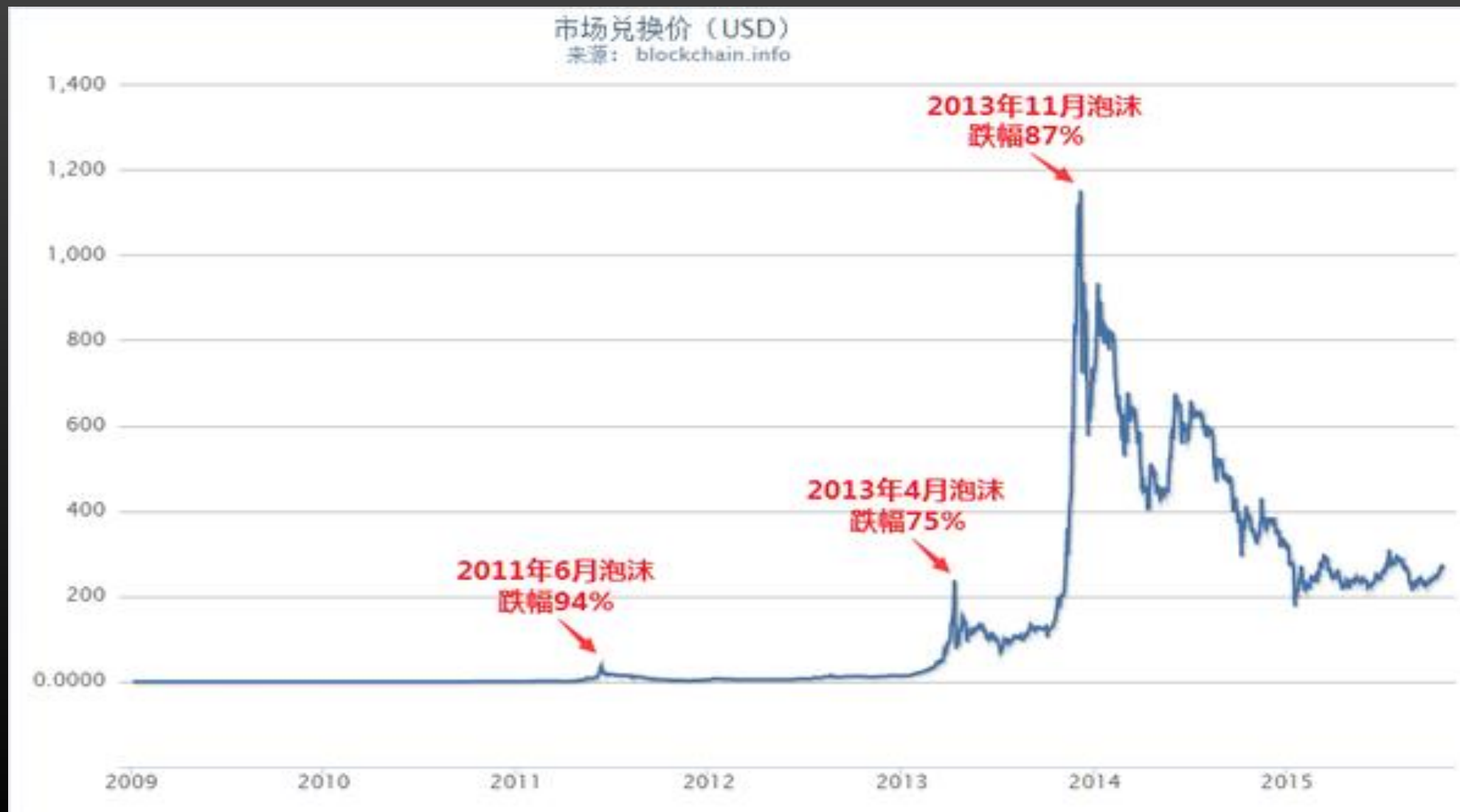
发货时间：11月1日-11月10日

¥ 9440 CNY



第四章：比特币的一些行业数据

2009-2015年价格走势



2013-2018年价格走势

Bitcoin Charts



比特币的活跃地址数（用户）



梅特卡夫定律 (Metcalfe's Law) 指出：

网络的价值与联网的用户数的平方成正比

网络使用者越多，价值就越大。

如果一个网络对网络中每个人价值是1元，那么规模为10倍的网络的总价值等于100元；规模为100倍的网络的总价值就等于10000元。网络规模增长10倍，其价值就增长100倍。

*梅特卡夫定律是一种网络技术发展规律，梅特卡夫定律是3Com公司的创始人，互联网先驱。

比特币网络的价值衡量（泡沫指数）



第二部分 区块链2.0

区块链代币经济的发展

ICO

IFO

Token

第一章：什么是ICO？

第二章：为什么会出现IFO？

第三章：Token代币经济的正反面

第一章：什么是ICO？

什么是ICO?

ICO:

首次代币发行
Intial Coin Offering

IPO:

首次公开发行
Intial Public Offering

- ICO是一种区块链行业术语，是一种为加密数字货币/区块链项目筹措资金的常用方式，早期参与者可以从中获得初始产生的加密数字货币作为回报。
- ICO的发起时间通常在项目完成之前，募集的资金用于创始团队的开发工作，帮助项目顺利发布，并投入相应的资金进行市场推广工作。
- ICO参与者有助于项目的成功。他们可以帮忙进行宣传，组建更大的社区，让更多的人认识这个新项目。并希望项目发布之后，代币价格会高于ICO期间的价格来获利。

ICO与IPO的异同

1.融资的主体不同

ICO融资的主体一般是基金会或非盈利组织，由基金会发起项目。IPO的对公司主体有严格的规定，满足一定要求的成熟企业才能上市。。

2.融资主体所处的阶段不同

ICO融资的项目一般处于概念期，一份白皮书，一个项目团队，一个项目发展计划，就可以进行ICO融资。没有对利润，对业绩，对市场规模等方面有任何要求。

3.投资拿到权益物不同

ICO投资人拿到是数字的代币，IPO投资人拿到的是股票，具体股东的相关权利。

4.投资使用的货币不同

IPO和股权众筹都是使用法币进行投资，ICO一般采用比特币或者以太坊等虚拟数字货币进行投资。这也规避了一些监管。

5.法律定位上不同

ICO目前处于监管空白，法律定位还不明确。IPO和股权众筹已有监管。比如中国的《证券法》、美国的《JOBS法案》等。

ICO与IPO的异同

6.投资主体范围不同

人人都可以参与ICO投资，没有任何限定，而IPO、股权众筹在监管上对投资人有相关限制。

7.ICO与股权众筹的差异性

ICO很多人把它当成股权众筹的2.0版本，但是股权众筹在流通性上跟ICO数字货币相比有非常大的劣势，股权众筹在没有IPO之前都依赖于场外交易。交易变现的周期长，流通慢，在情况好的时候等待公司上市至少也得6-7年。ICO的流通从投资到退出快的可以在几周内完成，这期间还可以翻几倍的回报。

