

区块链：颠覆式创新

— 区块链和数字货币系列报告之二 (上：技术篇)

证券分析师：

王胜 A0230511060001

刘洋 A0230513050006

谢伟玉 A0230512070007

联系人: 王洋阳 (18616723078)

2016.4.28



“慧博资讯”是中国领先的投研大数据分享平台

点击进入  <http://www.hibor.com.cn>

主要结论

- **比特币VS区块链,重申观点—区块链技术未来预料获更多产业青睐和投资**：比特币工作量证明引发矿机竞争高能耗，中国算力造成垄断和比特币本身分布式民主设置初衷产生冲突，1MB的区块限制造成网效降低，种种因素对比特币发展形成一定制约。但底层技术区块链部署方式的创新，比特币工作量证明机制外发展出权益证明、股份授权证明等多种创新高效机制，技术瓶颈解决，区块链技术相对比特币应用开始获得更多产业资本青睐，长期趋势有望强化。
- **区块链技术应用发展目前分四阶段**：第一阶段，**数字货币**为起点，相关应用和支持软硬件为区块链1.0。第二阶段，区块链2.0由**数字资产**开启，各类资产可在区块链上进行数字登记，得到资产安全和数据完整性保证。第三阶段，区块链更广阔应用场景的打开取决于**生态系统**进化，其中智能合约标准的制定普及是关键。第四阶段，数字资产结合生态系统可打开区块链**价值网络**的应用，总结八领域为跨境支付、金融市场交易清算、贸易金融、物联网、网络安全、P2P借贷、保险、以及类似审计的职业服务。
- **海外目前产业发展方向集中在生态系统搭建和价值网络应用的技术商业模式实验**：目前数字资产区块链登记储存发达市场已有较多成熟商业模式。生态系统搭建方面建议关注Ethereum的智能合约标准确立，各外部机构凭此标准开发应用可做到真正的互联共享。价值网络八大应用方面，Fintech金融创新应用有望加速推进，区块链可同时实现降低系统风险和减少监管负担两大原矛盾目标，同时提升系统实时性和交易效率，对于监管层和大型金融机构充满吸引力。物联网方面，随着智能设备数量从万级升至亿级，区块链可在设备间建立低成本点对点的直接沟通桥梁，使智能设备成为可以自我维护的自主个体，同时提升系统内信息安全私密性。物联网、P2P借贷、保险、职业服务目前更多处于模式探索阶段，陆续落地需要关注。
- **行业标准规范和人才跟进国内进行正当其时**。参照国外路径,数字资产登记和数据完整安全性保证或会成为区块链在我国最易落地的应用场景。金融应用方面，最可能在场外例如区域资本市场、机构间交易市场、交易所固收等场景获得突破。区块链在银行间转帐、理财业务的底层技术提供方面也存在应用潜力。三大商业机会包括技术提供者、运营商、解决方案开发和运营的综合体。基于区块链合作分布，以及底层协议的本质，行业内良好的协议层标准制定为长远发展关键，ChinaLedger的建立树立了良好开端，后期还需更多人才加入阵营，加快行业发展。
- **6月、9月区块链峰会，建议关注相关上市公司后期运作**。根据产业内人士观点，密码学、分布式、金融应用方案为构成区块链之应用核心，三者无二则非严格意义上区块链应用。二级市场目前多为三者有一，众多公司（例如**海立美达**、**广电运通**、**恒生电子**、**赢时胜**等）表示已开展区块链相关技术研究，或已有相关技术储备，充满潜力。2016区块链峰会6月22日在北京举行，上海区块链国际周9月19日举办，建议关注相关上市公司后期研发运作动态。

“慧博资讯”是中国领先的投研大数据分享平台

点击进入  <http://www.hibor.com.cn>

区块链 一下- 认识数字货币的风口！

"A technological tour de force" — Bill Gates

*"The biggest opportunity set we can think of over the next decade or so"
— Bob Greifeld, CEO of NASDAQ*



主要内容

上：技术篇

1. 区块链是什么？
2. 区块链有什么特点？

下：应用篇

3. 区块链有何应用领域？
4. 区块链技术存在何种投资机会？

主要内容

上：技术篇

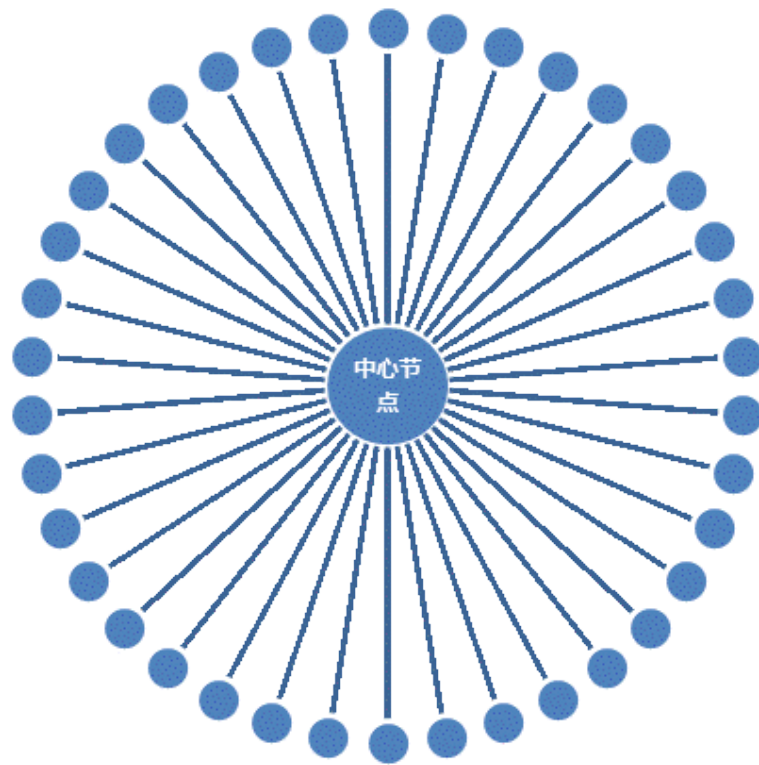
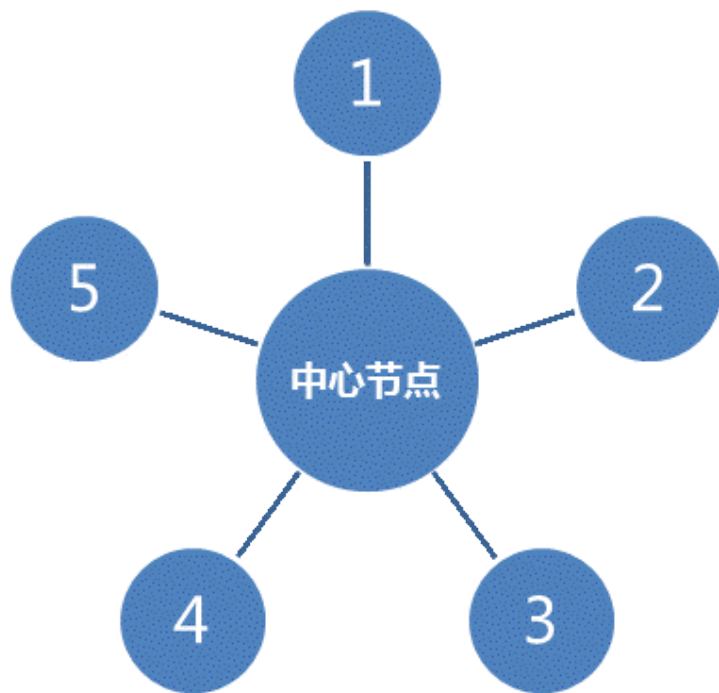
1. 区块链是什么？
2. 区块链有什么特点？

下：应用篇

3. 区块链有何应用领域？
4. 区块链技术存在何种投资机会？

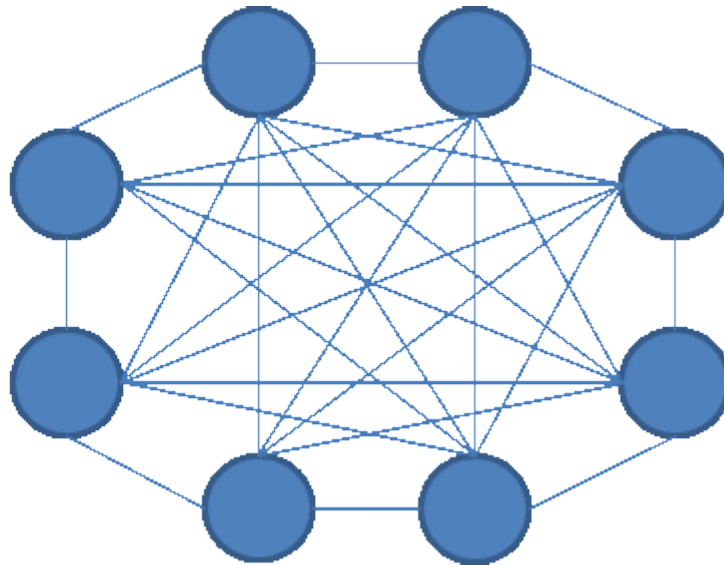
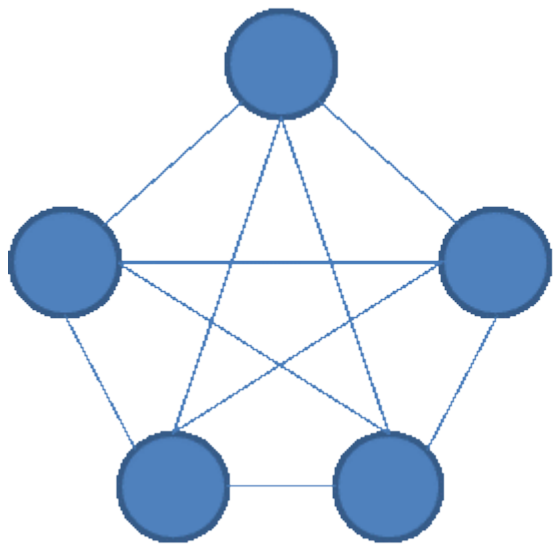
什么是区块链：——本质上，它是一种分布式记账版本

