区块链

2016最耀眼的新兴技术之一

BLOCKCHAIN - An Emerging Technology of 2016

吴志刚（ALEX.WU）

From 勤智数码

2016.10

中生代技术
FRESHMAN TECHNOLOGY

中生代技术
FRESHMAN TECHNOLOGY

区块链热潮

中生代技术
FRESHMAN TECHNOLOGY

当前处于期望膨胀期高峰

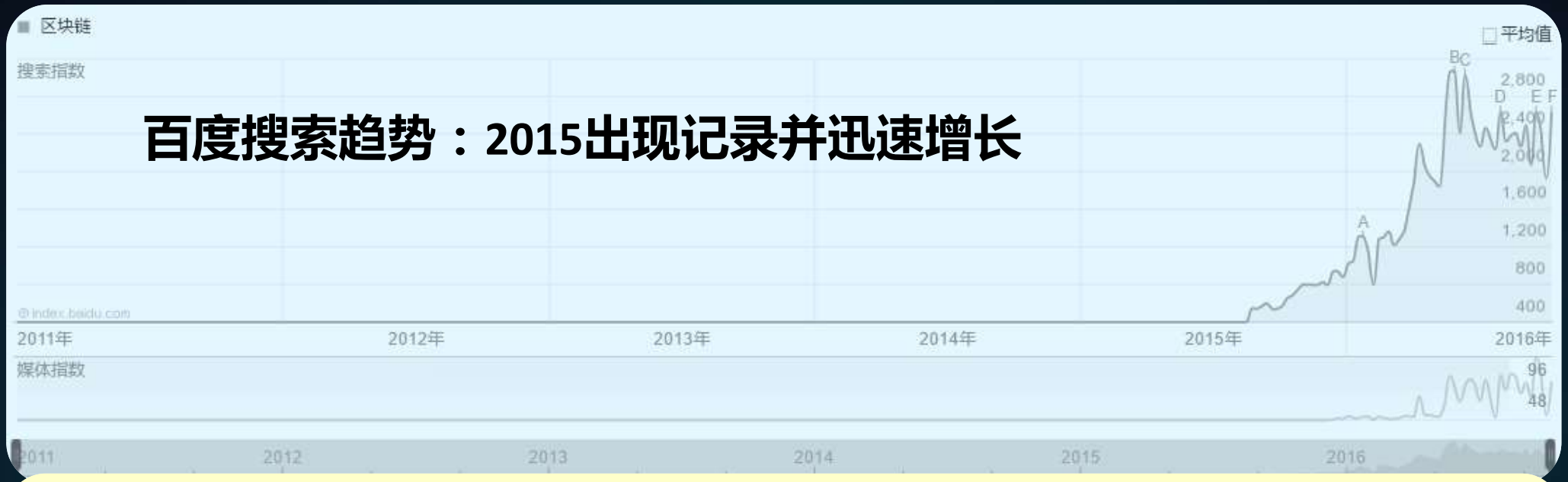
Hype Cycle for Emerging Technologies, 2016