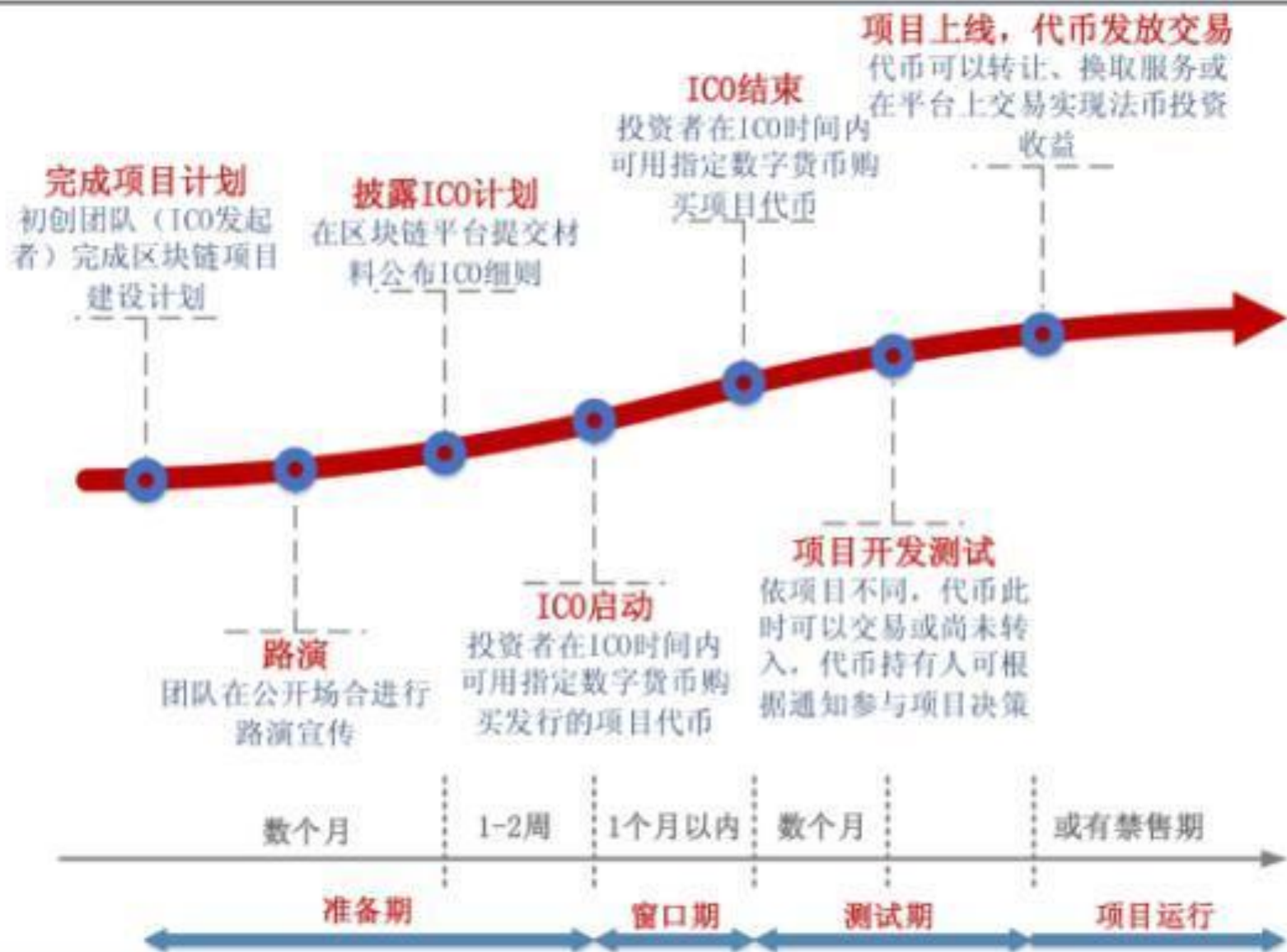
8.服务中介机构不同

目前ICO还没有服务中介机构，IPO则依赖于证券经纪商等。

9.产权归属不同，IPO主要是针对所有权，ICO针对的是使用权

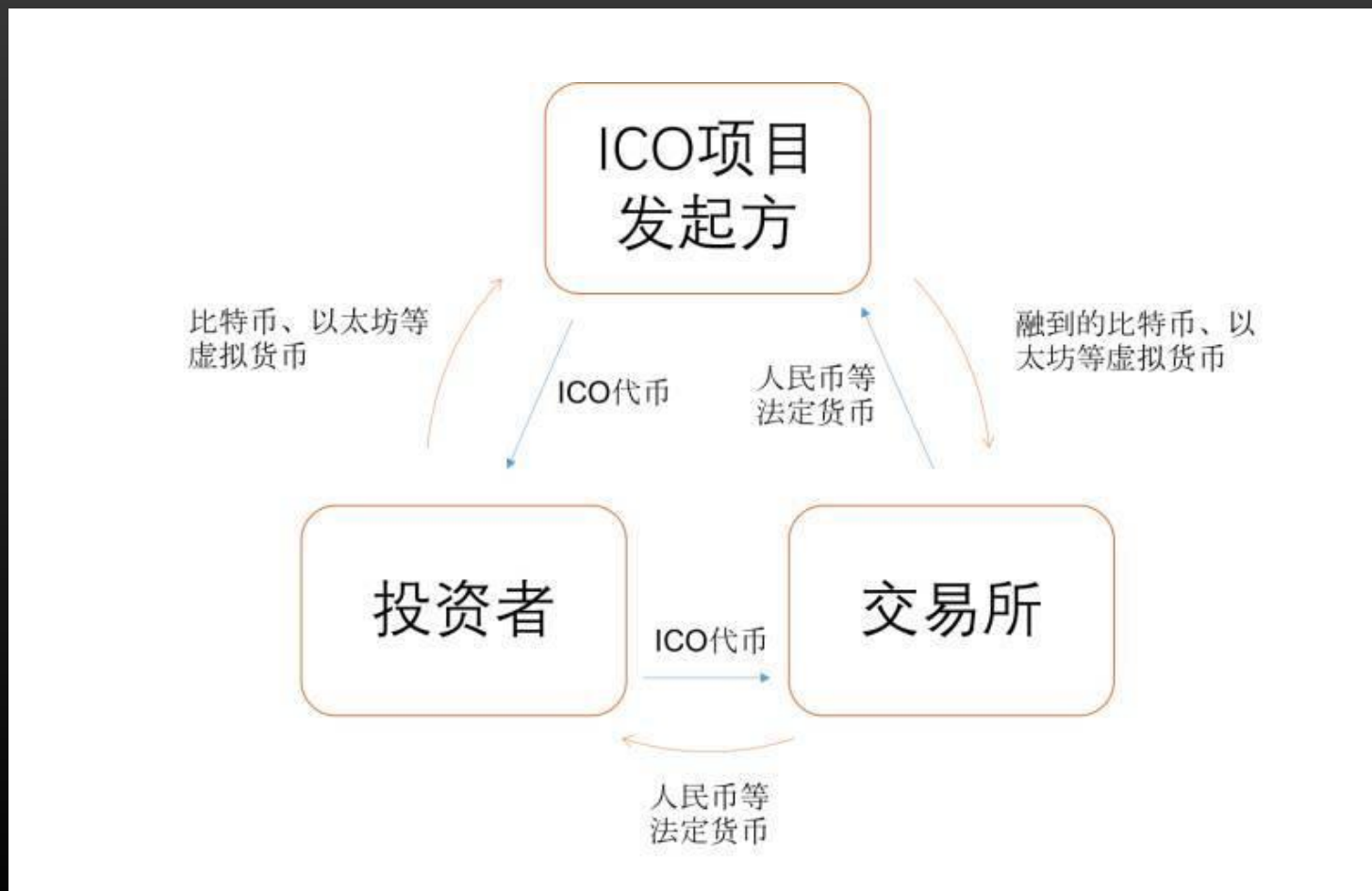
IPO把所有权证券化，ICO把使用权货币化。货币化的流通性超过股票流同性，更为高效。传统的企业IPO发行股票主要是售卖的是企业所有权，而ICO售卖的是使用权。比如以太坊售卖ETH，主要是卖的是ETH的使用权，有了以太坊可使用它的计算、存储等资源。

