6000年金融科技创新简史（FinTech）
实操区块链技术成为大师（Master)
探讨区块链应用落地（Business）

徐立春

根源链 COO

第一版：2015年8月6日
最新版：2017年9月24日
网站：ZhangLian.info（账链）

区块链，Block chain，真实可靠不可篡改，保护隐私和商业秘密？相关的讨论问题清单？

一．区块链为什么能火起来？

二．区块链在金融领域的应用除了做电子货币，还有什么什么应用？比特币与区块链的关系是啥？

三．区块链的技术架构、应用前景和市场规模

- ◆ 区块链从技术或者架构的角度来看有哪些突破？

四．目前区块链技术的应用难点或者障碍是什么？目前国内的区块链应用和研究有哪些？快不快？

五．创业机会在哪里？区块链对于时间银行和互助保险的应用除了金融行业，其他行业还有什么使用场景？区块链的创新应用场景未来区块链的业务

六．此应用以及该领域会不会有黑客？

七．区块链未来的方向？私有区块链的前景如何？

八．区块链的风险是什么？其技术的可靠性如何？

九．ICO是啥？

话题1：金融科技的进化。

1万年前，人类各部落从采集社会进入到农业社会之后，伴随着剩余物出现，开始出现私有制、专业分工和市场交换，从而市场经济、货币金融出现。

这时人类社会由游牧部落向定居的村落演变，规模在变大，超过150人邓巴数。而经过数百万年演化过来的人类的大脑并不擅长计数，所以必须要借助工具（技术）来完成对社会运营，税收，契约等等的记录。

考古以及历史记录说明：数学科技的主要目的是为了做税务和贸易等相关计算，为了解数字间的关系，为了测量土地，以及为了预测天文事件而形成的。

显然，金融技术要依靠、使用那个时代最新的数学理论发展。

曾经的金融市场是寺庙、当铺、咖啡馆。

目前学界的看法是：

- 金融起源于古代的中东
- 早期发展出现在中国和中亚
- 现在法人资本主义是西欧产品
- 而现代金融创新的地点是美国

善于想象的人类协作时 信息技术 的进化（Information Technology）三要素

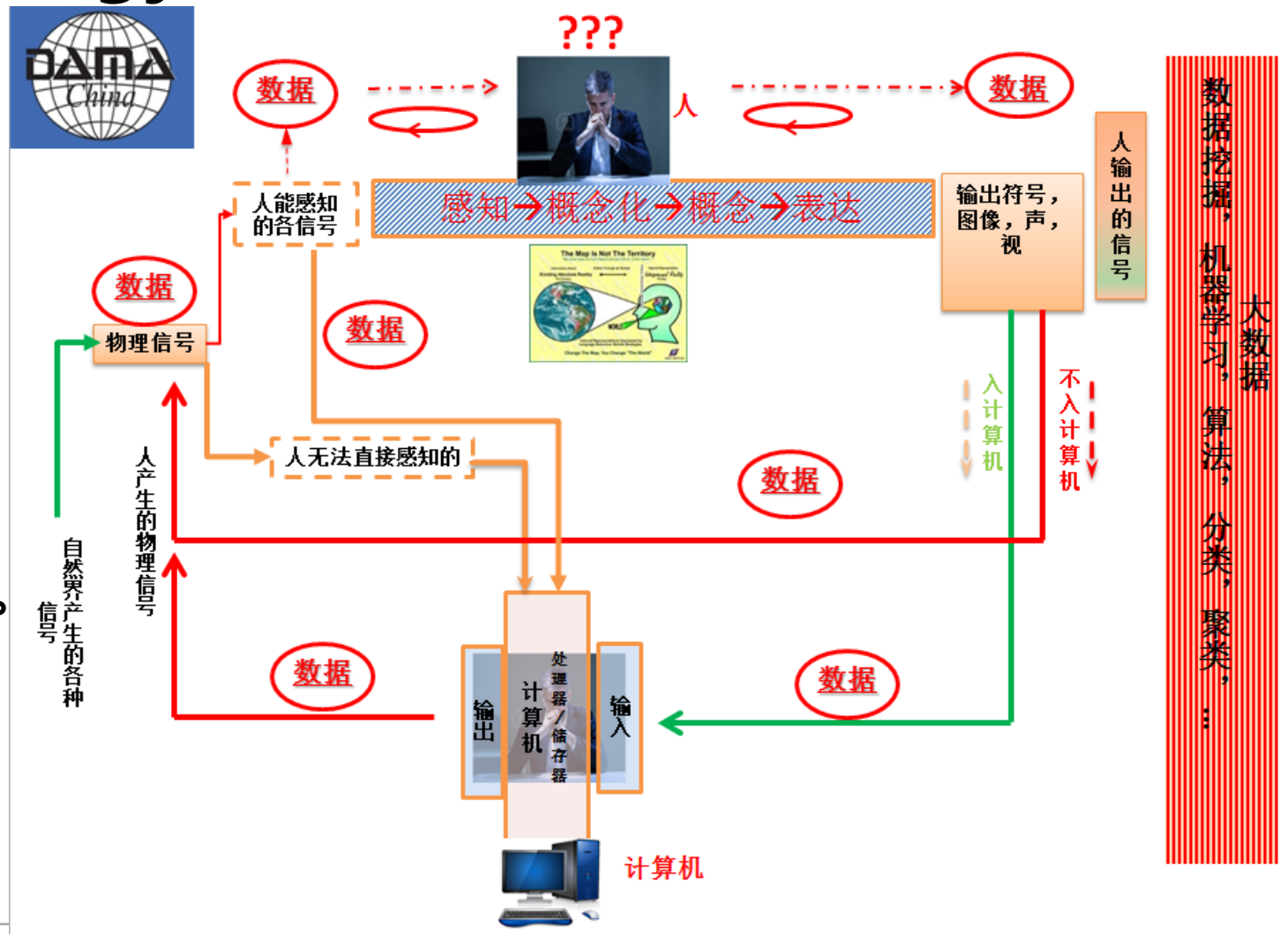
人脑的不透明，遗忘和欺骗等性质。

各时代（农业、工业）的信息技术：

一．运算，数得清
二．存储，存得住
三．传输，流得动

从而在跨越时空转移、调整价值时，
形成口说无凭，立字为据。
据为契约，“凭据、符号”是Token。

Token是信息的携带者。
Token是价值的承载物。
Token也会被流通交易。



金融技术的基础性作用是记录资产的合约，体现出一种物质属性和技术性质。各种技术演化围绕：如何证明权利的真实性(防伪）。

一．作用：

◆ 能够把相关协议或者合约记录下来，然后交易、流通。

二．合约的技术特征：

◆ 以媒体的形式确定着它们“所有者”的合法权益，确权。

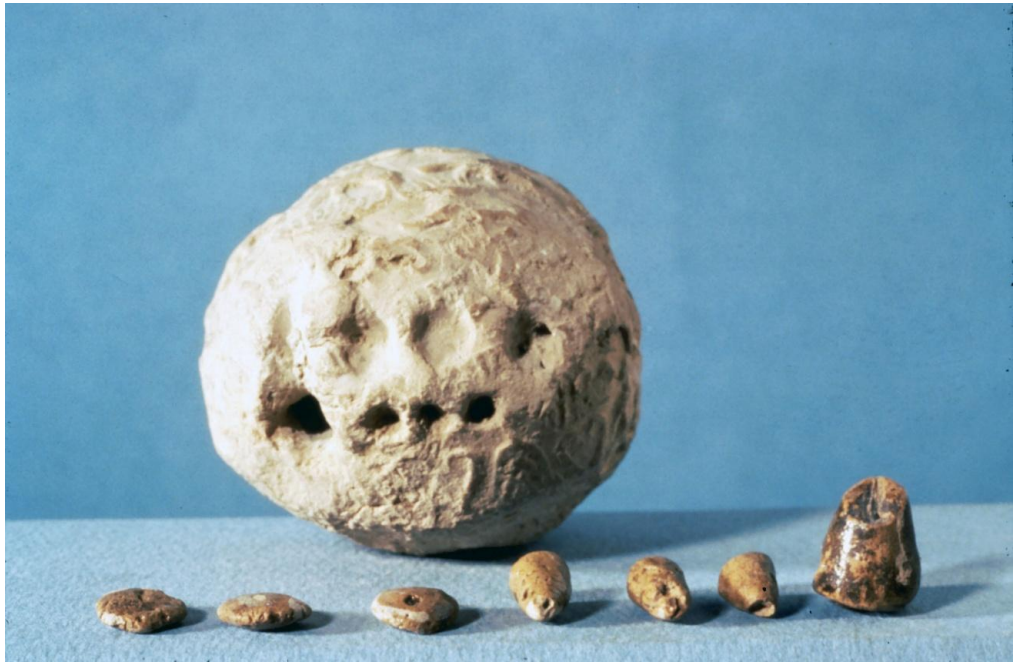
◆ 将金融追索权以契约内容、条款呈现。

序号	记录媒介、载体	存在形式
1	对自然物的加工，陶片，泥板，刻痕的木棍和木块，羊皮纸、纸张	有形
2	电子文档，数字存储	无形

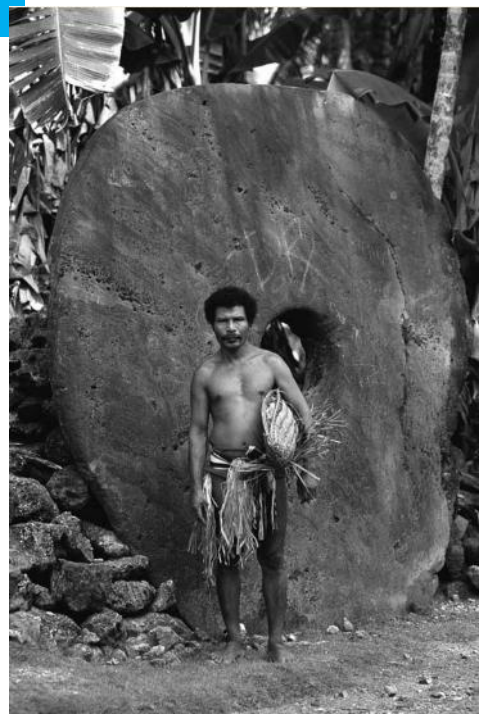
Clay Token有形 陶筹（Counting， Storage，Transforming），随之印玺陶箱 。公园前3000元，美索不达米亚。首个信息账务系统。

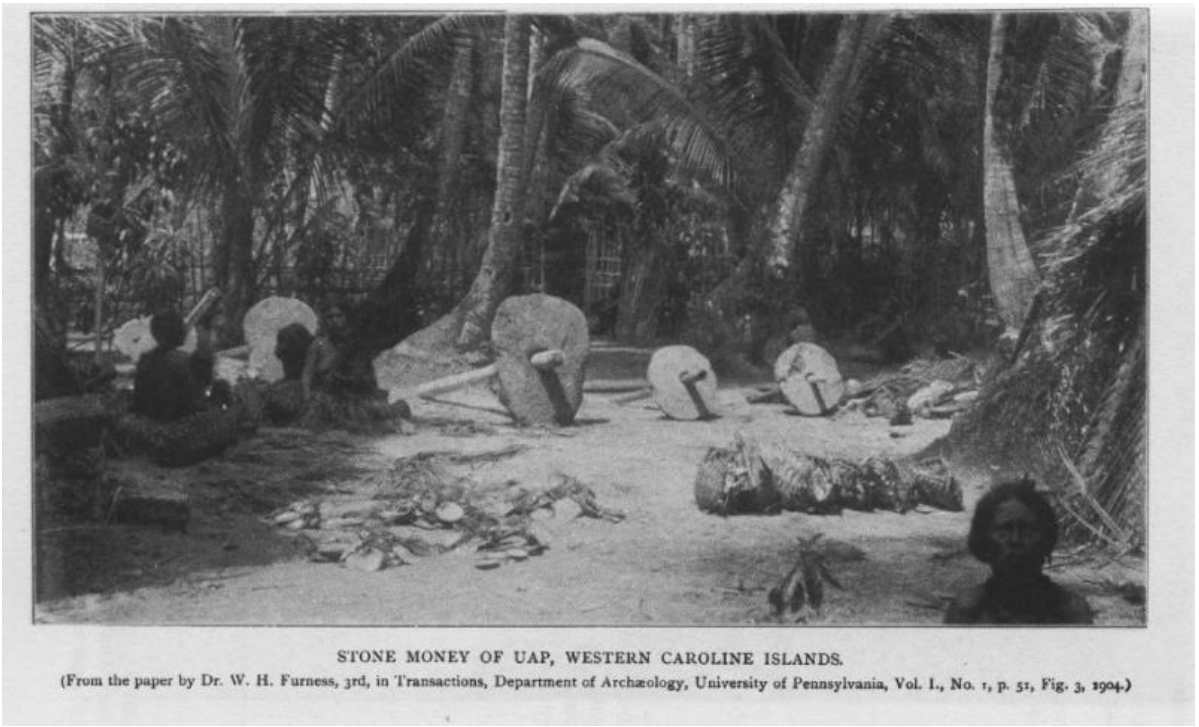
一．人们就用不同形状的泥块表示不同的物品：球形的泥块表示少量的小 麦；圆形的泥块表 示 大量的小麦；圆柱形的泥块表示一种动物，以及面包、蜂蜜、 金属等等，有500多种。

二．多方交易时，即用 盖上印记的陶箱（Envelope）封存、保管，↓7个。。



使用到1940年代，太平洋雅浦岛，Fei Stone， 费币，Token





STONE MONEY OF UAP, WESTERN CAROLINE ISLANDS.
(From the paper by Dr. W. H. Furness, 3rd, in Transactions, Department of Archæology, University of Pennsylvania, Vol. I., No. 1, p. 51, Fig. 3, 1904.)

这些圆饼状的大石头从400公里很远的地方采集过来，有特色花纹，很大很重。市场参与者在市场上交换完毕，或者用木棍滚动移动到家里。对于大笔交易，不移动这些费币，就是做一个标记，甚至标记也不做，就公开宣称一下。

凯恩斯、弗里德曼这些不同流派的经济学家提过。

雅浦岛的货币不是‘费’，而是背后一套以信用记账以及靠这种账目而进行清算所构成的体系”。作为大石轮的“费”，只不过是用来记账和进行清算的代币（Tokens）。

--《货币野史》菲利克斯·马汀

实物货币（商品货币）的发明以及演进

一．为什么是英磅？磅是重量单位

- 牛顿在1707年，通过安妮女王立法，创立金币和银币之间的联系，随后英国于1821年正式采用金本位制，英镑成为英国的标准货币单位，每1英镑含7.32238克纯金。
- 在中国金银的单位是两，也是重量单位

二．问题是：在人类社会早期，市场上交易的时候，如何称重？**靠天平和砝码，秤砣**。

- 公元前7世纪，手工铸币技术出现。
  - 模具是个创新。
  - 但是易于仿造。成色和重量
- 1696年，牛顿成为英国铸币厂的厂长。
  - 他的促进了蒸汽机作动力来铸币（铸币工失业）。
  - 同时在硬币的边缘加上锯齿形条纹避免磋磨、以及防止假冒。
    - 铸币机是个技术创新。

上埃及第三王朝 约公元前2500年

叙利亚天平　约公元前800年

古埃及公元前1500年

西汉海昏侯墓葬金币

总结：金融市场、金融产品领域“创新”的基本判断要素，以及判断所依据的基本原理。

一．金融创新的三个重要基础

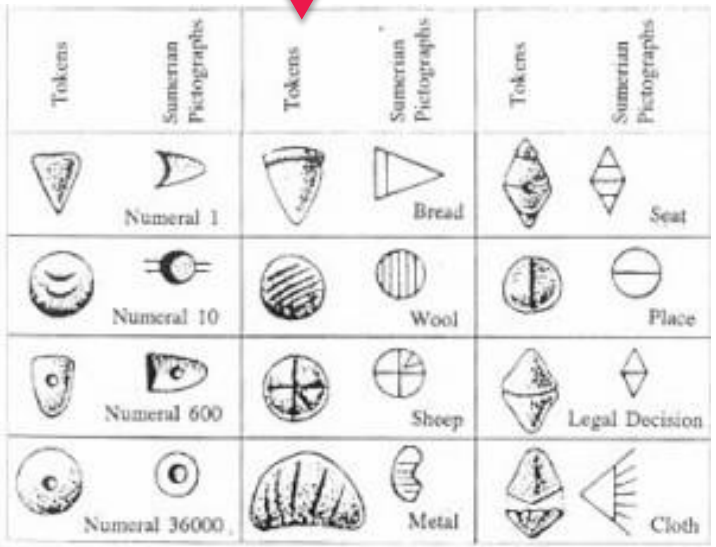
- **价值的跨时间、空间转移**
- **就未来结果达成的契约和收益权利，期间伴随风险。**
  - 一方按照某个事件的结果向另一方支付
    - 或有权利，一次打赌，
  - 交易对方（Counterparty)之间就风险定价、分解、对冲。
    - 新的风险出现、新的保险合约被订立。
- **在市场上形成可转让性、流通性（negotiability）**
  - 流转合约形成流动性
  - 资本市场是投资者们转让金融合约的地方，
    - 存在交易摩擦。（太大、太远、太笨重）
    - 资产证券化的过程（securitization）
  - 同时调整他们持有的金融权利的数量
  - 满足其储蓄和短期现金的需要
  - 并使他们就未来事件进行投资或者套期保值。

二．同时，需要能抗篡改，防止伪造。

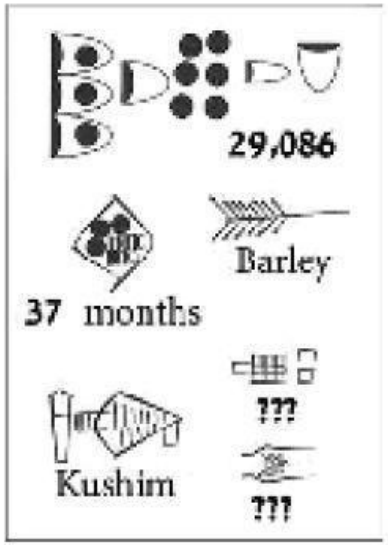
- 成本要足够的低

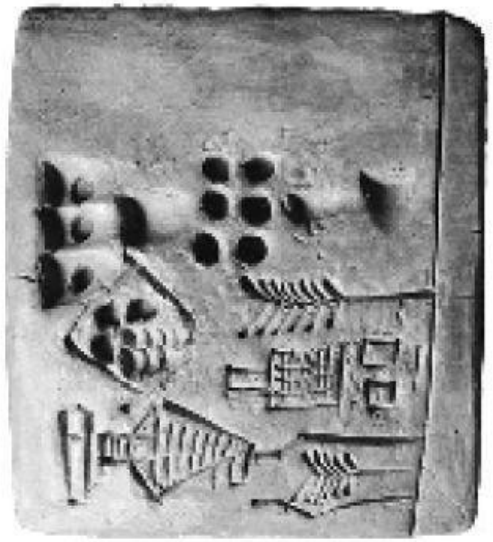
- 货币的出现
- 当代股票市场
- 期货市场
- 人寿保险
- 风险终结于金融创新

实物→抽象的文字：泥板，以及对应的工具（手），脑
苏美尔人的乌鲁克Uruk（伊拉克东南）泥板，楔形文字。
由三维的实物转变成二维的文字。记录技术的降成本，提高性能。



在37个月间，共收到29086单位的大麦。由库辛签发。



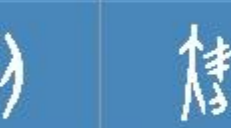


←Clay Tablet

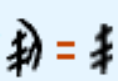
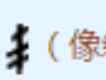
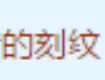
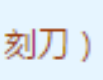
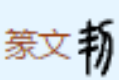
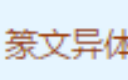
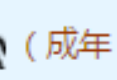
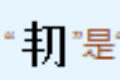
泥板，大约公元3400～公元前3000。

第一个有文字记录的文件：财务记录。记账。

集中化的记账核算系统，对成千上万个泥板的存取、管理、防止损害是当时的高科技。

甲骨文	金文	篆文		隶书	楷书	行书	草书	标准宋体
								
甲 1170	杕氏壺	说文解字	说文解字	叶慧明碑	柳公权	董其昌	孙过庭	印刷字库

字源解说

“”是“契”的本字。，甲骨文  =  （像纵横交错的刻纹）+  （刀，刻刀），表示用刀刮刻。篆文  承续甲骨文字形。篆文异体字  加“大”  （成年人），强调“契”为成年人的行为。**造字本义：古人用刀具在龟甲、兽骨上刻划记号、标志。**隶化后楷书  将篆文字形中的  写成  ，将篆文字形中的  写成  。

附 文言版《説文解字》：契，大約也。从大从。《易》曰：“後代聖人易之以書契。”

附 白话版《说文解字》：契，正式的协约文件。字形采用“大、”会义。《易经》上说：“后代的圣人用书契替代它。”

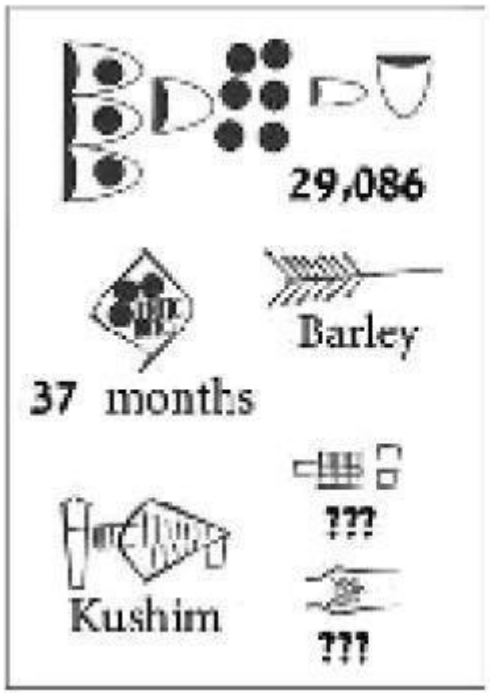
符号记录：结绳计数、算筹、符木，自然物

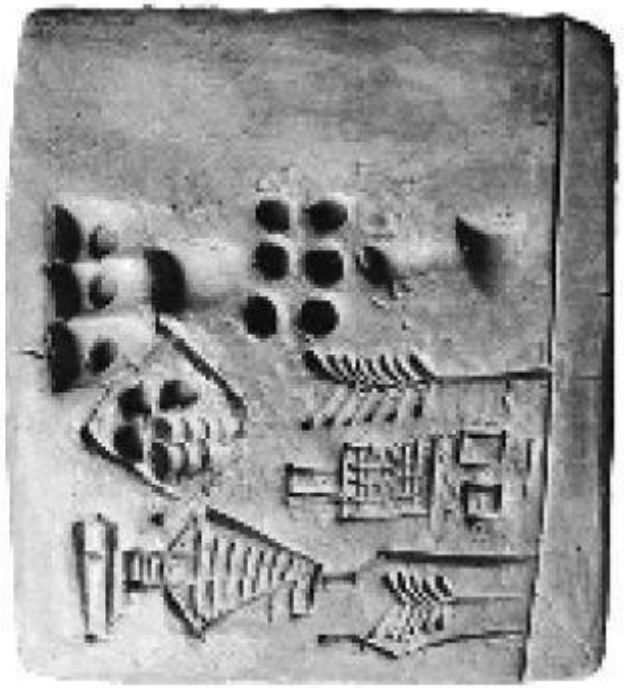
Foil（债务人)， Stock（债权人）
大约1250年， 英格兰财务署符木，山桃木
1834年财政部大火中幸存
Fulk Basset 因为Wycombe农场欠款9磅4先令4便士