Gartner®

2016新兴技术成熟度曲线

中生代技术 FRESHMAN TECHNOLOGY

区块链的搜索指数

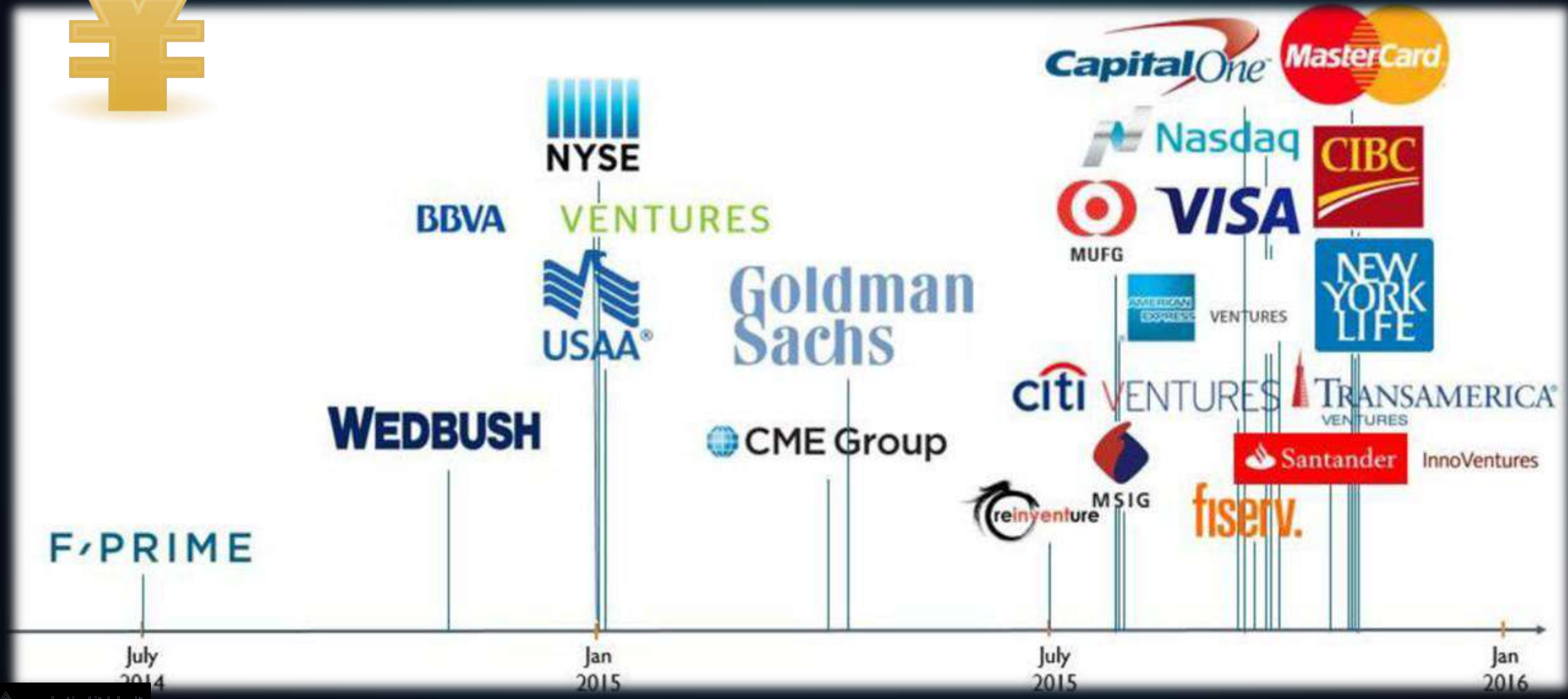


百度搜索趋势：2015出现记录并迅速增长

谷歌搜索趋势：2012就有记录，2015开始迅速增长

中生代技术 FRESHMAN TECHNOLOGY

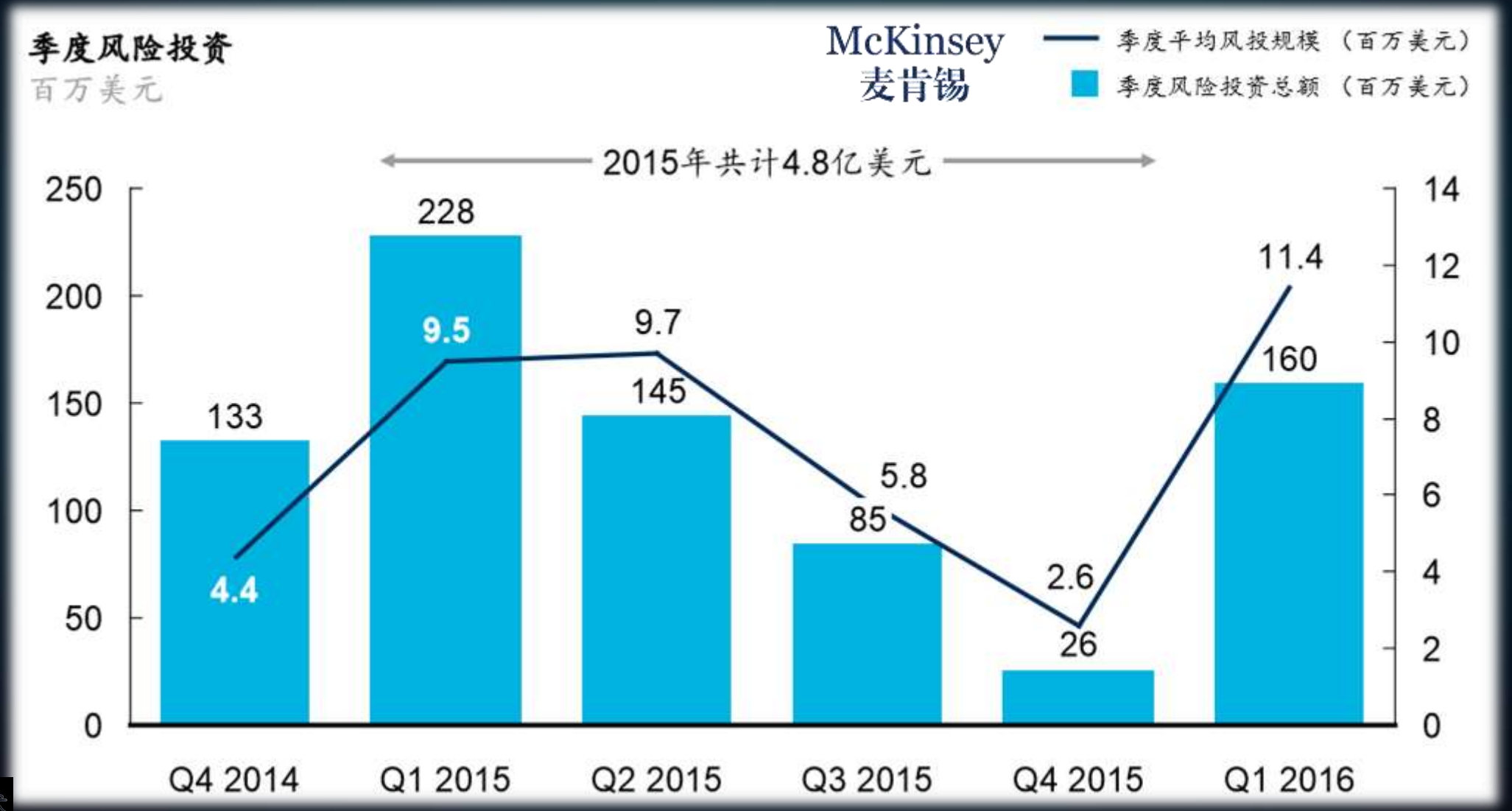
金融领域的投资布局



中生代技术 FRESHMAN TECHNOLOGY

风险投资趋势

2015年投资在比特币和区块链创新公司的风险基金约4.8亿美元，16年增速明显



中生代技术 FRESHMAN TECHNOLOGY

区块链与比特币

中生代技术
FRESHMAN TECHNOLOGY

区块链起源于比特币

区块链

关系？

比特币

区块链是比特币的底层技术，
比特币是区块链的一种应用。

了解比特币有助于我们认识区块链。

中生代技术 FRESHMAN TECHNOLOGY

比特币的出现

2008.10.31 《比特币：一种点对点电子现金系统》

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

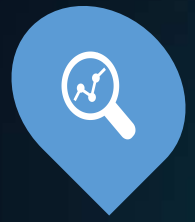
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. non-reversible transactions are not really possible, since financial institutions cannot