ICO的基本流程？



ICO是怎么运作的？

ICO行业生态体系，不仅包括了个人和项目。还包括了投资机构、ICO发行平台、ICO媒体、交易所及数字钱包等。



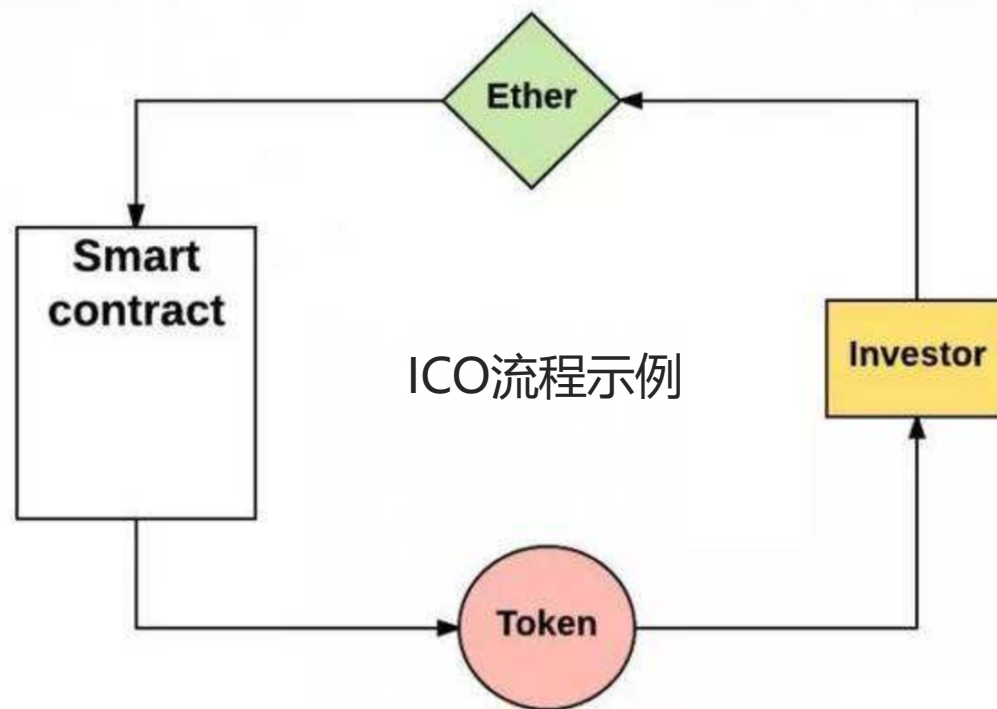
以太坊：ICO最重要的工具

以太坊（Ethereum）是一款能够实现智能合约、代币发行流通并且开源的底层区块链系统。

ERC20 Token

ERC20 token是以太坊平台上的数字货币标准，本质上是一种智能合约。

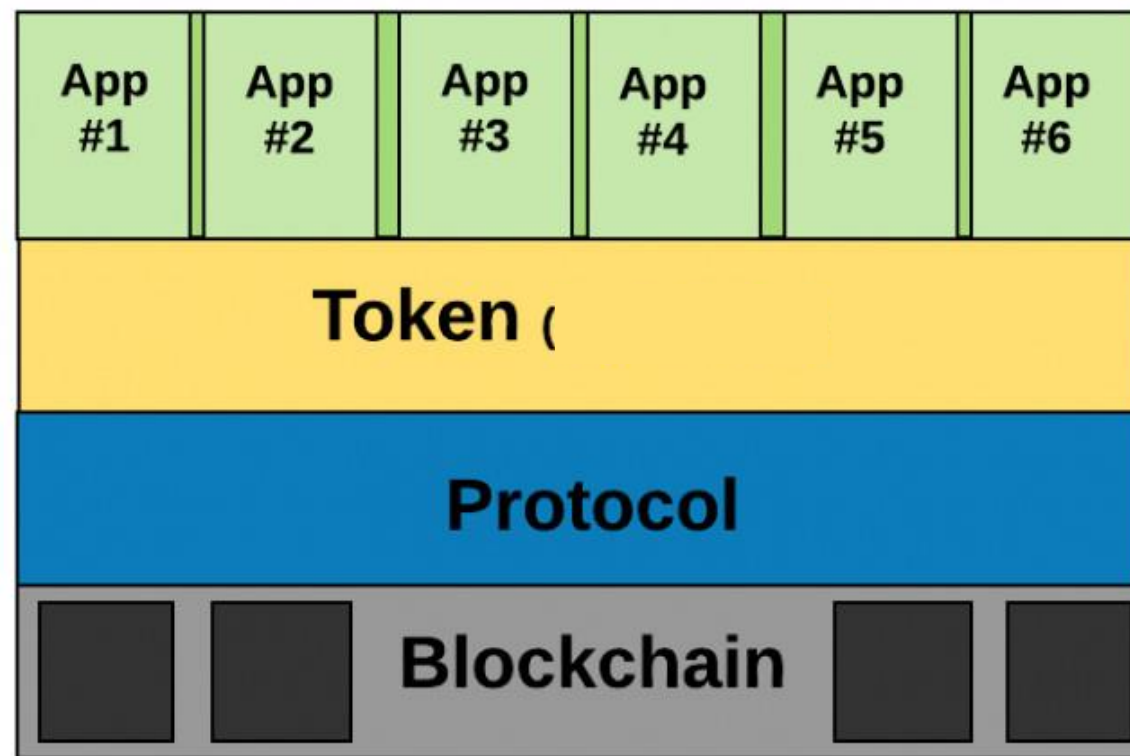
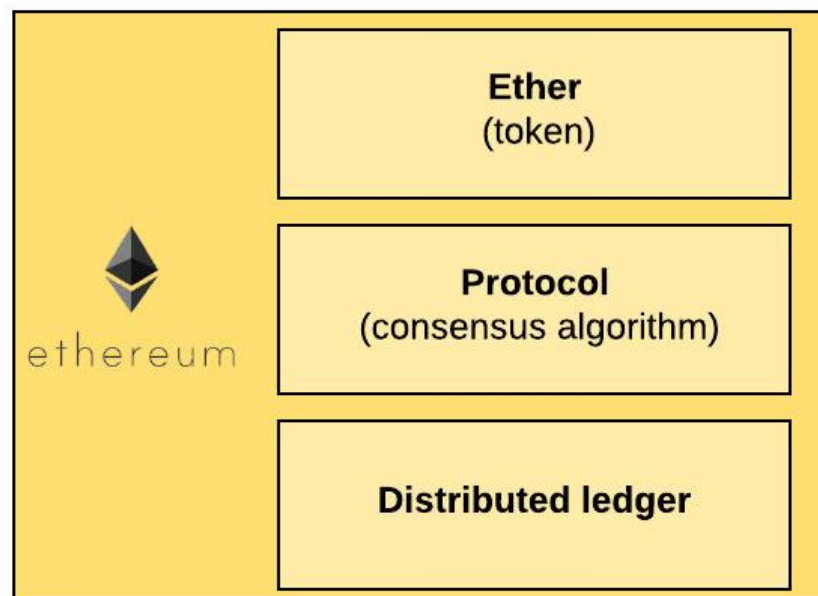
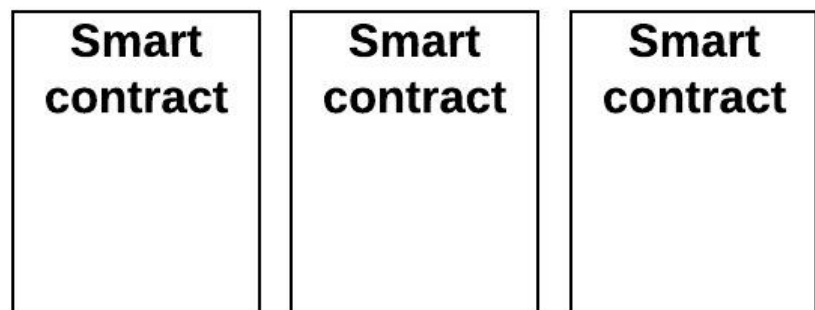
ICO在ETH的流程：



以太坊智能合约的技术架构

以太坊智能合约

区块链2.0



第二章：为什么会出现IFO?

2.3 什么是IFO?

IFO:

首次分叉发行

Intial Fork Offering

两 个 前 提:

比特币代码开源: 任何人都可以fork一份代码, 再找个理由进行二次开发。

比特币用户够多: 每个用户相当于1: 1免费获得分叉币, 省去推广费用。

Fork分叉是怎么来的？

随着比特币的交易和用户越来越多

比特币面临问题：1M区块限制



中本聪关于区块扩容的计划

satoshi
Founder
Sr. Member


Activity: 364

Ignore

**Re: [PATCH] increase block size limit**
October 04, 2010, 07:48:40 PM
#9

It can be phased in, like:

```
if (blocknumber > 115000)
    maxblocksize = largerlimit
```

