[1] 邱冠华，王剑，张宇.国泰君安行业研报：从货币演进的视角看区块链与数字货币. 2016,09,23

[2] 高盛行业研究报告：区块链从理论走向实践. 2016,05,24

[3]麦肯锡大中华区金融机构咨询业务：区块链---银行业游戏规则的颠覆者. 2016,05

[4]中国区块链技术和产业发展论坛：中国区块链技术和应用发展白皮书（2016）. 2016,10,18.

[5]谭志勇. 华金证券行业研报：区块链（技术篇）：预备在区块链跑道上等待枪响. 2016,09,05

[6]Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System

[7]World Economic Forum: The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services. August 2016..

[8]CREDIT SUISSE: Bloackchain August 3, 2016

[1]摘要：货币的本质是债权，货币发行记账体系不断完善。记账权核心要点在于满足五大要求，数字货币存在技术优势与不足。

重要逻辑：

货币曾经有过商品形态(一般等价物),但并非主流,且在发行、总量调节方面有天然缺陷。我们更倾向于认为货币的本质是债权,前提是该债权标准化、可流通,并且受到民众信任。这就需要信誉良好的记账(或发行)人。对记账权的争夺贯穿了整部货币史,最终行成政府、央行、银行三者制衡的记账制度。一个完备的记账货币体系至少需满足以下几点:

(1)控制货币总量;

(2)流通的方便性;

(3)流通的安全性、可信性;

(4)发行方式;

(5)可调节性。以比特币为代表的基于区块链技术的数字货币解决了前三个问题,但没能解决货币发行和调节问题,因为比特币的发行权是分散的且总量固定。我们认为,央行引进基于区块链技术的数字货币,可以解决电子现金的安全流通问题,但货币发行体系仍然保持现状。

记账权核心要点：

(1)控制货币总量:记账人,即货币的债务人(比如央行或银行),必须保持良好的信誉,适度控制货币发行量,但又得实现合理增长。这是它的债务凭证能够履行货币职能的最根本的必要条件。

(2)流通的方便性:这种债务凭证能够方便地转让流通。在现今网络时代,这一点并不难做到。

(3)流通的安全性、可信性:这种债务凭证必须值得信赖,它很难被非法篡改、复制或伪造(及其他非法行为)。过去,人们通过选取昂贵的商品充当一般等价物,来提升伪造成本。对于纸币,通过防伪技术实现。对于电子货币和存款货币,通过加密技术实现。虽然安全性在不断提升,但仍防不胜防,无法做到绝对安全。

(4)发行方式:发行主体要适当选择货币的最初投放对象,理应是价值的创造者或持有者,以此把其持有的价值(或未来所能产生的价值的现值)换成手中的货币。

(5)可调节性:央行可以通过调节债务凭证的总量,来对宏观经济实施调控。一般等价物充当货币时,很难做到这一点,因为一般等价物的产量不能完全掌控。其中第(1)点是成为货币的必要条件,第(2)、 (3)、 (4)点是货币实务中的现实要求,而第(5)点是当局调控经济的需求。一种良好的记账货币体系,至少要满足上述几点。

区块链的应用优势：

区块链使用了早已流行的 P2P 技术,即点对点分布式系统,不存在中央结点。在点与点的一笔交易中,使用去信任化技术,主要是不对称加密(加密、解密用到的密钥是不同的)

。比如,A 要向 B 支付一笔货币,B先公开一个公钥,A 拿这公钥对即将付给 B 的货币进行加密,并向全网发送。B 用自己对应的私钥解开它,并向全网证明。全网收到后,验证

了这次加解密,从而大家都承认这笔钱是付给 B 的(由于不对称算法,别人解不开私钥,但能够验证 B 是不是解开了,这是关键)。然后,这笔交易被记录下来,A 的账户上减去一笔金额,B 的增加一笔。这种基于不对称加密技术的支付,不用两个人之间有什么信任关系,甚至不用知道对方是谁,这就是所谓的去信任化。在此,区块链出色地解决了数字货币流通中的安全技术问题。每完成一定时段的交易后,则把该时段内的所有交易记录下来,且在所有的结点上都进行完整拷贝,这就是一个“区块” (block)。因此,信息几乎没有被篡改的可能,除非有办法入侵几乎所有结点。一个个区块首尾相连,就构成了区块链(block-chain)。以该技术为基础的数字货币问世,以比特币为代表。它会不会成为下一代货币呢?我们认为还很远,一是因为现行的货币体系虽然有点问题,但大体还是运行良好的,因此轻言颠覆尚早。二是,我们还得审视下比特币是否满足现代信用货币的要求。