- 传统中心化网络（下图）
- 中心节点掌握分布节点信息，分节点不掌握其他节点信息（中心化，交易非公开）
- 系统安全性取决于中心节点安全性，分布节点对此没有控制权
- 从5个节点到100个节点，系统风险性上升



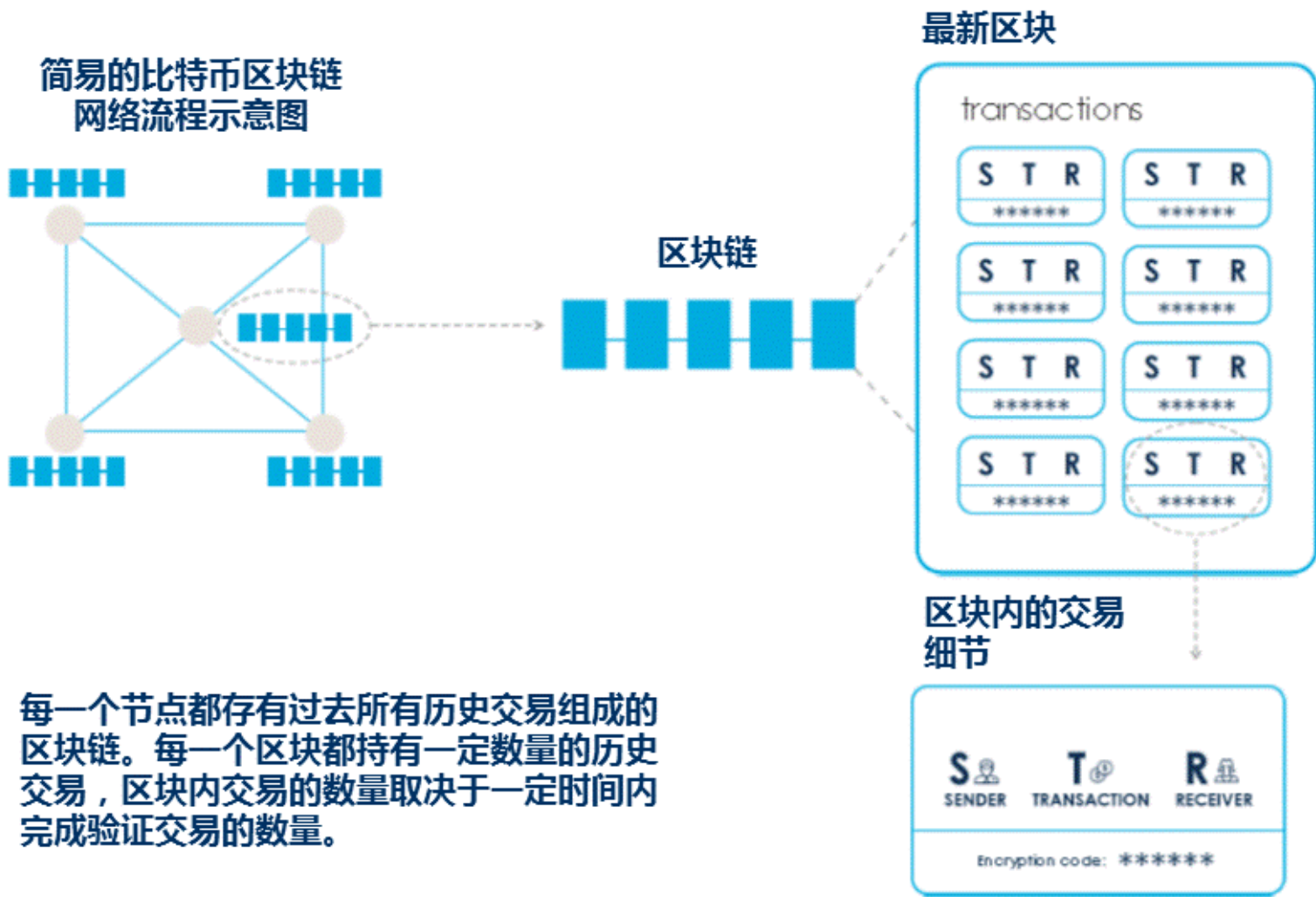
什么是区块链：——本质上，它是一个分布式账本

- 分布式去中心化P2P网络（下图）
- 每个节点掌握各个节点信息，信息可以采用匿名原则（交易公开）
- 系统内交易批准取决于所有节点共识性原则，规则对于所有节点公平且强制（去中心化）
- 从5个节点到100个节点，系统风险性指数性下降



什么是区块链：——本质上，它是一种分布式数据库

- 随着时间推移，交易增多，每个节点内同步更新的链条愈发变长，愈发难以被篡改



什么是区块链：—— 从比特币开始



- 什么是货币？
- 现今流通货币分为：商品货币、代用货币、法定货币
- 商品货币(Commodity)

- 价值与其作为普通商品价值相等的货币
- 多与贵金属挂钩



- 代用货币(Representative)

- 代表商品货币在市场上流通
- 通常为纸币，由政府或银行发行



- 法定货币(Fiat)

- 无实物资产（贵金属）支持
- 国家发行，债务形式，国家背书



THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE

Timothy F. Gaithan
Secretary of the Treasury

什么是区块链：——从比特币说起



■ 传统银行分类帐特点拥有中心化和交易非公开的特点

- 银行掌握所有用户帐户的信息和交易的历史记录（中心化）
- 用户只掌握了自己的记录，无法知晓其他用户交易记录（交易非公开）
- 如果掌握有所有的交易支付记录，可以倒推出帐户信息（中心化风险）

交易记录			
来自	至	日期/类型	金额
Jeff	Larry	3月25日/支票	(\$100)
	现金提取	3月25日/ATM取款	(\$200)
	现金存储	3月25日/存储	\$1,000
	Bob	3月25日/微信转帐	(\$100)
	Larry	3月25日/微信转帐	(\$100)
Larry	Bob	3月25日/微信转帐	(\$500)
	现金提取	3月25日/ATM取款	(\$500)
	现金存储	3月25日/存储	\$2,000
	Laura	3月25日/电传	(\$500)
.....



帐户	
Jeff	\$100,000
Bob	\$80,000
Lawrence	\$60,000
Warren	\$40,000
Laura	\$20,000
.....	\$8,800.80
.....	\$1,232.33
.....	\$1,402.43
.....
.....

“慧眼识珠”是中国领先的投融资研究大数据分享平台
资料来源：网络资料整理，交易记录和客户信息为虚拟展示信息

点击进入<http://www.chinabn.com.cn>

什么是区块链：—— 从比特币开始



■ 比特币有去中心化和交易公开的特点

- 在比特币中，不存在一个中心节点（去中心化）
- 所有交易都是公开的（交易公开）

交易记录			
来自	至	日期/类型	金额
Jeff	Larry	3月25日/支票	(\$100)
	现金提取	3月25日/ATM取款	(\$200)
	现金存储	3月25日/存储	\$1,000
	Bob	3月25日/微信转帐	(\$100)
	Larry	3月25日/微信转帐	(\$100)
Larry	Bob	3月25日/微信转帐	(\$500)
	现金提取	3月25日/ATM取款	(\$500)
	现金存储	3月25日/存储	\$2,000
	Laura	3月25日/电传	(\$500)
.....



帐户	
Jeff	\$100,000
Bob	\$80,000
Lawrence	\$60,000
Warren	\$40,000
Laura	\$20,000
.....	\$8,800.80
.....	\$1,232.33
.....	\$1,402.43
.....
.....

什么是区块链：—— 从比特币开始



■ 比特币有去中心化和交易公开的特点

- 在比特币中，不存在一个中心节点（去中心化）
- 所有交易都是公开的（交易公开）
- 但是所有的交易都是匿名的，因此即使有所有的交易信息，也无法推断出个人对应的帐户信息（安全性）

交易记录			
来自	至	日期/类型	金额
F53C2A	900EC1	3月25日/支票	(\$100)
	现金提取	3月25日/ATM取款	(\$200)
	现金存储	3月25日/存储	\$1,000
	302AB2	3月25日/微信转帐	(\$100)
	900EC1	3月25日/微信转帐	(\$100)
900EC1	302AB2	3月25日/微信转帐	(\$500)
	现金提取	3月25日/ATM取款	(\$500)
	现金存储	3月25日/存储	\$2,000
	211ZS2	3月25日/电传	(\$500)
*****	*****	*****	*****



帐户	
Jeff	\$100,000
Bob	\$80,000
Lawrence	\$60,000
Warren	\$40,000
Laura	\$20,000
.....	\$8,800.80
.....	\$1,232.33
.....	\$1,402.43
.....	
.....	

什么是区块链：—— 从比特币开始



■ 要点1：P2P网络（例：Napster，BitTorrent等）

- 众多电脑参与，为共同的目标进行工作
- 所有参与电脑分享工作量
- 所有参与电脑地位相对平等

■ 要点2：公共钥匙加密（Public Key Cryptography）

- 比特币区块链PKC目前为每位参与者提供两把钥匙
 - ✓ 一个为其他用户所知的**公匙**（相当于用户的用户名）
 - ✓ 一个只为用户自己所知的**私匙**（相当于用户的密码）
- 任何有你**公匙**的参与者可以给你发送一条加密信息，该信息只有你可以读到
- 使用**私匙**，发信人可以在加密信息中进行数字签名，向收信人证明发信人是你自己

什么是区块链：——从比特币开始



■ 如何发送比特币？

- 例：A向比特币区块链网络中发送一条或多条信息
- A在信息中指名发送人和收件人的地址
- 对于每个收件人地址，A指名发送的比特币数量
- A在信息中利用私匙对信息进行数字签名，向收件人证明身份
- 信息发送后，A等待比特币区块链网络对于信息进行验证和确认

一笔比特币支付交易记录的详细情况

Transaction View information about a bitcoin transaction

838d752769c97e64609a8996015bbb#58405b85d009d4e0f75b18d02e53090a

128pX3oGJwAYLWJw52GmSSBAzB9LRaMvu

➔

12MQHWqF33Ji9rGEedCJmv4CkPNeAubHoJ

\$ 8,965.26

Unconfirmed Transaction!