形式 \ 数字	1	2	3	4	5	6	7	8	9
纵式	𝍠	𝍡	𝍢	𝍣	𝍤	𝍥	𝍦	𝍧	𝍨
横式	𝍩	𝍪	𝍫	𝍬	𝍭	𝍮	𝍯	𝍰	𝍱

文字记录：数一数、计数、记账的历史考据
苏美尔人的乌鲁克Uruk（伊拉克东南）泥板，楔形文字。

在37个月间，共收到29086单位的大麦。由库辛签发。





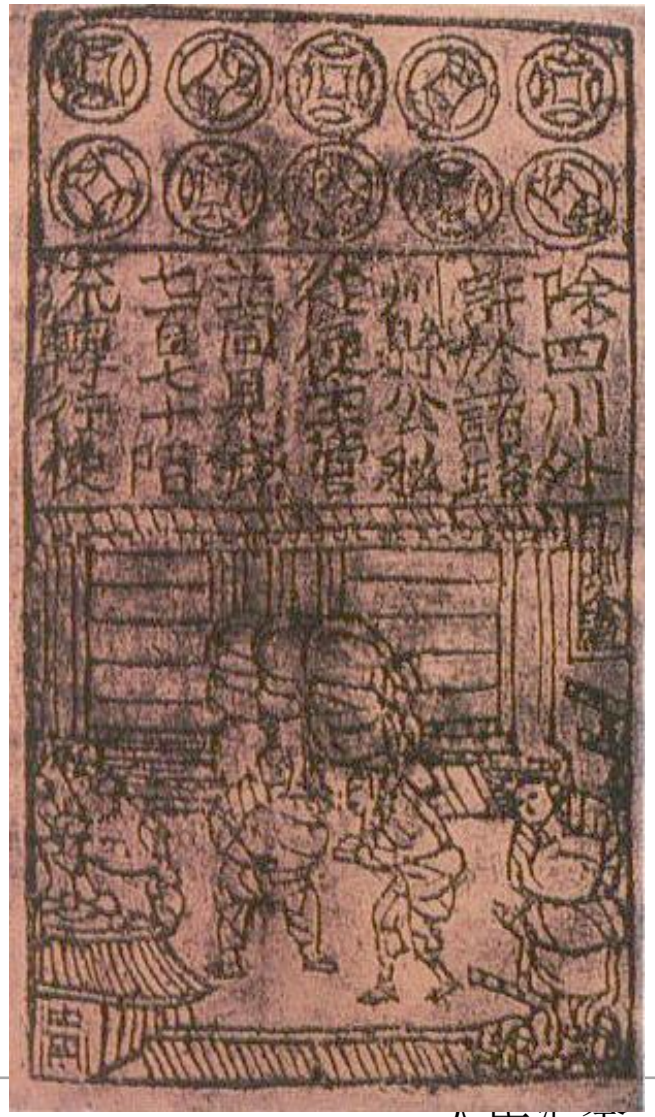
泥板，大约公元3400～公元前3000。

第一个有文字记录的文件：财务记录。记账。

苏美尔文字以6和10作为基数。

集中化的记账核算系统，对成千上万个泥板的存取、管理、防止损害是时代的高科技。

文字记录：北宋交子，先为票证，后演变为世界第一的纸币。印“交子”图案讲究，青黑红三版间错，隐作记号，亲笔押字，很难伪造。



地名：锦江区交子社区，交子大道。

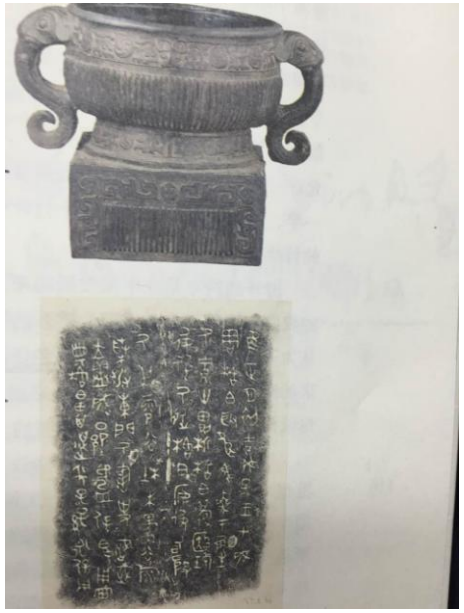
交子的交子是古代四川俚语，是票券、凭证的意思。“交”是合券取钱的意思。

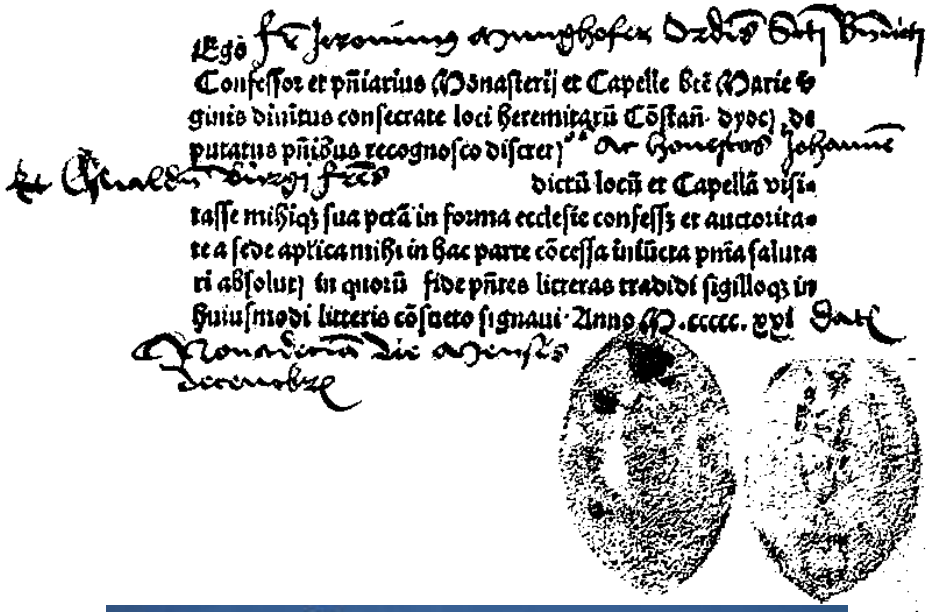
降低交易成本，提高流动性：经济发达，宋太祖下令回收四川的金银铜钱，运往中央。铸造铁钱，于是铁钱成为四川的主要货币。但铁钱原材料较廉价，同等价值重量更高，铁钱1000文可重25斤，经常要用车子拉钱，使用上十分不便。民众往往将铁钱寄存在“交子铺”中，换取票据交子，并在日常生活中用作交易。

历史环境：与西夏作战；产业链完整配套，天府的印刷业和造纸业比较发达，雕版印刷水平最高；民营专为官营：益州交子务。

缺点：容易通货膨胀。

文字记录以及手段：铸造、手写、印刷。
古登堡印刷技术：1450年前后，1455年《古登堡圣经》以及 “赎罪券”



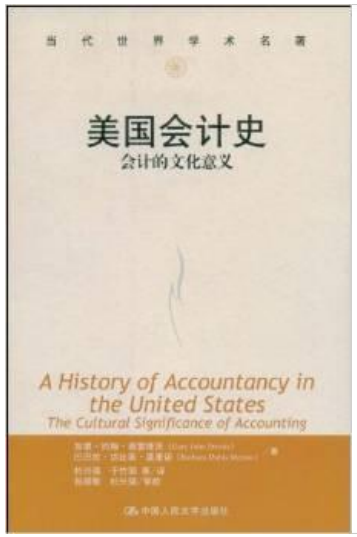


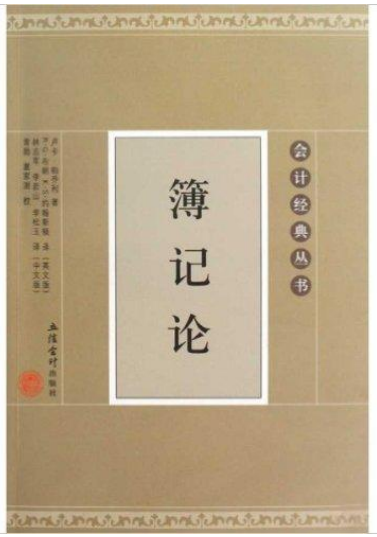
文字记录：卢卡•帕乔利《簿记论》，复式记账法，对数据的存取管理系统工具

一．1492年

复式记账法与资本主义的发展相互促进。

使企业所有者（股东）和经营者可以分开。





罗马数字	阿拉伯数字	罗马数字	阿拉伯数字	罗马数字	阿拉伯数字
Ⅰ	1	Ⅸ	9	C	100
Ⅱ	2	Ⅹ	10	CD	400
Ⅲ	3	Ⅺ	11	D	500
Ⅳ	4	ⅩⅩ	20	DC	600
Ⅴ	5	XL	40	CM	900
Ⅵ	6	L	50	M	1000
Ⅶ	7	LX	60	$\overline{\text{X}}$	10000
Ⅷ	8	XC	90	$\overline{\text{M}}$	1000000

西方阿拉伯数字	0	1	2	3	4	5	6	7	8	9
标准阿拉伯文数字	٠	١	٢	٣	٤	٥	٦	٧	٨	٩
东阿拉伯文数字	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹
天城文（梵文）数字	०	१	२	३	४	५	६	७	८	९
古吉拉特文数字	૦	૧	૨	૩	૪	૫	૬	૭	૮	૯
古木基文数字	০	১	২	৩	৪	৫	৬	৭	৮	৯
Limbu	᥆	᥇	᥈	᥉	᥊	᥋	᥌	᥍	᥎	᥏
孟加拉文数字	০	১	২	৩	৪	৫	৬	৭	৮	৯
奥里亚文数字	୦	୧	୨	୩	୪	୫	୬	୭	୮	୯
泰卢固文数字	౦	౧	౨	౩	౪	౫	౬	౭	౮	౯
卡纳达文数字	೦	೧	೨	೩	೪	೫	೬	೭	೮	೯
马拉雅拉姆文数字	൦	൧	൨	൩	൪	൫	൬	൭	൮	൯
泰米尔文数字	௦	௧	௨	௩	௪	௫	௬	௭	௮	௯
藏文数字	๐	๑	๒	๓	๔	๕	๖	๗	๘	๙
缅甸文数字	၀	၁	၂	၃	၄	၅	၆	၇	၈	၉
泰文数字	๐	๑	๒	๓	๔	๕	๖	๗	๘	๙
高棉文数字	០	១	២	៣	៤	៥	៦	៧	៨	៩
老挝文数字	໐	໑	໒	໓	໔	໕	໖	໗	໘	໙

相关例子：信息的传递，金融权益和债权债务信息的流通

一．意大利北部城市 皮亚琴察交易会 Piacenca
- 1557～1627年 布罗代尔
- 为西班牙、葡萄牙的海上探险提供金融支持，信贷体系开始高速运转。
- 保险、汇兑、支付、清算和结算中心。这些交易会集中众多的批发交易和国际支付业务，需要安排冲帐。
- 金融活动从几方面获利：利息、利上滚利、正签与反签汇票、买卖金银铸币，债券投机等等。

二．英格兰
- 1688年光荣革命，威廉三世
- 工业革命，明朝隆庆皇帝解海禁，西方的白银前往东亚参与贸易，并赚取东西方金银之间的汇差。
- 从尼德兰（荷兰）带来了新的独立的央行制度：英格兰银行。
- 以及国债、税务和货币发行制度。

三．纽约，以及香港？
- 为什么？

区块链，你们听到的翻译都是错的？应该是账链。

一．首先就区块链的字义做一个阐述，区块链是从英文*Block Chain*这两个单词直译过来，但信雅达的翻译为“账链”比较好。

二．翻阅下英汉词典可以知道 Block是可数名词，是**一段时间内很多笔交易**的意思，类似于会计中的凭证，把一些经济业务活动分录后形成一张账页。至于Chain翻译做**链，环环相扣**。

三．观众脑海里面可以想象一下场景：公司会计将一张张账页装订成账本成册，这个过程就是区块链技术的本意：将互联网上的信息装订到一个账本中，然后签字、盖章、盖骑缝章、经过审计后，就可以说这个账本中承载的数据是真实可靠、不可（或者很难）更改的。而至于被翻译成区块链这个很拗口的名字，那是因为英汉词典中的Block的常见的第一个释义是区块，所以被一些工程师随口将Blockchain翻译成区块链了，所以徒然增加了很多理解的难度。

四．详见：柯林斯字典、牛津词典中 Block的释义中有： A block of something such as tickets or shares is a large quantity of them, especially when they are all sold at the same time and are in a particular sequence or order. 尤指按特定顺序同时售出的，大量，大批，大套（票、股票等）等等。。

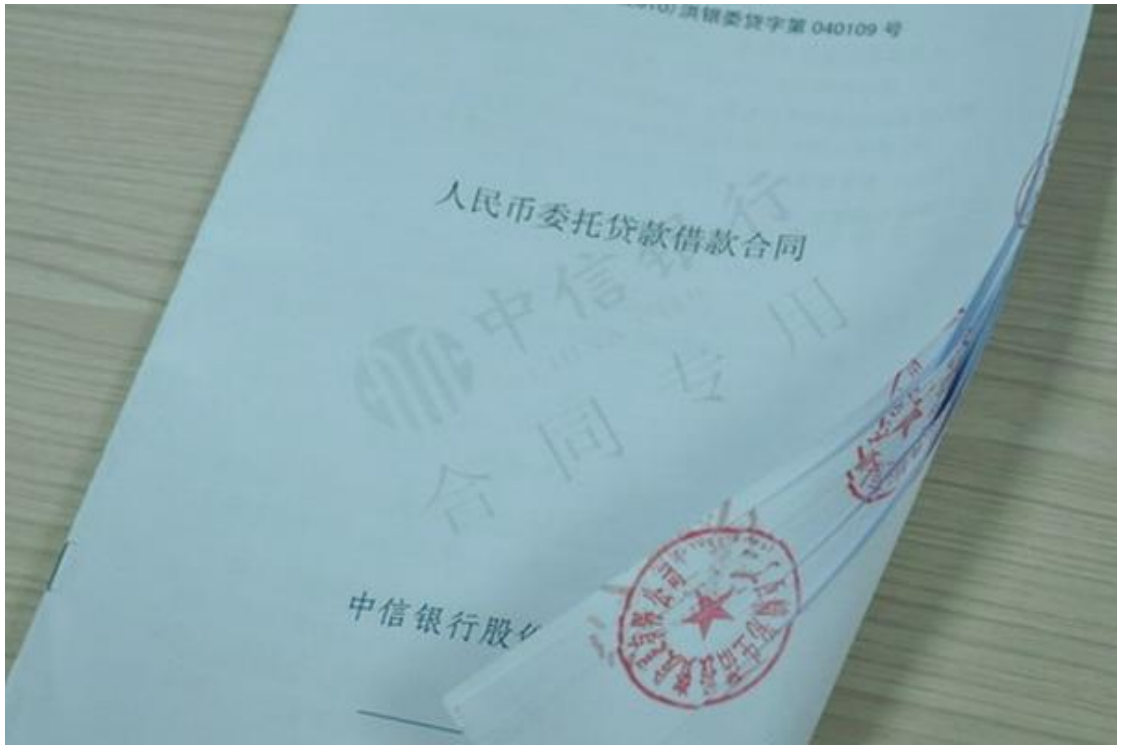
签名，骑缝章，一式四份

一．市场经济的活动是构架在记账、分账、销账、审账上面的。

二．对财产确权、发现价值、风险定价、交易流通。

三．在交换协作、交易流通、交割清算的时候，需要在纸上签名，盖章，骑缝章，以及一式四份。

- 实现了数据的真实可靠、不可篡改、保护商业秘密、避免权益灭失。
- 本质是分布式、互相制衡。
- 但是媒介是纸。



金融技术的基础性作用是记录资产的合约，体现出一种物质属性和技术性质。各种技术演化围绕：如何证明权利的真实性(防伪）。

一．作用：

◆ 能够把相关协议或者合约记录下来，然后交易、流通。

二．合约的技术特征：

◆ 以媒体的形式确定着它们“所有者”的合法权益，确权。

◆ 将金融追索权以契约内容、条款呈现。

序号	记录媒介、载体	存在形式
1	对自然物的加工，陶片，泥板，刻痕的木棍和木块，羊皮纸、纸张	有形
2	电子文档，数字存储	无形

但是，信息互联网的结构性缺陷

一．1960年～1994年

- 用分组传输的**技术**实现不间断的信息传播。
- 靠严格的军队保密管理**制度**来解决数据隐私秘密。

二．1994年（信息高速公路）～

- 制度层面：商业化、民用化后，人员甄别体制失效了。
- 技术层面：数据的创造者不拥有数据，对隐私的侵犯。而且从用户角度来看经常掉线，掉网。虽然研发出了PKI（数据，信息安全），和IP VPN（通道，网络安全）

看标准发展史，互联网技术出身名门望族，美国国防部远景研究规划署ARPA（阿帕），但早期不关注Privacy ，Security，靠制度，后期实现安全靠补丁，传递价值，权益交割碰到很多成本上的问题，效果不佳。

一．1969年 到 1987年

- RFC 0001 Host Software **April 1969**
- RFC 768 UDP；RFC 791 Internet Protocl；RFC 792 ICMP；RFC 793 TCP **Sept 1981**

二．RFC 987 Privacy enhancement for Internet electronic mail Part I : Message encipherment and authentication procedures

- **February 1987**
- Obsoleted by RFC1040, RFC1113

三．RFC1038 Draft revised IP security option.

- **January 1988**
- Obsoleted By RFC 1108

四． RFC 1244 Site Security Handbook

- **July , 1991**
- This FYI RFC is a first attempt at providing Internet users guidance on how to deal with security issues in the Internet.

五． RFC 1507 DASS - Distributed Authentication Security Service

- **September 1993**

六． RFC 1825 Security Architecture for the Internet Protocol

- **August 1995**.
- Obsoleted by RFC2401

七． Security 成为IETF研究重点

- 已经1995年了

区块链即互联网时代的记账、计数，信任基础也来自于数字，互联网上的计数以及随之而来 账本。

一．有人类以来，数学及其算法公式是全球文明的最大公约数，也是全球人类获得最多共识的基础架构。

- 区块链系统就是以数学算法的体现，以数学算法作为背书，所有的规则建立在一个公开透明的数学算法（程序）之上，能够让所有不同政治文化背景的人群获得共识。

二．互联网也是起源于数学。

- 1960年代，最初的关键问题要解决的问题是信息制造和传输，战争情况下的指挥信息的传递。
- 信息大爆炸、垃圾信息多，而且不能解决价值的传递。

三．区块链

- **互联网上的去中心分布式的、公开的、安全不可逆的加密账本。**
- Distributed Ledger
- 也是一套协议系统。

四．区块链创造出了可以信任的信息

- 因此创造了信用。
- 同时对风险的把控会更好。

五．经济互联网

- 从传递信息的信息互联网，到转移价值的信任互联网。

话题2：比特币究竟是啥咋回事？

一．在晶体管里面记录了一些信息，这个信息是真实可靠不可篡改的。
二．这些信息与实体经济发生了关联。
三．这些信息在不同的账户里面流动。

比特币商品的定价来源机制浅析:市场发现

一．2009年1月3日开始运转，这个记账体系开始运转。

二．比特币商品在第一次在现实中价格发现，价值确立。用法币定价。

- 价格是在2010年5月22日，来自美国佛罗里达州的程序设计员拉斯洛·汉耶兹被认为是第一个在现实世界使用“比特币”的人。当时，“比特币”还在电脑极客们手中流通，然而拉斯洛·汉耶兹将一万个“比特币”发给英格兰的一名交易者之后，后者接着用信用卡帮他从一家著名披萨零售店订购了两个披萨，就这样，这次跨越大西洋的交易也成就了历史。

三．“披萨很不错”

- 2017年7月，这两个披萨可能是世界上最贵的披萨饼，以当下3000美元的兑换价格来算，平均每个披萨价格超过1500万美元。

四．https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

数字加密货币的历史和变迁

一． 1980s，1990s, 加密技术，尤其是非对称领域
- B-money，HASHcash
- David Chaum：Ehash，DigiCash

二． 2009年到2013年1月
- 潜流，极客的工具
- 游戏币？

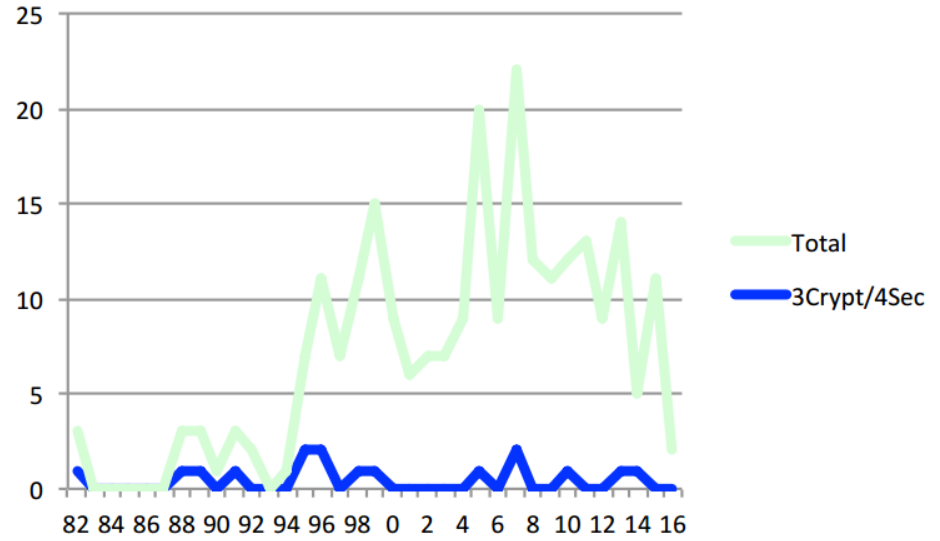
三． 2013年2月起
- 欧债危机，塞浦路斯资本管制
- 壹基金接受比特币捐款

