



信和研究院
CREDIT HARMONY RESEARCH

2018年区块链应用情况研究

2018/5/17

蜜蜂内参

让您深入洞察整个商业世界



每天精挑细选3份最值得关注的学习资料；
不定期分享顶级外文期刊。

关注公众号：**mifengMBA**

回复“入群”加入“蜜蜂内参”城市群

(不需要转发哦.....)



扫一扫

回复“入群”

目录
Contents

1

区块链发展历程

2

金融领域的应用

3

其他领域的应用

4

总结与展望

1

PART 1

区块链发展历程

- 1.0 加密货币时代 (2009—2013)
- 2.0 智能合约时代 (2014—2017)
- 3.0 大规模应用时代 (2018—)

BLOCKCH

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的链式数据结构， 以密码学的方式保证数据不可篡改

起源

- 区块链起源于中本聪在2008年发表的《比特币：一种点对点的电子现金系统》一文。
- 2009年1月，中本聪开发出创始区块0和区块1，将区块0的信息加入到区块1中，实现了区块的链接，区块链由此诞生。

狭义 区块链

- 区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的链式数据结构，以密码学的方式保证数据不可篡改、不可伪造，具有去中心化的特征。
- 从形式上看，区块是一个一个的存储单元，记录了一定时间内各个区块节点全部的交流信息。各个区块之间通过随机散列（也称哈希算法）实现链接，后一个区块包含前一个区块的哈希值，随着信息交流的扩大，一个区块与一个区块相继链接，形成区块链。

广义 区块链

- 区块链是一种利用加密技术来验证与存储数据，利用分布式共识算法来新增和更新数据，利用运行在区块链上的代码，即智能合约，来保证业务逻辑的自动强制执行的全新的多中心化基础架构与分布式计算范式。

区块链具有防篡改、去信任、去中心化、保护身份隐私性和交易公开性的特征

防篡改

依靠密码学原理和分布式算法，只有控制超过51%的节点，才能篡改数据

去信任机制

交易的确认基于密码学原理（Hash碰撞），而非信任机制

隐私性和公开性

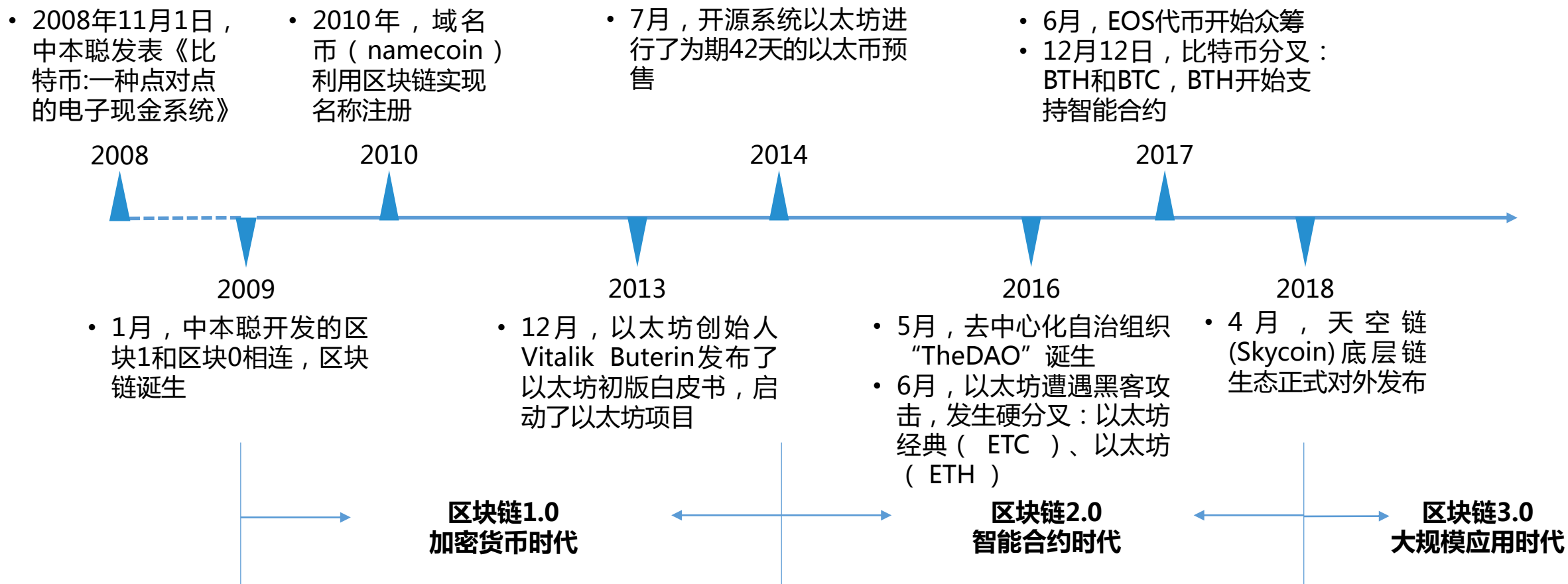
比特币的加密技术（Hash碰撞）使得全部人的账单并不会显示用户名字，而只是一串唯一识别码，保证了隐私性的同时也保证了公开性

自治性与去中心化

采用基于协商一致的规范和协议，使得系统中所有节点能在去信任的环境下自由交换数据。不存在中心化的硬件或管理机构，任意节点的权利和义务均等

注：在比特币中，目前由于算力不均衡导致节点权利不均等，这也使比特币的安全性受到质疑，工作量证明机制受到挑战。但区块链追求的是去中心化，暂时的中心化是技术待改进的体现。

区块链的发展经历了加密货币时代、智能合约时代，将进入大规模应用时代



加密货币时代，区块链技术主要用于发币和支付，被比特币统治



标志事件

- 2008年11月1日，中本聪发表《比特币：一种点对点的电子现金系统一文》，阐述了基于点对点网络技术、加密技术、时间戳技术、区块链技术的电子现金系统的构架理念。
- 2009年1月，中本聪开发出创始区块0和区块1，将区块0的信息加入到区块1中，实现了区块的链接，区块链由此诞生。

比特币基于密码学原理进行支付，而非基于信用，通过点对点分布式的时间戳服务器来生成依照时间前后排列并加以记录的电子交易证明，从而解决双重支付问题，开创了去中心化加密货币的先河，统治了加密货币时代。

- 在比特币协议中，比特币的获得基于工作量证明机制（挖矿），算力决定影响力，出现了挖矿热潮。
- 出现了很多山寨币，山寨币通过修改比特币源代码得到，出现“一链一币”的现象。
- 加密货币交易价格波动幅度极大，没有政府信用背书，且面临着政策不确定性。
- ICO成为区块链领域融资的主要模式，甚至超过VC投资。
- 区块链技术主要用于各种项目的发币筹资，甚至被不法分子用于洗钱。