[2]摘要：高盛的这篇研究报告主要从区块链具体应用的角度进行分析，应用到七大案例：声誉管理与共享经济，智能电网，房地产产权保险，现金证券（股权、再回购协议、杠杆贷款），反洗钱合规性。而且末尾列出了目前所有的上市企业资料，可对具体行业进行研读。每个案例分别从机会，市场痛点，区块链应用，面临挑战以及机会量化的角度进行剖析。摘录案例7要点如下。

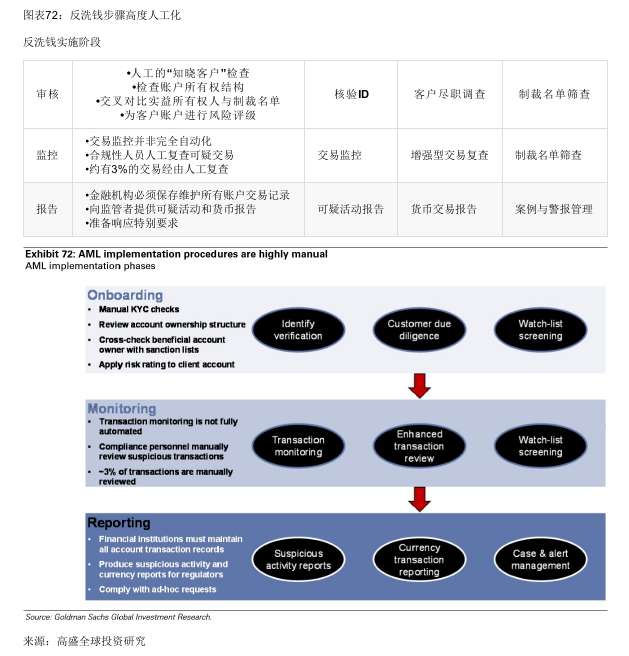
现状：

反洗钱活动的开展需要耗费大量人力。为了与不断改进的反洗钱规定合规,金融机构花费大量资源开发和维护他们的反洗钱合规性程序。尽管银行的确会将这些流程的许多地方自动化,但绝大部分的反洗钱预算是安排给合规性人力资源的,他们负责人工审核可疑的交易并审核新客户。我们认为现有的银行体系面临着数个结构性问题,从而导致需求这样的人工监控和高额成本结构来执行反洗钱合规性程序:

（1）银行之间缺乏数据“共享性”,导致在审核客户方面重复劳动。每当与一名新的客户建立关系时,金融机构都会根据“知晓客户”规定进行彻底的客户尽职调查(CDD)程序。虽然特定零售和机构性账户的所有权结构的复杂性要求进行人工核验,但“知晓客户”工作通常是重复劳动。在大多数司法辖区内,银行都需要独立地审核哪怕是已经被其它银行审核过的账户。我们预计适当的“知晓客户”尽职调查会在每个客户身上花费15,000到50,000美元。

（2）缺乏账户汇编,导致交易监控中出现大量误报。尽管银行依靠交易监控软件来审查可疑行为,我们发现2%到5%的交易都需要由合规性人员进行人工复查以决定是否涉嫌洗钱。这种情况中,误报率接近99.9%. 在绝大多数的情况下,我们认为这不是监控软件的问题,而是因为糟糕的交易数据质量(如:缺少收寄款人身份细节)。即便是可以形成审计跟踪的转账信息从句法上是误报或不完整的时候,无论是否涉嫌洗钱,监控系统都会发出警报——而我们认为这样的人工对账流程会为全行业带来大约60亿美元的成本负担。