It can start being in versions way ahead, so by the time it reaches that block number and goes into effect, the older versions that don't have it are already obsolete.

When we're near the cutoff block number, I can put an alert to old versions to make sure they know they have to upgrade.

更大的区块限制可以分阶段进行，比如：

当 区块高度(blocknumber) > 115000 时，
区块上限(maxblocksize)=更大的限制。

这段代码可以提早很多写在某个版本中，这样到指定区块高度，这段代码起作用时，不含有此代码的旧版本早就被淘汰了。

当我们接近截止区块高度时，我将在旧版本上显示一个告警，以保证旧版本用户知道他们必须升级了

但是社区出现意见不同的两派

Core派认为：

去中心化更重要

一笔交易费100美元也没问题

把交易驱赶到第二层网络上

扩容派认为：

中本聪论证大区块和去中心化不矛盾

高手续费杀死交易，就是在杀死比特币的价值
就是在杀死比特币

第二层网络遥遥无期，难以使用

Core坚决不同意扩大区块，社区开始谈判：

- 哪怕只是扩到2M（还是小区块）
- 哪怕是先升SW（隔离见证），1年后再升2M（香港共识）
- 哪怕社区绝大部分算力和公司都同意（纽约共识）
- 坚持锁死主链1M，发展自家公司Blockstream的侧链（Blockstream是一家以侧链为盈利点的公司）

Core踢走了：

- Gavin Andresen中本聪的指定继承人，主张根据中本聪计划扩容
- 一开始Core五核心中的两名（Gavin 和 Jeff）
- 诸多开发人员（建立了XT、Classic、BU、bcoin、ABC等版本）
- Vitalik Buterin（建立了市值排名第二的ETH）
- 大区块派（建立了市值排名第三的BCH）