发展特点

加密货币的主要用途是支付，多数基于比特币协议，少数基于原创共识机制和算法

市值较大的几种加密货币

币种	上市时间	用途	算法	特点
比特币 (Bitcoin, BTC)	2009.01	支付	SHA-256	<ul style="list-style-type: none"> 提出工作量证明 (PoW) 机制 交易确认较慢：每10分钟处理一个区块 预期产出2100万个比特币，随着比特币数量的增加，挖矿难度会增大
瑞波币 (Ripple, XRP)	2011.04	支付	Opencoin原创算法	<ul style="list-style-type: none"> 基于Ripple协议，自有共识机制，可以兼容所有法定货币与虚拟货币 “全节点”开源；总量1000亿，随着瑞波币数量的增加，后期产出数量逐渐减少 为避免恶意攻击，要求每个账户至少有20个瑞波币，每交易一次就销毁1/100000个瑞波币
莱特币 (Litecoin, LTC)	2011.10	支付	Scrypt	<ul style="list-style-type: none"> 基于比特币协议，使用工作量证明机制 交易确认较快：每2.5分钟处理一个区块 预期产出8400万个莱特币，每一个莱特币被分成1亿个更小的单位
点点币 (PPcoin, PPC)	2012.08	支付	SHA-256	<ul style="list-style-type: none"> 基于比特币协议，是第一个混合工作量证明机制和权益证明 (PoS) 机制的加密货币 创建了PoS利息体系，防止通货紧缩 总量无上限，通胀率1%/年
质数币 (Primecoin, XPM)	2013.07	解决数学问题，寻找质数	XPM原创算法，搜寻新质数	<ul style="list-style-type: none"> 基于比特币协议，每分钟产生1个区块，每个区块包含若干个XPM的奖励(奖励数量取决于破解质数的难度) 尚未有人研发出XPM的显卡挖矿程序，只能通过CPU挖掘 没有总量上限，但由于大质数的计算难度高，产生速度极慢
门罗币 (Monero, XMR)	2014.04	电子现金	RingCT (环形加密)	<ul style="list-style-type: none"> 基于CryptoNote协议 开源加密货币，更加注重隐私保护、去中心化、可扩展 公平发布，且不限每日交易数量

数据来源：根据公开资料整理

基于比特币协议的加密货币最大的优势是建立起基于密码学原理的去信任机制，最大的弊端是PoW机制易受算力的51% 攻击

优势

- 去中心化，每个区块记录全部节点信息，建立了PoW共识机制，防止运营者控制整个网络。
- 公钥匿名，对身份信息加密，每次交易生成一个新的地址，保证了身份隐私性。
- 每个区块节点可以查看全网账本，保证了交易数据透明性和公开性。
- 大部分的加密货币总量一定，可抵制通货膨胀风险。

- 算力可能进行51%攻击：比特币协议中工作量证明机制有可能会被集中矿力突破，控制超过51%的节点。
- 不具备图灵完备性，不能实现所有种类的计算。
- 协议缺乏扩展性：如，比特币网络里仅有比特币符号，用户无法自定义另外的符号，损失了一些功能。
- 交易速度慢：每秒约处理6笔交易。区块链需要承载上一个区块的全部信息，区块写入信息量会无限增大。
- 价值盲、状态种类欠缺、区块链盲：不能为账户取款额度提供精细的控制，限制了交易类型的发展。

不足

智能合约时代，基于以太坊协议的区块链开始可编程，出现了大量DAOs和Dapps

标志事件

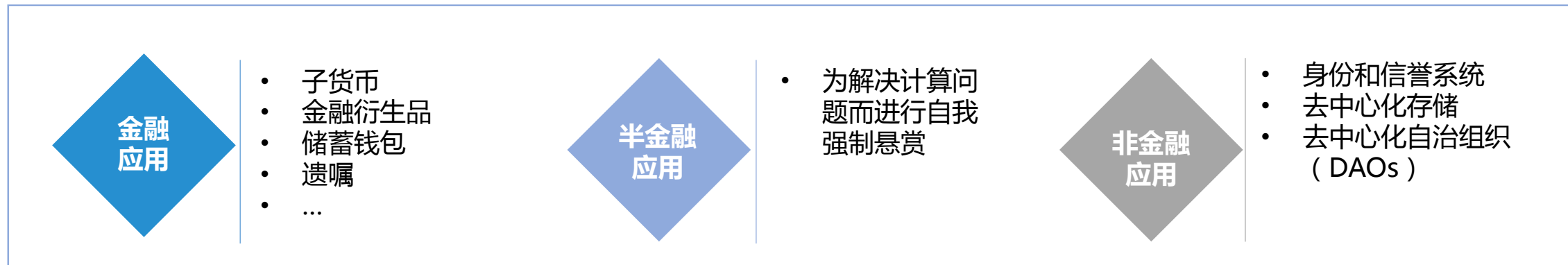
- 2013年年末，以太坊创始人Vitalik Buterin发布了以太坊初版白皮书，启动了项目。2014年7月24日起，以太坊进行了为期42天的以太币预售。2015年7月30日，以太坊系统正式上线。
- 2016年初，以太坊的技术得到市场认可，价格开始暴涨，吸引了大量开发者以外的人进入以太坊的世界，以太币（ETH）成为这一阶段的典型货币。
- 2016年6月，以太坊遭遇黑客攻击，发生硬分叉：以太坊经典（ETC）、以太坊（ETH）。

以太坊是一个开源的区块链底层系统，基于权益证明机制，交易速度提高，每秒可处理约30笔交易，并且支持智能合约。众多ICO的项目纷纷通过以太坊实现，目前已经有超过200多个应用在以太坊系统上开发。

- 出现了大量建立在以太坊协议上的去中心化自治组织（DAOs）和去中心化应用（Dapps），促进了区块链技术在发币以外的应用。
- DAOs的安全问题暴露出来，DAOs之间互相学习，避免技术漏洞的出现。
- 出现了许多行业区块链联盟，如企业以太坊联盟（EEA）、IBM发起的Hyperledger、R3等。

发展特点

智能合约的三大应用：金融应用、半金融应用、非金融应用



ETH智能合约金融应用举例

- 代币权益分红项目。典型的代币权益分红项目是去中心化的预测市场平台Augur，Augur的代币REP是具有分红权的，权益写在智能合约里面不用担心没有分红权益。用户可以用数字货币进行预测和下注，依靠群众的智慧来预判事件的发展结果，有效地消除对手方风险和服务器中心化风险，同时采用加密货币（如比特币）创建一个全球性的市场。
- 代币（Currency）项目。此类项目内置消费场景，进行代币使用消耗。此类项目典型的有Coindash（大师跟投）、Omise.go（去中心交易市场，法币兑换）、perss.one，这些项目的代币和货币都是同一种代币。