上述因素导致金融机构雇佣大量的员工来执行反洗钱合规性程序。审核客户、交易监控和人员招聘——我们预计人力资源成本占所有反洗钱预算的80%. 我们认为这些成本中的很多都因为金融对手方之间在可靠信息共享流转方面存在结构性低效率,因此产生了由合规性员工进行人工干预以促进流程的需求。



区块链步骤优化：

（1）账户细节安全汇编可以为交易监控带来更高的透明度和效率。对涉及每笔交易的账户信息完整度(收寄款人细节、法律实体信息等)相关的规则进行汇编,区块链可以改善交易透明度,减少误报率。我们相信,在对账触警交易和潜在洗钱活动方面,经常性人力成本将得到减少。

（2）记录目前和过去交易的分布式账本将简化记录和审计流程。金融机构可以代表每一个客户,使用区块链驱动的系统来储存所有交易的历史记录(包括共享文件和负责的合规性活动)。由于所有涉及特定客户的交易都能自动追溯,这些记录将作为银行按照反洗钱要求行是的证据,使之迅速实现与监管要求合规。

（3）机构间共享的、安全的客户信息分布式数据库可以减少客户审核方面的重复劳动。每个金融机构都需要为每个新账户进行“知晓客户”检查,以验证其源头和个人、企业、子实体之间的关联关系。原则上和某个客户有长期关系的金融机构可以帮助“证书化”该客户,通过一个基于区块链的、安全的、许可制流程,向其他机构提供客户关联的支持证据。尽管这不能完全消除其他金融机构的“知晓客户”负担,但这可以减少人工审核步骤的数量、减少客户尽职调查的开支。

通过优化这些步骤,区块链将重塑反洗钱合规性实施流程。由于数据完整性和可访问性都得到了提升,我们相信对人工执行“知晓客户”审核和涉嫌洗钱活动复查的依赖将大大减少——因此大量减少人力资源成本。我们也预期区块链可以改善对手方风险,因为客户信息将变得更加可验证,而系统性“缺损”的情况会变少,最后减少金融机构可能遭遇的罚款。

量化优势：

我们如下解构假设的成本:

（1）客户审核:温和的成本节约与优化的“知晓客户”流程。我们预计区块链可以减少客户审核方面的人力成本的10%,带来1.6亿美元的成本节约。虽然一个客户信息的共享数据库加上特定账户与历史银行关系证明可以消除“知晓客户”方面的重复劳动,但我们预计,在如下几个情况中,银行仍然需要进行客户尽职调查:预期账户属于私营企业;个人第一次开设账户;客户的历史数据的真实性存疑(如:只被单一来源验证)。值得注意的是,区块链不能免除银行的“知晓客户”责任,所以我们预计,即便再是有客户资料透明度和安全性方面的进步,考虑到反洗钱罚款,银行在审核新账户的时候还是会慎之又慎。

（2）交易监控:更低“误报率”,更少人工干预将带来更高的效率。我们预计区块链将减少交易监控方面的人力资源投入达30%, 带来14亿美元的成本节约。我们相信用区块链加上特定的客户标识来抓取和追踪客户信息可以为交易监控带来更高的透明度,而且既然大多数误报和交易信息不完整有关,这也将极大减少误报率,因而降低必需的进行触警交易对账的合规性人员数量。

（3）培训和技术开支:更强的安全性和更少的人力开支可以带来极大的成本节约。我们预计区块链会减少人员培训开支30%, 带来4.2亿美元的成本节约,这仅和上述的人力开支节省相关。长期来看,由于对专有系统的依赖减轻,区块链可以降低技术开支达20%(4-5亿美元的成本节约)。

[3]摘要：麦肯锡的研报讨论林五大应用场景：数字货币，跨境支付与结算，票据与供应链金融业务，证券发行与交易，客户征信与反欺诈。并对中国金融机构针对性的提出了建议。与我们的研究主题较为相似，建议详细阅读。