四． 2013年12月之前：价格狂飙
- 价格泡沫
- 中国政府关于《风险》通知

五． 2014年10月之前：地火酝酿
- 美国司法部拍卖比特币
- 纽约州审定金融牌照

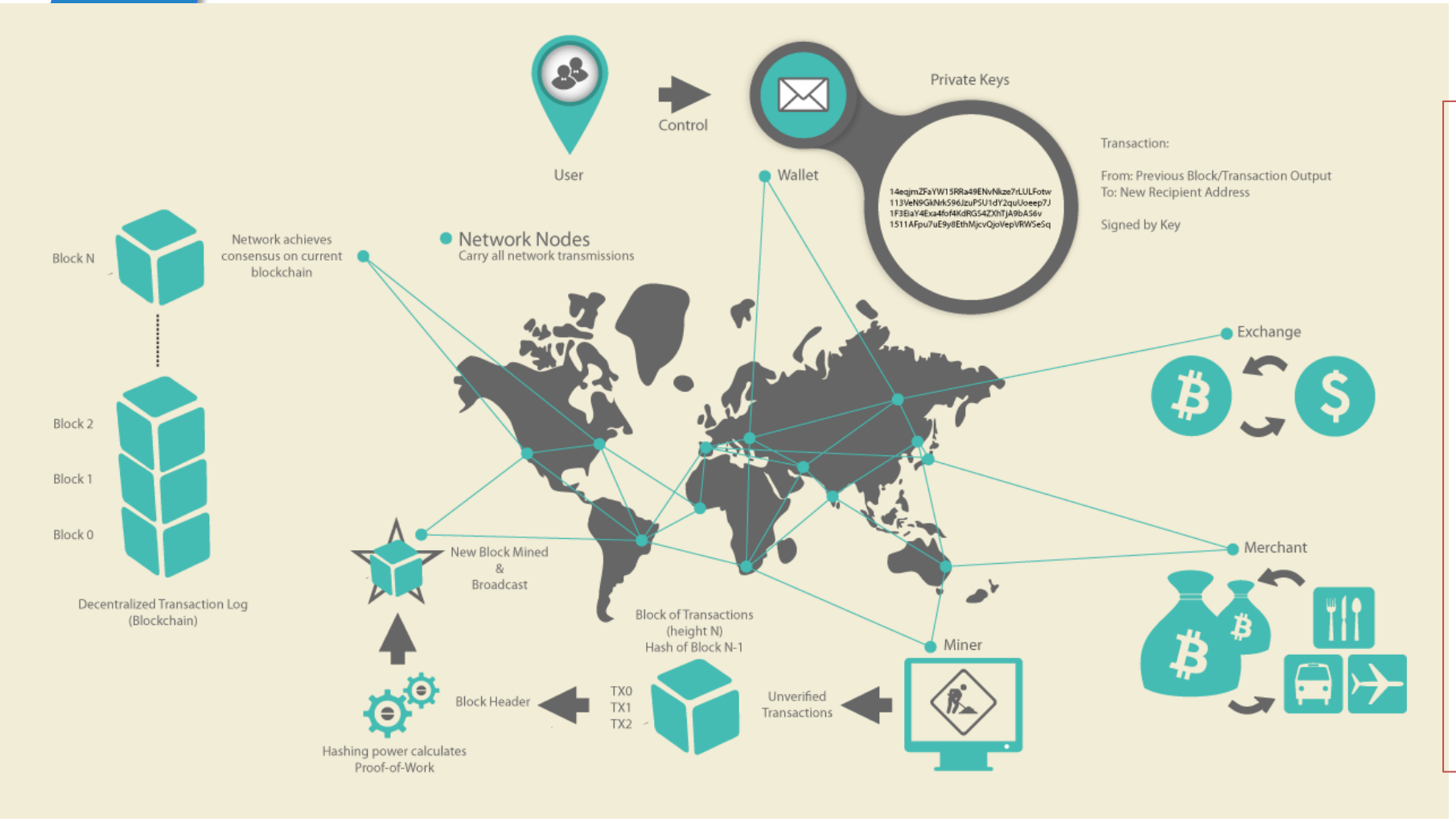
六． 截止到2015年9月：天雷勾引地火
- 希腊债务危机、苏格兰独立选举
- 花旗、纳斯达克、高盛、德勤、普华永道测试、投资、

七． 未来：三体到来
- 降维攻击



ACC	CyberCents	iKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone

区块链的全局系统图：市场角度



市场参与者（买卖双方）：

Merchant：机构，供应者

User：消费者，用户

bookrecording Worker：记账员

靠机器清算

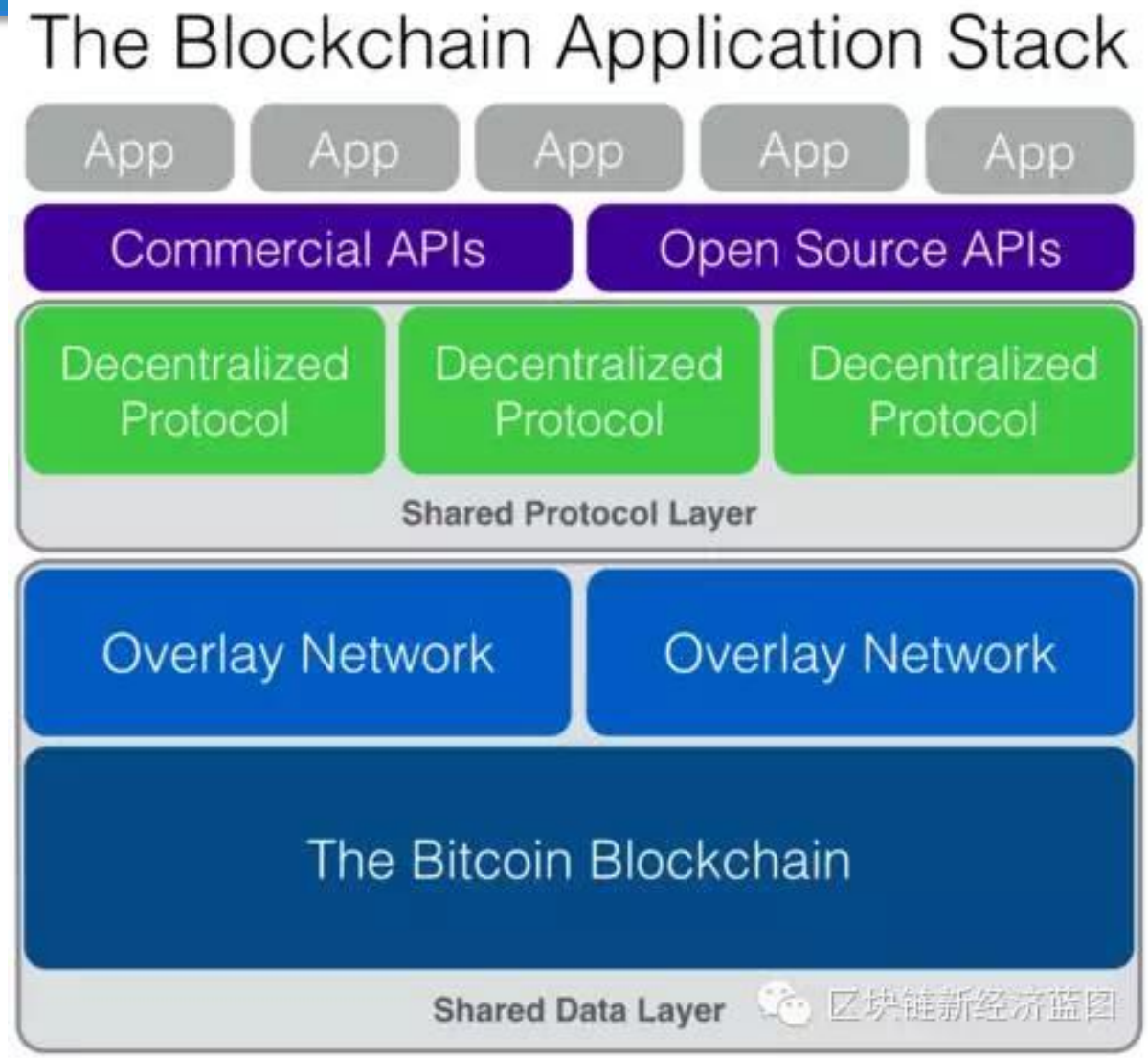
Wallet：存放资产的账户（加密）

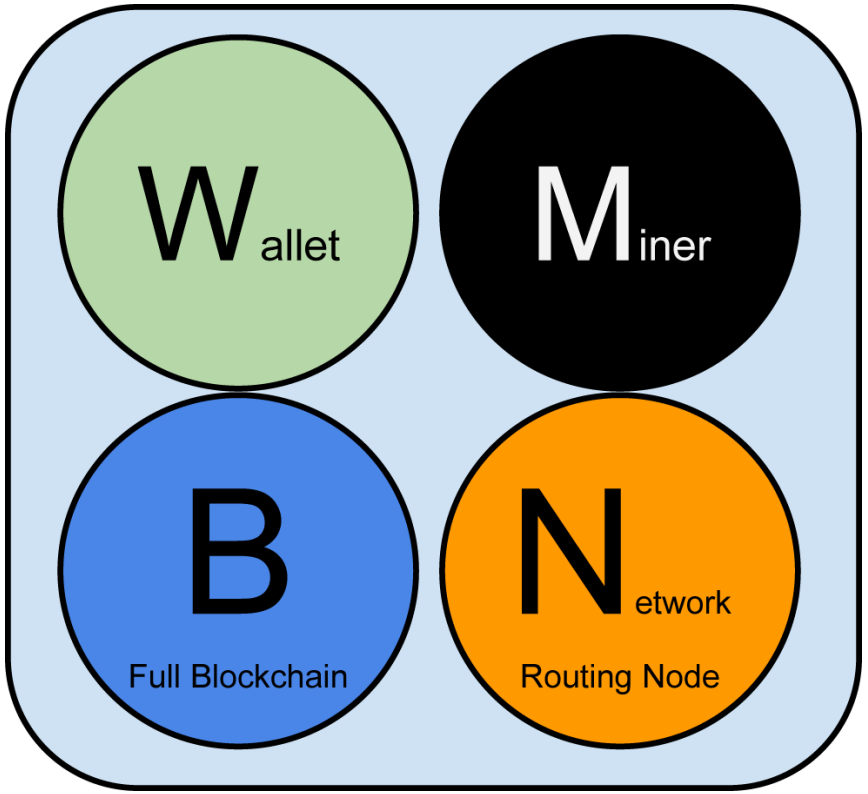
Exchange：兑换交易所

Source：《master bitcoin》

Andreas M Antonopoulos

区块链系统分层图和组成角色图





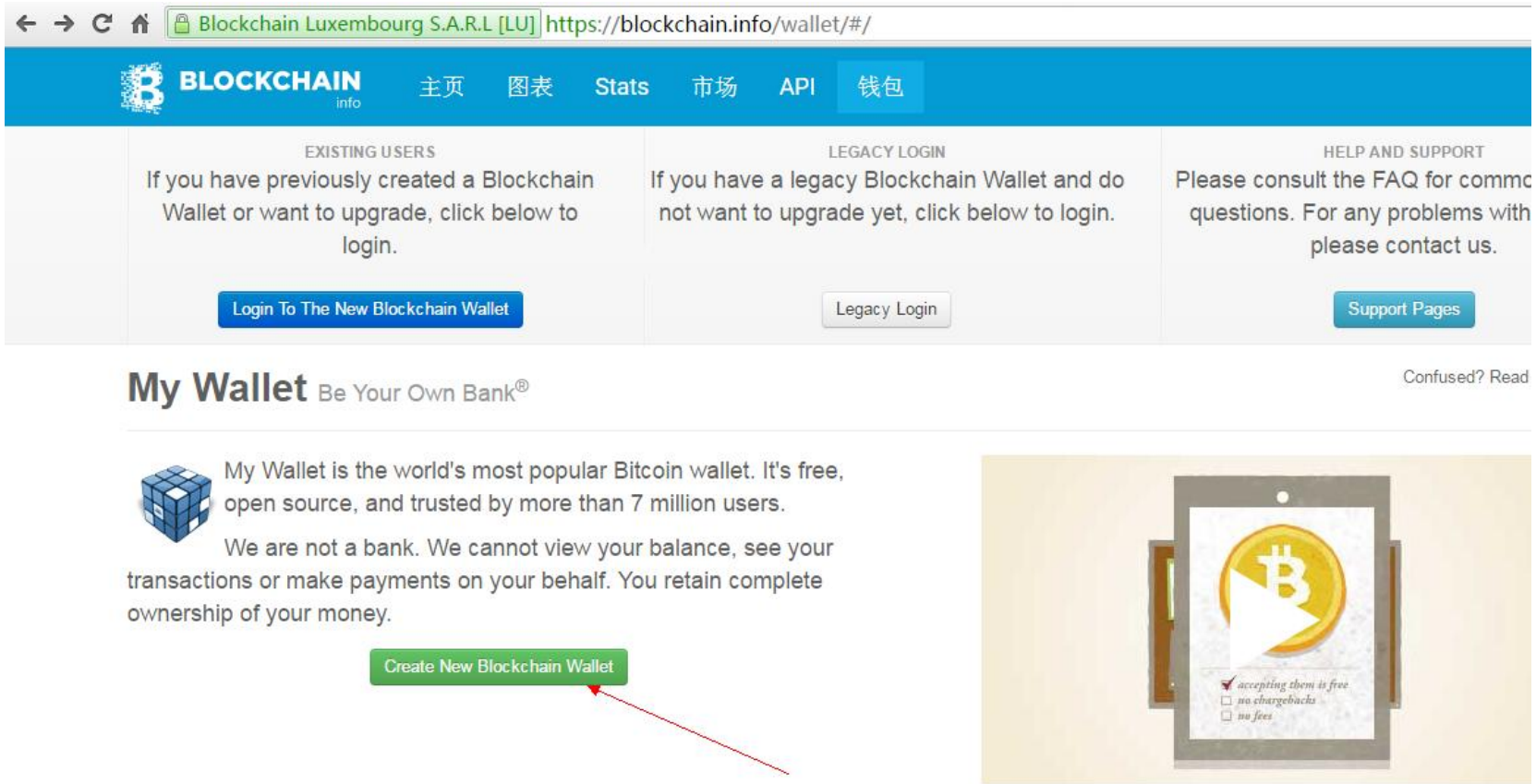
BitcoinD： https://github.com/bitcoin/bitcoin

术语 Term

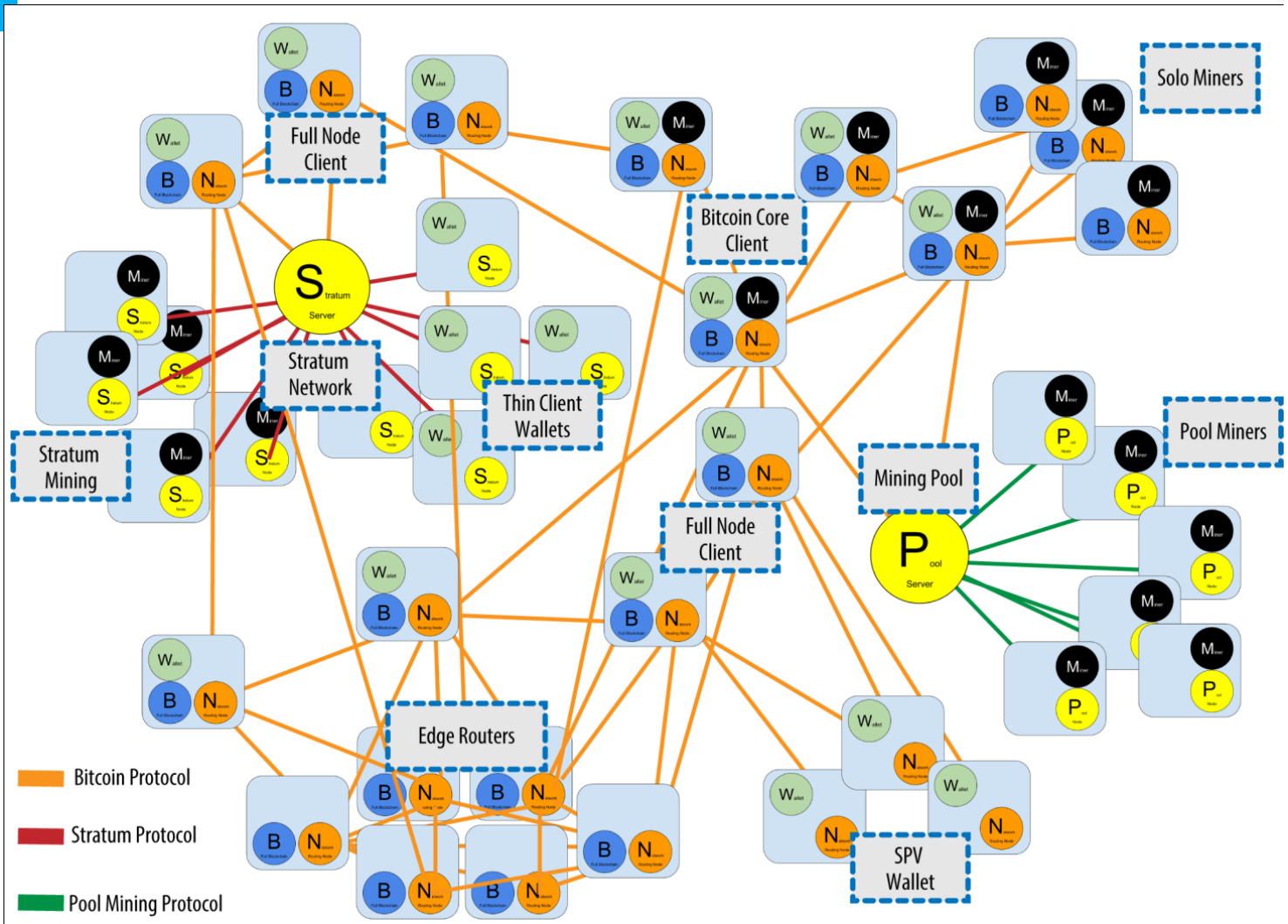
A. 对称加密
加解密的程序和算法是一样的，解密和加密的密码一样。
B. 非对称加密
1. 公钥和私钥（公钥公开，私钥开锁）
    1. 私钥：5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh
C. Address，地址，本质是公钥的体现
1. 数字钱包里面装的就是钥匙对，私钥一定保密存储。
2. 例子：1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp
D. Transaction，事务
1. 一个事务有线上和线下两个部分。转账是online的一个环节（两个步骤：卖方交付实物或者服务，买方转账付款）
2. 从一个地址转移到另外一个地址。使用一套脚本语言。
E. Block, 帐页，一张表格。
1. 特定时长（如10分钟）所有转账业务的集合。
F. HASH ， 哈希（类似于榨汁机，只可单向，不可逆）
1. 二进制数值的一个摘要，指纹。单向的。容易校验。
2. MD5， SHA256
G. 难度
1. 难度目标
2. 难度调整
H. 工作量 proof of work 运算一个函数。
1. 难度>SHA256(block)

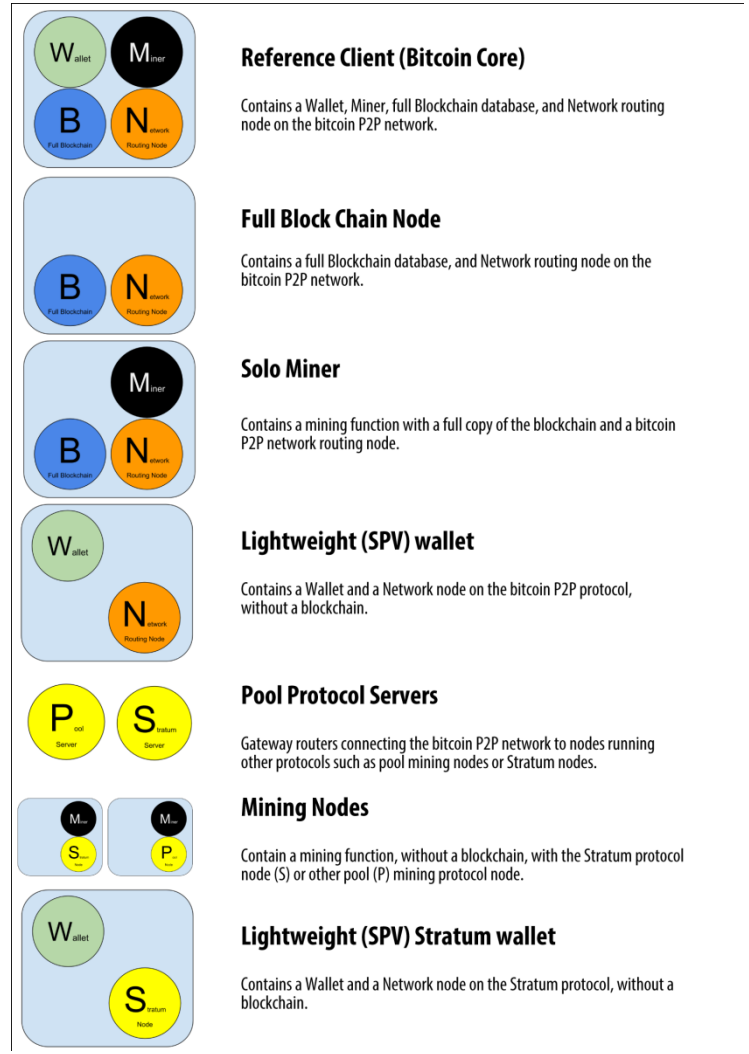
先动手操作下。

一．访问https://blockchain.info/wallet/#/



框图和类型





1.1 分布式产权管理(确定所有权，使用权，交易权）

一．产权管理涉及到价值转移，转账和交易。

- 非对称加密（公钥，私钥）
- 比特币区块链是全球公开的账本，一个可按照数据结构规则存取的数据库。每一笔转账都是在账链上的□ 个公开记录，含有输入值和输出值的数据结构。
-