统治智能合约时代的以太坊协议的最大优势是公有链开源，支持智能合约；最大劣势是PoS机制易被利益占有者控制

优势

- PoS共识机制解决了PoW共识机制中的资源浪费问题。
- 基于以太坊协议的区块链可编程，可以在此基础上开发各种应用，极大拓宽了区块链技术的应用范围。
- 智能合约具有透明可信、自动执行、强制履约的优点。去中心化的组织和代理合约不需要关心合约的每一参与方是什么类型的账户。
- 用户的各类资产都写在智能合约里面，不用担心资产的映射问题。

- 基于权益证明机制的网络可能会被利益占优者控制。网络变得中心化，从而给网络的安全性带来威胁。
- ETH的应用数量的增长速度远远超过了区块链扩容的速度，出现拥堵，使得每笔交易的手续费持续提高。
- 在ETH基础上很难开发复杂的大规模应用产品。智能合约大部分都不在区块链上，而是在身份识别层和交流与数据复制上，未充分发挥区块链的优势。
- 所有数据都和单一一个公钥联系在一起，在公布账户公钥后，任何密码漏洞都可能造成问题。

不足

大规模应用时代关键是去中心化、安全性与效率的平衡与提高；EOS、Skycoin等新的底层协议出现



标志事件

- 2017年6月，商用分布式操作系统EOS (Enterprise Operation System) 代币开始发行。发行期1年，首次公开发行2亿枚。
- 2018年4月，天空链(Skycoin)底层链生态正式对外发布，创新并完善了不同于PoW和PoS的新共识机制Obelisk，共识引入“动态观点”。建立一个基于信任度为共识基础的网络，由社区共识决定权力的平衡，由节点之间的订阅建立验证和信任，避免51%攻击的危险，交易速度可达3000笔/秒。

区块链应用场景的开发在逐步扩大，在支付、结算等金融领域的应用已经落地。区块链的发展将要进入大规模应用时代，但安全是前提，去中心化和效率之间的平衡优化将成为各底层协议未来发展的关键。

- 比特币、以太坊、EOS、NEO、BTM、Skycoin等多种底层协议共存，底层协议支持的应用开发数量将成为底层协议系统竞争成败的关键。
- 由于各底层协议的性能不同，不同类型的应用需要的底层协议可能不同。如，高频交易的应用对底层协议的效率要求相对较高，而低频交易的应用对底层协议的性能要求则相对较低。
- 区块链在金融、交通与物流、慈善公益、网络社交、共享经济等各种应用场景中落地。

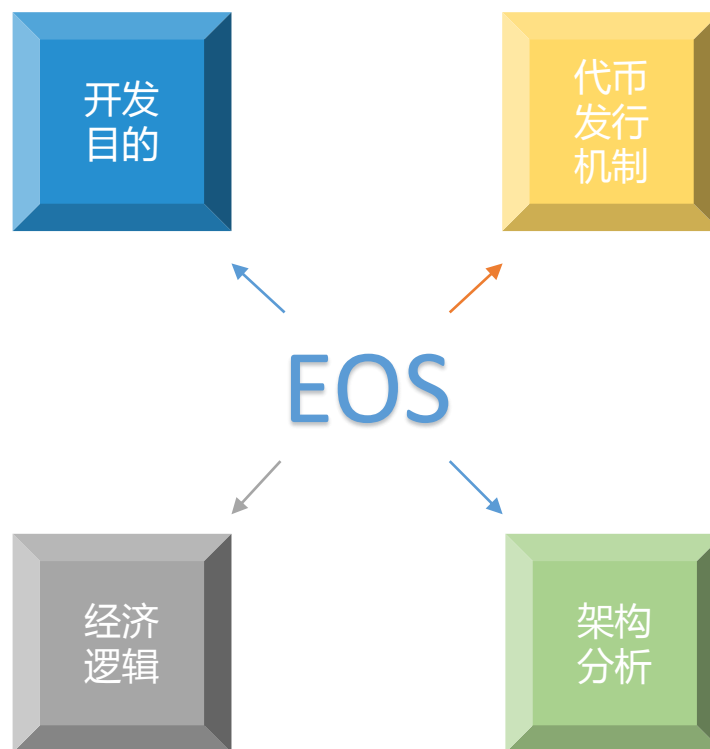


发展特点

EOS采用DPoS机制，挖矿无需比拼算力；石墨烯结构高度模块化，更具可扩展性

- EOS商用分布式区块链操作系统，设计的目的在于解决现有区块链应用性能低，安全性差、开发难度高以及交易手续费高的问题。
- EOS交易无需手续费。任何团队都可以在EOS上以比较快的速度开发出所需要的Dapp，EOS框架内发生的经济活动用EOS代币完成交易。

- 采用DPoS（Delegated Proof of Stake），在某一条区块链的所有节点中票选出21个超级节点，并从21个超级节点中随机选出一个节点产生新的区块。在这种票选机制下，21个超级节点是随机轮换的，并且21个节点中只能有一个节点可获得区块奖励，这种货币增发机制无需比拼算力。