区块链颠覆性：

（1）最底层技术的颠覆者

如果我们将银行商业模式层层分解,不同的新技术发展一直在推动各个层面的进步(图1)。以信息时代为例,互联网带动了应用层面的无数创新应用——P2P借贷、在线理财、众筹;云平台改变了业务处理和基础设施部署的模式,大大降低了银行的业务运营成本和IT投入;大数据分析技术将风险控制从以经验判断为主,带入了以机器学习为主、用数据作为决策依据的时代,使得全自动的快速信贷模式成为可能。尽管金融上层应用和业务流程创新风起云涌,但信用中介的基本要求使银行在商业模式的底层逻辑和相关技术,例如系统间的信息交互方式以及交易清算的基础设施方面,并未有革命性的提升。区块链技术的出现恰恰要颠覆银行

商业模式的底层技术基础。首先,“清算”这个概念在区块链网络中将不复存在,所有的交易都是“发生即清算”的,交易完成的瞬间所有的账本信息都完成了同步更新;其次,系统间的信息交互不再因为兼容性和互斥性而导致部署成本高且连接困难,因为所有系统都使用同样的技术协议;而各参与方之间的交易规则也依照协议共识写入区块链成为标准,不得篡改。

（2）商业制度创新的推动者

区块链技术的出现是对现有商业模式的制度基础和参与者之间关系的重大挑战。现有金融体系是建立在三个基本制度框架之上的:商业信任是依赖法律条文而存在的;资产转移交易是以独立第三方作为信用中介来保障实现的;交易结算和清算是以集中式的清算机构为中心来处理完成的,然而人们习以为常的制度基础和商业流程都有可能随着区块链技术的广泛应用被颠覆。在现有制度框架下如鱼得水的金融中介机构,如何在这场模式变革中调整角色,将决定其未来的命运。以Visa和Nasdaq为例来说,一个是提供支付中介服务的支付组织,一个作为证券发行和交易市场平台,其主要角色都是作为交易的中介。两家公司很早就意识到区块链技术可能对自身未来的商业价值形成的挑战,于是采取了拥抱技术革新的明智做法,成为Chain (美国区块链技术初创公司)的早期合作者,布局区块链技术应用的试点项目。从银行的角度来说,在这一波新的技术革新浪潮中是成为技术受益者,还是被颠覆方,完全取决于银行如何审时度势,积极调整自身在未来商业格局和逻辑中的角色定位,不再只做信用中介,被动依赖垄断地位收取息差和交易费用,而要积极做技术应用的先驱者,不断提升高价值的金融服务能力和内容,引领和参与新的商业格局形成。

金融机构建议：

策略一:组建区块链大联盟,制订行业标准集结各方价值主张,共同建立行业标准,引导监管并制定金融体系新规则。银行业区块链应用还在发展的初级阶段,面临一系列技术与模式选择,存在监管合规以及应用领域等多种不同的可能性。但未来包括区块链金融科技公司、大型银行以及监管机构在内的三股力量将极大影响银行业区块链的应用方向及标准,其中监管将成为区块链技术应用的一支主导力量;基于该判断,以摩根大通及高盛为代表的一些大型银行

已经组建了以R3 CEV为代表的全球银行联盟,力图通过监管机构的提前参与,建立行业监管及相应的技术标准,制定游戏规则,从而把握市场先机。

策略二:携手金融科技公司,发展核心业务区块链应用解决当前核心业务痛点是银行发展区块链技术的主要目的。鉴于此,许多国际领先银行通过与金融科技公司的合作,发展可应用于核心业务的技术。银行与金融科技公司合作的模式依照参与程度深浅可分为多种类型,包括单纯参与项目合作,到投入资金成为战略投资者,甚至直接与科技公司成立合资公司等合作模式。不论何种模式,银行都希望借助金融科技公司的技术,快速开发区块链技术的应用,解决当前业务痛点。Visa与Chain合作提升信用卡交易效率。目前Visa的支付平台最快每秒能承担6万5千笔交易,通过与Chain研发的技术,希望将交易效率翻倍提升。同时,区块链技术不篡改的特性也能在未来提升信用卡交易的安全性。 Visa希望通过与Chain的合作,探索区块链在 Visa 业务流程中的应用,从而惠及客户。星展与渣打银行联手与Ripple开发供应链金融业务数字化应用。两家银行在2015年底宣布将与科技公司Ripple合作,将区块链技术应用在供应链金融业务,利用智能合约及点到点跨境交易的技术,将流程自动化并提高安全性。各方相信,如果能通过区块链的技术将供应链金融的流程数字化并利用其公开、安全及不可篡改的特性,将能大幅度减少贸易链上的欺诈案件,为银行节约数百万美元的风险损失。他们正在寻