\$ 8,965.26

Summary		Inputs and Outputs	
Size	191 (bytes)	Total Input	\$ 8,965.35
Received Time	2016-04-28 04:47:44	Total Output	\$ 8,965.26
Estimated Confirmation Time	Very Soon (High Priority)	Fees	\$ 0.09
Relayed by IP	45.55.170.207 (whois)	Estimated BTC Transacted	\$ 8,965.26
Visualize	View Tree Chart	Scripts	Show scripts & coinbase

Network Propagation (Click to view)

什么是区块链：——从比特币说起



- 比特币钱包 — 一般参与比特币交易需要特殊软件，也就是比特币钱包

- 好的钱包需要以下功能：

- 公共钥匙和私有钥匙的创建
- 发送和接收比特币
- 签署支付转让协议
- 完成比特币和其他类型货币之间的转换
(虚拟或实体)
- 帐户结算和支付转让结算
- 额外的安全保护功能



- 钱包因为和银行账户有所联系，所以会牺牲一定用户安全性，本质上是安全性和私密性之间的权衡交换

- 用户也可以直接通过交易所加入比特币交易



- 通过交易所和钱包加入交易不参加比特币网络交易验证，对全网算力并无提升

什么是区块链：——从比特币开始



■ 比特币交易支付单点交易核查

■ A的交易信息发送后，当比特币区块链网络内任一节点上的机器收到了信息，其开始做以下处理：

- 检查该机器自身是否已经处理过此次交易（确定交易唯一性）
- 检查交易涉及地址是否合法有效
- 检查数字签名，以确保原发信者是Input地址合法有效的拥有者
- 检查发件人这笔比特币有没有在别的地方被花费提取过（解决“双花”问题）
- 检查发件人比特币数量至少是和收件人预收的比特币数量相同（ $\text{Input} > \text{Output}$ ，任何不同差额为手续费用）

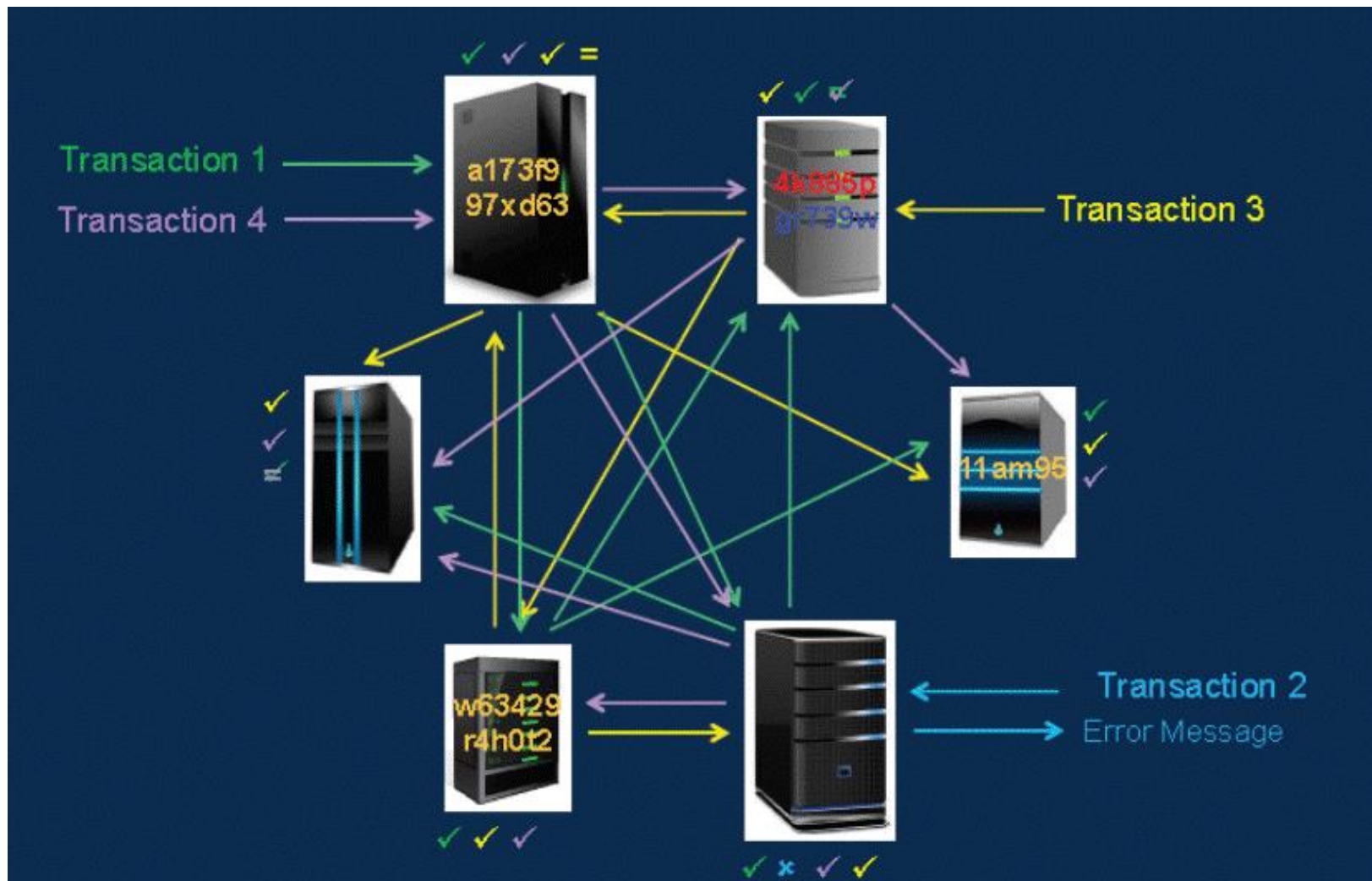
■ 如果以上检查没有问题，节点将交易标注成有效，将其列入“未确认交易”名单。然后将信息广播至网络内其它节点，网络内众节点开始对交易进行节点共识验证

-
- The diagram illustrates a distributed system with five nodes, each represented by a server rack icon. The nodes are connected in a mesh topology. A transaction flow is shown as follows:
- Transaction:** Indicated by a green arrow pointing to the top-left node.
 - Node 1 (Top-Left):** Labeled with the transaction ID `a173f9` and `97xd63`. It has a green checkmark above it.
 - Node 2 (Top-Right):** Labeled with `4h585p` and `gr739w`. It has a green checkmark and an equals sign above it.
 - Node 3 (Middle-Left):** Labeled with `11am95`. It has a green checkmark above it.
 - Node 4 (Bottom-Left):** Labeled with `w63429` and `r4h0t2`. It has a green checkmark below it.
 - Node 5 (Bottom-Right):** Labeled with `11am95`. It has a green checkmark above it.
- Green arrows show the transaction flow from the top-left node to the top-right node, and from the top-right node to the bottom-right node. Blue arrows show the transaction flow from the bottom-right node to the bottom-left node, and from the bottom-left node to the middle-left node. A legend on the right indicates that a blue arrow represents a **Transaction** and a red arrow represents an **Error Message**. A red 'X' is shown below the bottom-right node, indicating a failure or error.

什么是区块链：——从比特币说起



- 随着交易支付数量增加，可以预见网络内繁忙度大幅增加



“慧睿咨询”是中国领先的投融资研究大数据分享平台
资料来源：Morgan Stanley, 交易记录和帐户信息为虚拟展示信息

点击进入 <http://www.chinabai.com.cn>

什么是区块链：—— 从比特币说起



■ 网络内节点共识验证所依赖的算法—SHA-256

- 每一次交易的内容都会被加密
- 加密采用哈希算法 (Secure Hash Algorithm) , 计算过程将支付交易文本链作为输入内容, 生成256-bit(32-byte)数字字母链
- 从Input计算出Output比较容易
- 从Output反推出Input几乎是不可能完成的任务, 这也是哈希算法的使用意义
- 从同一个Output推算出两个不同的Input几乎是不可能发生的 (映射唯一性确保)
- 对于Input细小的变化会导致Output非常大的改变

Input	Output = SHA256(Input)**
Hello, World	03675ac5 3ff9cd15 35ccc7df cdfa2c45 8c521837 1f418dc1 36f2d19a c1fbe8a5
Hello, World.	02b5dcd5 f0ef1a39 cffec5f8 b625ec20 bffcf918 e4efd3f5 4babec4e ae03b347
Hello, World!	dffd6021 bb2bd5b0 af676290 809ec3a5 3191dd81 c7f70a4b 28688a36 2182986f

- 解密的任务和挑战：在输入文本“Hello, World”（也可以是“A传递给B100元”类似的文本或编码信息）后放置数字链，使得哈希算法运算结果给出开头为“0”数字串的哈希值
- 运算没有捷径，只能通过试错得出正确哈希值
- 所有节点都可以看到试图运算的节点是否进行了相关的运算工作
- “Hello World”后附属的数字是 **“工作量证明”（Proof of Work）**

Input	Output = SHA256(Input)
Hello, World!	df6d6021 bb2bd5b0 af676290 809ec3a5 3191dd81 c7f70a4b 28688a36 2182986f
Hello, World!1	b3e6153a 3ce901e2 769b77d7 96b0aeea 68ab0344 a98b94b7 84f9e2b7 94487540
Hello, World!2	d469e19a ae363334 35190ccc f4800a33 9ecc6b46 7bfdaa3b 4e6f757f 2dd0853f
Hello, World!3	b91abd0f c9eb7aeb 78ef3cd5 f5b9b5a9 139fb2fb 0c452e76 4e9639a6 c089c5ba
Hello, World!4	0f3af36d 81b5efc4 8feec2b5 f6484868 92699c64 5d8ad569 0c7bdfcf 8e6e0778
Hello, World!229	00b92f46 05232084 7022a3c8 21f8e830 8ce3a66b 9aaf9de6 f83572b5 babc9f8d
Hello, World!741	000c5644 054b75e9 5e220856 dbb4a8ce bf3923f7 848c5108 76c5df33 cce20f2d
Hello, World!280635	00001ed4 bc824777 27b6d2cd 4a991e92 b6d9b7d1 cf55c4a6 a24dc3d4 76ba80f8
Hello, World!1558215	000008fb 67e78dee 225c2bea 554b989b 164c1db4 cbc5d281 d00ffa81 724a83b3
Hello, World!12320463	00000080 883ee61b b729275d 87fc0491 b7f6c8b4 06af8928 aa4879a4 fb0c78de