求真相

中生代技术
FRESHMAN TECHNOLOGY

比特币的发展



2008.8.18

“bitcoin.org”域名注册

2008.10.31

中本聪（Satoshi Nakamoto）公开比特币的设计论文

2008.11.9

比特币项目在SourceForge.net网站创建

比特币创世区块创建

2009.1.3

2009.1.12-

第一笔比特币交易被记录在170号区块上。

已经超过43万个区块，占用空间超85GB，总市值约100亿美元

2016.10

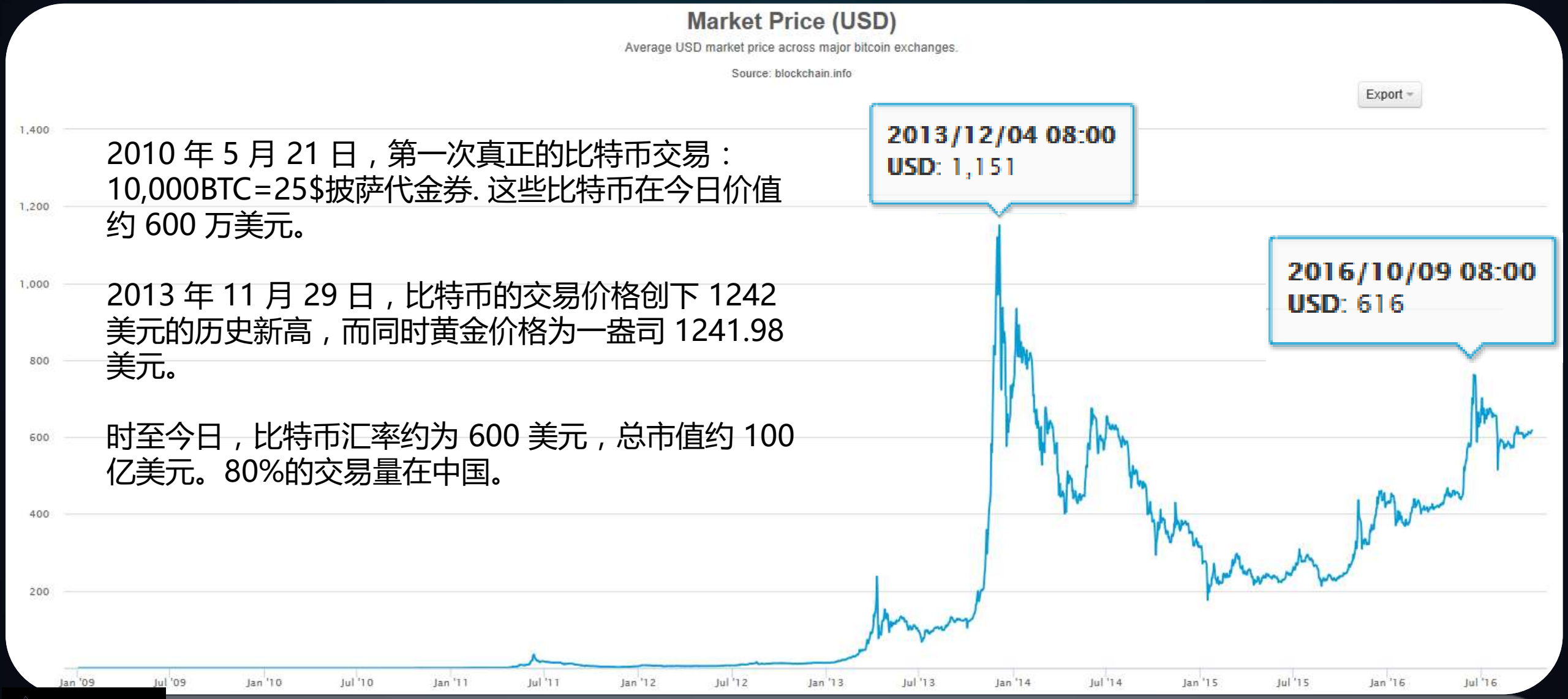
中生代技术 FRESHMAN TECHNOLOGY

比特币的价格走势

2010 年 5 月 21 日，第一次真正的比特币交易：10,000BTC=25$披萨代金券. 这些比特币在今日价值约 600 万美元。

2013 年 11 月 29 日，比特币的交易价格创下 1242 美元的历史新高，而同时黄金价格为一盎司 1241.98 美元。

时至今日，比特币汇率约为 600 美元，总市值约 100 亿美元。80%的交易量在中国。



中生代技术 FRESHMAN TECHNOLOGY

比特币的数量

中生代技术 FRESHMAN TECHNOLOGY

比特币区块链的结构

“区块”串连形成“链”

中生代技术 FRESHMAN TECHNOLOGY

真实的比特币区块

#0区块：创世区块

Block #0

BlockHash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Summary

Number Of Transactions	1
Height	1 (Mainchain)
Block Reward	50 BTC
Timestamp	Jan 9, 2009 10:54:25 AM
Mined by	
Merkle Root	0e3e2357e806b6cdb1f70b54c3a3a17b67…
Difficulty	0
Bits	1
Size (bytes)	1d00ffff
Version	215
Nonce	1
	2573394689
	2

Block #1

BlockHash 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Summary

Block #420658

BlockHash 000000000000000004226c0c0167883ccbbc68480bed178a85d52b46b5d43db62

Summary

Number Of Transactions	1255
Height	420658 (Mainchain)
Block Reward	12.5 BTC
Timestamp	Jul 14, 2016 3:34:28 PM
Mined by	AntMiner
Merkle Root	a6fa9ca3319d5b4b82e24ba648a8b5580f…

中生代技术 FRESHMAN TECHNOLOGY

比特币的工作方式

商家B接受比特币付款，消费者A拥有比特币，A购买了B的商品并采用比特币进行付款。

钱包地址

1

A和B的电脑上都有比特币钱包
A想付款给B

2

钱包是一种文件，可以让用户访问多个比特币地址。

3

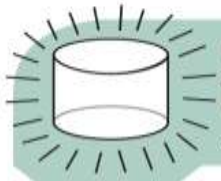
一个地址是一串由字母和数字组成的字符串

新建一个地址

4

每一个地址都有自己的比特币余额

5



B创建一个新的比特币地址，用于接收A的付款

提交付款请求

6

A告诉她的比特币客户端，她要向B的收款地址转账

私钥和公钥：
当B创建一个新地址时，他其实是生成了一个密钥对，由一个私钥和一个公钥组成。如果你使用私钥（只有你知道）对一个消息进行签名，它可以被对应的公钥（所有人都知道）所验证。B的新地址代表一个唯一的公钥，对应的私钥则保存在他的钱包里。公钥允许所有人来验证被私钥签名的消息的有效性。

可以将地址看做银行账号，但工作方式稍有不同。比特币用户可以任意创建多个地址，并且被鼓励为每一个新的交易单独创建新地址，以增强隐私性。只要没有人知道哪些地址是某人的，此人的匿名就能受到保护。

8

X、Y、Z都是比特币矿工

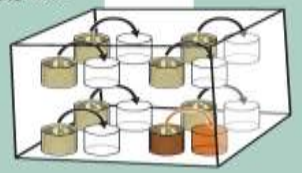
验证交易

9

他们的电脑将过去约10分钟内的交易打包成一个新的交易区块

矿工的电脑被设置用于计算加密哈希（Cryptographic Hash）函数

10



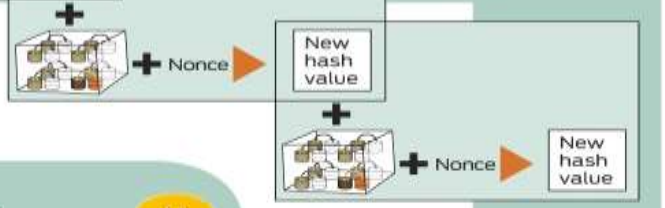
A的钱包里有她的每一个比特币地址的私[illegible]端用A此次使用的付款地[illegible]的这一交易申请进行签名

此时，网络上的任何人都可以使用公钥来验证，这个交易申请实际来自一个合法的账户所有者

• 每一个新的哈希值包含关于此前所有比特币交易的信息

12

矿工的电脑基于前一个区块的哈希值、新交易区块和随机数，来计算新的哈希值



加密哈希

11

加密哈希函数将一个数据集转换成特定长度的包含字母和数字的字符串，称为哈希值。源数据的细微改变会彻底改变哈希值的结果。并且基本不可能预测初始的数据集将会产生的特定哈希值。

为相同的数据创建不同的哈希值，比特币使用随机数来实现。随机数是在进行哈希计算之前，在数据中添加的随机数字。改变这个随机数会产生极不相同的哈希值

14

矿工无法预测哪个随机数会产生以要求的数量的0作为开始的哈希值，所以他们被迫用不同的随机数创建很多哈

创建哈希在计算上微不足道，但比特币系统要求新的哈希值拥有特定格式——必须以特定数量的0作为开始

13

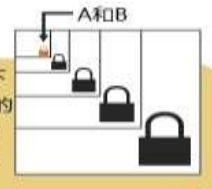
每一个区块都包含一个名为coinbase的初始交易，这是给胜出矿工的50比特币——在这个例子中是矿工X。X的钱包里生成了一个新地址，里面的余额是新挖到的比特币数量。