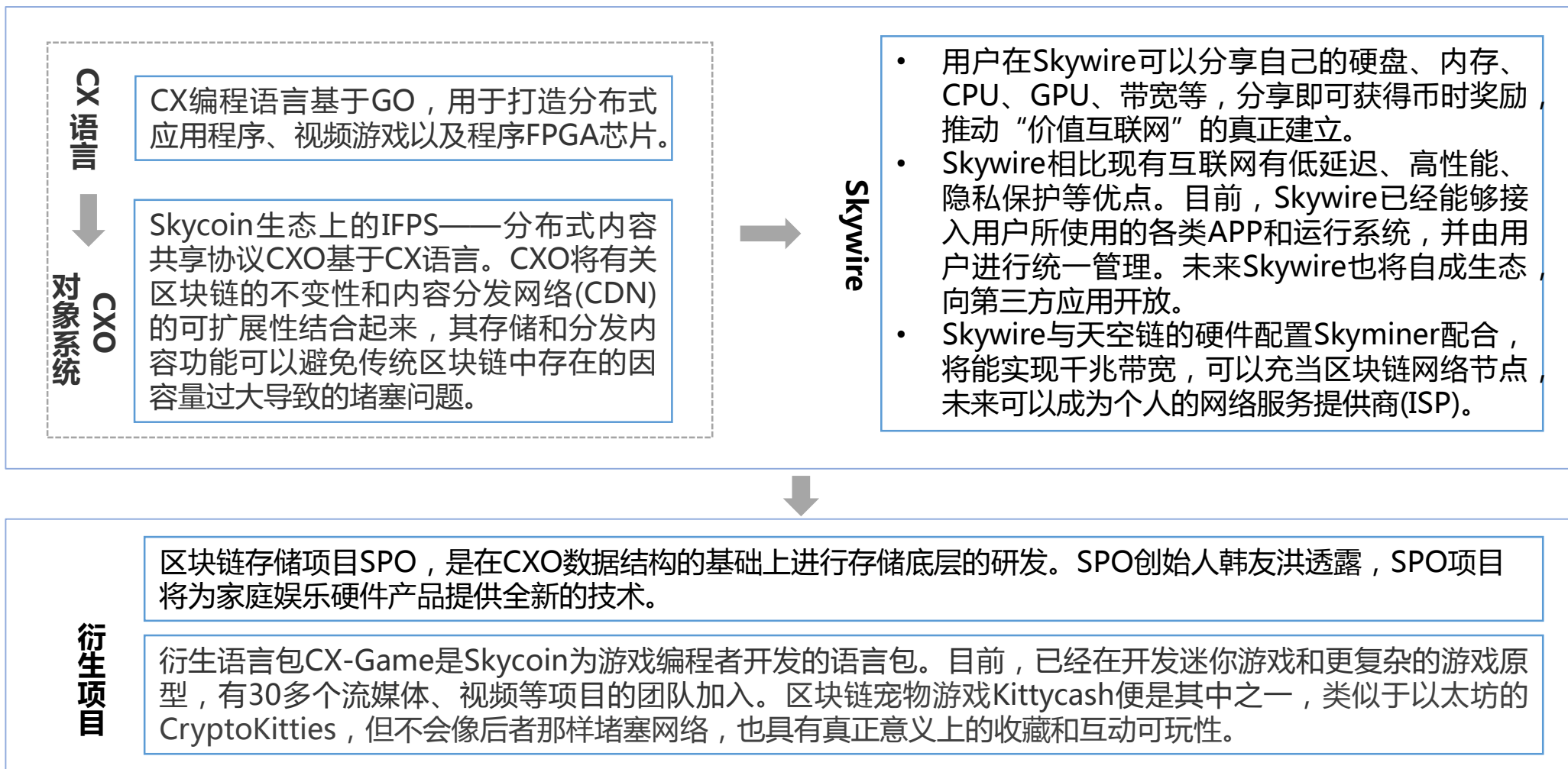


- 首次发行总量10亿枚，其中创始团队拥有1亿枚，9亿枚进行公募。
- 第一阶段（2017年6月~2018年6月）投放2亿枚EOS代币，7亿代币平均分成350份，每份200万，每23小时一份。
- 以后以每年不超过5%的增长率发放代币。

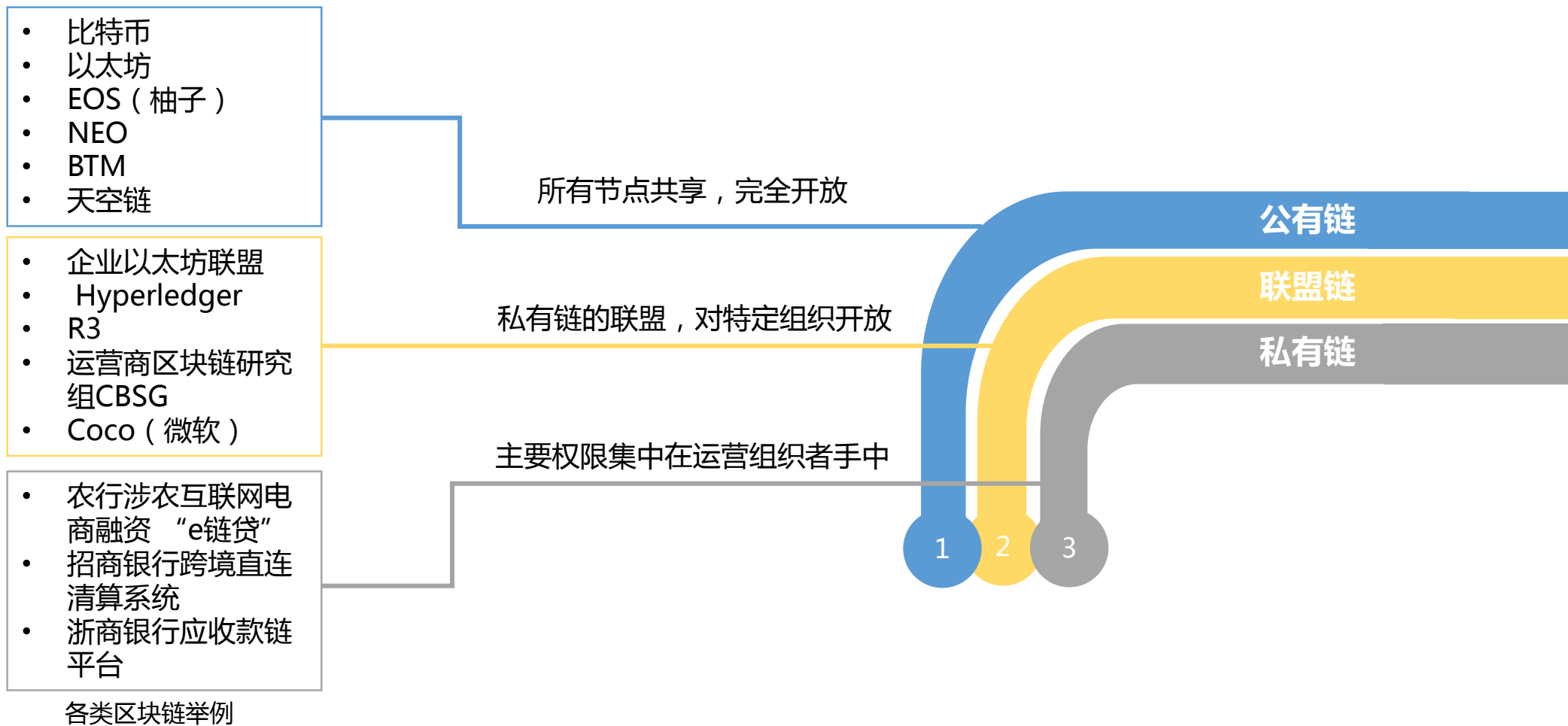
- 采用石墨烯结构，高度模块化，将内部节点间的分布式通信能力封装成插件（plugins），由上层的应用程序（Dapp）动态加载调用，使得应用开发者无需关注区块链底层细节，更具可扩展性。
- 主要包括应用层、插件层、库函数层和智能合约层。