什么是区块链：—— 从比特币说起



■ 支付交易网络内最终验证



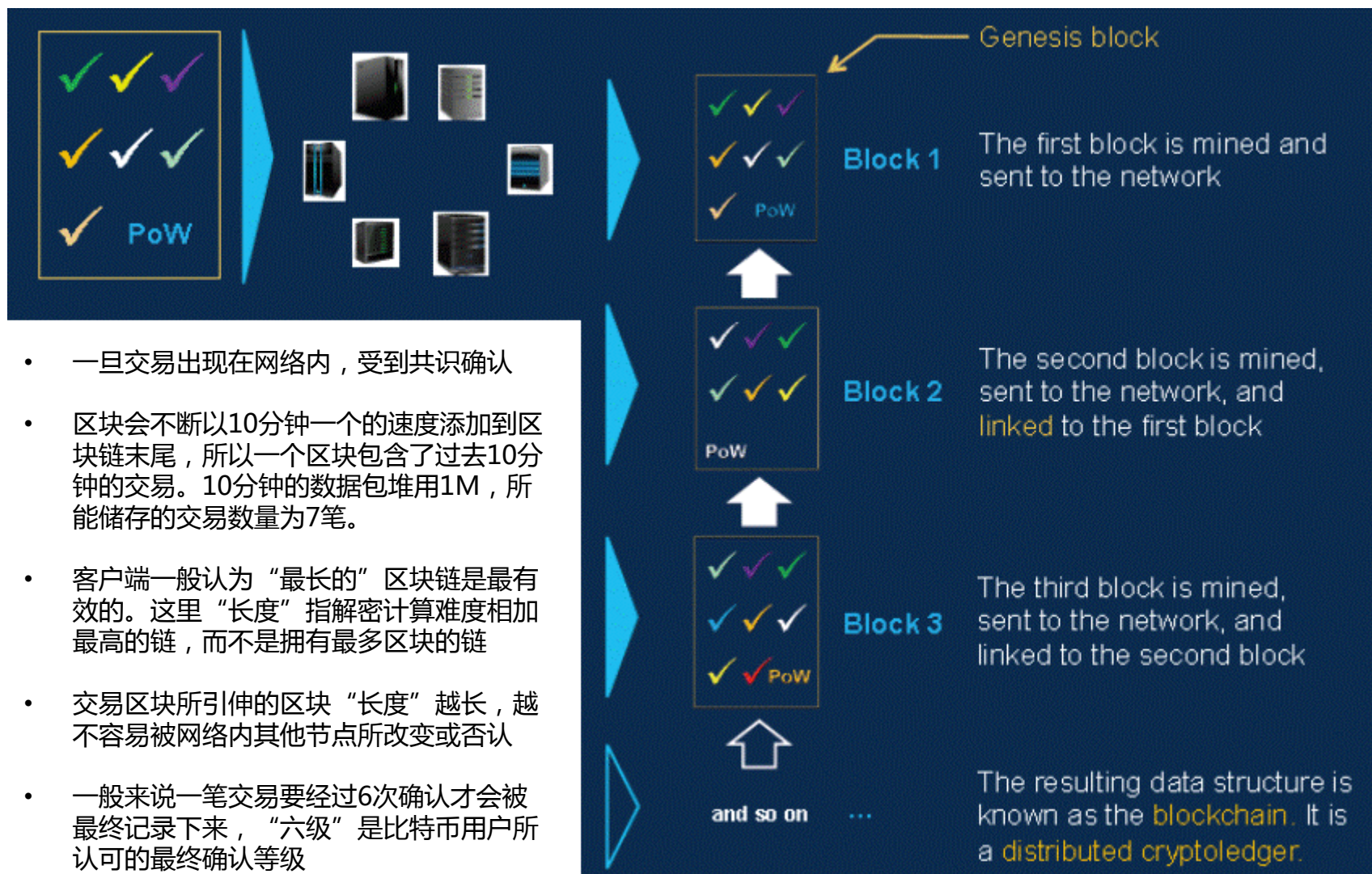
- 网络内节点收集有效但还未验证的交易
- 这些交易以时间先后顺序被放入到**区块 (Block)** 中
- 各个节点纷纷加入，试图解决工作量问题
- 节点这种行为被称为**挖矿 (Mining)**
- 如果节点哈希值运算成功，工作量被加入节点
- 新区块和各个节点工作量证明被实时播报至比特币网络中，成功运算出第一个有效工作量证明的节点胜出，矿工获得支付交易手续费，并获得新发行的比特币作为奖励。目前每个工作量证明的奖励为25个比特币



什么是区块链：——从比特币说起



■ 支付交易网络内最终验证



“慧博资讯”是中国领先的证券研究大数据分享平台
资料来源：Morgan Stanley, 交易记录和帐户信息为虚拟展示信息

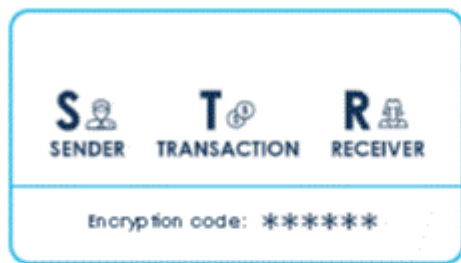
点击进入 <http://www.ealbor.com.cn>

什么是区块链：——比特币区块链又为何如此重要

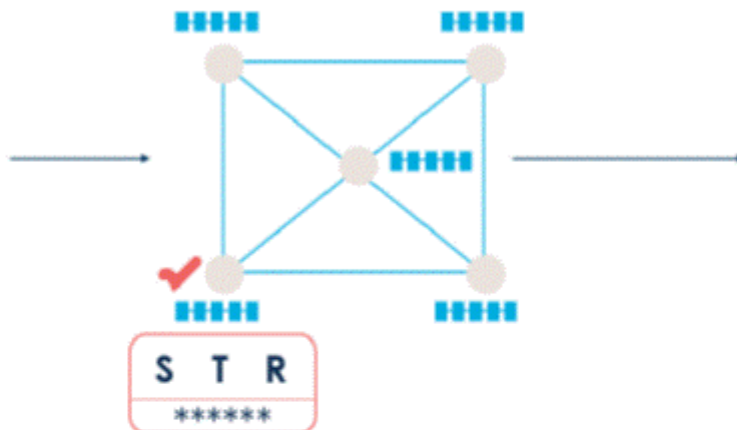


■ 整个流程花费大约3到10秒

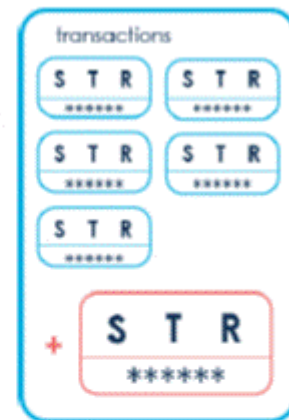
1 交易定义



2 单节点交易核查

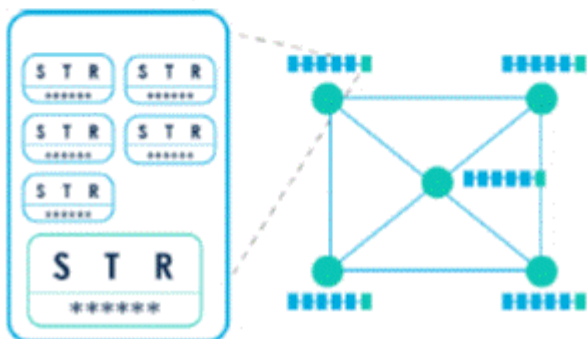


3 加入区块、区块创造

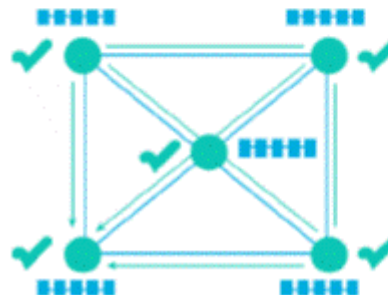


5 区块成链

Validated block:



4 节点共识验证



什么是区块链：——比特币区块链又为什么这么难懂



比特币交易是如何进行的

波比，是在线卖商家，决定开始接受比特币作为收款方式。
爱丽丝，是买家，拥有比特币，并且向要从波比那儿购买商品。

钱包和地址



在电脑中波比和爱丽丝都拥有比特币钱包



钱包是一种特殊文件通过它们可以访问多个比特币地址



一个地址是一串由字母和数字组成的字符串
例如
3HULMazEP
kEPeCh
438eKJLjyb
LCWHDpN



波比创建了一个新的比特币地址用于接收爱丽丝的款项

新建一个新地址



每个地址都有着自己的比特币数量余额

提交一个支付



爱丽丝告诉她的比特币客户端她要发送金额到波比的收款地址。

私钥 公钥

公钥加密算法 101
当波比创建一个新地址，他实际上所完成的动作是生成了一个“密钥对”由一个公钥和一个私钥组成。如果你使用私钥（只有你自己知道）对一个消息签名，它便可以被对应的公钥（大家都知道）进行验证。波比的新比特币地址代表了一个唯一的公钥，并且对应的私钥保存在他的钱包里面。这个公钥允许所有人可以对那个用私钥进行签名的消息进行验证。

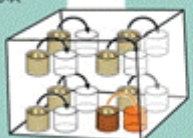
可以简单的认为地址就像是银行账号，但是运行机制又有一些不同。比特币用户可以随意创建任意多个地址。事实上，我们鼓励大家为一个新的交易单独创建新地址。这样一来就没有谁知道哪个地址是属于爱丽丝的，她的匿名性得到了保障。



Gary, Garth 以及 Glenn 都是比特币矿工

验证交易

他们的电脑将过去十分钟内的交易数据打包成一个新的“交易块”



矿工的电脑被用于计算加密的哈希函数

哈希值*

*每一个新哈希值都包含之前比特币所有交易的信息



+ 随机数

新哈希值

+ 随机数

新哈希值

加密哈希

加密哈希函数将数据转换成一系列特定长度的字符串，称为哈希值。源数据的任何一个细微的改变都会导致最终计算出来的哈希值的变化。并且，几乎无法预测一个初始数据集将会产生哪一种特定的哈希值。

The root of all evil
6d0a1899086a...
(56 more characters)
The root of all evil
486c6be46dde...
The root of all evil
b8db7ee98392...