15

交易被验证

16

随着时间流逝，A向B的转账被埋在了其它更近期的交易下面。任何人要想修改历史交易的细节，就必须重做一遍X的工作，然后再重做所有下一级矿工的工作，因为所有的改变都需要一个完全不同的胜出随机数。这样的操作几乎不可能成功。



中生代技术
FRESHMAN TECHNOLOGY

区块链的特点

去中心化
Decentralized
权利和义务均等，具有很强健壮性。
分布式记录+分布式储存+点对点通信

集体维护
Collectively maintain
数据块由整个系统中所有具有维护功能的节点来共同维护。

去信任
Trustless
运作规则公开透明，无需相互信任，也无需第三方权威机构。
非对称加密机制
共识机制

可靠数据库
Reliable Database
每个参与节点都能获得一份完整数据库的拷贝。

中生代技术 FRESHMAN TECHNOLOGY

区块链的技术原理

中生代技术
FRESHMAN TECHNOLOGY

区块链技术架构模型

中生代技术 FRESHMAN TECHNOLOGY

区块链核心技术及机制

分布式一致性
拜占庭将军问题/双花问题
共识机制PoW/PoS/PBFT

密码学相关技术
Hash/PKI/加解密

点对点通信技术
P2P

中生代技术
FRESHMAN TECHNOLOGY

区块链中的分布式一致性

拜占庭将军问题

拜占庭将军问题是一个共识问题：首先由Leslie Lamport与另外两人在1982年提出，被称为The Byzantine Generals Problem或者Byzantine Failure。核心描述是军中可能有叛徒，却要保证进攻一致，由此引申到计算领域，发展成了一种容错理论。
对于拜占庭问题来说，假如节点总数为N，叛变将军数为F，则当（N>=3F+1）时，问题才有解，即 Byzantine Fault Tolerant (BFT) 算法。

Leslie Lamport证明，当叛变者不超过三分之一时，存在有效的算法，不论叛变者如何折腾，忠诚的将军们总能达成一致的结果。如果叛变者过多，则无法保证一定能达到一致性。

Practical Byzantine Fault Tolerant（PBFT）最早由 Castro 和 Liskov 在 1999 年提出，是第一个得到广泛应用的 BFT 算法。只要系统中有三分之二的节点是正常工作的，则可以保证一致性。
PBFT 算法包括三个阶段来达成共识：Pre-Prepare、Prepare 和 Commit。

中生代技术 FRESHMAN TECHNOLOGY

区块链中的分布式一致性

一致性问题的研究热点极具学术价值，目前还没有十分完美的机制

CAP原理

一致性（Consistency）
可用性（Availablity）
分区容忍性 （Partition）

ACID原则

Atomicity（原子性）
Consistency（一致性）
Isolation（隔离性）
Durability（持久 性）

FLP不可能原理（Fischer，Lynch，Patterson）：
在网络可靠，存在节点失效（即便只有一个）的最小化异步模型系统中，不存在一个可以解决一致性问题的确定性算法。

分布式环境下的一致性问题

无解

采用适当的机制，永远无法达成一致的可能性极小

Paxos, Raft
PBFT
PoW/PoS/DPoS

中生代技术 FRESHMAN TECHNOLOGY

区块链中的分布式一致性

PoW：工作量证明机制（比特币使用的机制。缺点：资源浪费，交易量受限，交易确认时间长）

比特币系统通过难度调节算法，增加或减少目标Hash值的大小，保证没大约10分钟产生一个区块。

1. 搜集当前时间段的全网**未确认交易**，并增加一个用于发行新比特币奖励的Coinbase交易，形成当前区块体的交易集合；
2. 计算区块体交易集合的**Merkle根**记入区块头，并填写区块头的其他元数据，其中随机数Nonce置零；
3. 随机数Nonce加1；计算当前区块头的双**SHA256哈希值**，如果小于或等于目标哈希值，则成功搜索到合适的随机数并获得该区块的记账权；否则继续步骤 3 直到任一节点搜索到**合适的随机数**为止；
4. 如果一定时间内未成功，则更新时间戳和未确认交易集合、重新计算Merkle根后继续搜索。

中生代技术 FRESHMAN TECHNOLOGY

区块链中的分布式一致性

PoS： PPC(一种点对点的权益证明(Proof of Stake)电子密码货币);
以太坊-目前仍然采用的是PoW，会择机转为PoS。

PoS 共识本质上是采用权益证明来代替 PoW 中的基于哈希算力的工作量证明, 是由系统中具有最高权益而非最高算力的节点获得区块记账权。
解决了 PoW 共识算力浪费的问题, 并 且能够在一定程度上缩短达成共识的时间。

DPoS： 授权股份证明机制 (Delegated proof of stake, DPOS)-比特股

DPoS共识机制的基本思路类似于“董事会决策”，即系统中每个股东节点可以将其持有的股份权益作为选票授予一个代表，获得票数最多且愿意成为代表的前 101 个节点将进入“董事会”，按照既定的时间表轮流对交易进行打包结算并且签署 (即生产) 一个新区块。

Casper： 以太坊未来的PoS协议

Casper是一种基于保证金的经济激励共识协议(security-deposit based economic consensus protocol)。协议中的节点，作为“锁定保证金的验证人(bonded validators)”，必须先缴纳保证金(这一步叫做锁定保证金，"bonding")才可以参与出块和共识形成。