Skycoin生态系统包括自己的编程语言和不可变的对象系统，为Skywire网络的应用逻辑和数据分发提供基础

Skycoin生态系统



区块链可分为公有链、联盟链、私有链三类，公有链作为基础层服务促进技术进步，联盟链、私有链则重在商业应用



安全性、去中心化、效率之间的平衡是公有链竞争的关键

六种公有链对比

链名称	共识机制	匿名性	速度	货币发行机制	特点
比特币链	PoW	公钥匿名，地址非匿名	约10分钟/块 6笔/秒	对矿工的奖励	基于密码学原理的去中心化支付系统
以太坊链	PoS	——	30笔/秒	对矿工的奖励	任何人都能够创建合约和去中心化应用，并设立自由定义的规则
柚子（EOS）	DPoS	委任授权。 多用户授权， 授权匹配	3秒/块 目标百万TPS/秒	对矿工的奖励，每年 增长不超过5%	代币持有者给与矿工代币奖励，代币持有者权限大于矿工；存在超级节点，牺牲了一定的去中心化。若密钥被盗，用户可自主恢复账户
小蚁链 （NEO）	DBFT， 中性记账	地址由一组 公钥组成， 地址匿名	5~15秒/块 可能达1万TPS/秒	购买小蚁股，按持股 比例分配小蚁币	实现事务去中心化、“超导交易”，开发清算型区块链，对接实体金融，支持大规模商业化应用
比原链 （Bytom， BTM）	ASIC友好 型的PoW	——	——	私募、ICO、挖矿、商 业拓展、基金会预留 比原币（总量21亿个）	是一个去中心化的多元资产协议，可以实现（收益权、非上市股权、债权、数字货币等）的登记、流通、对赌和基于合约的更具复杂性的交互操作
天空链 （Skycoin）	Obelisk	地址匿名， 地址就是公 钥哈希	3000笔/秒，通 过调节可实现信 用卡级支付速率	用“币时”奖励用户 贡献的资源	解决PoW、PoS存在的逐渐中心化问题，取得去中心化、安全、效率的平衡

Hyperledger联盟是跨行业的、企业级的基于分布式账本的开放平台



HYPERLEDGER

- Hyperledger发起于2016年，由Linux Foundation领导，是一个中立、开放的跨行业区块链技术合作平台。执行董事Brian Behlendorf将Hyperledger的使命定为商业区块链伞（Business Blockchain Umbrella）。
- 目前，Hyperledger理事会由21个成员构成。Hyperledger已有200多名会员，成员覆盖多个行业的大、小公司，如金融、医疗、科技等。在成立之初，Hyperledger就有30名成员，并引入了两个超级账本科技开拓者Hyperledger Fabric和Hyperledger Sawtooth。

Hyperledger会员

会员类型	会员数量	会员举例
贵宾会员	18	埃森哲、Airbus、思科、百度、DAH、DTCC、英特尔、J.P.Morgan、IBM、SAP、戴姆勒、万达·非凡科技
普通会员	162	小米、BOSCH、招商银行、中信银行、德勤、房掌柜、H3C、Oracle、点融、中超区块链、R3、智链、华为
附属会员	27	英格兰银行、浙江区块链技术应用协会、Sovrin基金、新加坡金融管理局、云安全联盟、区块链研究协会
附属学术机构	10	Blockchain at Berkeley、Cambridge Center for Alternative Finance、北京大学、UCLA Blockchain Lab

注：以上会员信息为截至2018年5月11日的状态。

Hyperledger项目主要分为框架和工具两种类型，颇具前瞻性

类型	项目名称	简介	状态
框架	Sawtooth	建立、部署和运行分布式账本的模块化平台，案例有：海鲜产业供应链溯源、债券资产交易结算、数字资产交易	可用
	Fabric	最初由DAH和IBM建立，智能合约引擎，促进区块链产品和服务开发的模块化框架，为成员提供即插即用的服务	可用
	Iroha	是一种区块链平台实现方式，重在移动应用开发，建立基于链的拜占庭容错算法（Sumeragii）	可用
	Indy	去中心化识别的分布式账本，为创建和使用独立数字识别提供工具、字典和可再用的元素	孵化中
	Burrow	许可式智能合约应用引擎，为模块化区块链客户提供许可式智能合约解释程序，部分是按以太坊虚拟机标准建立的	孵化中
工具	Caliper	区块链基准工具，提供预定义的案例，供用户测试某一具体区块链的执行表现情况	孵化中
	Cello	区块链模块工具集，提供虚拟机、集成平台上的区块链多功能租赁服务	孵化中
	Composer	建立区块链商业网络的工具集合和稳健的区块链解决方案，是用JavaScript语言编写的程序	孵化中
	Explorer	创建用户友好型网络应用，可以对区块、交易、关联数据等存储在账本中的信息进行视图、调用、部署和查询操作	孵化中
	Quilt	通过跨账本协议（ILP）实现跨账本系统的可互操作性，ILP为每个账本中的账户提供单一账户名称空间，在账本间可进行原子互换（atomic swap）	孵化中

注：Hyperledger部分项目由Linux基金会领导，部分项目由成员组织开发，以上项目信息为截至2018年5月11日的状态。

R3联盟的服务对象从银行业拓展至多行业，Corda是其重要的企业级开源产品



- R3是一家总部位于纽约的区块链创业公司，致力于通过智能合约实现直接交易，以降低商业交易中因摩擦产生的成本，同时保障隐私和安全。
- R3始于2015年9月由9家银行发起的联盟，到2015年底，共有42家银行加入。2016年开始向非银行金融机构开放，至今已发展成为覆盖六大洲的200多家企业的联盟，企业类型包括银行、保险、科技、软件、监管机构等。

2016年，R3推出自主研发的开源区块链分布式私人账本Corda，并纳入Hyperledger企业级项目库，试图通过Corda建立行业标准，呼吁更多的企业使用该平台研发产品。Corda运行在Java虚拟机上，开发者可以在Corda上开发CorDapps。

Corda



企业级

作为开源软件或企业平台，Corda利用传统区块链科技元素，对其进行微调以供企业使用



共识

Corda的目的是使参与者在共享事实和消除费时费力的协调成本上达成共识



隐私

Corda通过仅共享与参与者有关的交易信息，将信息泄露最小化



互操作性

Corda是支持金融和商业应用可互操作性网络的门户。Corda将其称为CorDapps

由于关键联盟成员的离开，R3正在从会员联盟和实验室向技术供应商过渡

R3联盟重新定位导火索

- R3在为自己的平台Corda申请专利时，摩根士丹利和高盛没有支持，反而自己申请区块链专利。
- 2016年11月，R3联盟的创始成员高盛和西班牙桑坦德银行退出R3联盟，不再以R3联盟成员的身份继续探索区块链技术。

成员权益

- Corda培训：针对开发者的两天集中培训（在线或面授）
- 参与产品开发的每个阶段
- 与其他会员接触交流的权利
- 获得接触R3联盟的研究成果和知识的权利



R3联盟重新定位：区块链技术供应商

- 在见证多个关键成员离开后，R3表示将重新进行定位，以ETH为基础开拓具体用例，最终成为一个技术供应商。
- R3目前正在与外部机构合作开拓区块链用例，包括计划发行自己的基于DLT的数字货币的央行、需要在加密环境中传递数据的受信任的市场数据供应商等。