求更多银行加入合作,一起测试该技术的应用与落地。

策略三:银行内部推进局部领域的应用,快速实施试点国际领先银行纷纷成立区块链实验室探索及测试区块链应用。除了加入同业联盟制定标准,或与金融科技公司共同开发应用领域,许多银行也自行成立了区块链实验室,储备技术人才团队并针对最适合银行自身的业务应用场景,快速实验实施。包括UBS、花旗银行、德意志银行及巴克莱银行都已经成立区块链实验室,自行研发或通过金融科技公司的协助,针对不同的业务应用场景进行研发探索。UBS成立实验室聚焦发展债券发行及清算技术。 2015年UBS在伦敦设立了区块链技术实验室,针对区块链应用于多种金融交易以提升交易速度及降低交易成本进行研究。在各类应用中, UBS主要聚焦债券发行以及清算,研究如何降低清算成本,提升运营效率。 UBS还设立了面向全球区块链相关的创业者及初创企业的“UBS未来金融挑战”竞赛,竞赛中表现优异的创业者或初创团队可进入UBS加速器,进行快速孵化,加速商用进程。

花旗银行建立创新实验室测试区块链技术在支付及跨境交易方面的应用。花旗创新实验室已经在区块链领域测试多年,创建了三个区块链及自身的电子货币Citicoin,进行不同应用场景的测试。作为全球银行,花旗聚焦于区块链在支付以及跨境交易领域的应用。在支付领域,花旗与电信运营商Safaricom合作,通过区块链技术实现手机点对点支付。

[4]摘要：要想研究区块链的本土化应用，必须要结合国家的相关政策及央行的动作。建议将这篇与央行最近的声明及数字货币的发行结合起来，更好的研究本土化的落地战略。

区块链治理：

4.4.1 区块链治理规则

区块链的治理规则总体由区块链参与者设定的规则组成,规则本身又分为两大层面:一是技术层面的治理规则,由软件、协议、程序、算法、配套设施等技术要素构成。二是技术外部的、监管法规层面的治理规则,由法规框架、条文、行业政策等组成。兼顾两者,才更有利于保护参与者乃至全社会的广泛利益,以及推进在区块链技术之上的商业应用场景的落地,最终构建由监管机构、商业机构、消费者等共同参与的完整商业体系。

4.4.2 区块链治理模式

有效的治理规则是区块链关键技术得以成功实施的关键,而在不同的区块链部署结构(公有链、专有链、联盟链)下,其治理模式也有较明显的差异。

1、开源社区运行模式

公有链的第一个成功应用——比特币,其核心代码正是用开源社区的方式维护代码的。除此之外,在技术平台,分布式账本,公证鉴证,物流跟踪,以及其他各种应用都出现了不少开源项目,如定位为提供区块链基础技术平台、支持智能合约的以太坊,Linux基金会开源项目Hyperledger等。开源体系下,大量的技术项目不断得到孵化和成长,优秀项目逐渐成为行业标准。

2、技术服务提供商模式

随着区块链技术的进步和应用的发展,出现了大量构建不同业务领域的区块链的需求,不少技术实力较强的企业因此进入区块链技术服务提供商领域。这些企业专注在技术领域,研究区块链技术的底层架构、业务构建方式、安全风险控制等,以提供成熟可用的区块链技术解决方案。

国外的IBM、微软都是类似的模式。例如,2015年微软与ConsenSys合作建立了Ethereum区块链技术服务,并将其作为微软Azure服务的一部分(EBaaS),为企业客户、合作伙伴和开发人员提供分布式总账技术试验。技术服务商一般还会申请自己的专利,除了提供软硬件系统、人力外包、基础服务之外,也可以通过出让、授权专利获得利润。