表5-1 交易结构

大小	字段	描述
4字节	版本	明确这笔交易参照的规则
1-9字节	输入计数器	被包含的输入的数量
不定	输入	一个或多个交易输入
1-9字节	输出计数器	被包含的输入的数量
不定	输出	一个或多个交易输出
4字节	时钟时间	一个UNIX时间戳或区块号

表5-3 交易输入的结构

尺寸	字段	说明
32个字节	交易	指向交易包含的被花费的UTXO的哈希指针
4个字节	输出索引	被花费的UTXO的索引号，第一个是0
1–9个字节（可变整数）	解锁脚本尺寸	用字节表示的后面的解锁脚本长度
变长	解锁脚本	一个达到UTXO锁定脚本中的条件的脚本
4个字节	序列号	目前未被使用的交易替换功能，设成0xFFFFFFFF

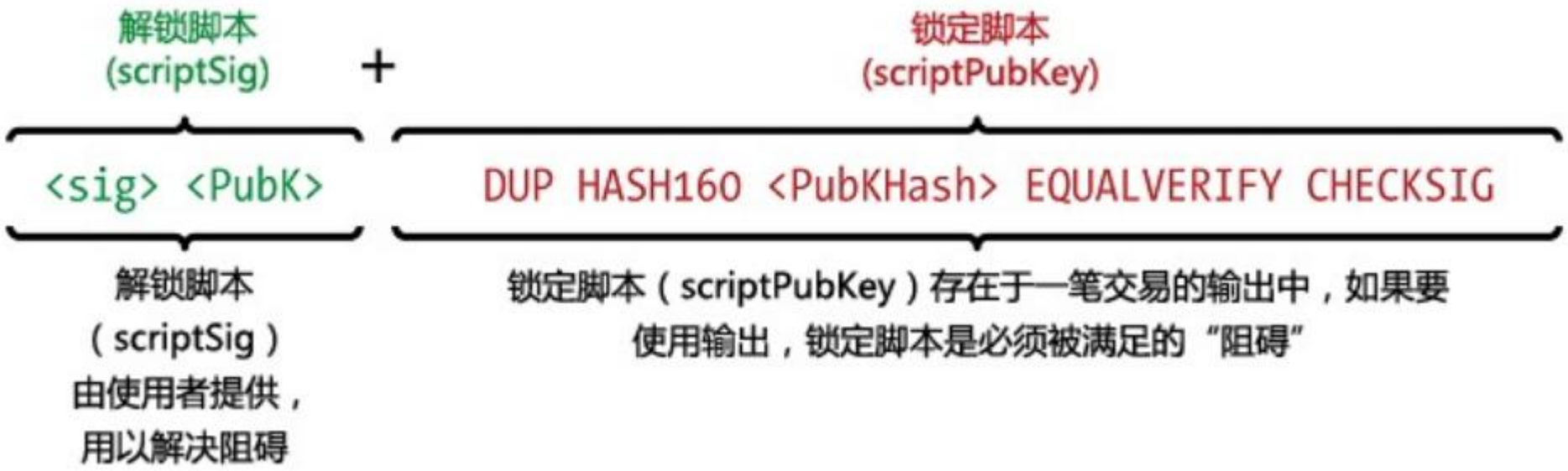
表5-2 交易输出结构

尺寸	字段	说明
8个字节	总量	用聪表示的比特币值（10-8比特币）
1–9个字节（可变整数）	锁定脚本尺寸	用字节表示的后面的锁定脚本长度
变长	锁定脚本	一个定义了支付输出所需条件的脚本

1.2组合后的交易脚本(可编程性）(智能合约的实现）

一．***锁定脚本***，是实质是一个公钥，一个放在输出值上的障碍，指出了未来动用这笔钱的条件。

二．***解锁脚本***，是实质是一个私钥，即私钥产生的签名，匹配放在输出值上的锁定脚本，从而可以动用这笔钱。



1.3 交易记账

概览	
地址	1HtF7xbaDwJu1j5sKpetG91xr4AZHYmJTL
Hash 160	b933036b1f143e6ee5f9038c4205f6bbe41e49cc
工具	源流分析 - 相关的标签 - 未动用的转出项

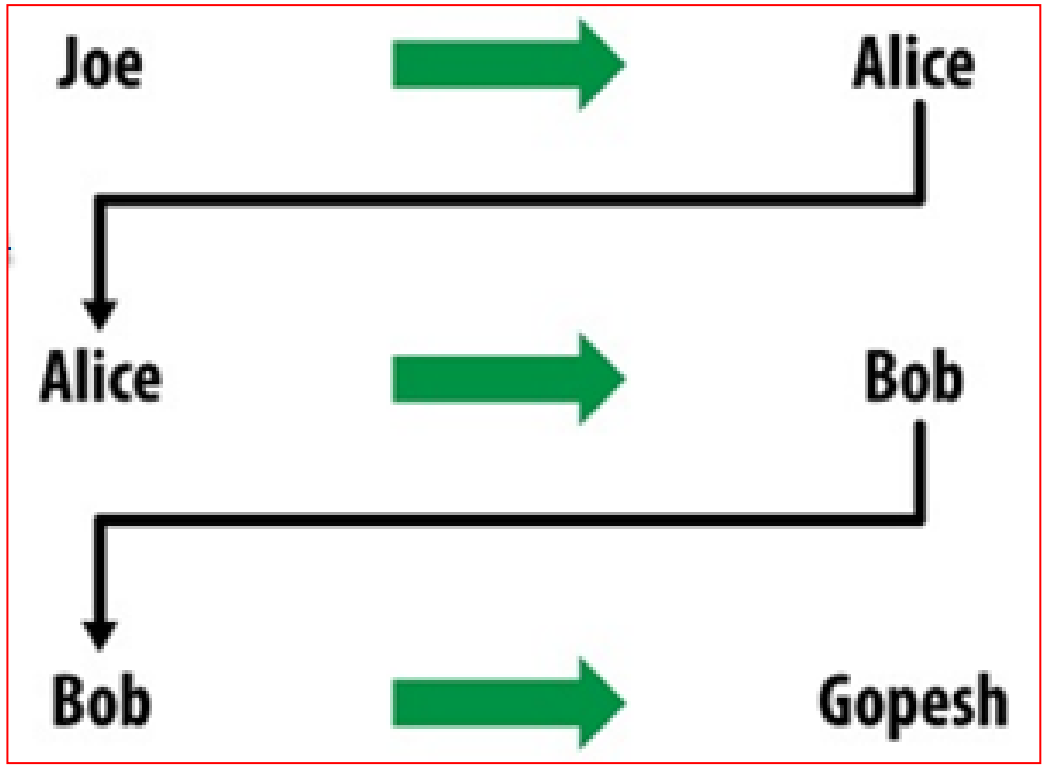
交易记录	
交易次数	2
总计收款	94 BTC
最终余额	0 BTC

付款招贴　捐赠按钮

交易记录（老条目在前）　筛选

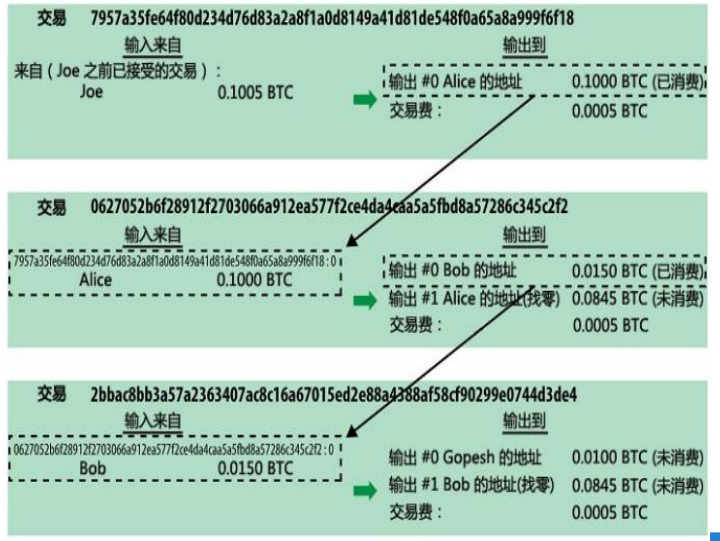
360c0ee799aa6e00032f87d62751d5a20cd9e6c6245f6420971647c45aca59e9			2012-09-22 22:29:24
1HtF7xbaDwJu1j5sKpetG91xr4AZHYmJTL	→	13fc8v6QTk4uAUvzgRmQnuDAznxtFCVTMw 1ELTk39zzoh5AQXjE2Nrux1NtSMrnDhM7	93 BTC 1 BTC
			-94 BTC
e03a9a4b5c557f6ee3400a29ff1475d1df73e9cddb48c2391abdc391d8c1504a			2012-09-22 10:31:02
1DC8mbgdVFNZn7ie6wUVGegKHsqvKkN7Qn	→	1HtF7xbaDwJu1j5sKpetG91xr4AZHYmJTL	94 BTC
			94 BTC

区块链 –权属链：被转账、记录的数据也可以是股权、债券、信托单位等等。甚至聊天信息。

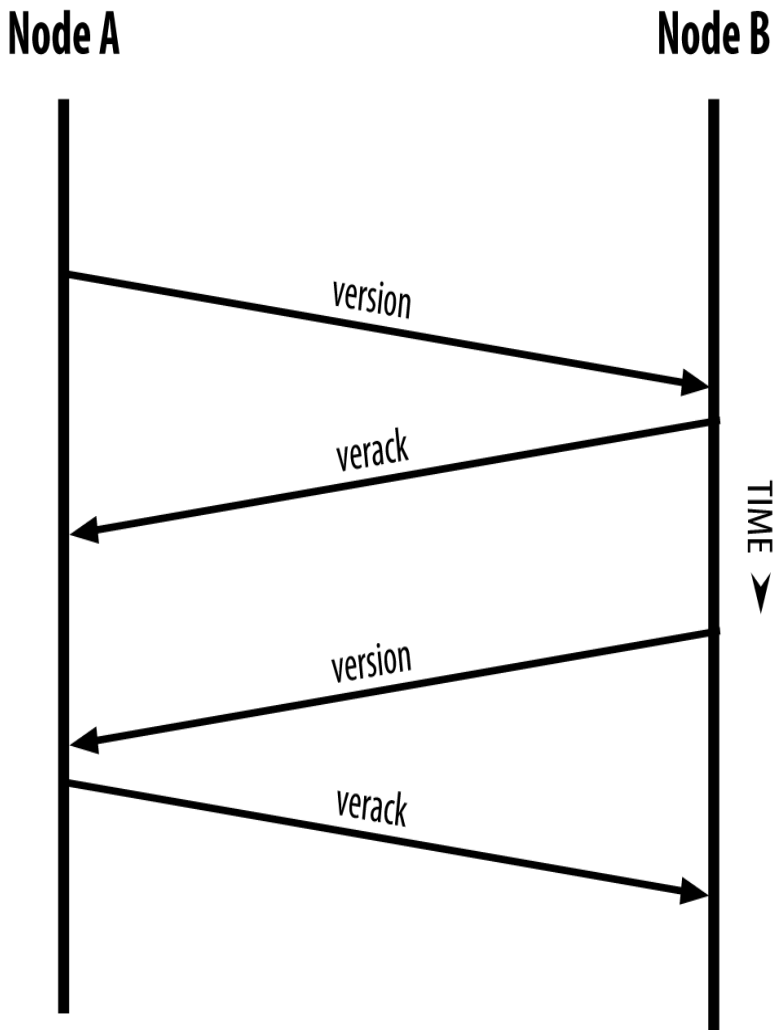


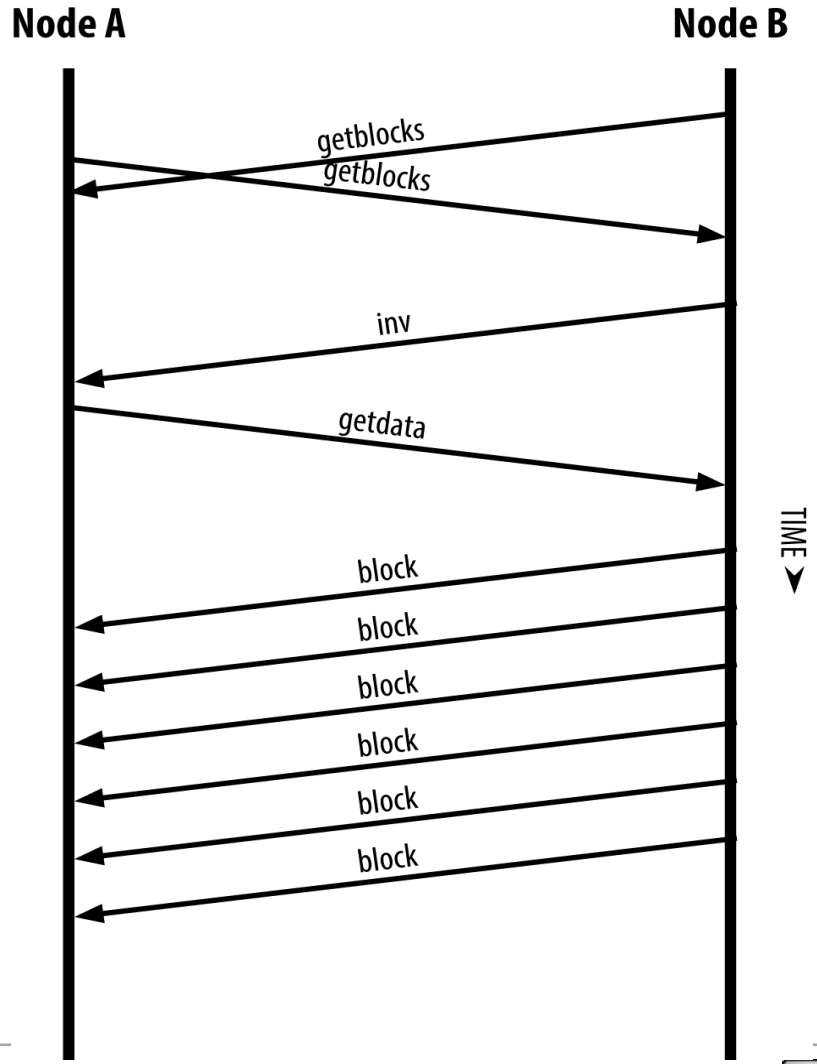
笔账户的输出必须被当做另　笔新账户的输　，这样随着钱(计量单位）从个地址（账户）被移动到另　个地址（账户）的同时形成了　条所有权链，同时也记录了每个账户上的余额。具有借贷关系的现金日记账，流水账。

即：权属链



2、分布式传播：网络层（传输）,类似BT协议





BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

SUPPORTED BY 21.CO

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Jan 06 2016 12:43:14 GMT+0800 (中国标准时间).

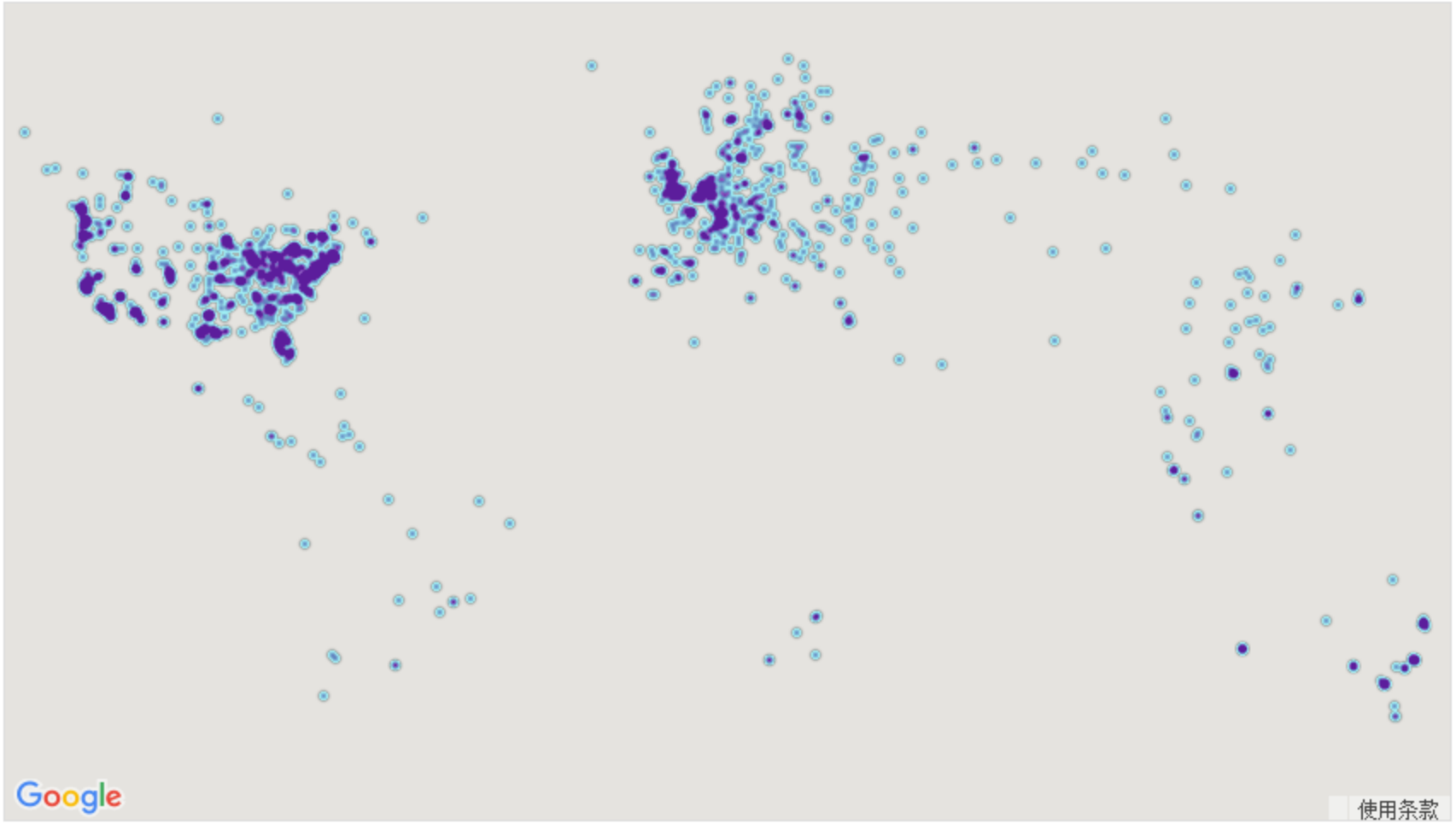
5610 NODES

24-hour charts »

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

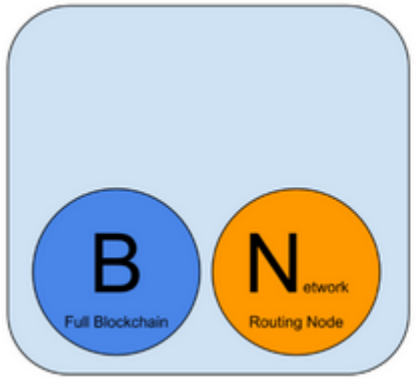
RANK	COUNTRY	NODES
1	United States	2001 (35.67%)
2	Germany	748 (13.33%)
3	France	403 (7.18%)
4	Netherlands	297 (5.29%)
5	United Kingdom	283 (5.04%)
6	Canada	260 (4.63%)
7	Russian Federation	145 (2.58%)
8	Sweden	121 (2.16%)
9	China	113 (2.01%)
10	Australia	111 (1.98%)

More (85) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

3、区块链blockchain，分布式数据库



Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

1 大数据就在里面！
2 交易记录（数据结构）
3 一万多个全节点，40Gbyte

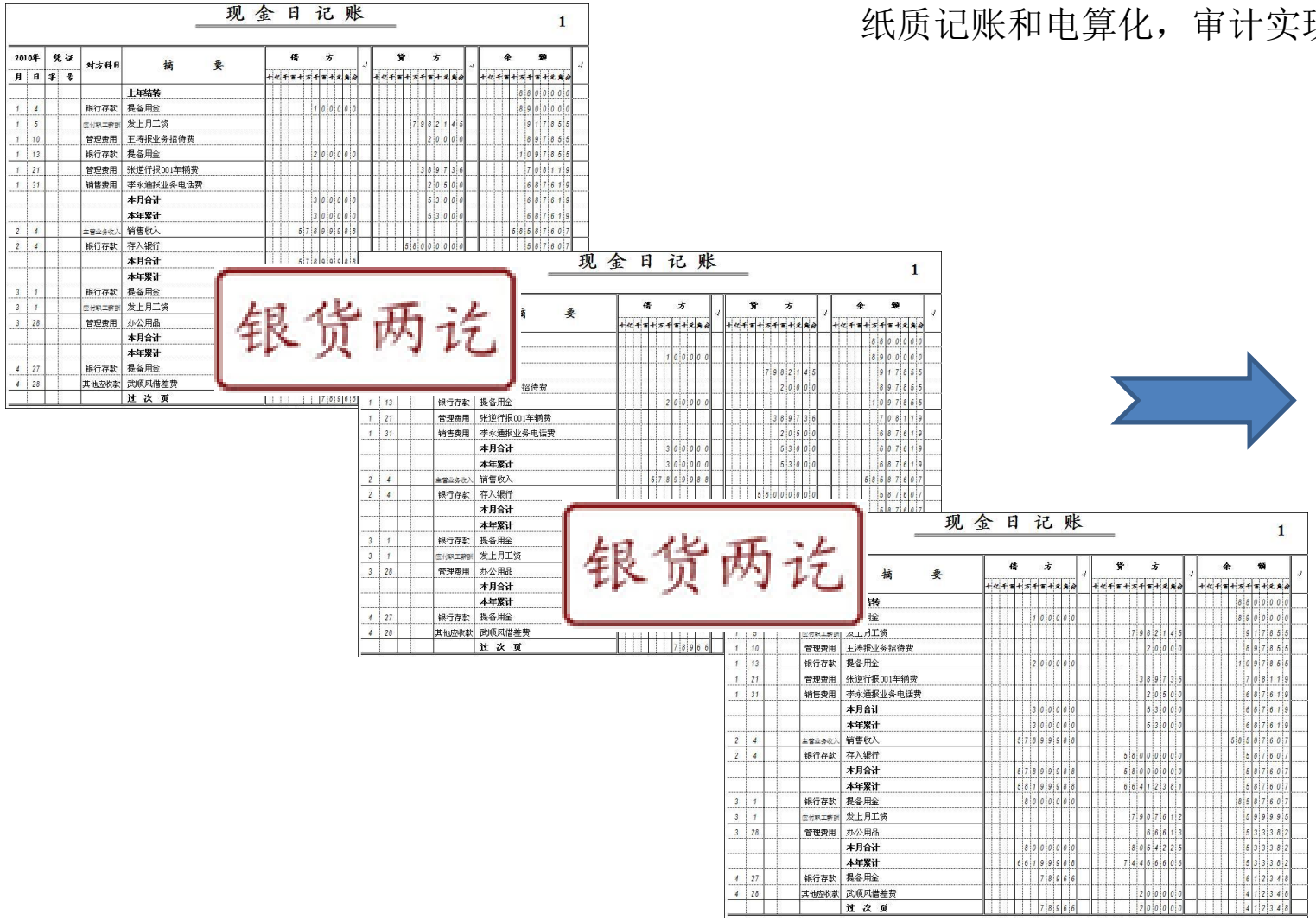
	2014年1月1日	2015年7月5日	增长的倍数
比特币全网算力	10.5p	380p	35倍
每一个区块平均交易次数	207次	702次	2.4倍
每一个区块平均交易额度	525个比特币	1528个比特币	1.9倍