应用案例

- 为瑞士信贷、荷兰安智银行开发证券信贷方案平台，2017年完成概念测试，2018年3月初，在开发的区块链平台上完成了一笔3000万美元的证券交易。
- 2018年3月，德意志交易所宣布，计划研发更高效的证券结算系统，由财务管理公司HQLAX和R3的Corda平台提供技术支持。

2

PART 2

金融领域的应用

加密货币

跨境支付/结算

证券/私募交易

票据与供应链金融

BLOCKCH

区块链中的分布式账本技术，有助于去中心化、削弱中间商的控制权，提升金融交易效率，并降低成本

金融领域面临的问题与区块链技术可提供的对策

问题	对策
受经济周期影响和政府信用限制，货币超发，产生资产泡沫循环；各国货币与美元挂钩，受美元牵制	创造超主权货币，不受政府信用限制，在去中心化、去信任机制的技术应用场景中可进行支付
各国货币不统一，跨境支付需多个中间商进行确认，流程长，汇兑效率低，交易会产生巨额汇兑损失	区块链去中心化的机制，交易双方可以直接确认交易；统一使用一种加密货币，不产生汇兑损失
证券发行与交易中，中间商费用高，证券交易确认、清算流程长，效率低	区块链中，资产交易记录的确认基于密码学原理，具有不可篡改性，可以节省第三方确认等环节
私募股权交易信息不对称，投资人利益可能面临被侵蚀风险	分布式账本中每个节点掌握全部的交易信息，解决信息不对称问题
供应链上下游厂商市场信息不对称，信任机制难以建立，资产证券化程度低，资产周转效率较低；票据市场人为操作多，成本高，欺诈风险大	使用分布式账本技术，供应链上下游厂商资产、交易记录可供交易双方查询，建立去中心化、去第三方的机制，提高资产周转效率；降低票据交易成本和人为操作风险

私人加密货币受到区域市场认可，证券交易所开始支持加密货币交易；但私人加密货币不能作为法定货币，只能被视为一种虚拟资产

私人加密货币 获得区域 市场认可

- 比特币可用于支付购买商品，如2014年12月，Windows和Xbox商店的商品可以用比特币购买。
- 衍生出比特币借记卡、ATM机，比特币与法定货币交换的平台诞生，如OKCoin支持多国法定货币与比特币和OK Dollar的交易。
- 2017年12月10日，芝加哥期权交易所正式启动比特币期货交易。
- 2018年1月17日，纳斯达克交易所上线区块链指数基金Reality Shares Advisors，纽交所旗下电子交易所上线区块链指数基金Amplify Trust ETF。

- 前中国人民银行副行长吴晓灵女士曾指出，私人加密货币可以算是一种虚拟投资资产，但不能当作支付手段。
- 加拿大银行的高级副行长夏洛琳·威尔金斯（Carolyn Wilkins）正在主持对数字货币的研究，认为数字货币并不是真正的货币形式，但“它的确是一种资产，或者是一种安全保证，所以应该同等对待”。

专家观点：私人加密货币是一种虚拟资产

部分国家允许私人加密货币交易，部分国家完全禁止私人加密货币交易

不同区域市场对私人加密货币态度和做法的对比

- 美国：美国加州率先将比特币合法化。
- 英国：央行行长马克·卡尔尼（Mark Carney）将数字货币视为金融领域的潜在“革命”。
- 德国：政府表示，应把比特币当作私人货币和货币单位，纳入监管，个人使用比特币一年内免税，进行商业用途要征税。
- 韩国：正在考虑限制加密货币交易，只在合格的交易所进行交易，并对加密货币的交易征收资本利得税。

- 泰国：全面封杀比特币。2013 年 7 月，泰国外汇管理和政策部表示，由于缺乏适用的法律和资本管制措施，买卖比特币、用比特币买卖任何商品或服务、与泰国境外的任何人存在比特币的往来等活动在泰国都被视为非法。
- 中国：央行打击私人数字货币发行商，禁止比特币和其他数字货币的交易。
- 法国：官员表示“建议对比特币采取谨慎态度，因为公共机构尚未对其树立信心。历史上，所有私人货币的下场都很糟糕。比特币甚至拥有黑暗的一面——数据攻击。”

多国央行重视区块链在金融系统中的应用，并着手研究法定数字货币

- 基于区块链技术的加密货币具有减少发行、流通的成本，交易透明化，可以避免偷税漏税，便于管理和提高央行的控制力等特点，被各国央行重视，但对新技术的认识和应用的探索需要时间。

不同国家对数字货币的态度及研究情况

国家	态度及研究情况
美国	2014年底，美联储发布改善支付系统的白皮书，提出要研究一种加密货币，但这种加密货币依赖的是中央总账系统和当局机关
英国	央行在2016年1月发布的《分布式账本技术：超越区块链》报告中提到，正在探索类似区块链的分布式账本技术，分析区块链在传统金融业中应用的潜力。英国央行委托伦敦大学设计数字货币RSCoin，已完成数字货币测试。但英国央行行长马克·卡尔尼表示数字货币还有很长的一段路要走
德国	2016年3月1日，德国联邦金融监管局公开《分布式账本：以虚拟货币背后的技术区块链为例》报告，对分布式账本在跨境支付、银行转账和交易数据存储等领域的潜在应用进行了探讨
瑞典	央行现金的使用量已经下降，正在研究发行法定数字货币——电子克朗，用于小额支付
厄瓜多尔	禁止比特币，但在2015年推出法定数字货币美元
中国	经历了否定、质疑到肯定的过程。2014年，中国人民银行成立数字货币研究小组；2016年1月，中国央行召开数字货币研讨会
土耳其	2017年11月，土耳其中央银行行长表示，如果设计完善，数字货币可能有助于金融稳定；数字货币将为中央银行带来新的风险，包括如何控制货币供应量和保持价格稳定，以及货币政策的传导。但数字货币仍有可能成为无现金经济中的一个重要元素，加快支付速度，使支付体系变得更有效
荷兰	2015年，荷兰中央银行建立了自己的数字货币，名为DNBcoin，但仅用于内部循环使用，以便更好地了解它的运作方式。2017年，主持该项目的罗恩·伦德森（Ron Berndsen）展示了区块链实验成果，并表示，在复杂金融交易的结算中运用区块链是“很自然的”
日本	央行行长黑田东彦在2017年10月的一次讲话中表示，日本央行近期不打算发行数字货币，“向公众发行CBDC（中央银行的数字货币）如同允许任何人访问央行账户，关于CBDC的讨论牵涉到中央银行的根本性问题”
印度	印度央行对数字货币持否定态度，认为它可能成为洗钱和恐怖融资的渠道。不过，印度储备银行设立了一个小组，正在研究全球央行是否支持数字货币，是否可将其用作法定货币。目前，在印度使用数字货币是违反外汇规定的