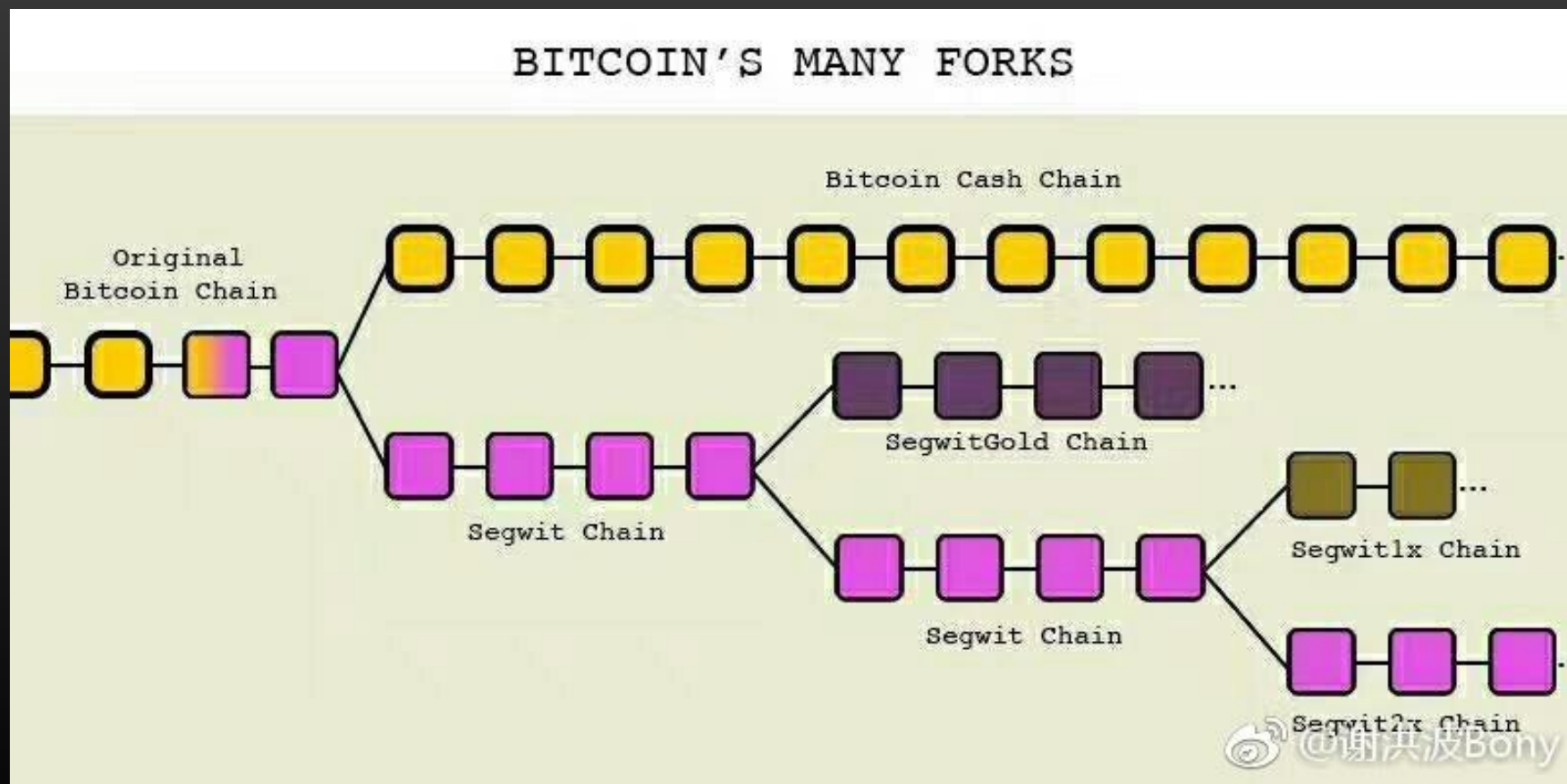
UASF (BIP148) 政变:

2017年8月1日:

- Core在没有足够算力投票支持的情况下，发起UASF，强行激活SW
- 扩容派为避免主链被UASF链覆盖，发生交易回滚，丢币。
发起UAHF（用户激活硬分叉），
分叉出8M的 **比特现金 (BCH, Bitcoin Cash)**

长达四年的争吵、撕逼和互相敌视，最终导致社区一分为二

区块链分叉的原理：



2.3 三个因素促成了大量的IFO

比特币社区决裂：

2017年8月，比特币扩容问题，社区出现分裂，比特币硬分叉，诞生了bitcoin cash。

ICO被禁止：

2017年9月3日，中国央行等七部委发布《关于防范代币发行融资风险的公告》，规范ICO代币融资活动，ICO在中国被禁止。

IFO变得有利可图：

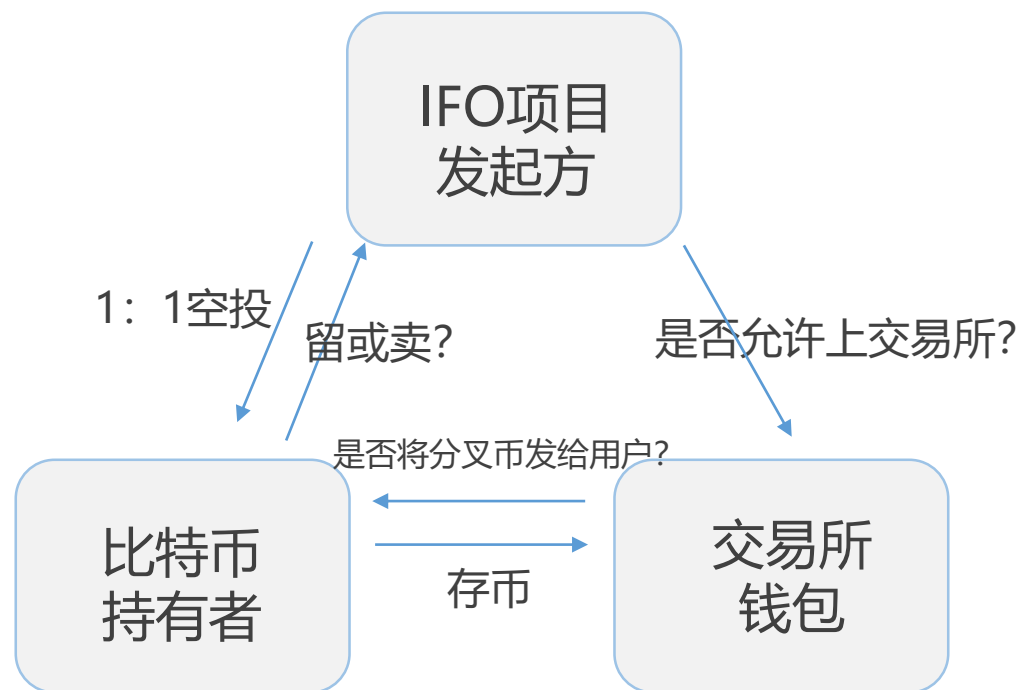
IFO团队主导代码开发和维护，可以随便修改发行总量，提前预挖，团队保留代币等行为，其实是变相的ICO，并通过1:1的方式空投给所有比特币用户。