随机数

从相同的数据创建不同的哈希值，比特币协议使用了“随机数”。一个随机数就是一个添加在数据前面的一个随机数字。改变随机数可以产生大量不同的哈希值。

矿工的电脑负责计算新的哈希值，这些哈希值基于前一个哈希值、新交易块以及随机数的组合。

The root of all evil ???
0000 0000 0000 ...
创建哈希的计算微不足道，但是比特币系统要求新的哈希值拥有特定的格式——必须以一连串特定数量的0开始。

矿工无从知道哪一个随机数可以产生一个这样的哈希值（以特定数量的0为开头）。所以他们不得不使用不同的随机数生成大量的哈希值，直到他们碰巧找到一个符合规则的哈希值。



每一个区块都包含一个名为“coinbase”的初始交易，这个交易是胜出挖矿挖矿所得，金额为50BTC——在这个例子中，是Gary。新挖到的比特币会被支付到Gary的钱包里面一个新生成的地址中。

交易验证

随着时间流逝，爱丽丝发给波比的传送被埋藏到其他最近交易下面，因为只要有人修改了细节，他就必须重新做一遍Gary所做的事情——因为所有的改变都需要一个完全不同的胜出随机数——然后，其他所有下一级的矿工又继续重复这个工作，这样作弊就几乎不可能实现。



波比和爱丽丝

“慧眼识珠”是中国领先的投融资研究大数据分享平台






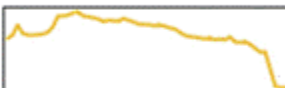



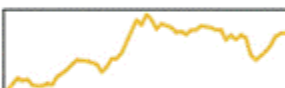










点击进入 <http://www.chinabn.com.cn>



■ 区块链所解决问题

- 解决双花问题
- 解决拜占庭将军问题*
- 建立了全球皆共识的交易准则和游戏规则
- 解决对于比特币拥有者的共识问题
- 让伪造比特币变成不可能
- 让伪造虚拟支付变成不可能
- 隐秘性强，不容易被追踪

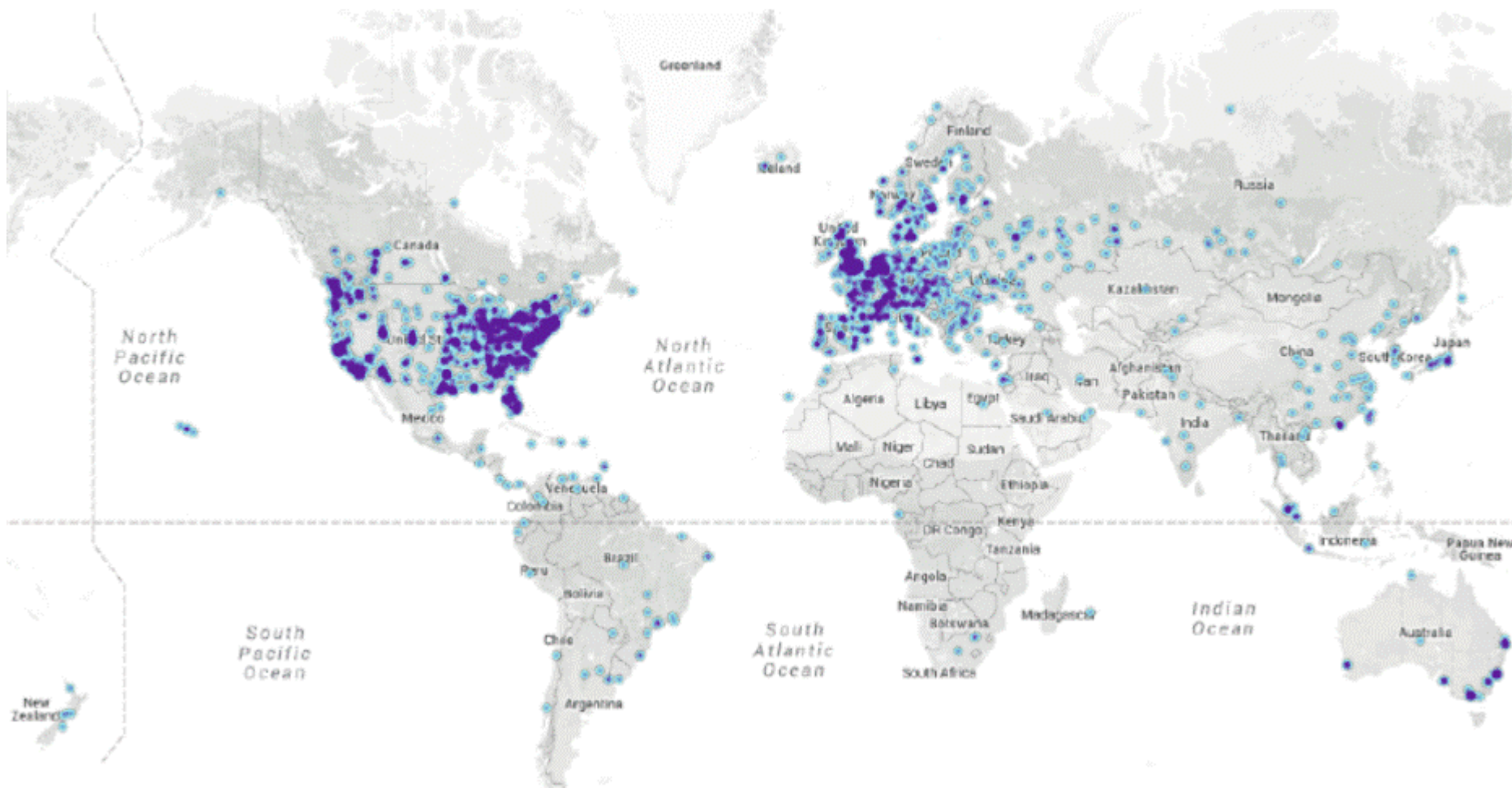
比特币是目前最热门的数字货币

▲ #	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$ 6,539,757,721	\$ 425.50	15,369,475 BTC	\$ 57,546,600	-0.14 %	
2	 Ethereum	\$ 908,325,546	\$ 11.56	78,551,091 ETH	\$ 18,770,800	2.39 %	
3	 Ripple	\$ 261,702,720	\$ 0.007599	34,439,870,367 XRP *	\$ 2,432,970	-5.12 %	
4	 Litecoin	\$ 147,594,991	\$ 3.27	45,119,801 LTC	\$ 763,113	-0.67 %	
5	 Dash	\$ 45,004,910	\$ 7.11	6,328,078 DASH	\$ 551,172	2.00 %	
6	 MaidSafeCoin	\$ 40,264,810	\$ 0.088973	452,552,412 MAID *	\$ 196,236	-1.21 %	
7	 Dogecoin	\$ 22,756,910	\$ 0.000219	103,683,687,450 DOGE	\$ 163,553	2.16 %	
8	 Monero	\$ 16,966,142	\$ 1.48	11,440,419 XMR	\$ 471,820	-4.29 %	
9	 BitShares	\$ 15,426,521	\$ 0.006050	2,549,926,690 BTS *	\$ 336,478	-2.33 %	
10	 Factom	\$ 14,980,697	\$ 1.71	8,753,219 FCT *	\$ 352,615	-3.61 %	

比特币区块链的节点在哪里：



- 截止至2015年9月14日，比特币网络中共有5,995个节点
- 每个节点有比特币的完整交易历史（大约83,000,000次交易）



“慧峰资讯”是中国领先的投融资研究大数据分享平台

资料来源：Bitnodes, <https://bitnodes.21.co/nodes/live-map/>

点击进入 <http://www.chinabn.com/cn>

比特币历史价格走势



■ 目前比特币价格波动性较大

■ 金融体系风险、监管态度、应用范围成为左右价格走势关键因素



“慧眼资讯”是中国领先的投融资研究大数据分享平台

点击进入 <http://www.chinabai.com.cn>

- 发达国家普遍接受程度较高，发展中国家普遍对于比特币持怀疑态度
- 特定国家可以利用比特币达成特定目的（例：菲律宾）

中国：

2013年12月5日，五部委联合发布《关于防范比特币风险的通知》：比特币交易作为一种互联网上的商品买卖行为，普通民众在自担风险的前提下拥有参与的自由。

2016年1月20日，中国人民银行数字货币研讨会要求，人行数字货币研究团队要积极吸收国内外数字货币研究的重要成果和实践经验，在前期工作基础上继续推进，建立更为有效的组织保障机制，进一步明确央行发行数字货币的战略目标，做好关键技术攻关，研究数字货币的多场景应用，争取早日推出央行发行的数字货币。

日本：

2014年3月，日本内阁禁止银行证券公司从事比特币业务，但未对比特币作出定性，并不采取对比特币交易进行监管，同时对比特币购买的消费征税上采取灵活弹性政策。

2014年，东京比特币交易所Mt Gox破产后，日本政府开始积极地规范比特币活动。

2015年12月，日本金融服务机构工作小组的高层金融监管机构制定了一系列的建议，以便监督全国的交易所。该提议已经接近于完成，并将提交给日本的国家立法机关——国会，明年会纳入考虑。

欧盟：

2015年10月，欧盟法院裁定，比特币及其他虚拟货币的交易将免征增值税（VAT）。这意味着，在接下来的虚拟货币交易中，将无需为其缴税。

2013年8月，德国财政部表示比特币没有被归类为电子货币或者外汇，但它是一种在德国银行业条例下的金融工具。与私人货币更接近，可用来做多边结算。

2015年3月，财政部发表数字货币相关报告，建议反洗钱法规将适用于英国的数字货币交易所，英国财政部将在议会中商议数字货币的监管模式，政府将与英国标准协会（BIS）以及数字货币行业共同制定一个“最佳”的监管框架，以保护消费者权益。此外，英国政府增加1000万英镑经费用于研究数字货币，旨在将数字货币转化为就业机会和相关服务产业。

世界各国对比特币监管态度



比特币受监管政策影响



■ 发达国家普遍接受程度较高，发展中国家普遍对于比特币持怀疑态度

■ 特定国家可以利用比特币达成特定目的（例：菲律宾）

欧盟：

西班牙国会将会把比特币视为一种电子支付系统，并强调比特币企业应当遵守其他法律。

2015年，西班牙财务部作出了对数字货币免征增值税的决定；同年8月，西班牙税务总局（DGT）明确了该国现行税法应如何适用于因为比特币交易所的崩溃或者骗局破产而造成用户财产损失的情况。