安装一个这样的节点，对于理解区块链，比特币区块链是非常有帮助的。

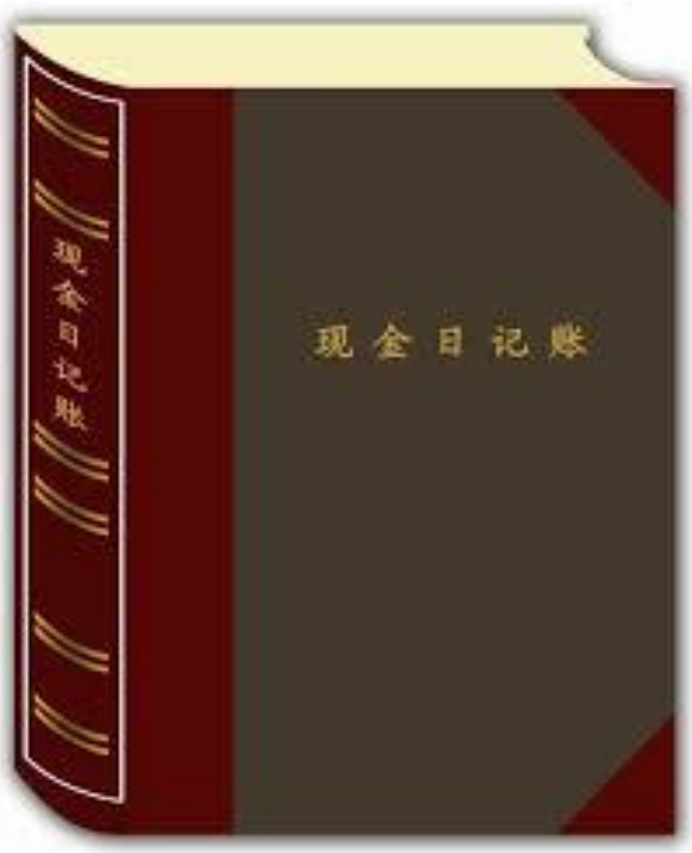
先看看一个blockchain数据库

- 看电脑
- 看Bitcoin Core

3分钟说明白区块链：复式记账法及其安全手段：骑缝章

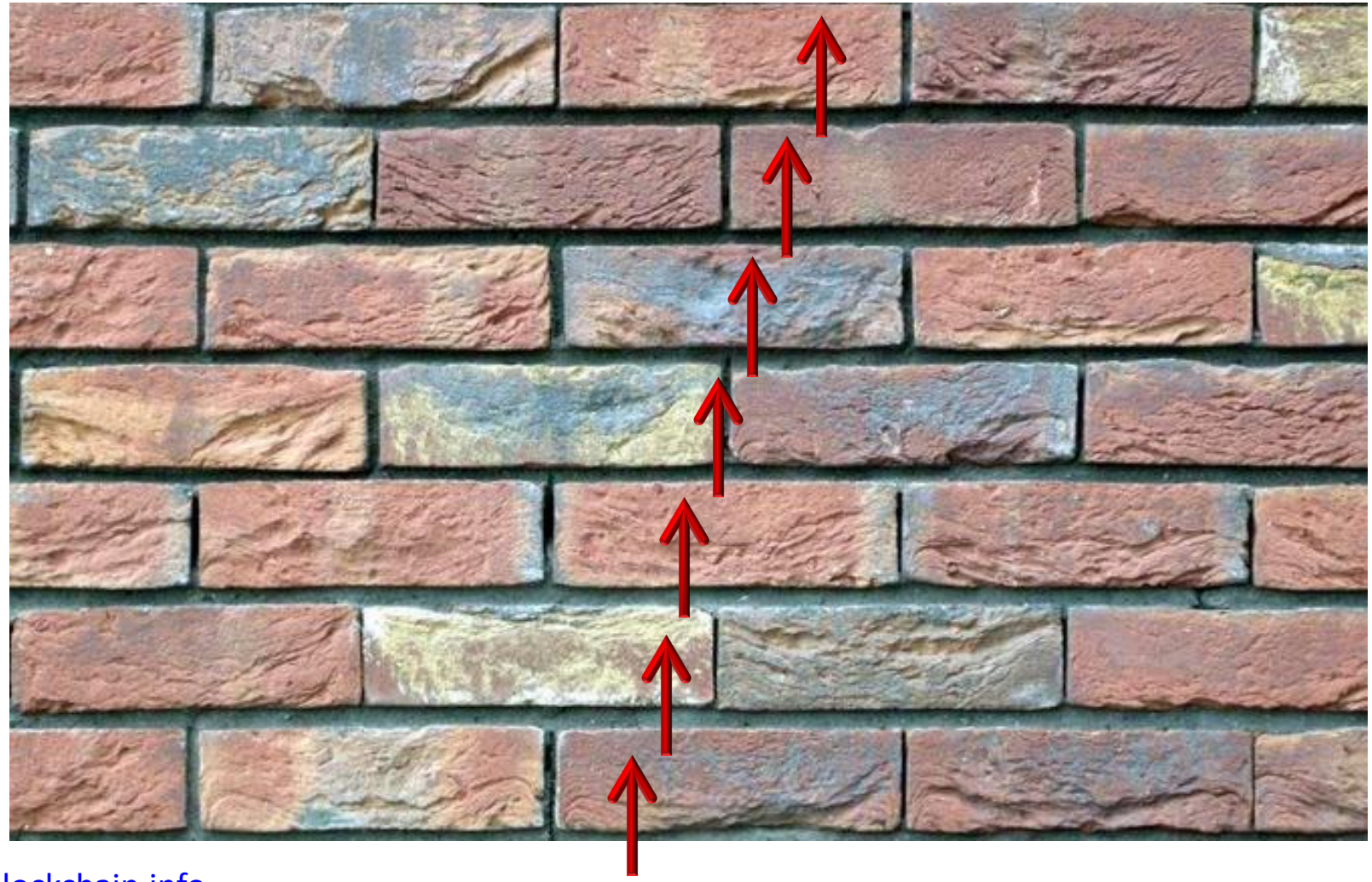


纸质记账和电算化，审计实现每一笔记录安全、不可逆。



目前区块链厚度（高度），帐页数量：高364203层
2015-7-7 11:01:26

- 开始于2009年1月8日
- 区块链生成：10分钟/块



最新数据：www.blockchain.info
www.zhanglian.info

4、分布式记账和清算，分布式记账（挖矿），去中心化信任（共识）。

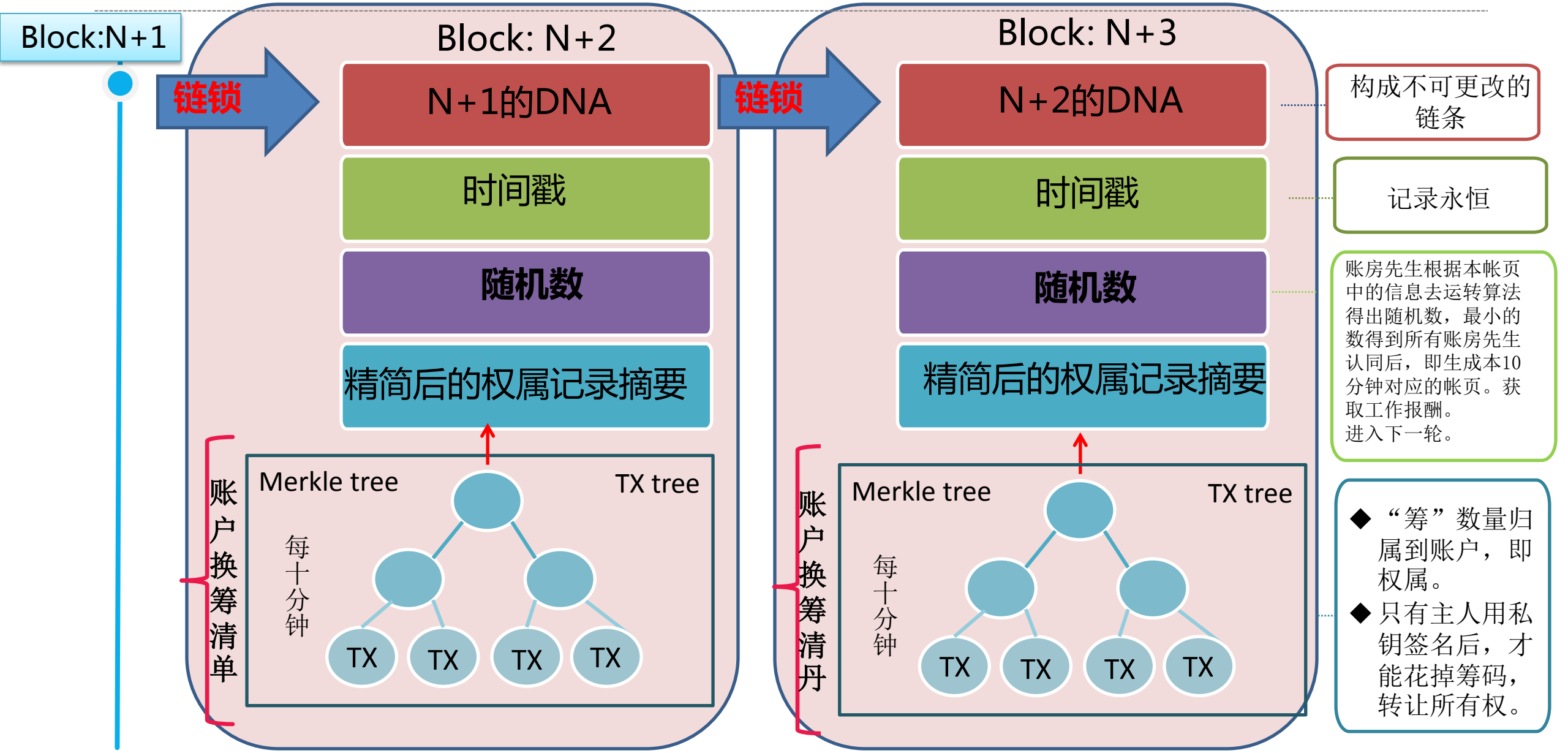
一．记账区块链系统实现共识（consensus），防□ 欺诈交易，避免“双重□ 付”。

- ◆ 遵守简单的规则、异步交互。
- ◆ 没有明确选举、没有固定选举时间。

二．记账员通过竞争性的记账工作来换取获得奖励的机会。

- ◆ 类型1：交易手续费
- ◆ 类型2：额外奖金，每10分钟25个，是增加□ 特币代券（Token）供应的□ 个过程。

Block+Chain=blockchain 区块链→账页链→账链



4.1 ： 4个独立过程（比特币的过程）

一．每个节点依据综合标准对每个交易进□ 独□ 验证。

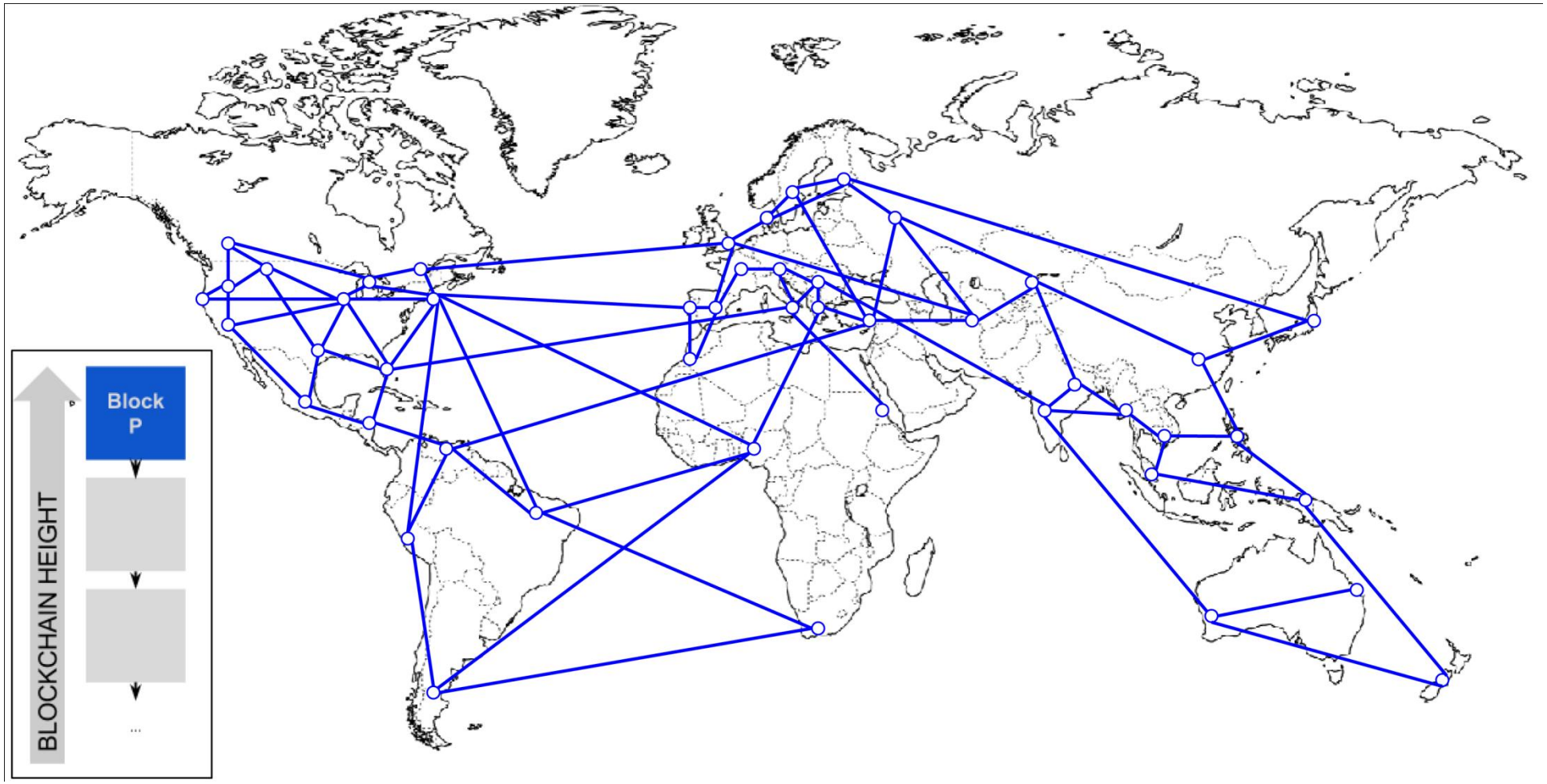
二．完成□ 作量算法的验算后， 挖矿节点将交易记录独□ 打包进新帐页。

1. 工作量 proof of work 运算一个函数：难度>SHA256(block)