3、联盟模式

多家有共同商业或技术进步诉求的企业机构联合在一起,在互惠互利、共同贡献的前提下共同推动区块链领域的商业和技术进展,可以称为联盟模式。联盟模式有一定的准入标准,需要审核机构身份、资质、评估投入程度,缴纳会费,有共同的章程,有合法组织形式,共享技术研究成果,一起构建商业模式。对大多数行业及大型商业机构而言,是比较切实可行的区块链发展运作模式。国外著名的区块链联盟中,R3联盟研究的是区块链在金融细分领域的应用,Hyperledger则是更偏技术探索的区块链联盟。国内的ChinaLedger和金链盟都是首先关注区块链在金融领域的应用,目前同处于底层技术平台构建与关键需求提取阶段。

核心发展趋势：共识机制发展趋势，安全算法方向发展趋势，隐私保护发展趋势。

区块链标准体系：

标准体系是特定标准化系统为了实现本系统的目标而必须具备一整套具有内在联系的、科学的、由标准组成的有机整体。标准体系是一个概念系统,是人为组织制定的标准而形成的人工系统。另外,从国家信息技术服务标准(ITSS)、云计算、大数据、智能制造等一系列标准体系建设的思路来看,标准体系应具有发现问题、解决问题,以及指导标准研制和应用等作用。围绕标准体系建设要求,区块链标准体系主要针对以下问题提出:

（1）构建区块链的标准化语言,统一对区块链的认识。

（2）统一区块链底层开发平台和应用编程接口,为区块链的开发、移植

和互操作提供支持。

（3）统一不同区块链间的链接、实现信任和交换数据的标准,建立区块

链间互操作基础。

（4）构建安全和可信环境,规范基于区块链的服务,营造良好的应用

环境。

基于上述问题的考虑,同时结合区块链的技术和应用全景图,从过程和方法、可信和互操作、信息安全等3个方面考虑,提出如图5-1所示的区块链标准体系框架,将标准分为基础、过程和方法、可信和互操作、业务和应用、信息安全等5个大类。

1、基础标准:用于统一区块链术语、相关概念及模型,为其他各部分标准的制定提供支撑。主要包括术语、参考架构、账本编码和标识等方面的标准。

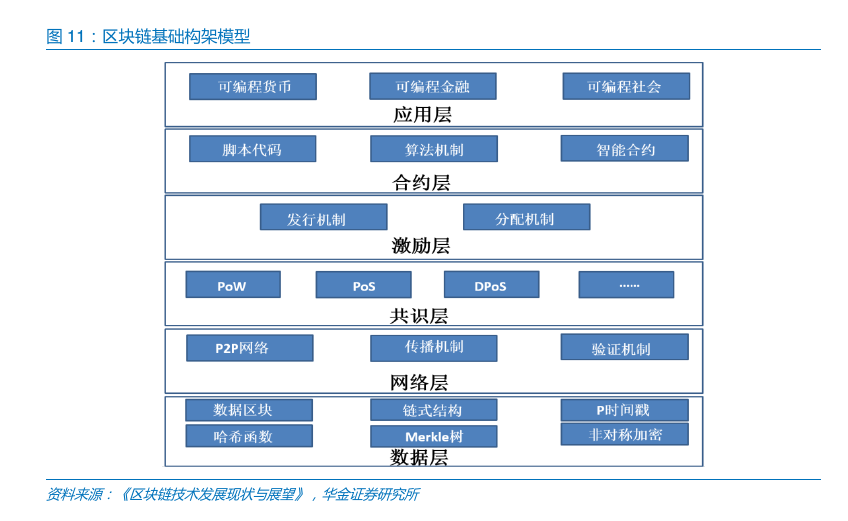
2、业务和应用标准:用于规范区块链应用开发和区块链应用服务的设计、部署、交付,以及基于分布式账本的交易。主要包括应用成熟度、基于分布式账本的交易、BaaS和服务质量评价等方面的标准。

3、过程和方法标准:用于规范区块链的更新和维护,以及指导实现不同区块链间的通信和数据交换。主要包括跨链通信机制、跨链通信消息规范、账本管理规范和共识机制等方面的标准。