在ICO被国家明令禁止之后IFO或许是必然的结果。

ICO禁止风波短暂过后，在bitcoin cash 疯狂之后，一条明晃晃的路摆在了人们面前—I FO。这堪称是一个完美的操作，分叉一个币，比特币玩家满意，发起方满意，交易所争先恐后，而又不是ICO，没有圈钱，最多是用传统的预挖，虽然缺乏正义性，但是央妈也找不到好的理由来干涉，完美。

IFO产生的囚徒困境

随着分叉的越来越多，分叉团队、交易所、比特币持有者的陷入囚徒困境。

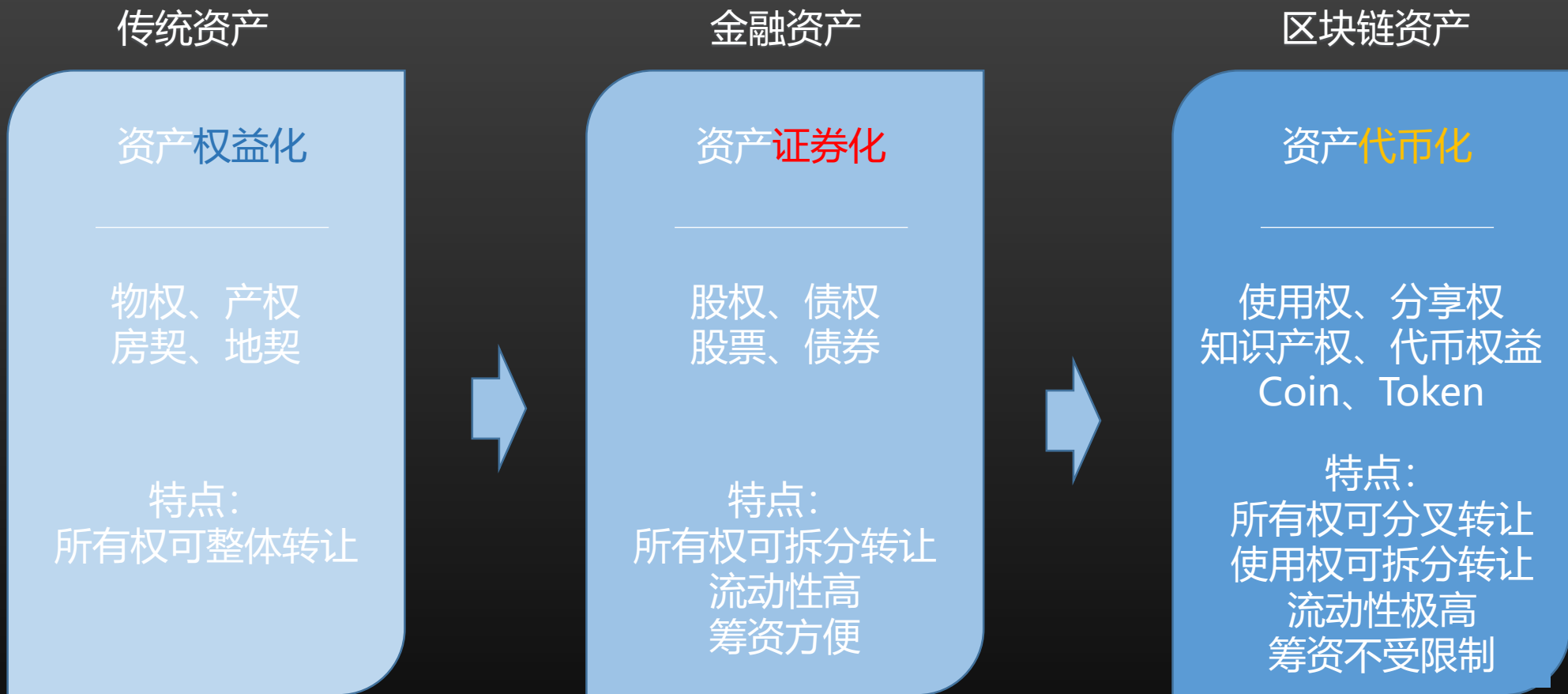


已经分叉出来的分叉币种

对照	BTC	BCH	BTG	BCD	B2X	SBTC	BCHC	BTX
分叉时间	-	2017.8.1	2017.10.25	2017.11月底	2017.11.16	2017.12.17 (试验)	2017.8.1	2017.4.24 (非分叉产生)
总发行量	2100万	2100万	2100万	21000万	2100万	2121万	2100万	2100万
分配方式	挖矿	挖矿 分叉获得	挖矿 分叉获得	挖矿 分叉获得 可预挖 (4000万)	挖矿 分叉获得	挖矿 分叉获得 可预挖(21万)	挖矿 分叉获得	挖矿 空投 快照索赔
共识机制	PoW	PoW	PoW	PoW	PoW	不明	PoW	PoW
算法	SHA256	SHA256	Equihash	SHA256	不明	不明	SHA256	Timetravel 10
挖矿设备	ASIC	ASIC	GPU	ASIC	GPU	不明	ASIC	GPU
块大小(实际)	1M(2-4M)	8M(8M)	1M(2-4M)	8M(8M)	2M(4-8M)	8M(8M)	8M(8M)	20M
块间隔	10分钟	10分钟	10分钟	10分钟	10分钟	不明	10分钟	2.5分钟
难度调整	2周	DAA	EDA	2周	DAA	不明	EDA	Diff64_15
SegWit	支持	不支持	支持	支持	支持	不明	不支持	支持
重放保护	-	支持	支持	支持	支持	支持	支持	-
其他特性	-	-	唯一地址格式	交易金额加密	-	智能合约 闪电网络 零知识证明 移除动态 检查点保护	-	-
团队	Bitcoin Core	BitcoinABC Bitcoin Unlimited BitcoinXT	Bitcoin Gold	Evey团队 007团队	BitcoinX团队	Super Bitcoin	团队未知 官网介绍 抄袭BCH	Bitcore