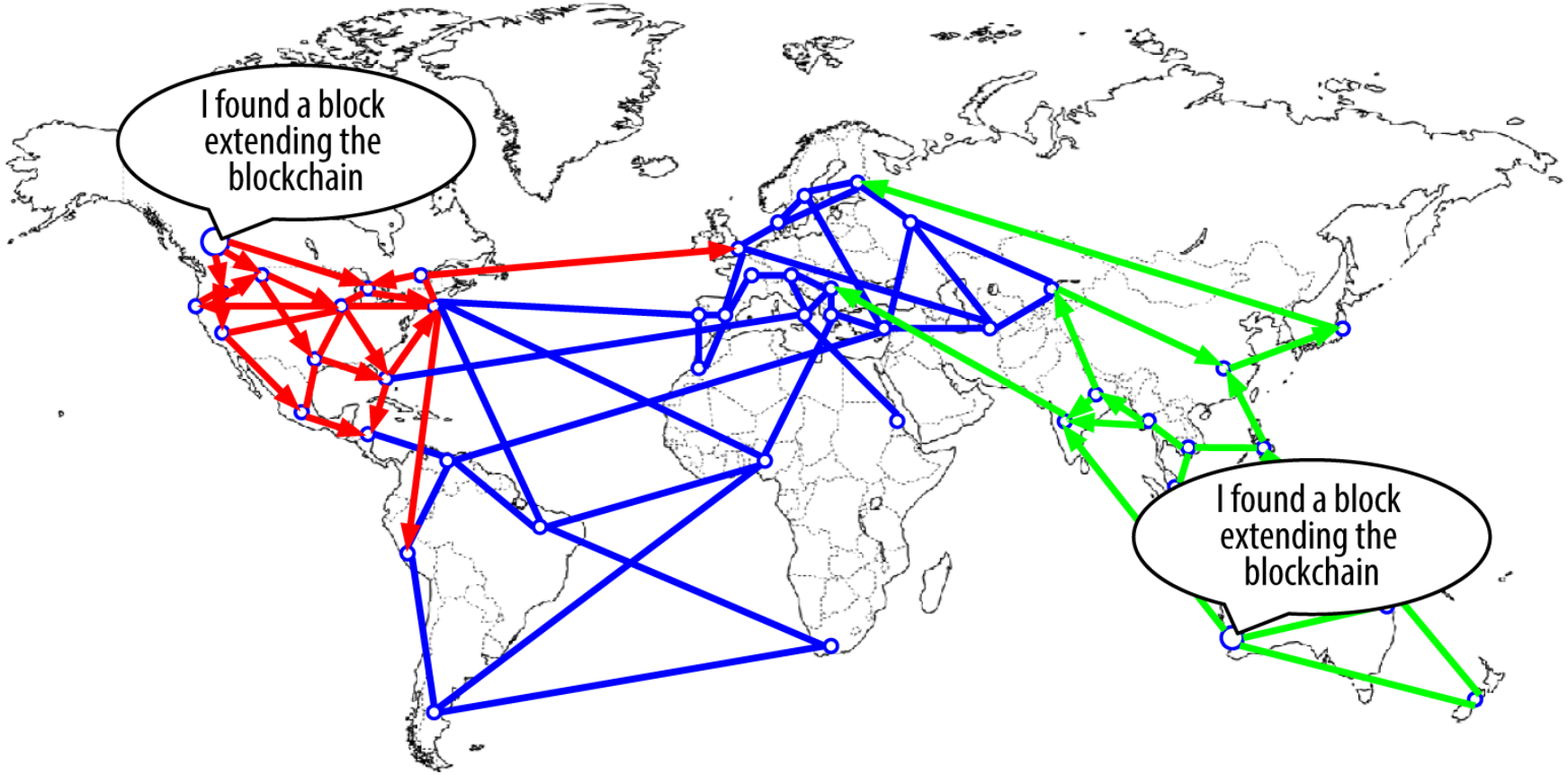
三．每个节点独□ 选择累计□ 作量最长的区块链。

四．每个节点独□ 的对新帐页进□ 校验并添加进区块链。

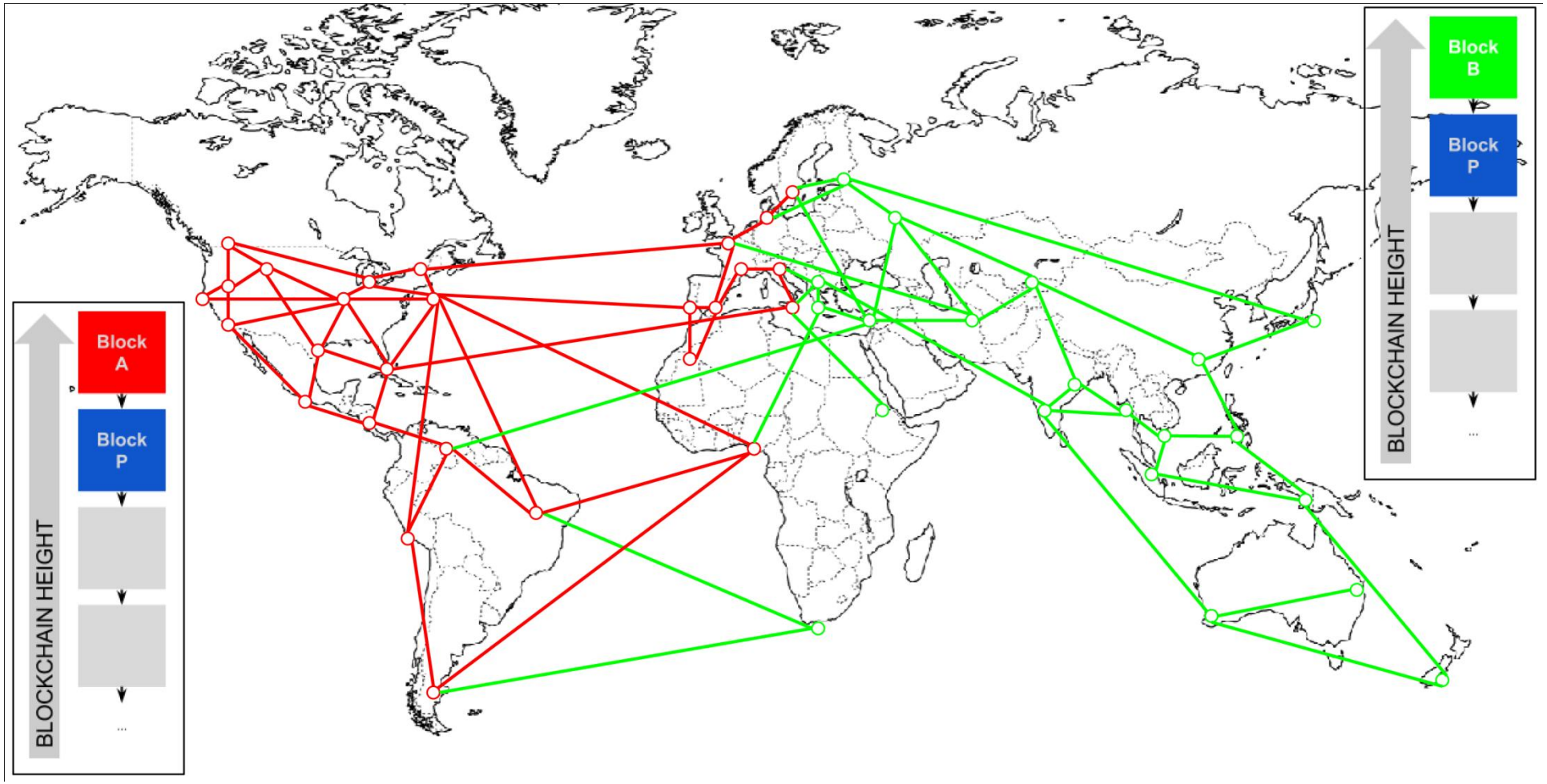
共识过程：时间1，意见一致



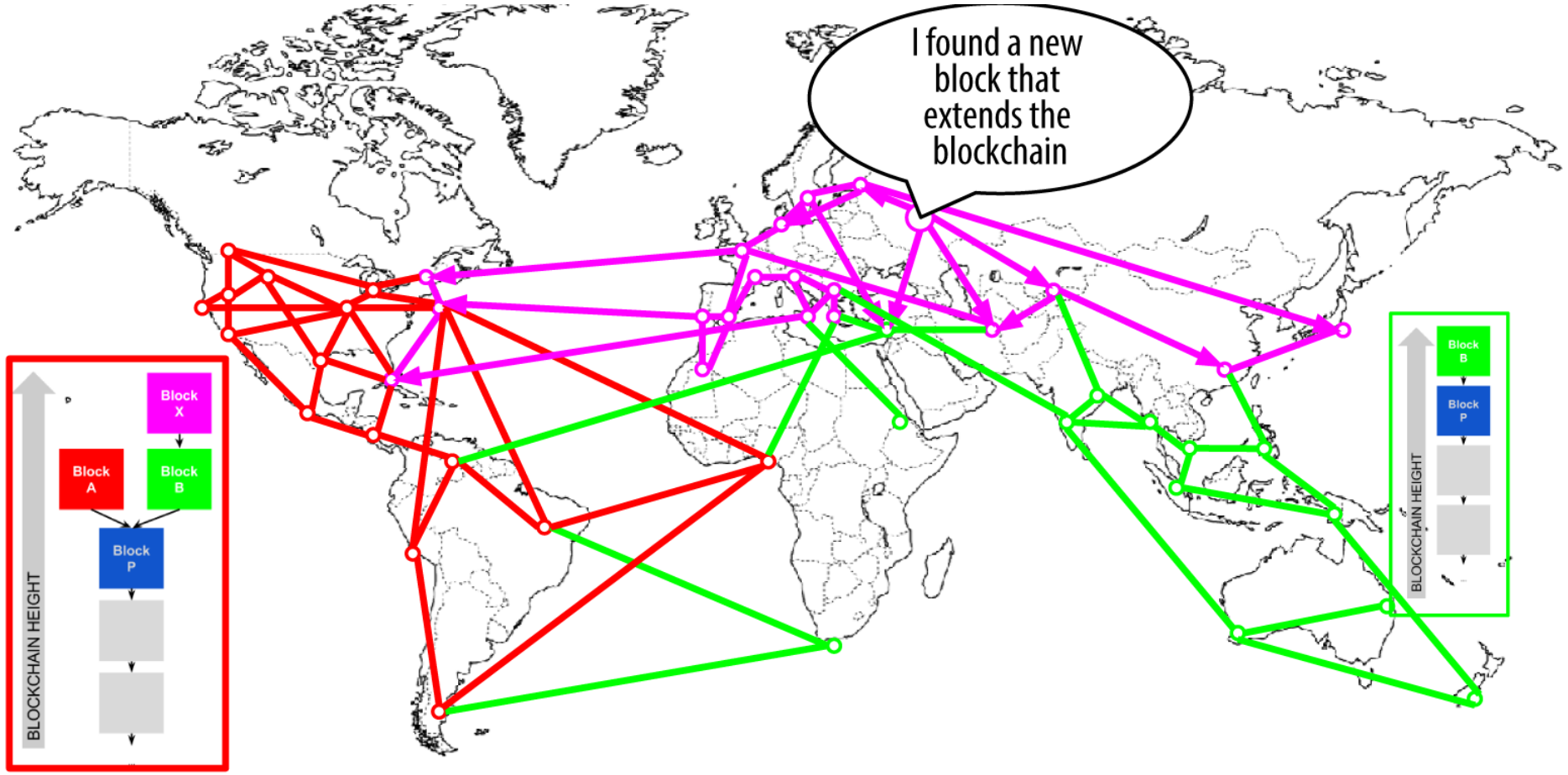
共识过程：时间2，记账出现冲突



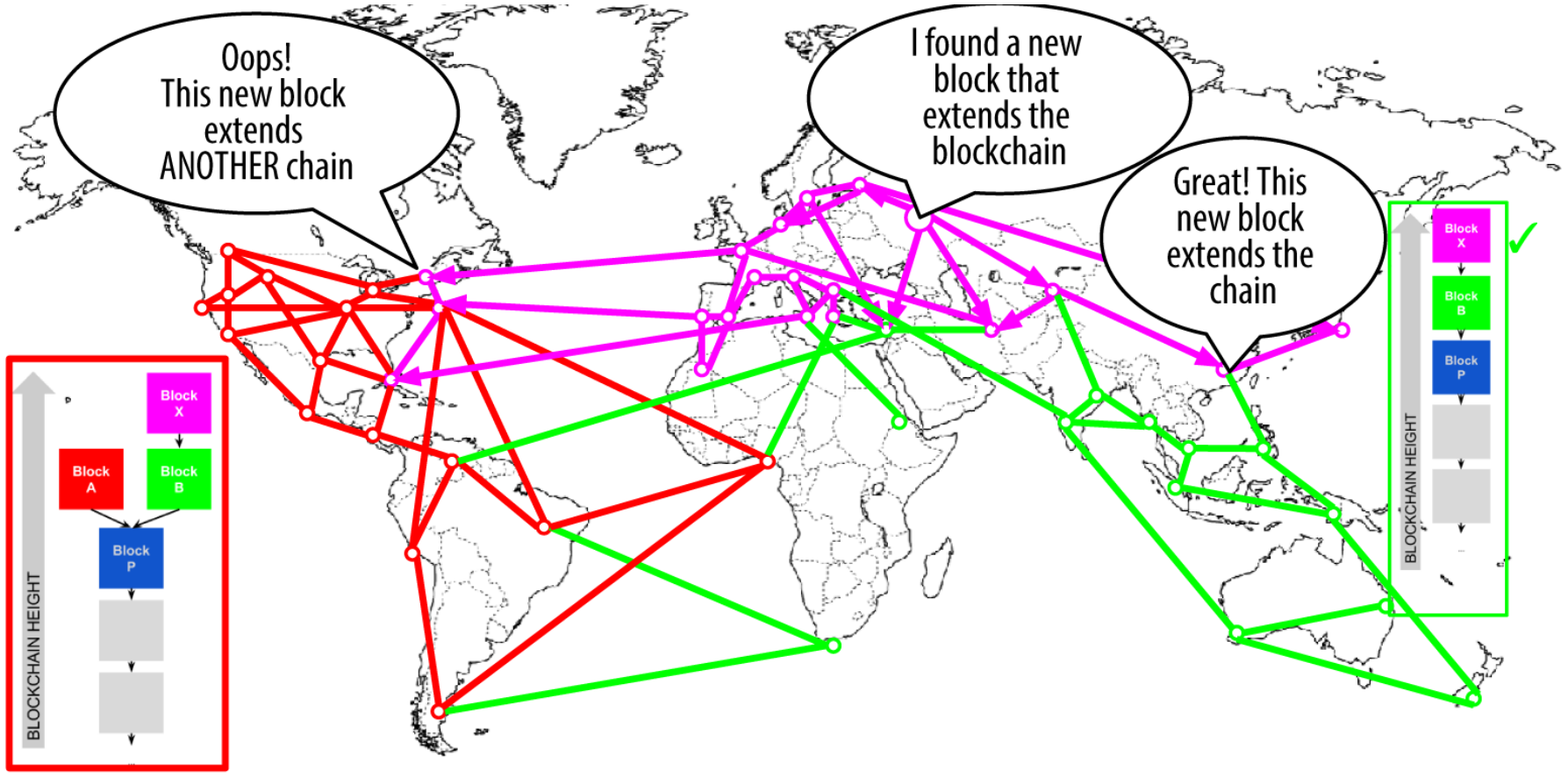
共识过程：时间3，分歧产生于全网



共识过程：时间4，节点自行选择，吵架无意义，但时间继续，记账继续。



共识过程：时间5，消除分歧，再次共识并合并链条。



记账算法是共识算法的一部分

一．□ 特币协议包括了内置算法， 该算法可以调节□ 络中的记账速度（挖矿）功能。

二．记账员（矿□ ）必须完成的任务——在□ 特币□ 络中成功地完成一个帐页记录——的难度是在动态调整的， 因此， □ 论何时有多少矿□ （ 多少CPU） 在记账， 通常每10分钟就会有□ 成功。

三．这个区块的到来标志着终结了产出账页277,315竞赛， 与此同时也是产出账页277,316竞赛的开始。

对比特币支付系统的共识攻击

一．共识攻击只能影响整个区块链未来的共识， 或者说， 最多能影响不久的□ 个区块的共识（ 最多影响过去10个块）。 □ 且随着时间的推移，整个□ 特币块链被篡改的可能性越来越低。 理论上， □ 个区块链分叉，但实际上， 要想实现□ 个□ 常长的区块链分叉需要的算□ □ 常□ 常□ ，随着整个□ 特币区块链逐渐增中， 过去的区块基本可以认为是□ 法被分叉篡改的。

二．同时， 共识攻击也不会影响□ □ 的私钥以及加密算法（ ECDSA）。共识攻击也不能从其他的钱包那□ 偷到□ 特币、 不签名地□ 付□ 特币、重新分配□ 特币、 改变过去的交易或者改变□ 特币持有纪录。

三．共识攻击能够造成的唯□ 影响是影响最近的区块。

花边：数量

一．新□ 特币的□ 成过程被称为挖矿是因为它的奖励机制被设计为速度递减模式， 类似于贵重□ 属的挖矿过程。 □ 特币的货币是通过挖矿发□ 的，类似于中央银□ 通过印刷银□ 纸币来发□ 货币。 矿□ 通过创造□ 个新区块得到的□ 特币数量□ 约每四年（ 或准确说是每隔210,000个块） 减少□ 半。

二．开始2009年1□ 每个区块奖励50个□ 特币， 2012年11□ 减半为每个区块奖励25个□ 特币。 之后将在2016年的某个时刻再次减半为每个新区块奖励12.5个□ 特币。

三．基于这个公式， □ 特币挖矿奖励以指数□ 式递减， 直到2140年。 届时所有的□ 特币 20,999,999,980） 全部发□ 完毕。

四． 换句话说在2140年之后， 不会再有新的Token生成。

比特币商品的定价来源机制浅析:市场发现？

一．比特币第一次在现实中价格发现，系统价值确立

- 价格是在2010年5月22日，来自美国佛罗里达州的程序设计员拉斯洛·汉耶兹被认为是第一个在现实世界使用“比特币”的人。当时，“比特币”还在电脑极客们手中流通，然而拉斯洛·汉耶兹将一万个“比特币”发给英格兰的一名交易者之后，后者接着用信用卡帮他从一家著名披萨零售店订购了两个披萨，就这样，这次跨越大西洋的交易也成就了历史。
- 2009年1月3日开始运转

二．“披萨很不错”

- 2016年7月，这两个披萨可能是世界上最贵的披萨饼，以当下650美元的兑换价格来算，平均每个披萨价格超过325万美元。

三．https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

结合多种区块链应用提炼出来的最重要特点

去中心化（Decentralized）	• 整个网络没有中心化的硬件，分布式的定价、交易和流通
透明（Transparent）	• 系统每个节点之间进行数据交换无需信任，系统运作规则公开透明，易于监管，逻辑上取得了最高效的监管中心
集体维护（Collectively maintain）	• 系统中的数据由整个系统中所有人共同维护，大规模协作。
可靠数据库（Reliable Database）	• 系统通过分布式数据库形式，让每个参与节点都获得一份完整拷贝
开源（Open Source）	• 由于系统运作规则公开透明，所以整个系统必定会是开源的
隐私保护（Anonymity）	• 由于节点和节点之间无需信任，因此节点无需公开身份，系统中每个参与节点的隐私都受到保护

Distributed Ledger技术手段特性：一套社会性技术，支[illegible]算那些依附上面的权益，通过市场发现价值，根据供需由市场定价，流通。

名称	技术要点	价值用途
1 分布式产权管理	分布式交易脚本、智能合约，数据资产权限清晰。	促进流动性，方便资产证券化
2 分布式路由	基于支付清算的多点接入，全网标签路由，P2P网络层。	永不掉线的互联网，大量无人驾驶新能源汽车。
3 分布式数据库存储	大容量、高速度加解密，数据权限就绪和踪迹，零知识证明，同态加密，盲签名。	保护隐私，维护商业秘密。用价格来调整。超低成本
4 分布式共识	分布式记账、激励。	用价格调整，发挥人性优势，规避人性弱点。

总结：区块链思想、制度安排、技术体制

一．从西方经济学角度：区块链（Blockchain）是市场经济体制中确定所有权（确权）的核心制度全新安排。

二．从政治经学角度：它是一种革命性的新型生产关系，适应了生产力的发展。

三．从信息经济学角度：区块链是一种首次可以大规模低成本对经济活动中信息流、资金流、实物流进行记账、对账、分账、销账的全新思维、手段。

四．从ICT信息通讯技术来讲，它是一种将分布式计算、分布式路由和分布式加密发布等相结合形成的全新的信息技术范式。

五．区块链思想的出现适应了社会发展进入了移动互联、万物互联、随时互联的时代之后，对安全可靠透明应用系统的需求，同时也更加满足对信息时代隐私保护商业秘密保护的强烈需求，也使对互联网治理体制中的共享共治找到了坚实的技术体制。

六．基于区块确权(账链）思想的价值互联网将颠覆基于分组传输思想的信息互联网，因为区块链能提供确权、隐私保护；同时还能公开透明，增强流通。

话题三

- 互联网的演进与区块链Blockchain账链

工业革命，华尔街的国际金融地位建立与信息技术：电报

一．信鸽，烽火台，驿送（马），旗语，灯光旗语。

二．华尔街从一条木板墙下的便道发展成汇聚全球资本，影响世界经济的金融中心，信息技术的进步功不可没。。

三．摩尔斯电码（**Morse code**），由美国人萨缪尔·摩尔斯在1836年发明，摩尔斯电码是一种早期的数字化通信形式，但是它不同于现代只使用0和1两种状态的二进制代码，它的代码包括五种。

纽约股市的开盘价格以从30秒钟内从华尔街传到费城的时间从30分钟锐减到几秒钟的巨大变化过程中，华尔街对于其他地区性证券市场的影响力大大增加，地区性证券市场被边缘化，从而确定了纽约作为美国金融中心的地位。

1866年，大西洋电缆竣工，老摩根是项目出资方合伙人

金融电子化时代：中央支付、清算体系，以及数据中心，数据安全。

1. 无线电报
   •拍电报
2. 电路交换
   - 全球电话网络
3. 分组传输，1960’S～1999年
   - 1957年，前苏联卫星上天，冷战，
   - 对应于电路传输。IPX/SPX, IBM SNA，ATM。
   - ARPAnet，BITnet（因时网），NSFnet，FidoNet
   - ARPA（NCP）→Internet（TCP/IP) 1983.01.01

但是：互联网的结构性缺陷—

一．1960年～1994年

- 用分组传输的**技术**实现不间断的信息传播。
- 靠严格的军队保密管理**制度**来解决数据隐私秘密。

二．1994年（信息高速公路）～

- 制度层面：商业化、民用化后，人员甄别体制失效了。
- 技术层面：数据的创造者不拥有数据，对隐私的侵犯。而且从用户角度来看经常掉线，掉网。虽然研发出了PKI（数据，信息安全），和IPSec VPN（通道，网络安全）

看标准发展史，互联网技术出身名门望族，美国国防部远景研究规划处ARPA（阿帕），但早期不关注Privacy ，Security，靠制度，后期实现安全靠补丁，传递价值碰到很多成本上的问题，效果不佳。

一．1969年 到 1987年
- RFC 0001 Host Software **April 1969**
- RFC 768 UDP；RFC 791 Internet Protocl；RFC 792 ICMP；RFC 793 TCP **Sept 1981**

二．RFC 987 Privacy enhancement for Internet electronic mail Part I : Message encipherment and authentication procedures
- **February 1987**
- Obsoleted by RFC1040, RFC1113

三．RFC1038 Draft revised IP security option.
- **January 1988**
- Obsoleted By RFC 1108

四． RFC 1244 Site Security Handbook
- **July , 1991**
- This FYI RFC is a first attempt at providing Internet users guidance on how to deal with security issues in the Internet.

五． RFC 1507 DASS - Distributed Authentication Security Service
- **September 1993**

六． RFC 1825 Security Architecture for the Internet Protocol
- **August 1995**.
- Obsoleted by RFC2401

七． Security 成为IETF研究重点
- 已经1995年了

凯文•大卫•米特尼克 Kevin Mitnick，进出不设防花园。从技术角度其实也没啥可多谈的。

一．**凯文•米特尼克**（**Kevin David Mitnick**，1963年－），是美国计算机安全顾问，作家和黑客。有评论称他为“世界头号黑客”。

二．他在15岁时（1978年）就破解北美空中防务指挥系统成功，在他16岁时就被逮捕，他也因此而成为了全球第一名网络少年犯。

三．破译太平洋电话公司的密码，修改上万美国家庭的电话号码

四．1994年，米特尼克向圣迭戈超级计算机中心进行入侵与攻击。

缺陷2：世界上第一个WEB Server。 HTTP 协议（以及HTML5）促进了互联网发展，但也留下了：大数据垄断和隐私侵犯，数据丢失。

在1989年的时候，CERN是全欧最大的互联网节点。伯纳斯-李因此看到了将超文本系统与互联网结合在一起的机会：“我只要把超文本系统和传输控制协议、域名系统结合在一起，就能得出万维网WWW了！”但却是Client-Server模式。

This Machine is Server,
Do Not POWER DOWN!!