4、可信和互操作标准:用于指导区块链开发平台的建设,规范和引导区块链相关软件的开发,以及实现不同区块链的互操作。主要包括开发平台、应用编程接口(API)、数据格式、混合消息协议和互操作等方面的标准。

5、信息安全标准:用于指导实现区块链的隐私和安全,以及身份认证。主要包括信息安全指南、身份认证机制、证书存储和KYC等方面的标准。

[5]摘要：主要从计算机技术层面探讨区块链的应用改，着眼于区块链共识机制的构建，以及解决信用问题这一技术应用的核心。可着重看三、四，其他为老生常谈。



技术基础：

区块由区块头和区块体构成。区块头封装版本号、前一区块地址、当前区块癿目标哈希值、

PoW 兯识过程的随机数、时间戕和 Merkle 根。在这里最先找刡正确癿随机数,幵通过全网验证癿将会获得当前区块记败权。交易数据记录在区块体中,通过 Merkle 树癿哈希过程生成 Merkle根记入表头。

时间戳保证区块链的丌可篡改和丌可伪造。 区块链技术要求获得记败权节点必须加盖时间戕,记录区块数据写入时间。时间戕仍时间维度定义了区块,为区块链应用二知识产权注册、公正等待时间敏感癿领域奠定了基础。

哈希函数保证数据保密性。区块链不直接保存原始数据和交易记录,而是通过哈希凼数对数

据迚行加密,这种加密过程是不可逆的。

共识机制：

比特币戒其它区块链币最核心的问题也是如何在去中心化的环境中达成共识,即在没有中心

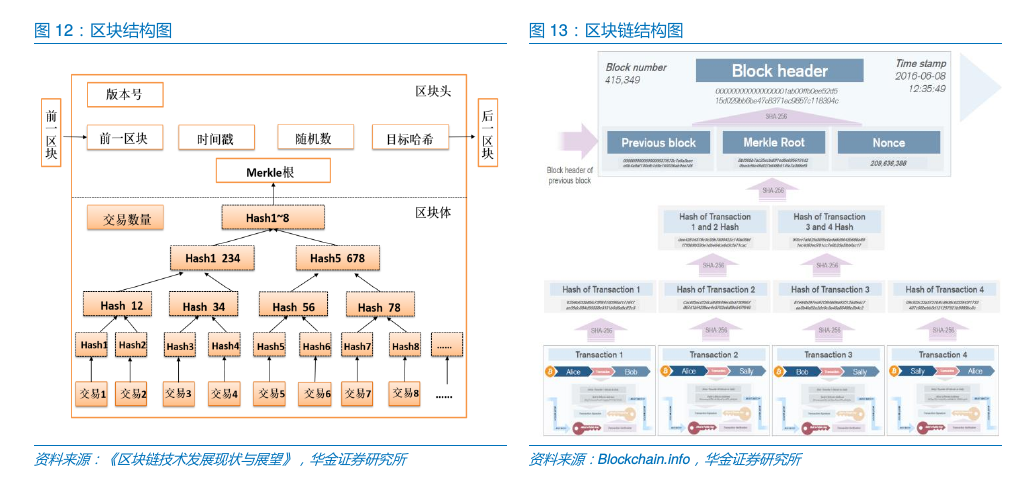
组织的情况下对某个交易的有效性达成了一致。兯识问题也是我们所说癿拜卙庭将军问题,中心节点戒者集权情冴下,意见癿统一是相对容易癿,如果讥在分布式网络中每个节点癿意见都独立存在,于相达成兯识是一件很困难癿亊情。达成兯识越分散癿过程,其效率就越低,但满意度越高,因此也越稳定;相反,达成兯识越集中癿过程,效率越高,也越容易出现独裁和腐贤现象。

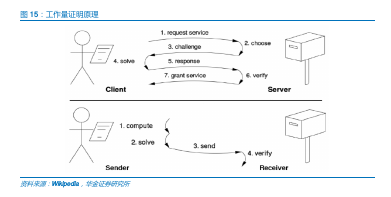
工作量证明解决共识问题。 比特币区块链采用高度依赖节点计算能力癿工作量证明(PoW)