第三章：Token代币经济的正反面

代币经济的主要特点及对比



资产被完全液化，获得全方位的流动性

代币经济的优点

- 小微企业融资，打破资金垄断

初创公司现在不需要与传统风险投资公司分享收益，而是可以回报他们的早期采购商和最早相信他们项目的人。

- 资产代币化，价值快速流通渠道

包括有形资产和无形资产，以及对于项目未来价值的代币化变现。

- 价值流通加速，解决流动性问题

投资者通过ICO获得代币，可以马上在市场上进行流转，而传统的投资，从VC到ipo公开流转往往要5~8年左右。

- 智能合约共识机制，解决信任问题

公开透明、去中心化的共识机制，消除了投资者转账信任的问题。

- 代币全球流通，解决产品国际化流通问题。

全球各地的投资者都可以用手里的btc或者eth来投，而不会受到地域限制，并且代币的交易在全球都可以进行。

- 规避监管问题

传统金融体系对资金的流进流出有严格限制，效率慢，且存在诸如非法集资等不可预知的法律监管风险。

代币发行行业发展乱象

- 逃避监管，缺乏披露

通过异地注册，基金会等方式，剥离项目主体监管风险；项目关键信息和动态披露少。

- 项目风险极大

过度溢价导致价格虚高，泡沫横行，且有各类跑路风险。

- 浮躁短视，真正落地的少

过度营销，虚假宣传，洗脑式传销，项目有实质性进展和落地的少。

- 对传统股权的颠覆，导致的纠纷

代币权益和传统股权的界限及权益区分，存在法律空白。（李笑来和郑伊廷纠纷案）

- 团队护盘严重，操控代币价格走势

团队为了拉高代币价格，投入海量资金护盘，或大量抛售代币引发恐慌，损害投资者利益。

ICO案例回报情况

一些ICO融资案例：

EOS：一期融资超1.8亿美元，仅仅出售20%的代币

BNT (Bancor)：1.6亿美元，三个小时内完成

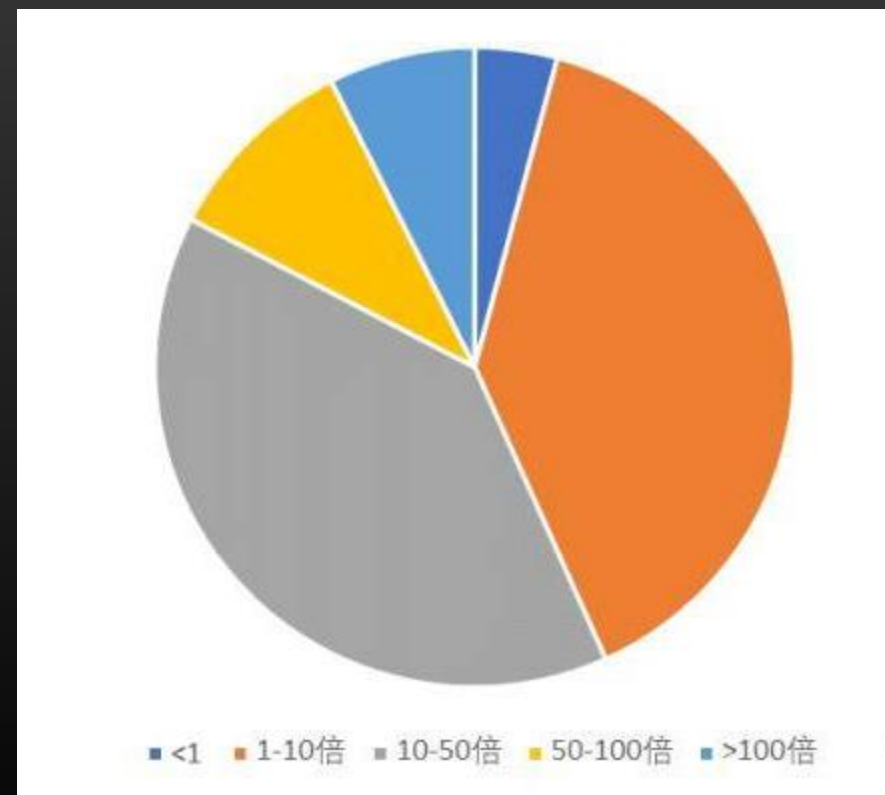
BAT (Basic Attention Token)：3500美元，30秒内完成融资

Storj：3000万美元

Waves：1600万美元

Qtum(量子链)：1570万美元

ICO项目回报情况分布



第三部分 区块链3.0

区块链技术的应用和普及

第一章：区块链的社会意义

第二章：区块链平台、应用、货币

第一章：区块链的社会意义

区块链技术的意义

机器信任

价值互联网

智能合约

开放透明商业规则

智能资产

“怎么证明我妈是我妈”？

过去，我们的出生证、房产证、结婚证等，需要一个中心的节点比如中国政府背书，大家才能承认。但一旦跨国，你就会遇到无穷的麻烦，跨国以后合同和证书可能就失效了，因为缺少全球性的中心节点。而现实中的货币流通要依靠中心化的组织做背书来维护运行，比如微信支付、支付宝、银联等。

区块链技术则用代码构建了一个最低成本的信任方式

—— 机器信任

从个人信任、制度信任进入到机器信任的时代。

互联网的第一波只是交换信息，本质是信息的拷贝。可以称之为信息互联网；
有了区块链则可以交换价值。

区块链技术有望带领人类从

信息互联网过渡到价值互联网。

价值是什么？

货币、资产、股权、债权、版权、物权等等，区块链可以
使得这些价值都能自由发行和流通。

开放透明的商业规则

区块链生态思维关注的核心是**开放透明**的商业规则，
而传统金融关注的核心是**垄断**和**中间人利益最大化**。
从规则不透明、仲裁不平等的黑箱操作进化到开源透明、公平仲裁、自动执行。

人类文明已经从“身份社会”进化到了“契约社会”，
而在区块链有望带领人类从契约社会过渡到智能合约的社会。

智能合约 几乎能替代所有的纸质契约。

智能合约特点： 权益关系对等 履约成本低 违约成本高

智能资产

智能手机
移动互联网
在线

智能设备
物联网
在线

智能资产
区块链
在线+在链



资产受区块链保护
所有、使用权可分叉转让
流动性极高
筹资不受限制

区块链技术五个主要特点

1、去中心化

由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。

2、透明开放

系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

3、机器信任

区块链采用基于协商一致的规范和协议(比如一套公开透明的算法)使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