中生代技术 FRESHMAN TECHNOLOGY

区块链中的密码学知识和技术

Hash算法
MD4/MD5/SHA-1/SHA-2

数字摘要
数据的Hash值即为其数字摘要

加密算法
对称加密：DES/3DES/AES/IDEA
非对称加密：RSA/椭圆曲线

数字签名
用私钥对数字摘要加密构成数字签名
多重签名/群签名/环签名

PKI体系
CA/RA
身份认证/防抵赖

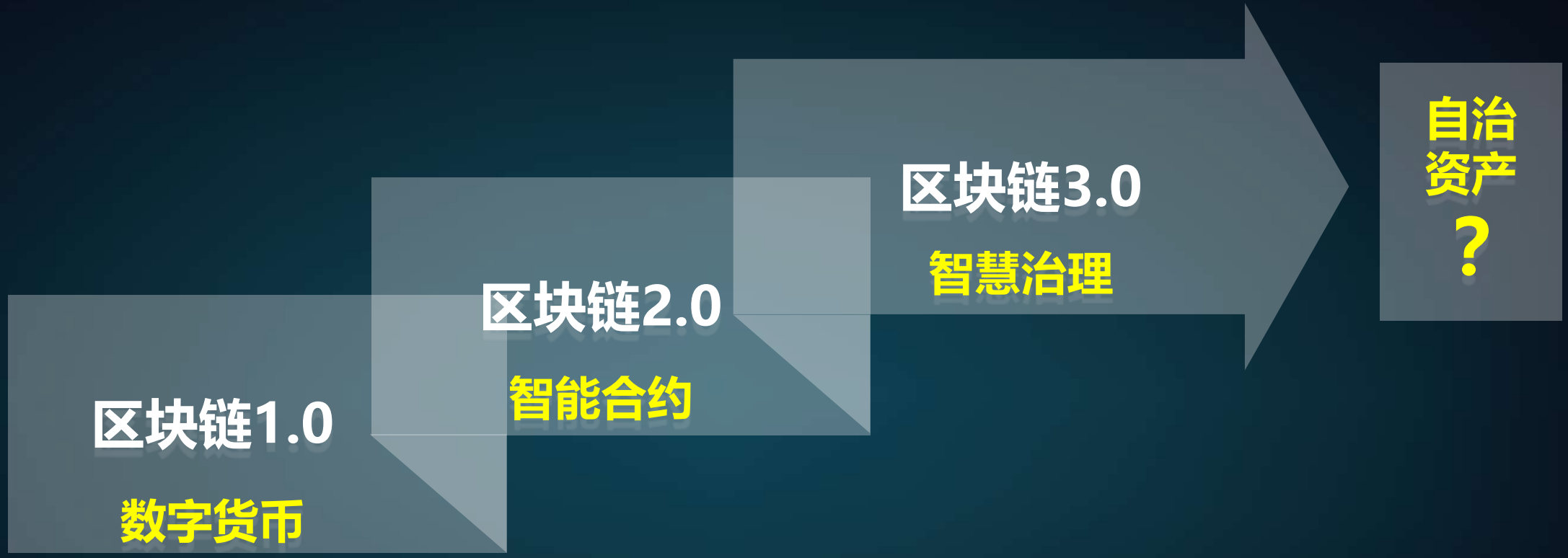
哈希树/Merkle树
快速判同/修改定位/零知识证明

中生代技术
FRESHMAN TECHNOLOGY

区块链的发展

中生代技术
FRESHMAN TECHNOLOGY

区块链的发展



数字货币

区块链解决了数字货币的“双花”问题和“拜占庭将军”问题。

可编程货币/经济

通过脚本编写合约来自动执行，从而实现了可编程的货币。但智能合约的意义远不止货币方面，可以说是无限。

资产数字化（数字资产）

区块链社会

通过区块链的公开公正特性能够完成各种商业模式及管理模式，将从根本上改变社会的管理模式。

资产智能化（智能资产）

中生代技术 FRESHMAN TECHNOLOGY

区块链的类型

任何人都可以参与使用和维护，典型的如比特币区块链，信息是完全公 开的。

集中管理者进行限制，只有组织内部的人可以使用，信息公开程度完全由组织控制。

介于两者之间，由若干组织一起合作维护一条区块链，有权限的管理，相关信息会得到保护，典型如银联组织。

中生代技术 FRESHMAN TECHNOLOGY

区块链即服务BaaS

区块链即服务

云的出现，让传统信息行业变得前所未有的便捷。只要云中有的服务，通过简单的几下点击，就可以获得一个运行中的服务实例，节约了大量的研发和运维的时间和成本。

目前，业界已经开始有少数区块链前沿研发团队开发了区块链即服务（Blockchain as a Service，BaaS）的平台。

BaaS平台可以面向用户群体提供联盟链及公开链两种服务，并根据不同的服务类型进行不同的架构设计及优化。

中生代技术 FRESHMAN TECHNOLOGY

4

区块链的应用

中生代技术
FRESHMAN TECHNOLOGY

各种领域的应用

126项目

43

学术

身份识别

股票交易

物联网

政府

银行

音乐

媒体娱乐

健康

安全

智能合约

汇款支付

供应链

贸易

客户审计

防伪

公共事业

拼车

电商

预报预测

药物

中生代技术
FRESHMAN TECHNOLOGY

金融领域的应用

数字货币	提高货币发行便利性
跨境支付与结算	实现点到点交易，减少中间费用
票据与供应链金融业务	减少人为介入，降低成本及操作风险
证券发行与交易	实现准实时资产转移，加速交易清算速度
客户征信与反欺作	降低法律合规成本，防止金融犯罪