通过区块链实现法定货币的跨境支付/清算，解决跨境支付成本高、效率低的问题

传统跨境支付/结算中存在的主要问题

流程长

收付款行需重复执行KYC/AML程序，在执行KYC/AML程序时，常有误报风险，需要人工验证。代理行和SWIFT模式耗时长，复杂的清算传统导致了信息流和资金流的脱节。交易后，定期向监管机构报送数据，需要多个部门的配合。

成本高

据世界银行数据，2015 年全世界的小额跨境汇款总额是 5540 亿美元，跨境支付每年增长的速度约在 5% 左右。目前，跨境汇款的成本高昂，每个汇款人所承担的平均手续费率达 7.68%。

效率低

多方参与、误报风险等导致流程长，效率自然降低，资金利用率也降低。跨境汇款一般需要2~3个工作日到账，影响交易的进行，同时造成大量在途资金闲置。

区块链技术可以提供的解决方案

避免收付款行重复执行KYC/AML程序，通过智能合约自动执行收款程序；消除代理行中间人的角色，节省时间和成本。区块链上的数据可供央行查询，避免定期报送数据的协调成本和时间成本。

据麦肯锡测算，全球范围内在B2B跨境支付与结算业务中应用区块链技术，可帮助把每笔交易的平均成本从26美元降到15美元，节省的成本中75%为中转服务费，25%为合规、差错调查和汇兑成本。

避免KYC重复执行程序，消除代理行中间商角色，区块链记录客户信息，减少AML误报风险，节省时间和人工成本。

跨境支付案例——OKLink使用区块链技术节省跨境支付的时间和费用



- OKLink是OKCoin在2016年8月发起的基于区块链的小额跨境支付平台，连接转账用户和合作伙伴（拥有货币转让许可证的国际货币转账公司），为其合作伙伴提供API接口，接入OKLink区块链。
- 创始人来自巴克莱银行、VISA、阿里巴巴、腾讯等金融和互联网科技领军企业。



投资人：策源创投、曼图资本、创业工场、旺家投资、隆领投资、极客邦、清华五道口等。



总部设在香港，在北京有办公室，24小时服务。业务范围已经覆盖了亚洲、欧洲、美洲等40多个国家，并且每周都会有新的国际客户加入。

Advantage

费用低于同类机构：跨境支付的平均费率约为7.68%，而OKLink收取的费率在0.1%~1.1%不等，部分区域市场会收取一笔固定服务费用。所有的费用都被转换成比特币或OK Dollar（数字美元和美元1:1兑换），并在汇款过程中扣除。每笔支付费用有最大和最小额度限制，汇款时间从10分钟到2天不等。



佣金赚取规则：注册为开发者，制定标价（markup），接入OKLink API或者登陆，根据交易规模按月结算佣金。

区块链可实现证券资产的实时转移，提高交易效率；去中心化账本可增强私募交易的透明性，最大限度地减少中间人角色

在现有证券交易系统中，交易效率低

- 客户、证券公司（经纪人）、托管方、交易所、清算所、监管方（证监会）多方参与，交易流程长。
- 全球证券结算系统碎片化，运作成本偏高，仍有很多确认工作需要人工参与。
- 根据普华永道的数据，每年全球的OTC市场（场外市场）因为清算失败给卖方带来的直接损失高达数百亿美元，尤其是在交易后的清算对账环节，每天会发生大量异常。

区块链可以帮助减少人工参与，提高效率

- 运用区块链技术可以减少证券交易中交易者身份信息的确认、托管方的审核等环节中的部分工作，节省交易成本，提高交易效率。
- BIS在2018年3月发布的报告中指出，支持加密货币的区块链或分布式账本技术（DLT）可以提高证券和外汇交易的效率。
- 高盛分析师在2016年发布的《区块链：从理论到实践》研究报告中预测，区块链应用于美股现金股票市场，根据2015年美股交易数据，可节约14亿美元的费用。

交易所在证券交易中采用区块链的尝试

澳大利亚证券交易所（ASX）在2017年2月17日表示，计划加大在分布式账本（DLT）领域的投资力度，力求成为世界上首家采用DLT提供交易后服务的交易所。ASX曾参与了数字资产控股（DAH）的A轮融资，并考虑评估能否用DLT取代现有的CHESS平台，其考虑开发的新系统的技术支持就是由DAH提供。在新系统中，允许所有参与者在同一个数据库中进行实时资产交易，数字资产在交易对手双方间直接进行转移，达到实时交易的效果，把结算时间从2个工作日缩减到几分钟。

Digital Asset Holdings为金融机构的结算与清算提供分布式账本解决方案



Digital Asset Holdings (DAH) 创立于2014年，为金融机构的结算与清算提供分布式账本解决方案，其开发的平台具有保密、可审计、支持分析、可扩展、无需对账、通用工作流等特点。



创始人兼首席执行官Blythe Masters曾是摩根大通大宗商品全球主管。
首席业务发展官 Chris Church之前曾担任SWIFT证券部负责人兼美洲地区首席执行官。
非执行董事 Cristobal Conde为前SunGard总裁兼首席执行官。
其他高管来自大型金融机构、科技巨头和创业公司等。

团队



权益类应用：支持交易所、中央交易对手、中央证券信托及其市场参与者的点对点清算和结算。
固定收益类应用：从发行、拍卖、结算到柜台交易和资产管理，为市场参与者提供隐私保密和监管透明度。
回购协议类应用：为实时回购利率结算提供基础设施，降低操作成本和风险。

产品



融资情况：A轮获得6000万美元融资；2017年10月，获得4000万美元的B轮融资。
投资方：主要为大型银行、交易所、金融解决方案供应商等，包括荷兰银行、法国巴黎银行、花旗银行、澳洲证券交易所、芝加哥交易所、德意志交易所集团、DTCC、PNC金融服务集团、桑坦德风投、ICAP、Broadridge、埃森哲等。

融资情况

Chain通过区块链平台进行数字化证券产品管理，并且开源



Chain创建于2014年，位于旧金山，主要提供加密账本服务，以促进金融产品和服务领域的突破。
2015年10月，与Nasdaq一起推出私募股权交易平台Linq，是首个通过区块链平台进行数字化证券产品管理的平台。
2016年10月，Chain转向开源，推出Chain Core开发者版本。



首席执行官Adam Ludwin是一位风险资本家，投资了大量的金融科技公司。如Venmo、Braintree和OnDeck。
Chain团队前身是Albumatic，一个照片共享的应用程序。
2017年4月，前高盛总经理Tom Jessop出任新总裁。