4、信息不可篡改

一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

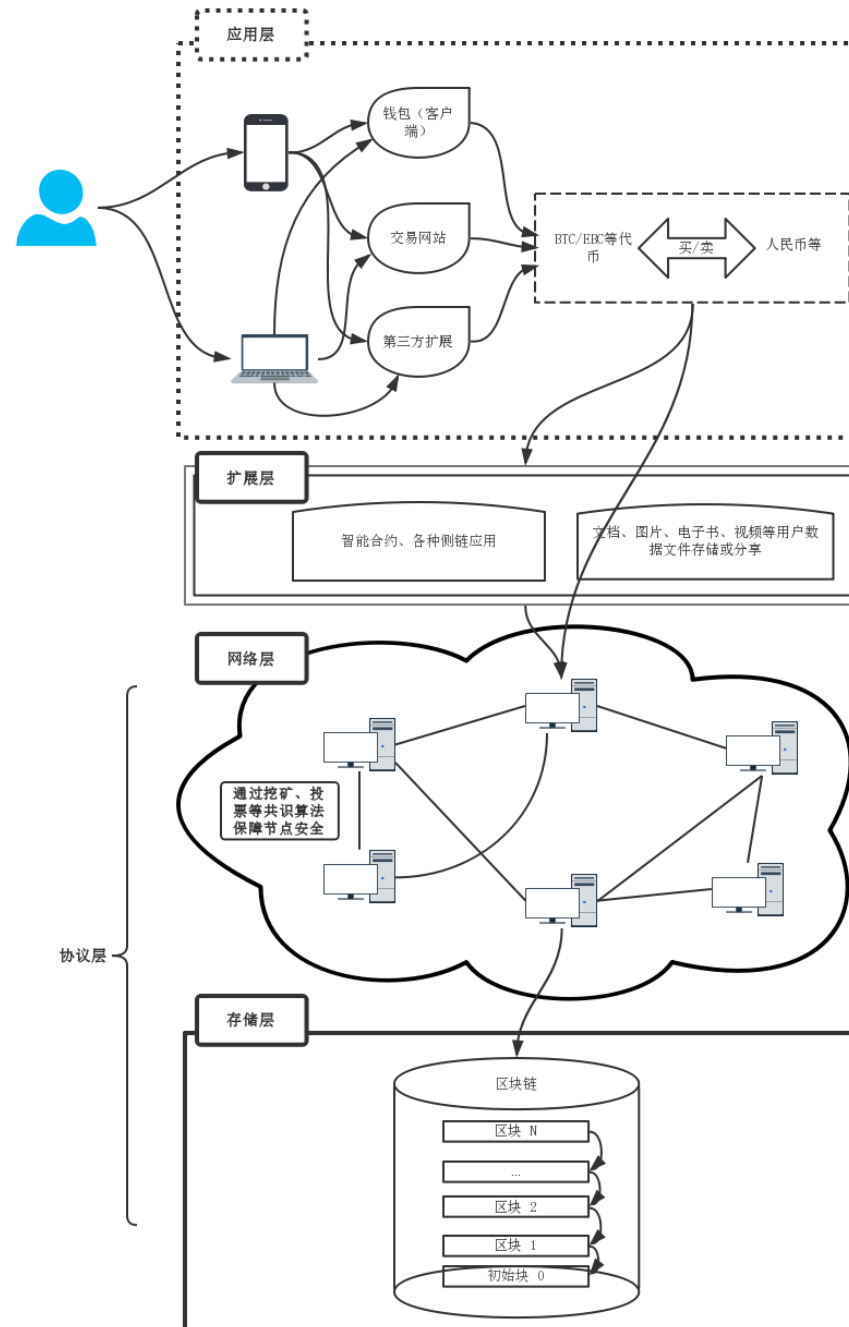
5、匿名性

由于节点之间的交换遵循固定的算法，其数据交互是无需信任的(区块链中的程序规则会自行判断活动是否有效)，因此交易对手无须通过公开身份的方式让对方自己产生信任，对信用的累积非常有帮助。

区块链3.0的技术基础架构



区块链架构设计图



第二章：区块链平台、应用、货币



区块链正在进行的应用和项目

- 1.底层区块链：以太坊、比特股、Waves、EOS、Tezos、Q-tum、Nxt、Omni、Counterparty
- 2.分布式存储：Storj、Sia、IPFS、MaidSafe
- 3.分布式计算：Golem、Elastic、iExec
- 4.物联网：IOTA
- 5.跨链：Bancor、infinite、COSMOS
- 6.匿名货币：Digital Cash、Zcash、Komodo
- 7.资产管理：Iconomi、Tass、Melonport、Blockchain capital、DigixDAO
- 8.借贷：HumanIQ、Wetrust
- 9.游戏：FirstBlood、GameCredits、BitCrystals
- 10.支付：OmiseGO、Plutus、BlockPay
- 11.借记卡：TokenCard、Monaco、TenX
- 12.汇款：Ripple、Stella、Cloaking
- 13.内容分享：Decent、Steemit、BAT、SinularDTV
- 14.预测市场：Augur、Gnosis、Truthcoin
- 15.社交通讯：Status、Matchpool
- 16.开发工具：Stratis、Lisk
- 17.知识库：Lunyr
- 18.众筹平台：Wings、Virtual Accelerator、Swarm
- 19.存在证明：Factom
- 20.身份验证：Civic
- 21.招聘平台：Chronobook
- 22.积分：Incent
- 23.票据金融：Populous、Hive
- 24.保险：InsureX
- 25.博彩：Casino.DAO、TrueFlip

区块链经济模式

传统经济模式：

1) 做好产品，卖出规模 >> 2) 建立信任，打造平台 >> 3) 设计生态，输出规则

区块链经济模式：

基于区块链的**数学加密算法**建立**信任**，基于**分布式**的计算机节点建立**共识机制**，设计好**生态经济模型**，基于智能合约制定**规则和奖罚措施**，通过区块链钱包应用发行**生态流通代币**，通过ICO获得资金，启动**生态模式**。

从产品思维转向**生态思维**，颠覆传统思维逻辑。

区块链的价值传递：

第一层是简单的价值全球性流通，让价值传输无比便利。

- 资产全球化流通，使得效率极大提高。
- 资产代币化，使得资产流动性增加。

第二层是代币的流通或者说代币经济学带来的价值吸纳。

- 代币发行让融资更加便利。
- 代币的流通会吸纳价值，**购买代币背后不是简单的购买服务，而是购买了整个生态。**

区块链的逻辑，就是把消费者同时变成投资人。

区块链技术从1.0到3.0

区块链1.0

区块链1.0 就是以比特币为代表的虚拟货币，也是最基础的，他的特点是去中心化、世界流通、专属权、无隐藏成本、数量固定、发行不受控、交易方便、交易费用低廉等。

区块链2.0

区块链2.0就是可编程区块链，他的主要特征就是智能合约，可以运用在金融领域方面。如银行结算支付，跨境支付，投融资。

区块链3.0

区块链 3.0 就是个人、社会资产代币化，区块链价值网络覆盖社会生活的方方面面，不再依靠某个第三人或机构获得信任或建立信用，还有节约人力和时间成本，提升社会信任和资产流通效率。

谢谢！



加我的微信，讨论