2015年9月，比利时财政部(FPS)正式宣布：境内所有虚拟货币交易将免征增值税。但目前，比特币仍未被官方承认为法定货币。

巴西：

2015年9月，巴西众议院举行了关于比特币监管议案的听证会，如果该议案通过，该国的中央银行将有权监管数字货币。

新加坡：

2014年1月，新加坡承认比特币交易，同时出台了比特币交易的税收规则，然而，这种征税方式却在一些比特币交易中，引起双重征税问题。

美国：

2014年6月，加州州长签署的AB-129法案指出，包括数字货币、积分、优惠券在内的美元替代品为合法货币；2015年6月4日，美国纽约州金融服务局（NYDFS）发布了最终版本的数字货币公司监管框架BitLicense。

尼日利亚：

2015年8月，尼日利亚中央银行（CBN）呼吁对比特币进行监管，目的是防止洗钱、以减少国际刑事犯罪。

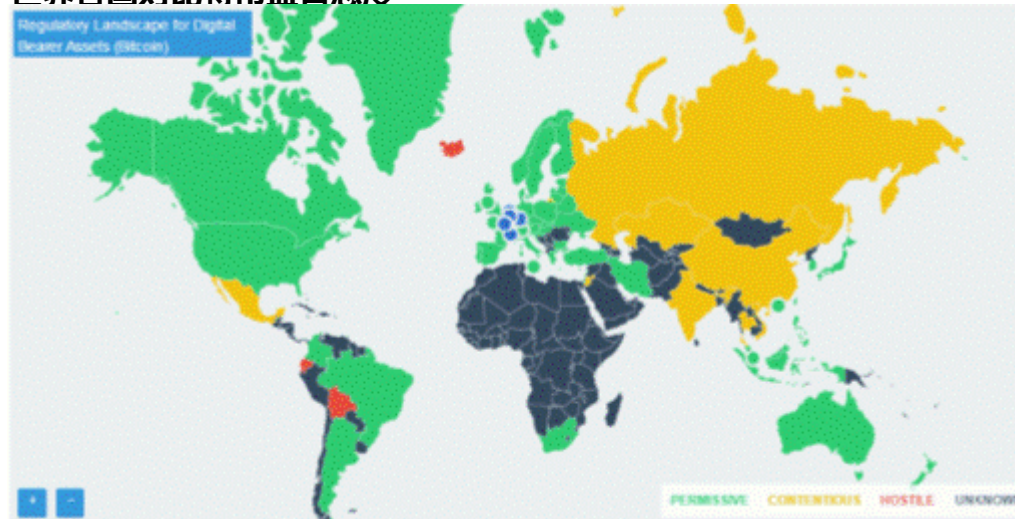
泰国：

泰国政府在2013年宣布加密货币非法。但比特币相关企业却能够获得许可和在国内运营，这表明该禁令并没有非常严格的实施。

菲律宾：

目前尚无明确监管比特币的法律法规，但国家境外汇款额巨大，比特币社区成长迅速。

世界各国对比特币监管态度



资料来源：网络资料整理

比特币商家应用案例增加



- 目前世界上已经有大量商家接受比特币
- 截至2015年5月，全球超过10万商家开始接受比特币



“慧峰资讯”是中国领先的投融资研究大数据分享平台

点击进入 <http://www.chinabiz.com.cn>

■ 比特币10大优势

- 24小时7天全天候交易
- 实时货币收发，手续费低速度快
- 无需个人信息，隐秘性强
- 钱包容易使用理解
- 如果没有拥有人持有者的合作，比特币无法被权威机构（央行）所没收或追踪
- 大量且更多的商业实体开始接受比特币
- 用户可以有大量的匿名地址
- 区块链可以有效抗衡单节点饱和攻击，网络安全性强
- 可以有效对冲实体货币存在的一些货币现象
- 先发者优势明显，比特币的流通市值目前全球最高



■ 比特币10大缺点

- 存有普遍质疑，比特币到底是否有价值，是否合法或有被合法化趋势
- 交易存在不可逆，没有权威背书监管，如果出现纠纷无法解决
- 较大的交易对手风险
- 使用比特币钱包时，如果丢失了密钥，会丢失所有比特币
- 价格波动过大，难以成为储值货币
- 比特币难以追踪的特点容易被犯罪分子所利用
- 如果规模继续扩大，或会对央行形成挑战，难以被监管层所接受
- 目前市值仍较小，存在操纵市值的可能
- 最终会固定下来的供给（2100万固定货币供给）或会造成通货紧缩，大范围国家级使用潜力有限
- 各国家安全局有可能利用技术验证用户的假名使用

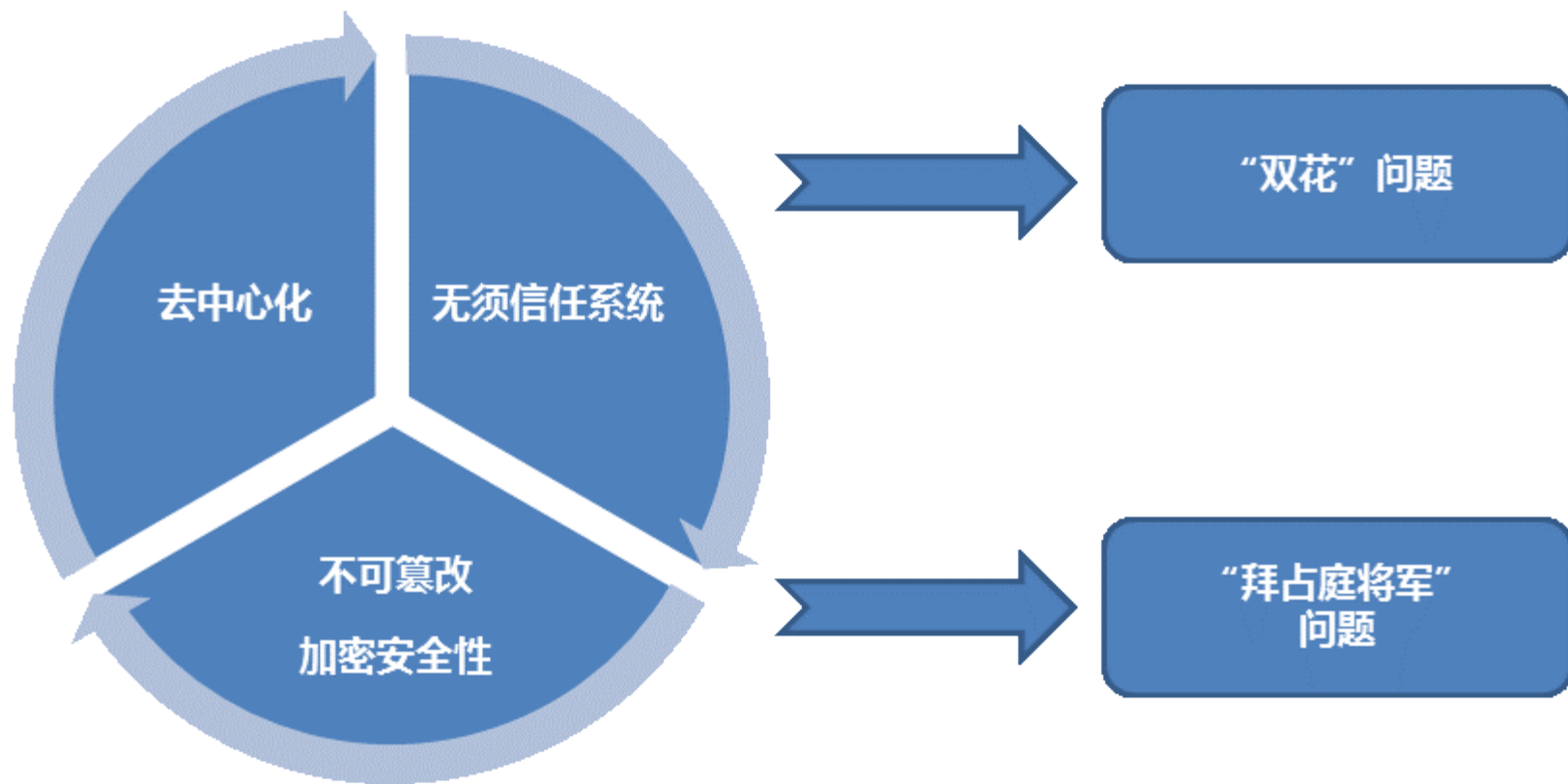
主要内容

上：技术篇

1. 区块链是什么？
- 2. 区块链有什么特点？**

下：应用篇

3. 区块链有何应用领域？
4. 区块链技术存在何种投资机会？

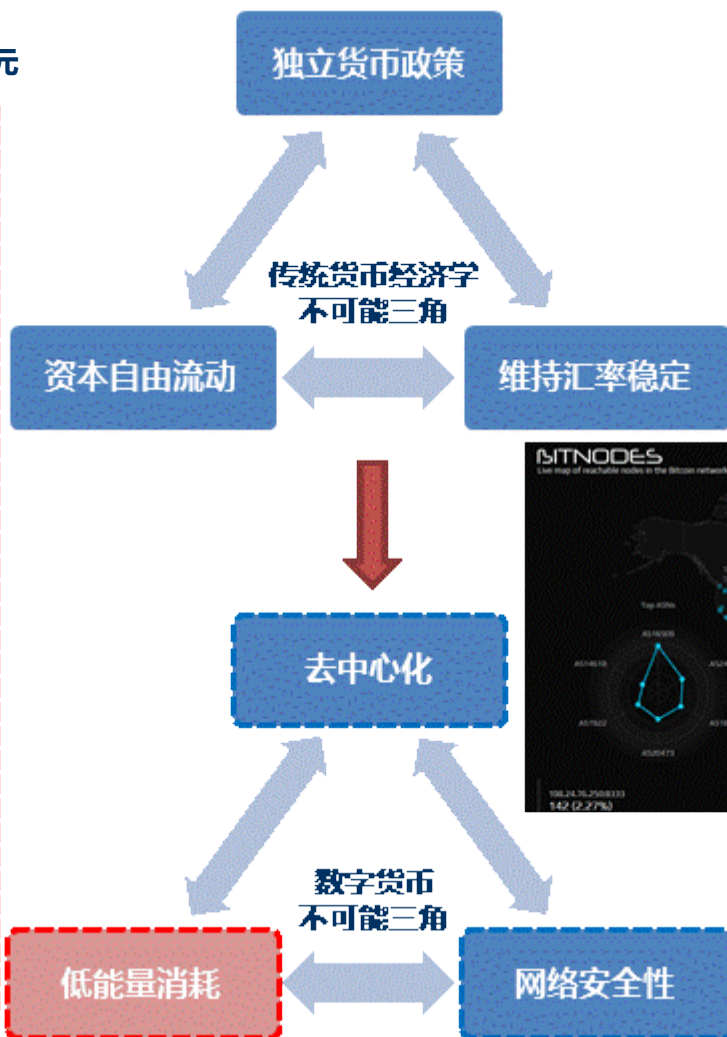
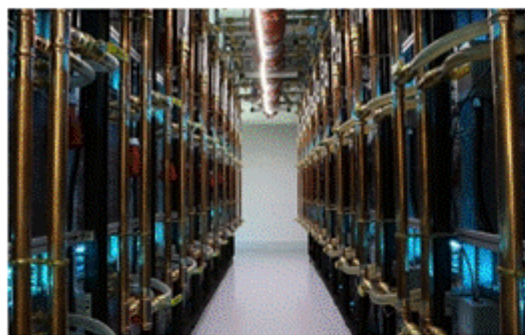