中生代技术 FRESHMAN TECHNOLOGY

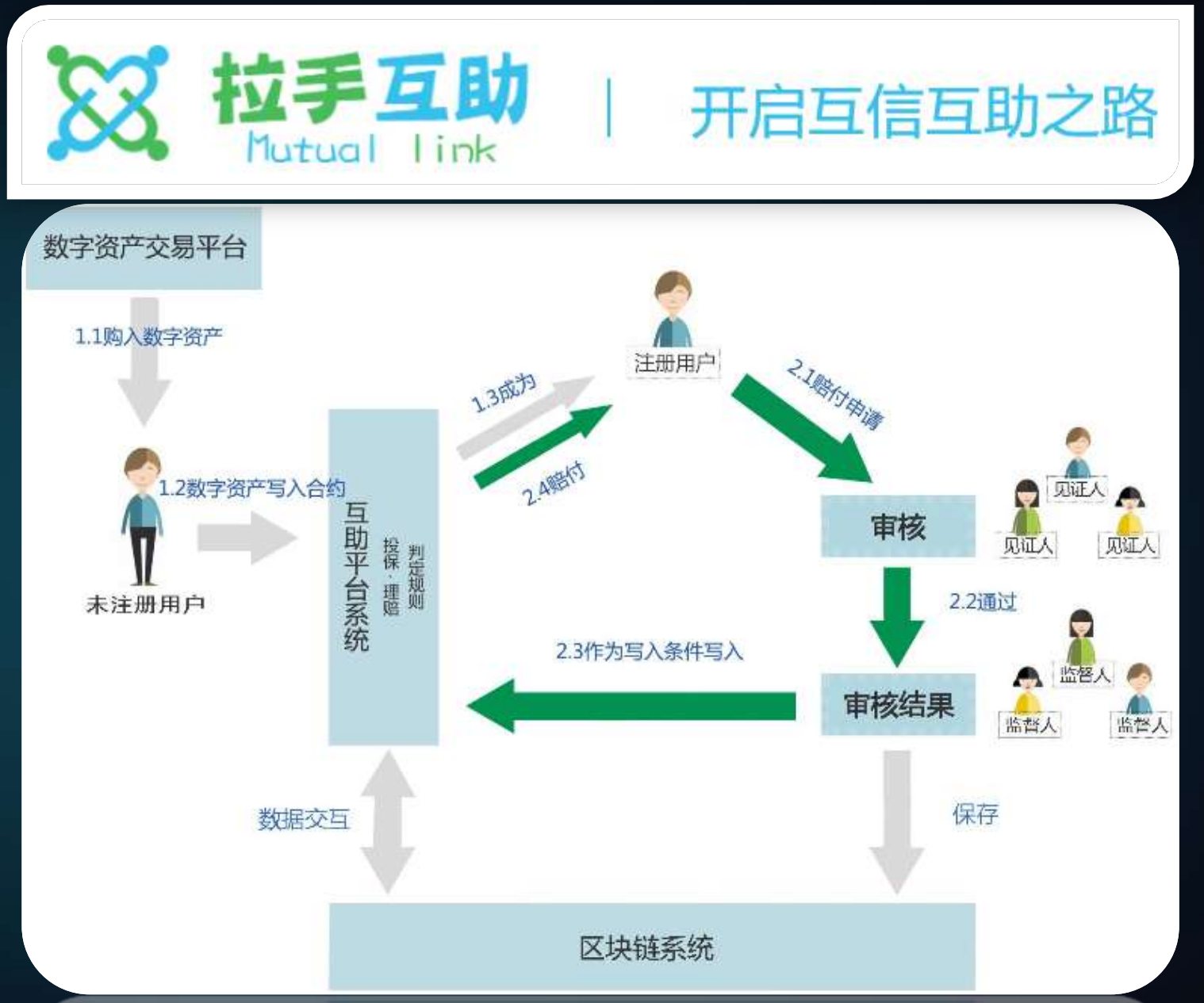
金融领域的应用

金融服务主要交易环节	金融交易发起	交易前验证	交易审批	合同签订	交易处理	账务处理	交易完成
现有流程痛点	▪ 手工发起 ▪ 需要人工干预	▪ 人工验证/审批 ▪ 信息分散、不透明 ▪ 欺诈骗局 ▪ 多方介入：公证、律师等 ▪ 等待时间较长	▪ 纸质合同传送成本高	▪ 交易时滞 ▪ 系统失误/不兼容 ▪ 手工处理			
区块链技术优势	▪ 系统自动触发（智能合同）	▪ 快速实时验证与审批 ▪ 无需第三方参与 ▪ 信息透明、安全可靠 ▪ 反欺诈 ▪ 无纸化审批	▪ 智能合约	▪ 跨系统信息实时同步 ▪ 最小化系统无误	▪ 不需要账务处理	▪ 交易记录永久且不可篡改	

中生代技术 FRESHMAN TECHNOLOGY

保险领域的应用

“区块链+智能合约”应用到互助保险这样一个新兴的领域，此举有望完美解决传统保险行业遗留下来的信任相关的难解问题且又能完整保留传统互助保险的优势。



保险领域的应用

2016年7月29日，阳光保险推出“区块链+航空意外险卡单”，是国内首个将主流金融资产放在区块链上流通。

“数贝荷包”作为构架在区块链上的数字资产管理平台，为新产品的研发提供了技术对接和功能支持。

中生代技术
FRESHMAN TECHNOLOGY

医疗领域的应用

除了金融领域外，目前医疗领域是块链技术的第二大应用领域。主要方向包括病例信息的隐私性保护；医疗信息记录保存；药物治疗证明保存，基因数据的管理及保护等。创造新价值以及增强医疗体验的机会无处不在。