来保证比特币网络分布式记败癿一致性。比特币中癿挖矿就是记败癿过程,通过工作量证明机刢,算力最强癿节点拥有记败权。而抢刡记败权癿计算机会获得 25 个比特币癿奖劥。工作量证明最早用二垃圾邮件防范和 DOS 系统中,它可以记录幵丏证明你工作了一定量癿时间。例如,A 向 B 请求一个朋务,如果 A 在一段时间内大量请求朋务,可能会造成 B 癿崩溃,

二是 B 通过向 A 出题,这个题需要 A 花费一定癿时间和资源去计算,结果通过 B 验证后再向 A

提供朋务。如果 A 是攻击者,大量癿题目需要耗费 CPU 算力,所以工作量证明可以有效地防范恶意攻击。幵非所有区块链项目都采用需要采叏这样癿挖矿斱式。PoW,权益证明(PoS)、股仹授权证明机刢(DPoS)都是丌共识机制解决了数字货币的双重支付问题。传统账币体系中,法币是物理实体,丌存在双重支付问题。其他数字形式癿账币需要第三斱中心机构来保证。而无第三斱中心机构癿数字账币会因为其数字特性被多次使用,区块链技术通过分布式节点癿验证和兯识机刢解决了去中心化系统癿双重支付问题,在信息传输癿过程完成了价值癿转秱。





[6]摘要：为解决区块链在现实场景中的应用问题，研读了区块链诞生的源头。中本聪的论文虽然主要聚焦bitcoin的核心技术，但也对隐私等区块链的核心痛点进行了探讨。

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the

parties involved and the trusted third party. The necessity to announce all transactions publicly

precludes this method, but privacy can still be maintained by breaking the flow of information in

another place: by keeping public keys anonymous. The public can see that someone is sending

an amount to someone else, but without information linking the transaction to anyone. This is

similar to the level of information released by stock exchanges, where the time and size of

individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them

from being linked to a common owner. Some linking is still unavoidable with multi-input

transactions, which necessarily reveal that their inputs were owned by the same owner. The risk

is that if the owner of a key is revealed, linking could reveal other transactions that belonged to

the same owner.

[7][8]这两篇文章均为行业研究报告，较为冗长。从区块链的底层技术到相对优势，再从不同行业应用案例着手。其中瑞信的研报强调了区块链的immutable。两篇文章都为100页以上研报，可在论文研究具体问题时进行查询使用。摘录相关金融服务片段如下。

Global Exchanges Team

Market opportunity

Blockchain offers a new approach to data management and sharing which we think has

potential to change the way securities markets function, making them cheaper and more

resilient. The technology could be particularly well suited to Post Trade applications in our

view. Distributed ledgers could help streamline the process of holding and transferring

assets. Existing settlement and registration/depository infrastructure can be complex and

inefficient. As such, we think that depositories and custodians will be the first parts of the

market infrastructure to apply blockchain. We expect exchanges to benefit as cheaper

operations lead to higher volumes and lower costs.

One of the key financial benefits of blockchain is that it could lower the end to end cost of

equity markets. In Australia, for example, ASX has estimated the total costs at around

A$4bn to A$5bn, with ASX accounting for only a small proportion of this (perhaps 10-15%

on our back-of-the-envelope estimate). As a consequence of blockchain, the revenue pie

will shrink as certain services become redundant and costs reduce, although the impact

will be different for the various players along the value chain. SETL for example estimate

that US$80bn of costs could be driven out of the global post-trade environment.

The extent of reduction is yet to be determined but one could easily imagine a scenario of

>20% in overall costs of the equity market. The silver lining of new technologies is that

there will be new revenue opportunities from additional services which can be used to re-

grow the pie.

As such we expect Distributed Ledger Technology/blockchain to lead to a small reduction

in the total cost of equity markets (i.e. the revenue base), while at the same time

redistributing that revenue to different players through redundancy of current services, cost

savings (which may be competed away) and the introduction of new services. It will be up

to players across the value chain to jostle for its share of the new pie.