但比特币区块链的数字货币中不可能三角



- 比特币区块链以高能量消耗为代价获得去中心化和网络安全性，目前全球每天用于挖矿的电费高达100万美元

香港一家比特币矿场，每月电费消耗5万美元

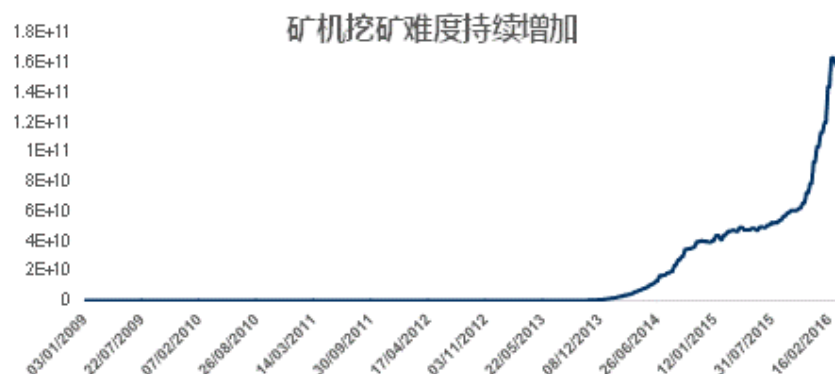
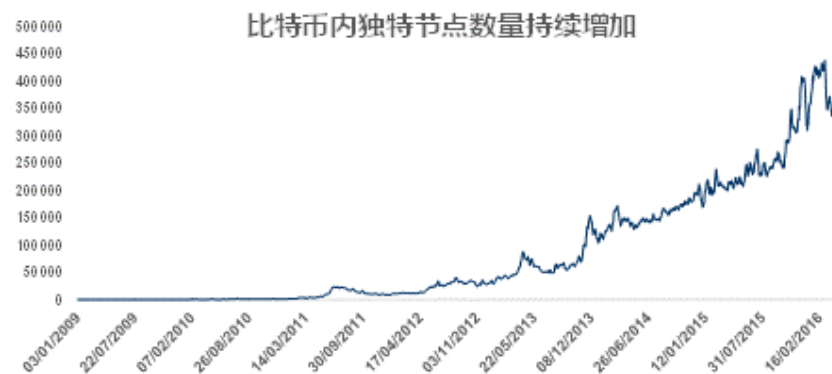
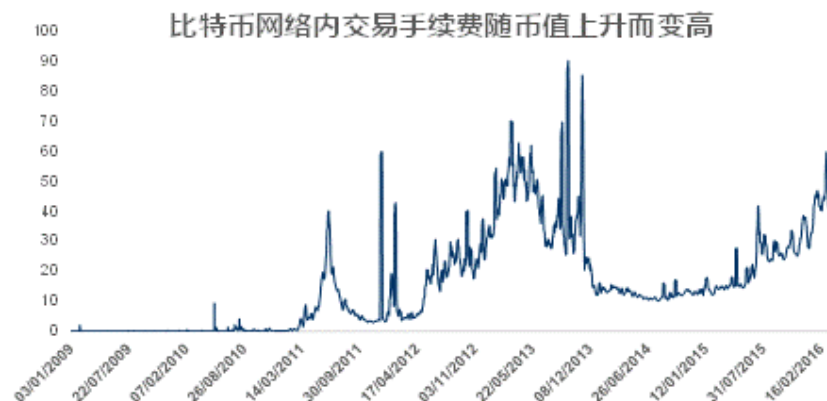
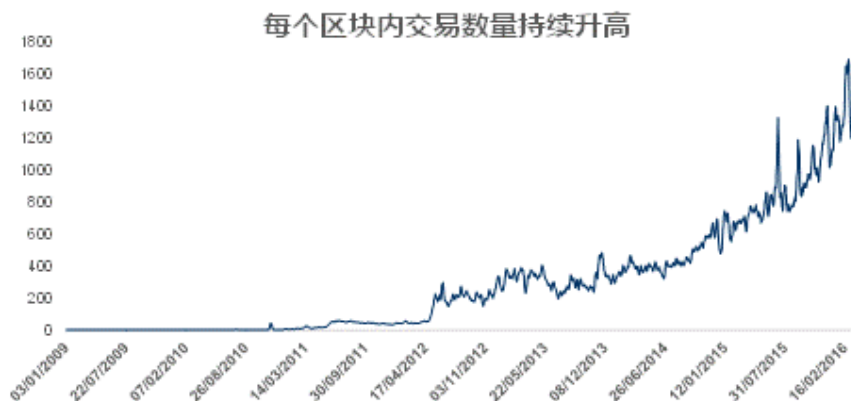


资料来源：网络资料整理，Bitnodes平台

比特币区块链



- 比特币价格上涨叠加交易频率变高大幅提高交易成本
- 初始区块容量人为设置为1MB，比特币交易增加导致容量捉襟见肘，交易量增加叠加容量设置限制导致确认时间变长
- 中国控制全网70%算力，和比特币去中心化民主的机制初衷相违背，矿机恶性竞争导致能量消耗加大



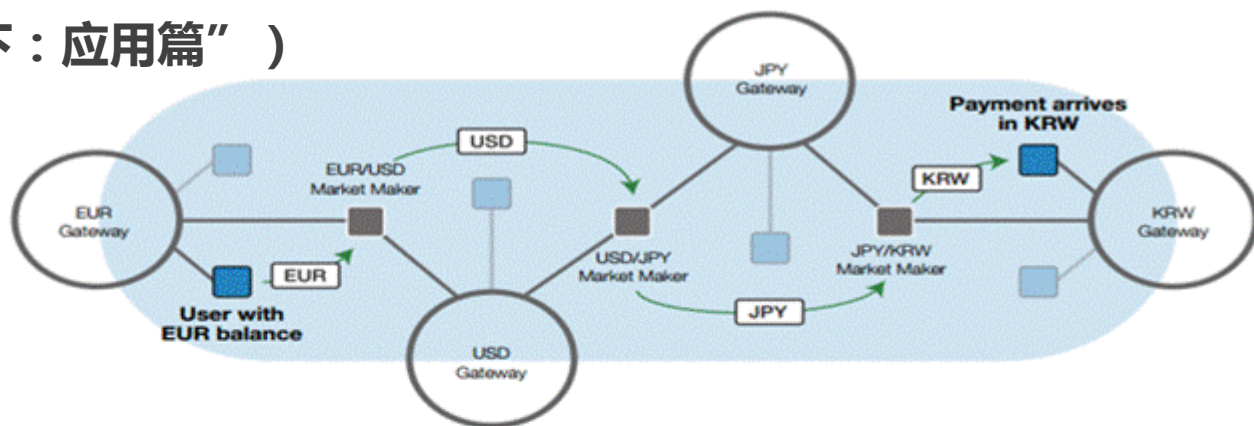
作为延伸拓展，数字货币区块链应用

■ 另类区块链（竞争币）

- 利用区块链技术，适当改进，提供比特币以外的数字货币应用
- 例如：Ripple币、以太币、狗狗币等

■ 例：Ripple币（详见“下：应用篇”）

- 第一个开放支付网络
- 网关系统（Gateway）
- 中介桥梁货币
- 安全性保证
- 基于比特币区块链去中心化的Ripple支付协议



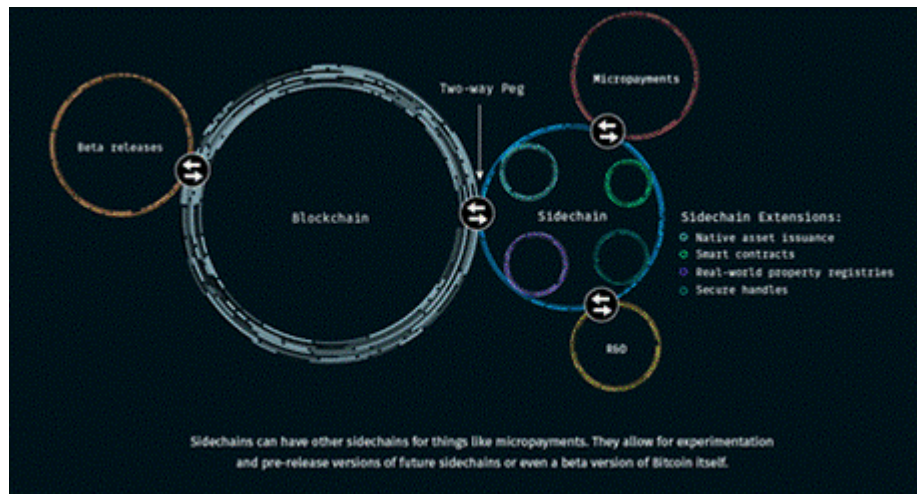
■ 局限：使用较小众，比特币区块链网络效应较强



■ 彩色币

- 利用比特币区块链技术提供数字货币应用以外其他类型资产的应用（详见“下：应用篇”）
- 资产例子：公司股权、债券、商品证书、智能财产、彩票等
- 优点：直接利用比特币区块链网络规模效应
- 缺点：加大比特币区块链扩容负担