-Tim Bernes
-1990年12月25日

微信用的也是HTTP协议，用HTTPS也没用。

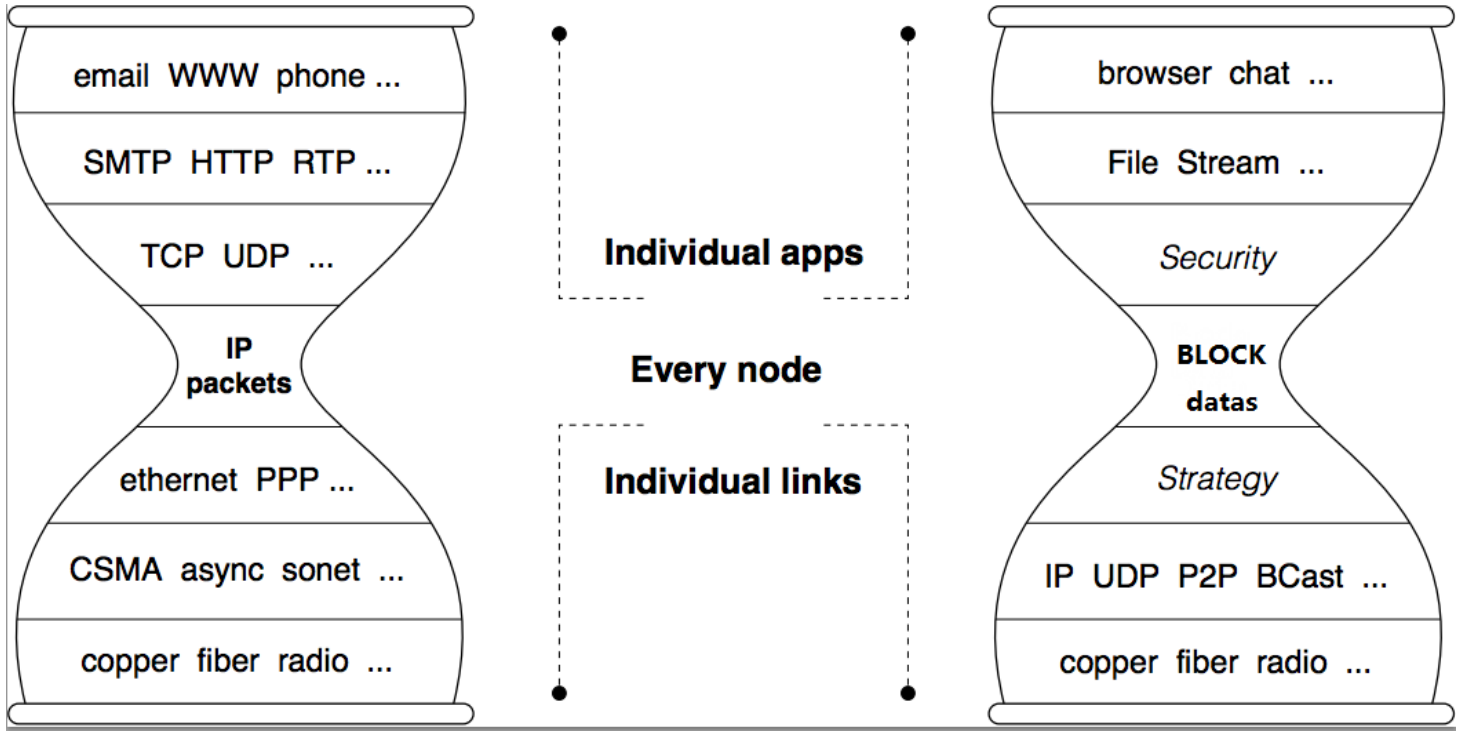
2016年4月4日 巴拿马律所法律文件泄露，2100万份离岸公司的电子法律文书丢失。

IT行业的技术范式变迁，及其市场形态的演进 (Alpha)

时间	特征	关键词	代表公司	代表性产品	运算	存储	传输
1945~	集中式→ ↓	大型机，小型机 庞大，昂贵 大主机+哑终端	IBM	System/360系列 程控交换机	IBM	IBM	IBM
1985~	分布式→ ↓	个人电脑 笔记本 服务器 + PC	Intel 微软 思科	X86 Windows 路由器、Novell	HP 联想	希捷 西数	思科 中兴 HW
1990~	集中式→ ↓	IaaS PaaS SaaS	亚马逊 Google	AWS，Azure， 阿里云，腾讯云	Google VMware	EMC	安卓 Apple
1995~	分布式→	网格计算，P2P 区块链，物联网	IBM 易链科技	Napster、Bitcoin、 Blocked Networking	谷歌 IBM	中兴 易链	易链 中兴

IT行业发展初期，欧美国家领先中国20~30年
如今，欧美国家只领先3~5年，在互联网部分领域，甚至已经被中国赶超。

对确权后数据用标签地址存取



从ICT通信的角度来看，弥补了互联网体系结构中的技术缺陷，数据确权隐私保护、网络安全、促进交易。

在网络空间中引入经济激励因素，使制度、技术、产品、标准正循环互动。

区块链标准将首先叠加在IP之上，成为一种传输层，成为整个互联网协议的蜂腰。

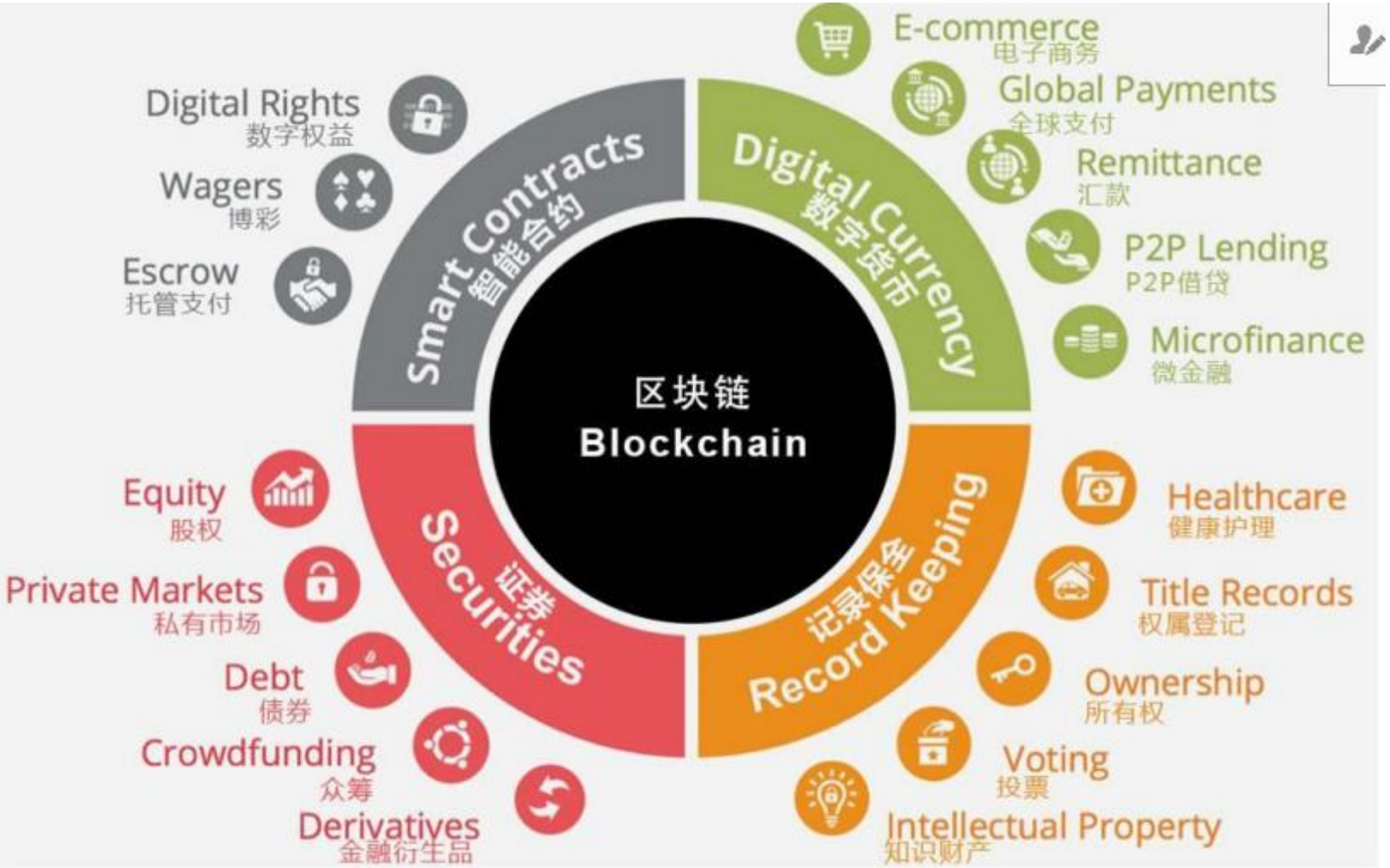
Block Router将会成为新型设备。

Modified by 王立仁，Source：named-data.net

话题4：区块链思想模式，以及应用落地

1. 区块链是一种全新技术范式。
2. 区块链为彼此不认识的人们之间大规模协作沟通，提供了基础设施，创造信任，并发展信用。
3. 区块链思想的出现适应了互联网发展进入了移动互联、万物互联、随时互联的时代之后，对安全可靠透明应用系统的需求，同时也更加满足对互联网时代隐私保护商业秘密保护的强烈需求，也使对互联网治理体制中的共享共治找到了坚实的技术体制。
4. 区块链是一种对市场经济中确定所有权（确权）的核心制度全新安排。确定数据生成以后就是不可更改的，即可以对外防抵赖，对内防篡改。在创建记录的同时，并且验证记录，可以简单地说是事账合一。
5. 区块链是一种大规模低成本对全球化后全球经济活动中信息流、资金流、实物流继续深层次、高频次进行记账、对账、分账、销账的全新思维。

更多应用以及标的物



区块链非金融应用


区块链
（用例）
数字资产买卖市场和所有权证明
Company: MyPowers
APP开发中应用模块的所有权证明
公司：Assembly
去中心化的员工绩效评估
Company: TRST.im
数字内容存储和交割的所有权证明
Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN
针对股票市场、政策的去中心化预测平台
Company: Augur
点对点的拼车应用
Company – La'Zooz
去中心化的病历管理
Company – BitHealth (Healthcare IT)
数字安全交易：所有权和转让
Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA
数字内容的所有权证明
Arts, pictures and images
Companies: Blockai, Bitproof, ascribe, Artplus
Other companies: Chainy.Link, Stampery
文件和合约的数字化和转移所有权的证明
Company: Colu (Colored Coins)
资产数字化：改进防伪措施
Consumer electronics, Automotive
Companies: The Real McCoy, ChainLink
Other companies: Everpass, BlockVerify
Degree Verification
Company: Degree Of Trust
通过区块链计算机网络分散存储
Company: Storj
提供数字身份保护客户隐私
Internet, car locks: Onename
Customer identification: Trustatom
Elections Voting: Follow My Vote
分布式物联网
家庭自动化：Chimera-inc.io
工业：Filament
确保评论的真实性
Helps users engage, share reputation and collect feedback
Company: The World Table
Through trustworthy endorsements
Company: Asimov
提供数字身份保护客户隐私
Companies: Sho Card, Uniquid
对所有家庭和企业开放的去中心化互联网和计算资源
Company: ePlug
托管服务
Gaming industry
Companies: PlayCoin, Bitnplay
Gaming industry and loan servicing
Company: New System Technologies
E-commerce
Company: Fundrs.org
公司成立、权益或所有权转让和管理的数字化
Company: Otonomos
应用于电子商务和制造业的自动履约智能合约应用
Company: UbiMS

区块链应用和落地的一些实践，互联网经济本地化、泛在化，数字社会和数字经济

一．互联网数据本地化，在当地创造出一个互联网的生态，区块链征信。

二．能源区块链，将能源产业领域中的“经济活动行为”，用区块链对“社会必要劳动时间”进行记账、对账、分账、审账、销账。

三．纺织区块链

四．农业区块链

五．供应链金融区块链

六．文化影视版权登记区块链

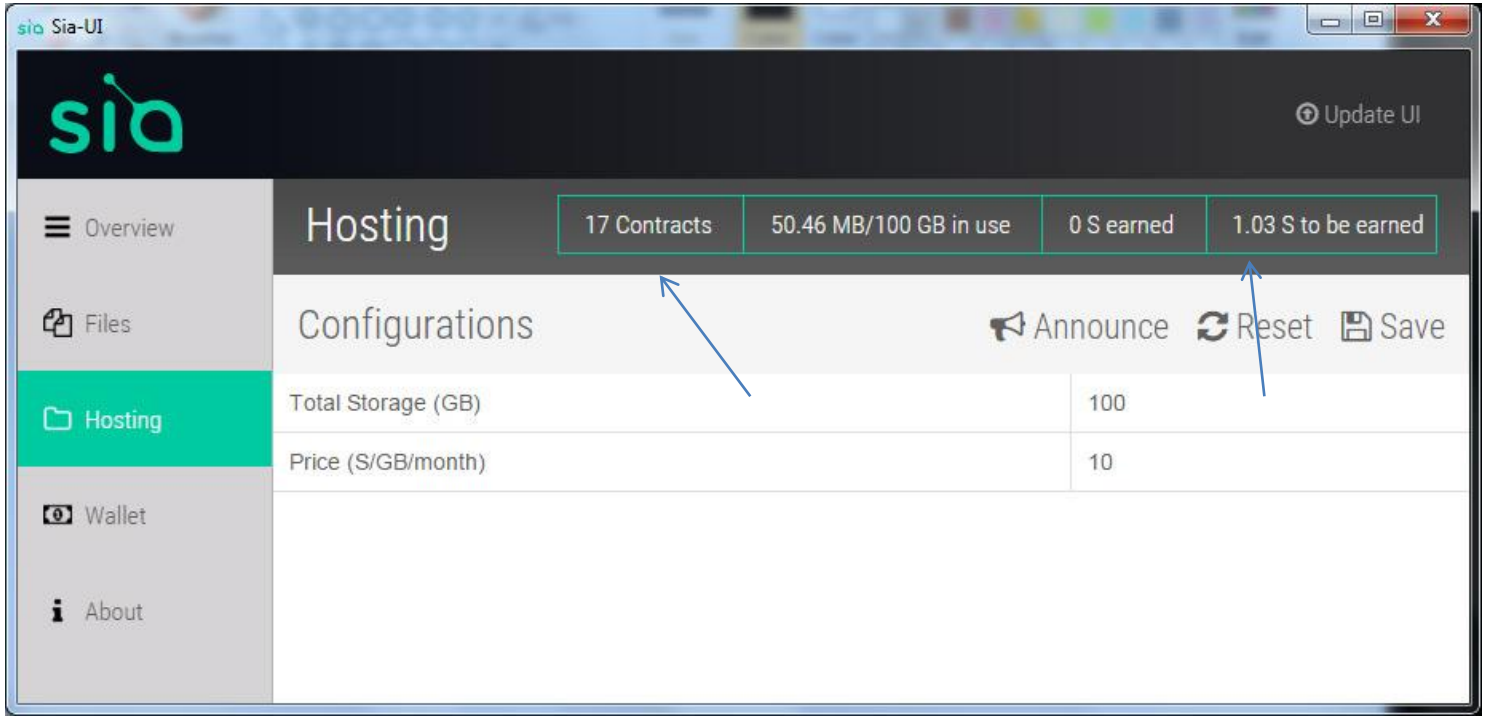
七．易货贸易跨境支付区块链

八．大型企业集团的区块链系统（乐视生态区块链）

九．基于个人个性数据的人工智能区块链

一○．2016年9月初，瑞银、德银、桑坦德和纽约梅隆银行宣发开发新的电子货币。

案例一：Sia 分布式企业级存储系统，以及生态中的支付、清算。



一．解决存储用户的痛点

- 中心化市场的数据丢失问题
  - 7家关闭：金山快盘、新浪微盘等
  - 只剩下：360，百度。
- 隐私被侵犯，数据被分析解读。
- 价格垄断
  - 10块钱/2T*month
  - 上传速度很慢，多种原因造成。

二．Sia.tech是分布式存储，

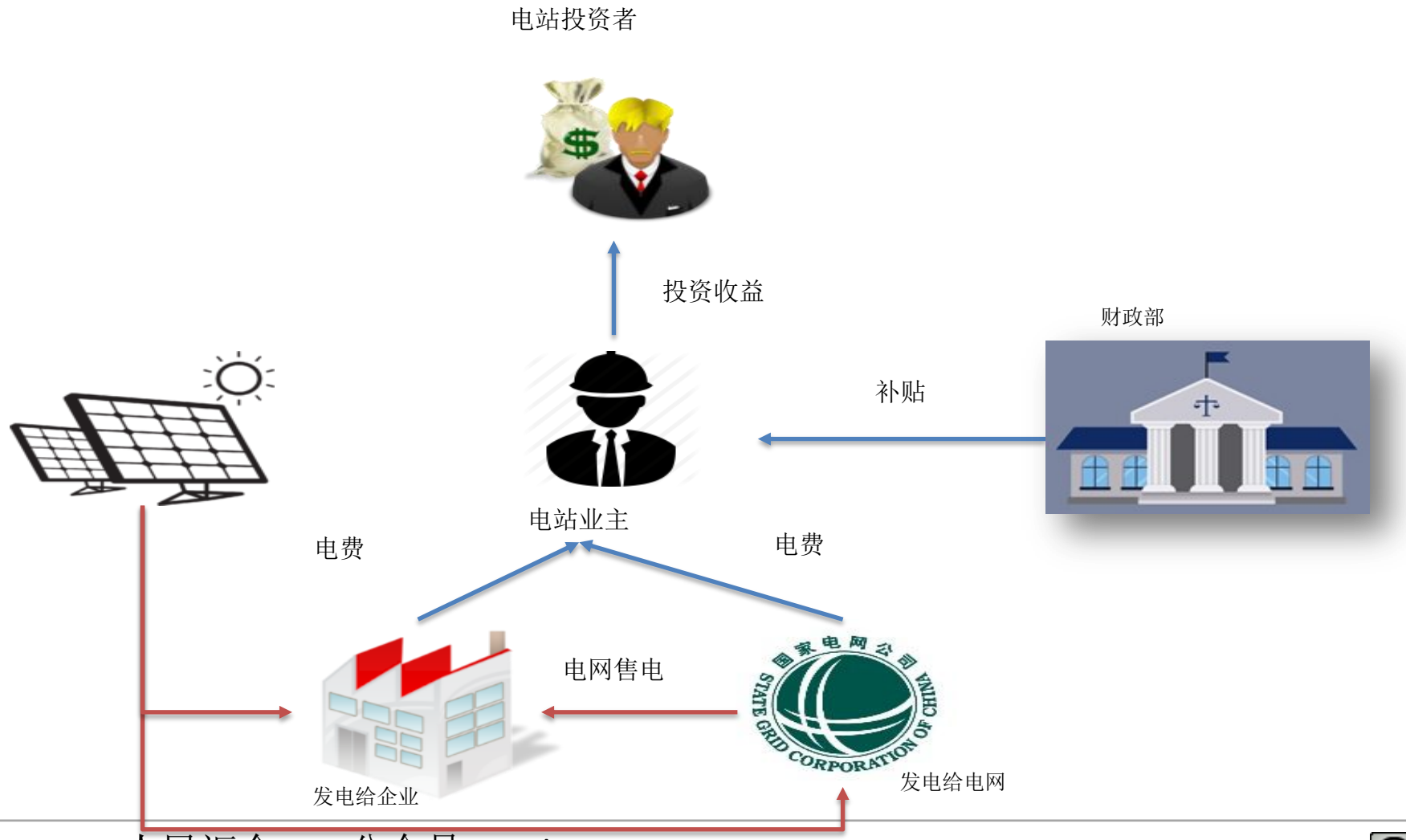
- 基于区块链合约.
- 基于代币交换（租赁者，主机空间供应商，记账员）.
- 市场喊价确定合约，存储。合约靠SiaCoin来运作。96%在线，否则惩罚。
- 绝对安全可靠。用价格来决定存储多少份，以及下载上传速度。 0.4元/T, month

案例2：目前能源互联网的设施存在缺陷，难以实际推广

精确计量		**能源信息源头|控制决策的基础** 实现能源系统运行状态的广泛数字化感知	✗ 数据真伪
泛在交互		**能源信息无阻流动** 传感器/设备与决策主体交互，主体间交互，人机交互	✗ 主体信任
自律控制		**本地动态响应，提高系统运行效率和可靠性** 面向分布式能源技术，利用本地信息实现快速的控制	✗ 预言机缺失
优化决策		**更精细的能源生产、传输和消费决策** 各个参与主体在给定的边界条件下最优化自身的行为	✗ 中心悖论
广域协调		**全能源系统的参与者行为相互协调** 有效的机制/合理的信号，激励系统参与者协调行为	✗ 内卷发展