飞利浦医疗和TIERON 合作，希望让飞利浦医疗通过区块链技术来完成关于病历资料的认证，或者是病历方面的隐私保护。

可有效解决医院之间对检查数据的互认问题。

中生代技术
FRESHMAN TECHNOLOGY

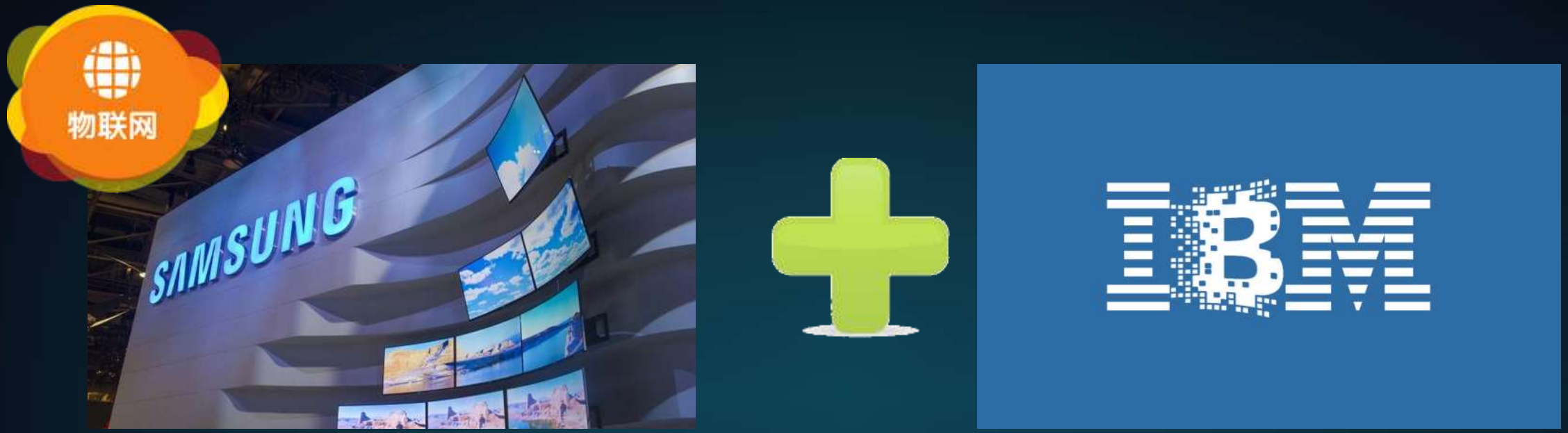
证明记录的应用

学历证明：通过区块链技术来管理和核实学生获得学历证书。可有效防止学历造假。

钻石防伪：Everledger主要为钻石认证账户及其交易历史提供一个防篡改的数字化分类账，可同时提供认证服务，主要客户为保险公司，同时有助于法律监管实施

中生代技术 FRESHMAN TECHNOLOGY

物联网领域的应用

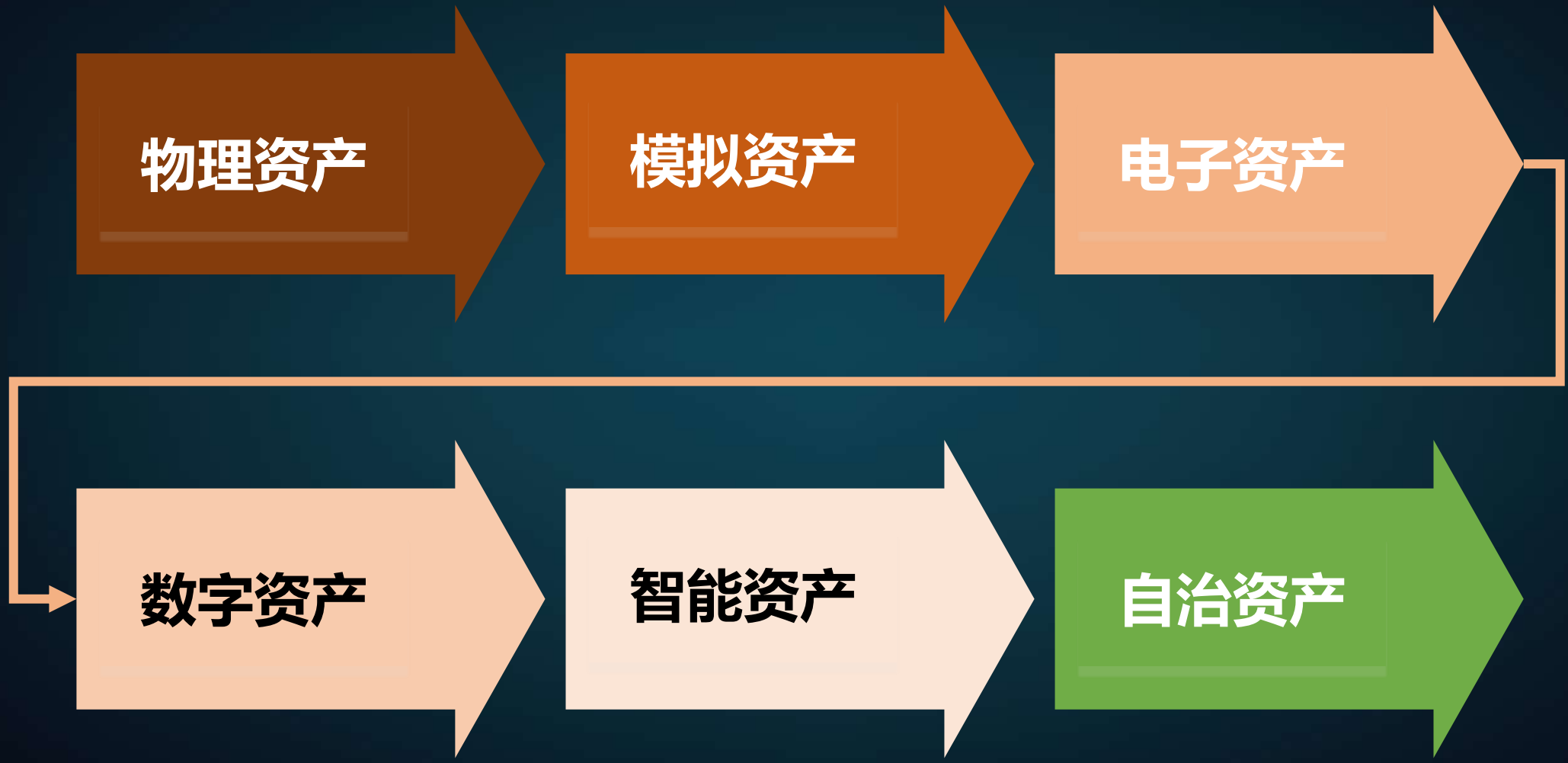


高容错性的物联网区块链技术，具有广阔的发展前景。区块链是解决物流系统中信息传输不确定性问题的理想方案，对供应链中的物流信息提供认证服务，并通过区块链数据库追踪问题所在，解决各类高端消费品的仿制问题。

市场上比较知名的是IBM 和三星提出的以太坊物联网解决方案，并融资约1800万美元支持项目研究。
另一个例子是Skuchain，利用区块链技术可以解决假货的问题，具体来说可以解决某个葡萄酒品牌年产1万瓶却在中国销售了10万瓶的情况。