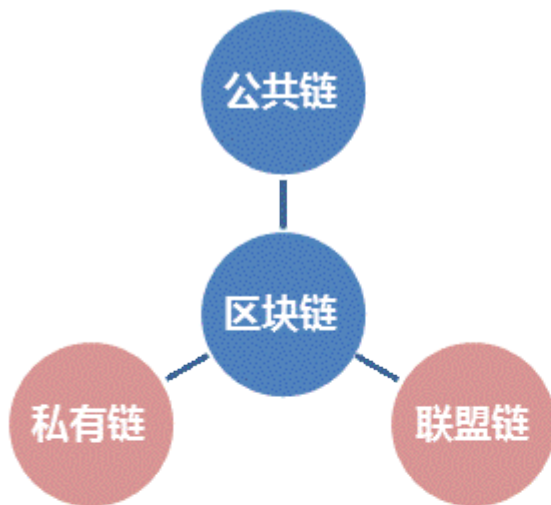
侧链和彩色币的图示



■ 侧链

- 双向挂钩
- 连接比特币区块链和彩色币区块链
- 可在侧链内进行智能合约商业模式创新
- 但不会影响核心比特币区块链的运营，加重其负担
- 侧链的发展需要获得核心比特币区块链>50%节点认可

区块链在部署方式上及展开二种形式



- **公共链**：系统安全性由工作量证明或权益证明机制保证，一般需要数字货币提供交易验证激励，容易进行应用程序大规模部署，全球范围可以访问，不依赖于单个公司或辖区，匿名性强，任何参与者都可以在中写入、读取、参与交易验证（例：比特币）。
- **联盟链**：多中心，参与人为预先根据一定特征所设定。系统内交易确认节点为事先设定，并通过共识机制确认，一般不需要数字货币提供交易验证激励。联盟链容易进行节点权限设定，拥有更高应用可扩展性。联盟链可大幅降低异地结算成本和时间，比现有系统更简单，效率更高，同时继承去中心化优点减轻垄断压力（例：全球银行加入R3，详情请参见“下，应用篇”）。
- **私有链**：没有去中心，但有分布式特点，中心控制者制定可参与和进行交易验证成员范围，系统内不需虚拟货币提供奖励（例：中国银行可以联合其全球各城市分行，完成内部数据传输备份，转帐等业务。）



	共有链	联盟链	私有链
中心化程度	分布式去中心化	多中心式	单中心式
参与主体控制	任何节点可接入	预先设定具有特定特征的参与主体	由中心控制者制定参与成员
信息公开程度	账本完全公开(可匿名)	联盟内部公开(可匿名)	公司内部公开(可匿名)

■ 另类协议机制

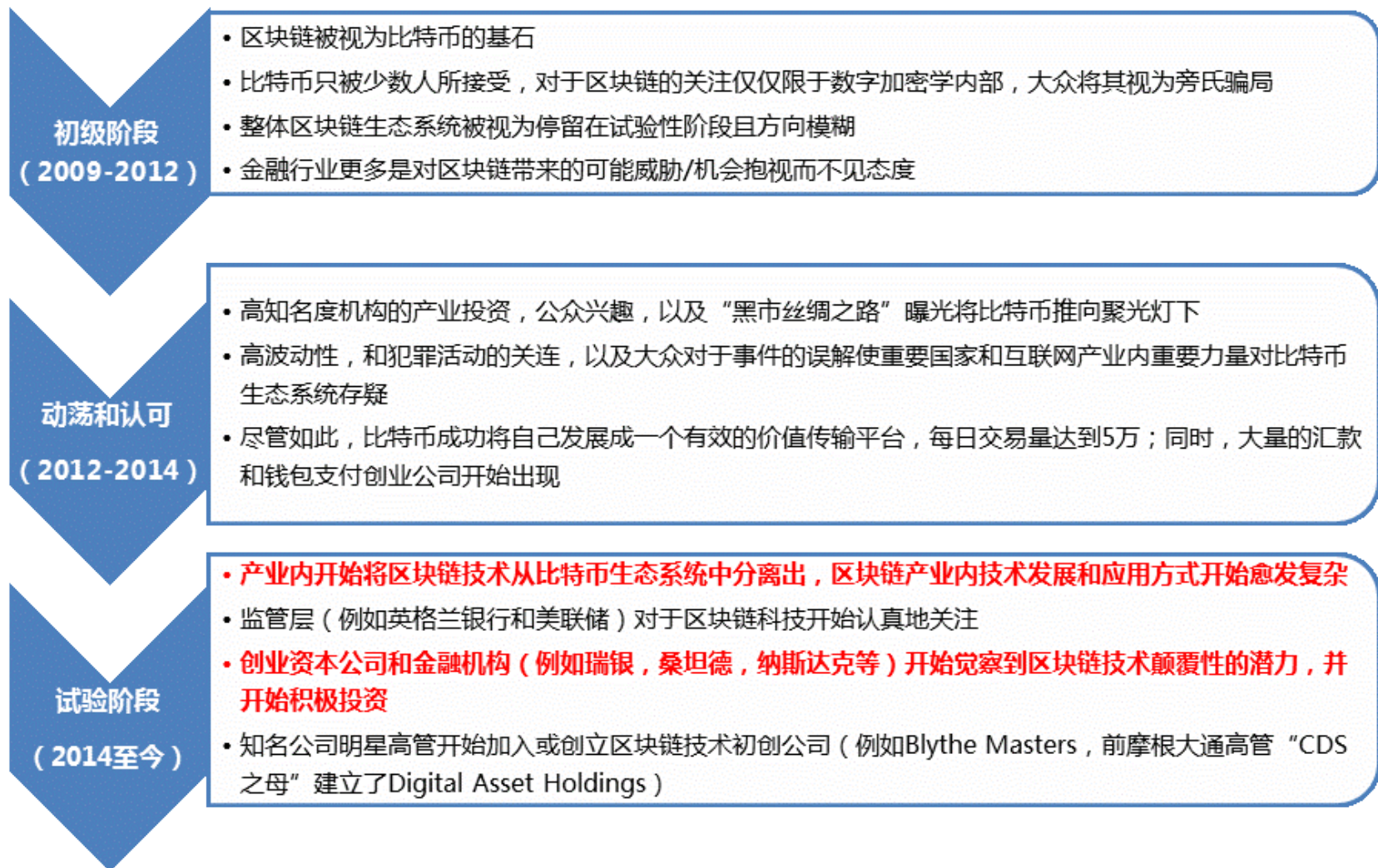
- 比特币采用的工作量证明 (Proof of Work)：实际上是算力和经济激励相结合的机制，全网计算机加入运算，算力最强的节点有临时记账权，决定交易有效性。
- 权益证明 (Proof of Stake)：“权益”概念和“公司股权”概念相类似，权益大的节点有更大概率获得记账机会。
- 议会拜占庭式证明 (Quorum/BFT)：Quorum类似于民主议会的法定最低人数，BFT则是拜占庭容错机制，运作机制为首先选择一批记账人员（节点），每隔一段时间这批记账人采取类似于议会民主投票的形式对这段时间的交易进行打包投票，达成共识。
- 另类协议机制可以大幅提升交易速度，降低能量消耗。目前新型区块链基本上都采用的是另类协议机制。

■ 另类系统运作生态系统出现 — 例，以太坊 (Ethereum)（详情请参读“下：应用篇”）

- 以太坊区块链采用权益证明（各节点通过已有的虚拟货币数量进行交易和确认），替代工作量证明
- 和比特币10分钟区块产生时间不同，以太坊新区块产生时间只需要17秒
- 无区块大小尺寸限制
- 图灵完备，可以完成复杂的计算，包括无限循环，同时具有并行处理能力，未来可以达到每秒10万次交易
- 全开源，支持编程，因此适合设计和生成智能合约



■ 区块链的发展历程简释





- 领先的数字货币
- 应用于在大量的个体、中小、以及金融服务付费、价值转移服务应用
- 因为其高度波动性和流动性，受投机者和高频交易者青睐，目前也有发达国家对冲基金参与比特币交易套利中
- **比特币挑战的是各国央行的铸币权和货币政策，未来或会面临较强监管。中国在比特币中挖矿量占据强势（70%矿产），或会对其分布民主形式造成挑战。**

- 数字加密式分布式账本
- 潜在的对于在金融交易产业内中层网络和清算所的升级和替代
- 对于对数据真实安全性强依赖的网络或应用，区块链存在广泛应用可能
- **2015年呈现投资强增长态势**
- **区块链以及衍生出的多种形式另类区块链可以帮助金融机构、物联网、各大型公司在支付、交易、信息记录等方面提升效率，存在广大应用空间**

有关区块链技术发展路线、应用场景、相关投资机会、以及国内外最新进展，请参读 **《区块链：颠覆式创新——区块链和数字货币系列报告之二（下：应用篇）》**

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。发布证券研究报告，是证券投资咨询业务的一种基本形式，本公司可以对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向本公司的客户发布。

本公司在知晓范围内履行披露义务。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、静默期安排及关联公司持股情况。

法律声明

本报告仅供上海申银万国证券研究所有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。

本报告是基于已公开信息撰写，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人作出邀请。

本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

本报告首页列示的联系人，除非另有说明，仅作为本公司就本报告与客户的联络人，承担联络工作，不从事任何证券投资咨询服务业务。

客户应当认识到有关本报告的短信提示、电话推荐等只是研究观点的简要沟通，需以本公司http://www.swsresearch.com网站刊载的完整报告为准，本公司并接受客户的后续问询。

客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为作出投资决策的惟一因素。客户应自主作出投资决策并自行承担投资风险。本公司特别提示，本公司不会与任何客户以任何形式分享证券投资收益或分担证券投资损失，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司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。市场有风险，投资需谨慎。

若本报告的接收人非本公司的客户，应在基于本报告作出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告的版权归本公司所有，属于非公开资料。本公司对本报告保留一切权利。除非另有书面显示，否则本报告中的所有材料的版权均属本公司。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。

诚信 · 进取 · 共享

INTEGRITY · INITIATIVE · SHARING



申万宏源研究S微信订阅号



申万宏源研究S微信服务号

上海申银万国证券研究所有限公司
(隶属于申万宏源证券有限公司)

王胜

wangsheng@swsresearch.com