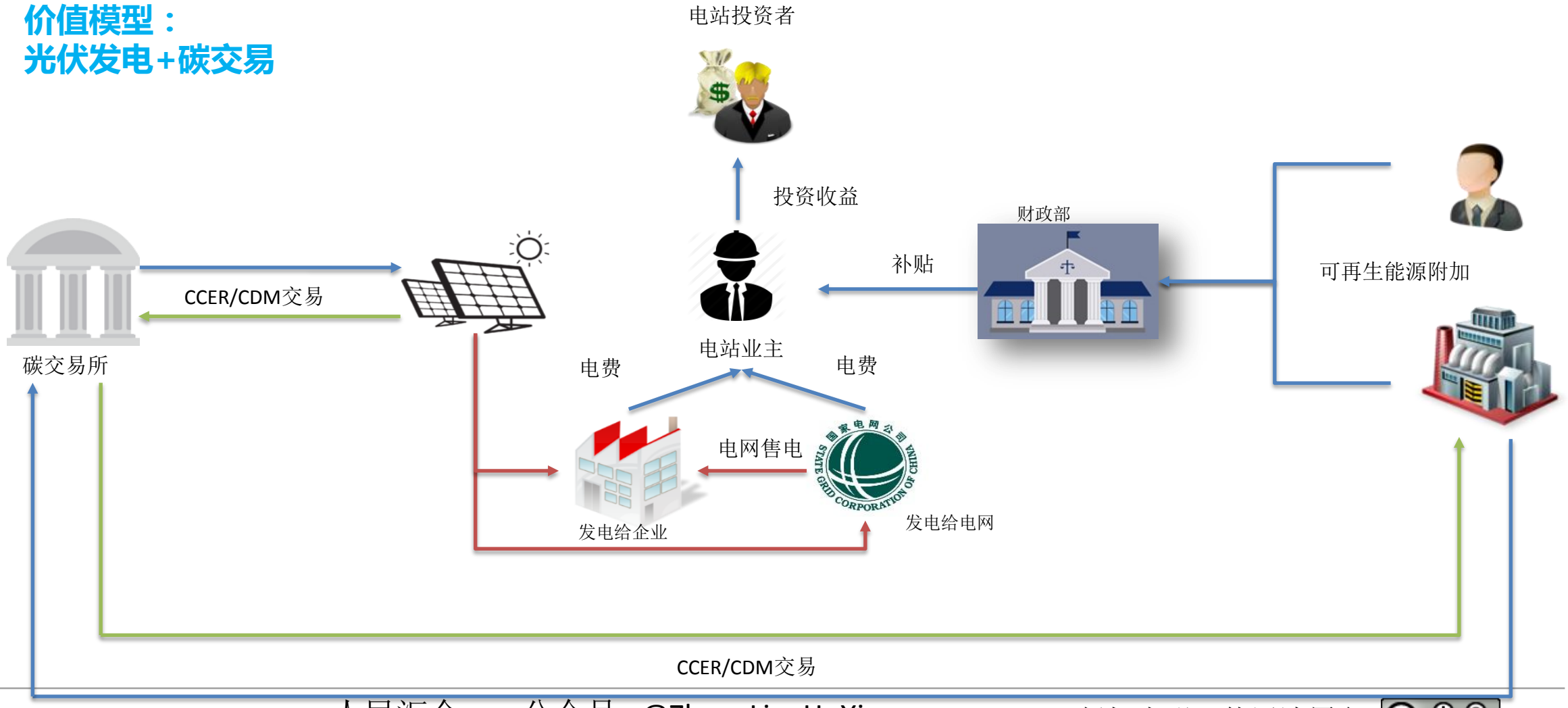
能源行业的多边关系日益复杂：以光伏发电为例

价值模型：
光伏发电

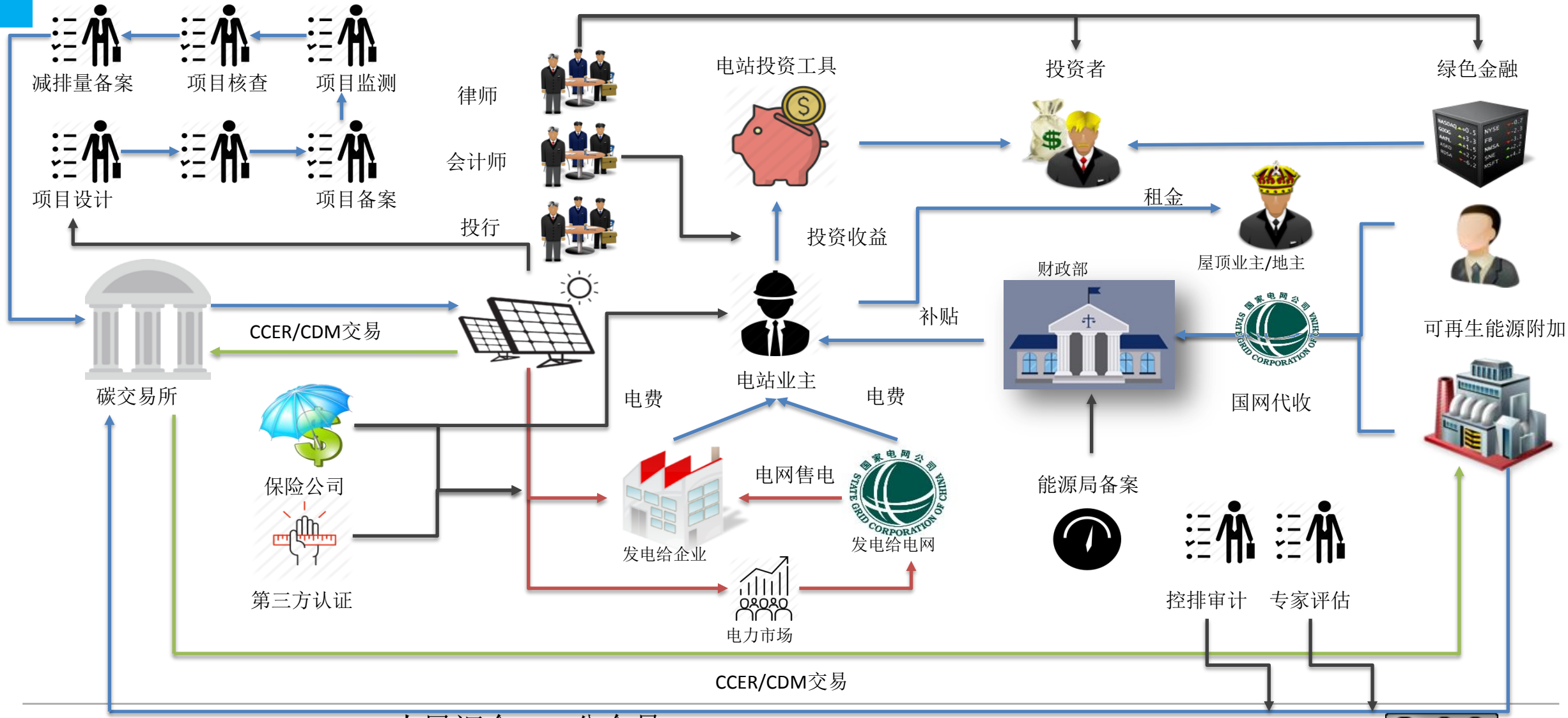


能源行业的多边关系日益复杂：以光伏发电为例

价值模型：
光伏发电+碳交易



能源行业的多边关系日益复杂：以光伏发电为例



创办能源区块链实验室探索下一代能源

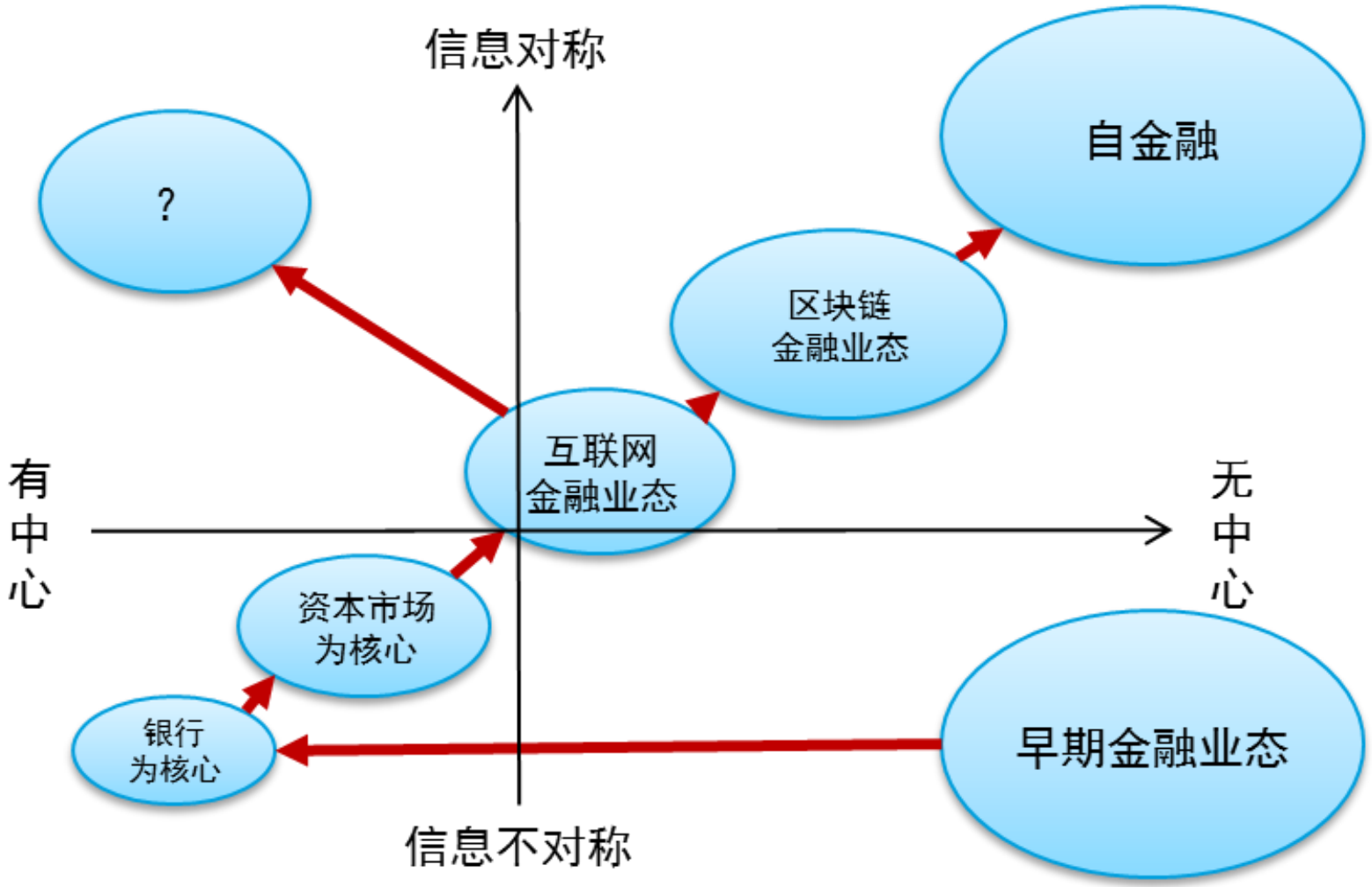
交易的主体将是设备，交换的商品是带有权益的数据和信息。

为实现安全、高效、可扩展，
互联网必须重构

历史上，每一次拐点都引爆
计算设备的激增

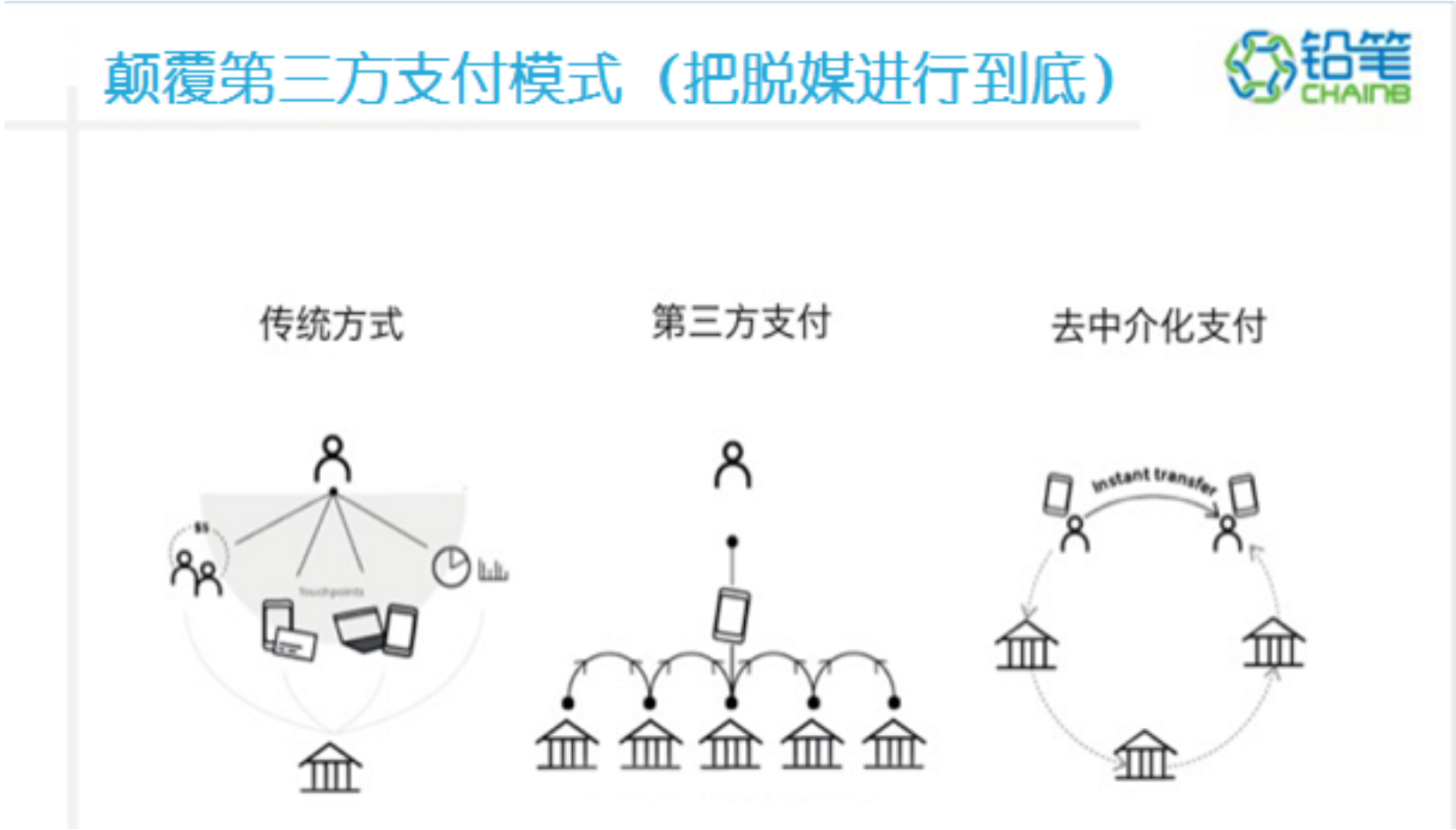
Surce: IBM

金融业态的变迁



Source：中国区块链研究联盟-曹彤

自金融路线图



自金融路线图：

用户自行发布竞争性数字资产
先进的金融交易和清算系统（实时准实时）
超低成本和超高安全系统
规避绝大多数法律问题
公开透明的开源解决方案
智能资产和智能合约

案例3：下一代分布式金融存储基础设施造价和运营思路：[illegible]统机房，1%的建造成本，5%的运营成本，所有现代云计算模式无法与其竞争。

为成功记账的共识的经济成本很低。

影响：对建造基础设施的金融业、IT工业、互联网公司的影响，监管

一．实时：确权数据、定价权益、交易收益

- ◆ 金融与经济融为一体，脱虚就实。
- ◆ 供给侧改革，农业区块链，医疗保健体育区块链、能源区块链、纺织区块链。

二．对IT工业，由原来的保护节点（IP），变成保护数据

- ◆ 防火墙Firewall、入侵防护IPS及衍生品的生存基础没有了。
- ◆ DDoS被治理了，流量清洗设备没有市场了。
- ◆ 等级保护、分级保护的市场会起来。
- ◆ VR对数据需求会起来，人工智能中对数据的垄断解脱了。
- ◆ 真正的无人驾驶汽车可以在不掉线的互联网中上路
- ◆ 加密行业的春天来了。大数据的交易变得切实可行。
- ◆ 区块链银行出现了。金融（银行）常在，但金融媒介不在了。

三．从数据确权、交易的角度来思考，哪些互联网企业巨头会被颠覆？

话题5:创新的挑战

一．《创新者的窘境》

- 每一轮新的技术革命，原来的成功者都被颠覆。所谓的“窘境”，就是说管理良好的企业，由于它的管理良好，使得它对于一个特定的“价值网”，我更愿意叫它“生态系统”，而成功，也正是由于它的管理良好，或者说，是对于某生态系统的过度优化，使得它对于另一个特定的“生态系统”，会遭遇失败。
- 破坏式创新

二．《困境和出路》

- 成立或者投资新单位
- 收购新公司

第一部分　大公司为什么会倒闭

第1章 大公司怎样会倒闭
第2章 价值体系和创新的推动力
第3章 机械挖掘机工业中的突破性技术变化
第4章 上升了的东西不能下降

第二部分　管理突破性技术的变化

第5章 按用户需要开发突破性技术
第6章 使公司规模与市场规模相匹配
第7章 发现新的和刚开始出现的市场
第8章 产品所提供的性能、市场需要和产品的生命周期
第9章 管理突破性技术的变化：实例研究
第10章 创新者的窘境：总结

说到创新，在IT领域，大家担心的技术问题都不是问题

一．问题：

- 速度不是问题
- 容量都不是问题
- 共识机制也不是问题

二．定律

- 摩尔定律还在起作用，以及More than Moore（超越摩尔）
  - 从应用端来驱动芯片研发
  - 从消费者角度来看
- 梅尔卡夫定律

三．激励为促进区块链系统的快速发展

创业、投资必问的几个问题：

一．对于创业项目，可以询问的几个问题是：

- 1 这个项目的共识机制是啥？
- 2 这个项目产生信用的机制在哪里？
- 3 你的分布式P2P交易模式是如何实现的？
- 4 开源后，你的盈利来源在哪里？

二．基于以上，可以询问创业公司的问题有：

- 5、在你的帮助下能上网的价值是哪些？
- 6、在价值流转的过程中，你是否创造了新的价值？

三．基于此，你可以与创业公司交流的问题有：

- 7 你使用了什么区块链？
- 8 你会自创一个区块链基础设施吗？
- 9 若是自创，如何确保系统的安全？

投资啥？那些创新能成功？

一．或者在一个特定行业市场中进行全面产业链塑造、颠覆。（空间专注）

- ◆ 交通、能源、纺织、农业、云存储、新能源电池梯级利用

二．或者面向所有的市场进行一个简单的创新（时间上专注）

- ◆ Factom、供应链、

三．与上一代投资不同，但是可以投资的东西有啥？

- ◆ 各种Token, 是数字权益的代表和象征。
- ◆ 进入区块链领域的公司。
- ◆ 基础设施

请想象一下造纸术后被大规模推广后的市场经济、金融大发展。

话题6：哪些企业巨头会被颠覆？

一．从数据确权的角度来思考

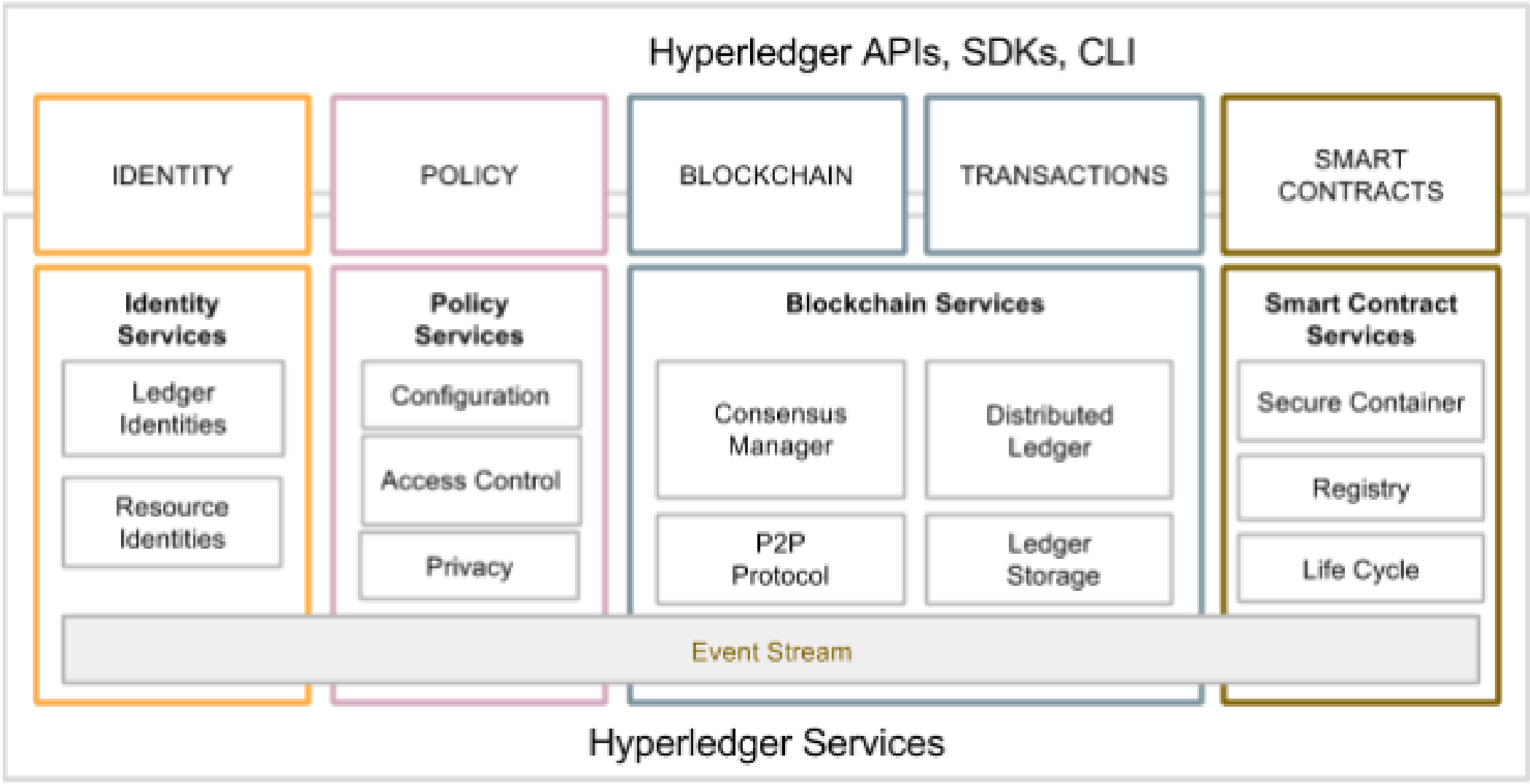
话题7：政府监管, RegTech？ 新型市场的出现

一．从数据确权的角度来思考
二．Regulator Technology
三．人工智能，自动驾驶，物联网支付
四．市场会更多，监管的手段会充分利用计算机。

Bonus1： Ethereum 以太坊的情况探讨

一．以太坊项目的起步
二．以太坊的目标
三．以太坊的技术特点
四．以太坊的下一步
五．以太坊的风险与问题
六．如何参与以太坊

Bonus2：HyperLedger的情况



若干预测和参与的实践，必定是个实践性的命题。

一．肉身在哪里，总是逃不脱，自利利他，通过规则的中心化促成基础设施的中心化。

- 人出现的地方，总是有江湖，受民族国家政权的法律管理。
- 规则的中心化，历史上的首次可以较大规模的逻辑上的中心化。
  - 中本聪的代码对系统的影响。代码是人写的。
- 监管沙盒的塑造, 监管科技RegTech的发展。
  - 引领潮流的地方政府，将会取得金融上的大规模创新。

二．分布式的、不可摧毁的Token交易所的涌现。

- 易台 BitTrade.com.cn
  - 欢迎大家一起来实践，针对一个ICO交易所的ICO。
  - “从咖啡馆到互联网网站。”
- Blocks & Exchange
  - 国外的分布式交易所，也有代币系统。
- 溯源系统 GenYuanLian.com 根源链
  - 直接以人民币的方式

参考书籍和信源推荐1

一．国家博物馆、首都博物馆、广东省博物馆、镇江博物馆
二．《通信的数学理论》克劳德·香农
三．《价值起源》 书籍 威廉·N·戈兹曼/K·哥特·罗文霍斯特
四．《比特币：一种点对点的电子现金系统（Bitcoin: A Peer-to-Peer Electronic Cash System） 论文 中本聪（Satoshi Nakamoto）
五．《代码-塑造空间的法律CODE and Other Laws of Cyberspace》 劳伦斯·莱斯格 Lawrence Lessig
六．《技术赋权-中国的互联网、国家与社会》郑永年
七．《投资革命:移动互联时代的资产管理》 肖风
八．《资本全球化-国际货币体系史 Bloballizing Capital- A hisotory of the International Monetary System》巴里·艾肯格林 Barry Eichengreen
九．《区块链新经济蓝图 Blockchain: Blueprint for a new economy》 MELANIE SWAN 韩峰等

参考书籍和信源推荐2

一．《货币金融学》弗里德里克·米什金
二．《宏观经济学》曼昆
三．《金融学》黄达
四．《债，人类第一个5千年》
五．《货币简史》塞加尔
六．《货币野史》菲利克斯·马汀
七．《罗马史》特奥多尔·蒙森
八．《伦巴第街》白芝浩
九．《资本论》马克思，恩格斯
一〇．《新新媒介》莱文森
一一．《财政学》陈共
一二．《资本主义大变形》《资本主义还有未来吗》等等
一三．《货币的非国家化》哈耶克
一四．《论人类不平等的起源和基础》卢梭

参考书籍和信源推荐3

一．《金融炼金术》 索罗斯
二．《千年金融史》 威廉·戈兹曼
三．《货币大师》埃里克•罗威
四．《大分流》彭慕兰
五．《脑的进化》约翰·埃克尔斯
六．《光速思考 新一代光计算机与人工智能》戴维·D·诺儿蒂
七．最后还有4个网站： coindesk.com ，8btc.com 以及 bitcoinmagazine.com 及其对应公众号，维基百科 wikepedia.org
八．以及最重要的Google

个人介绍

先后在金融机构和互金企业任职，拥有近十年产品创新与与运营管理经验，擅长农村电商、农村合作金融等，对农村、农民和农业比较了解。善于区块链技术的应用落地。