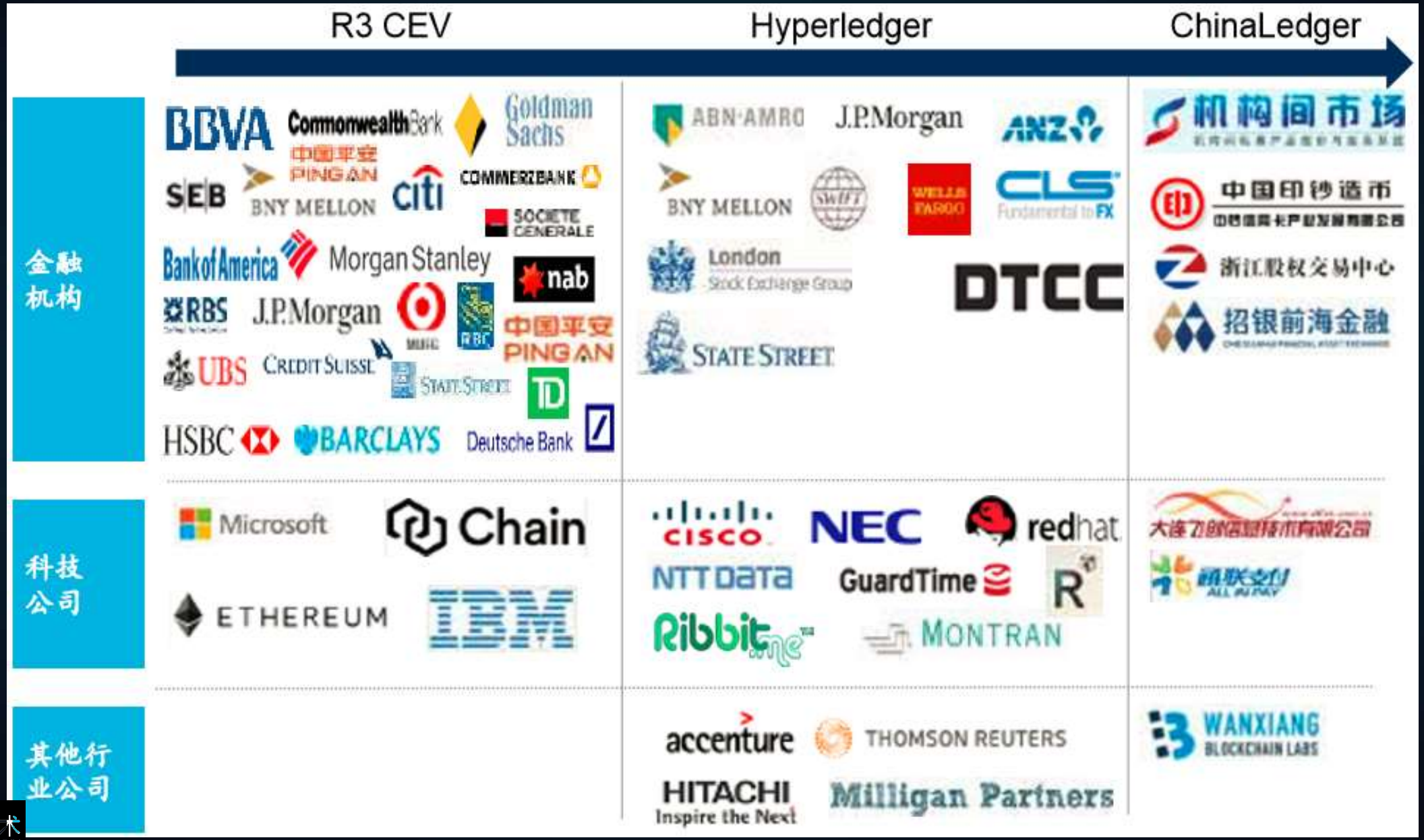
中生代技术 FRESHMAN TECHNOLOGY

区块链的应用路径



中生代技术
FRESHMAN TECHNOLOGY

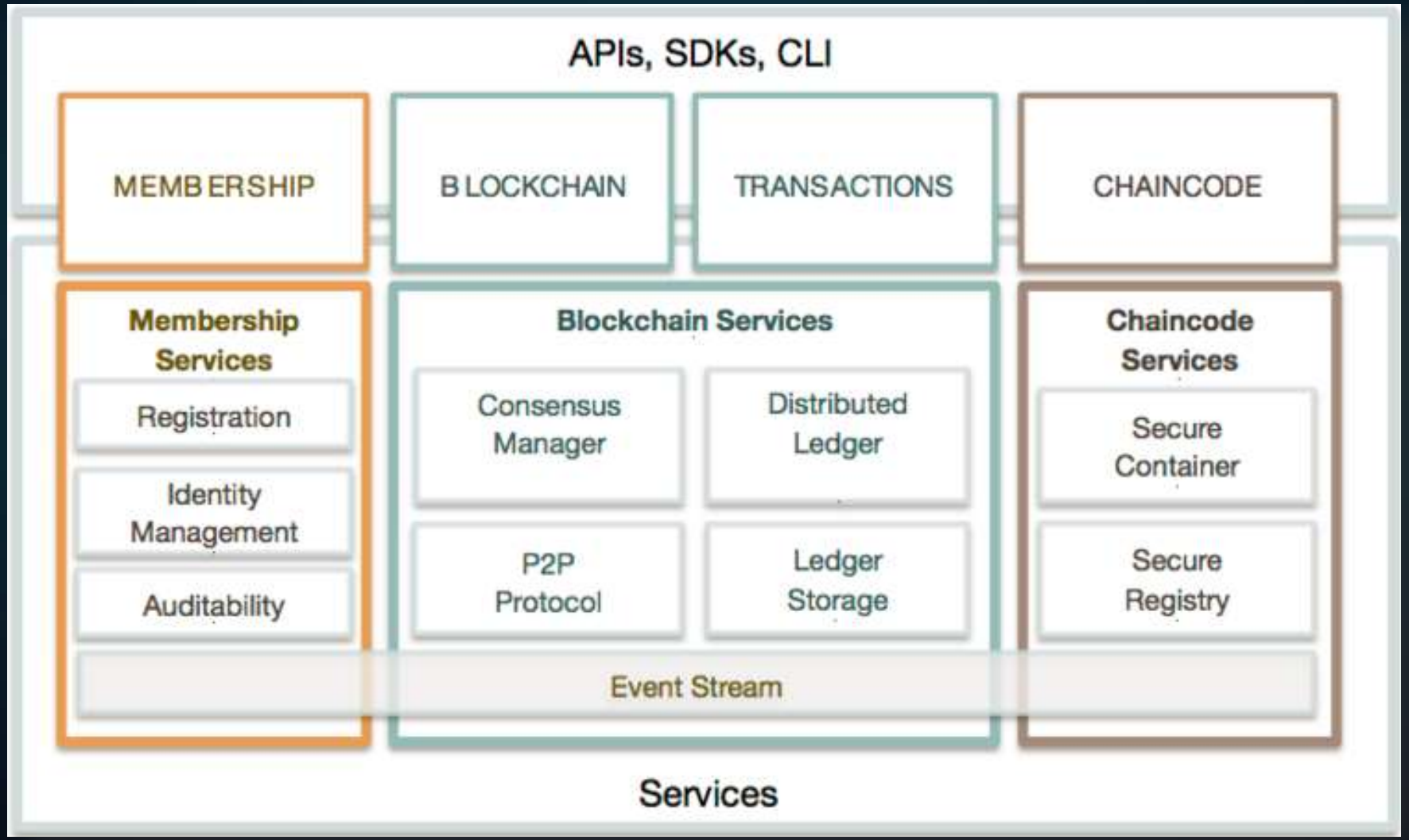
区块链联盟



中生代技术
FRESHMAN TECHNOLOGY

区块链开源项目-Hyperledger

Hyperledger项目是开源界面向开放、标准区块链技术的首个重要探索，在Linux基金会的支持下，吸引了众多科技和金融巨头的参与。



中生代技术 FRESHMAN TECHNOLOGY

区块链开源项目-Hyperledger

Demo示例

一：信息公证

chaincode_example01.go
主要实现如下的功能：
1. 初始化，以键值形式存放信息；
2. 允许读取和修改键值。

代码中首先初始化了hello_world的值，并根据请求中的参数创建修改查询链上key中 的值，本质上实现了一个简单的可修改的键值数据库。可通过REST API操作智能合约。

二：交易资产

chaincode_example02.go
主要实现如下的功能：
初始化A、 B两个账户，并为两个账户赋初始资产值；
在A、 B两个账户之间进行资产交易；
分别查询A、 B两个账户上的余额，确认交易成功；
删除账户。

中生代技术 FRESHMAN TECHNOLOGY

区块链开源项目-Hyperledger

Demo示例

三：数字货币发行与管理

该智能合约实现一个简单的商业应用案例，即数字货币的发行与转账。在这之中一共分为三种角色：中央银行，商业银行，企业。其中中央银行可以发行一定数量的货币，企业之间可以进行相互的转账。

四：学历认证

该智能合约实现了一个简单的征信管理的案例。针对于学历认证领域，由于条约公开，在条约外无法随意篡改的特性，天然具备稳定性和中立性。
该智能合约中三种角色如下：

学校
个人
需要学历认证的机构或公司

学校可以根据相关信息在区块链上为某位个人授予学历，相关机构可以查询某人的学历信息，由于使用私钥签名，确保了信息的真实有效。为了简单，尽量简化相关的业务，另未完成学业的学生因违纪或外出创业退学，学校可以修改其相应的学历信息。

中生代技术 FRESHMAN TECHNOLOGY

我们区块链技术的应用探索

WiSERV 勤智数码 Technologies
Your IT Managed Wiser

HYPERLEDGER PROJECT

01 政务数据共享交换

02 数据交易

03 新金融监管

中生代技术 FRESHMAN TECHNOLOGY

TNANKS

中生代技术
FRESHMAN TECHNOLOGY