团队



Chain旗下账本即服务产品Sequence为机构客户提供余额管理服务，将基于代币的数据模型建立在云上，可以安全记录任何形式的资产。
客户：包括移动钱包、加密资产交易、借贷平台、共享经济应用、支付、筹资、资产管理等企业客户。
费用：月交易额在100万美元以下，免费；超过100万美元收费。

产品和客户



目前，Chain已获得超过4000万美金的融资。
投资方：包括Khosla Ventures, RRE Ventures。
战略合作伙伴：Capital One、花旗、Fiserv、纳斯达克交易所、Orange和VISA。

融资与战略合作

区块链可直接实现点对点的价值传递，降低票据操作风险和成本，提高资产周转率

区块链应用于供应链金融的方式

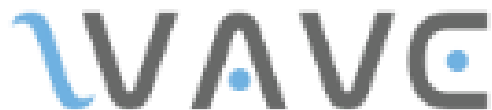
- 所有参与方都使用去中心化的账本分享文件，并按照智能合约的约定自动交易，减少人工操作可能造成的失误和风险，提高效率。
- 运用区块链技术去中心化、公开透明和不可篡改、支持智能合约的特性，解决企业应收账款的真实性确认、流转速度低等问题。

区块链应用在供应链金融中，可以节省巨额成本

据麦肯锡测算，全球范围内，区块链能帮助供应链金融业务中各参与方降低成本，其中：

- 银行的运营成本一年能缩减约135亿~150亿美元，风险成本缩减11亿~16亿美元；
- 买卖双方企业可以缩减资金成本11亿~13亿美元、运营成本16亿~21亿美元。

Wave致力于通过区块链记录商业文件，改善贸易运输业务



以色列区块链创业企业，致力于用区块链改善海运贸易，为客户提供提单解决方案，推进无纸化贸易。Wave早期为巴克莱银行加速器项目，已经顺利“毕业”。

合作案例1：与巴克莱银行合作，完成贸易文件转移



- Wave与巴克莱银行达成协议，通过区块链推动贸易与供应链业务的数字化应用，将信用证与提货单、国际贸易流程的文件放到区块链上，通过区块链进行认证。
- 2016年9月7日，Wave的分布式账本系统帮助农业合作社Ornua与食品经销商Seychelles完成真实交易中的贸易文件转移。该笔交易担保了价值约10万美元的奶酪和黄油产品，将需要耗时7~10日的交易处理流程缩短到4个小时以内，节省了文件快递和审计认证的成本，同时降低交易过程中的操作风险。

2017年11月，Wave与西班牙第二大银行西班牙对外银行（BBVA）合作，推出了一个基于区块链的试点项目，以自动化西班牙和拉丁美洲之间进出口业务的文件证明。巴塞罗那的Frime公司从墨西哥的Pinsa Congelados公司购买了25吨冷冻金枪鱼，利用区块链技术，银行、进口商、出口商都可以追踪信用证明文件的进展，使对外贸易交易的发送、验证和授权时间大大降低，从7~10天压缩到2.5小时。

合作案例2：与西班牙对外银行合作，自动化文件证明



中国人民银行、浙商银行开发数字票据交易平台



- 2017年2月，中国人民银行推动的基于区块链数字票据交易平台测试成功，由央行发行的法定数字货币已在该平台试运行。工商银行参与了数字票据交易平台的建设。
- 2018年1月25日，中钞区块链技术研究院团队承接并组织开发的基于区块链技术的数字票据平台在票交所成功进行实验性生产。

- 早在2016年，浙商银行就推出业内首个移动数字汇票平台，在此基础上，2017年下半年，浙商银行开发上线了一款自主设计研发的应收款链平台。
- 浙商银行开发“池化融资平台+应收款链平台”方案。以浙江超威动力能源有限公司为例，在具体操作中，超威向上游供应商签发并承兑应收款，用以采购原材料，同时以超威为核心设立佣金票据池，用入池的商票、电子票据可生成额度向浙商银行申请应收款保兑；上游供应商在收到经浙商银行保兑的应收款后，可将应收款质押入池或转让给浙商银行，提前获得融资。这样，上下游优质企业的商业信用价值被充分挖掘，盘活应收账款，减少资金占压，降低融资成本，营造良好的供应链生态圈。



中国分布式总账基础协议联盟(ChinaLedger)致力于开发中国的区块链底层技术



- 2016年4月19日，由中证机构间报价系统股份有限公司、中钞信用卡产业发展有限公司北京智能卡技术研究院、浙江股权交易中心、深圳招银前海金融资产交易中心等11家机构共同发起。
- ChinaLedger聘请多位海外资深区块链专家作为项目的海外技术顾问，包括瑞银集团高级创新经理Alex Batlin、多伦多交易所首席数字官Anthony Di Iorio、比特币核心开发者Jeff Garzik和以太坊创始人Vitalik Buterin。



深入理解区块链技术

致力于研究和了解全球区块链技术的最新动态，探索区块链技术多种技术路线的变化，特别是对加密算法、私有链、联盟链、侧链技术以及闪电网络技术等进行深入的研究和分析。



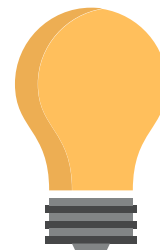
开发中国的区块链底层技术

开发中国的区块链底层技术，成为探索底层技术的重要力量，以增加中国政府、央行及各金融机构在全球内的话语权，从而更好的维护国家经济金融主权。



进行多种业务逻辑和技术方案的试验

根据联盟成员的不同情况，量身定制不同的技术方案，并且组织专业团队来进行多种技术的路线。在这个区块链基础协议之上，各成员可以使用区块链技术改善现有的业务流程，在提高效率的同时也大大降低了运营的成本。



共享成果的知识产权

是一个开放的组织，成员能够共享联盟各项成果的知识产权。联盟在研究和探索中，所获得的多种技术路线经验和源代码对于成员而言都是公开透明的，让所有成员都成为该项技术的受益者。

金链盟旨在打造安全可控、适用于金融领域的开放性区块链底层平台



- 2016年5月31日，金融区块链合作联盟（深圳）（简称“金链盟”）由深圳市金融科技协会等二十余家金融机构和科技企业共同发起成立。
- 目前，金链盟成员已涵盖银行、基金、证券、保险、地方股权交易所、科技公司等六大类行业的80余家机构。

金链盟区块链底层是开源平台，由金链盟开源工作组协作打造。工作组成员包括微众银行、深证通、腾讯、华为、四方精创、神州数码、博彦科技和越秀金科等金链盟成员机构，旨在打造安全可控、适用于金融领域的区块链底层平台。

服务	特点
源自BCOS商用的新一代数据交换基础设施	<ul style="list-style-type: none">• 可快速开发业务应用，灵活管理用户账户• 基于CA的节点准入机制，基于密码学的隐私保护算法• 可平行扩容，支持海量服务，插件式设计的共识算法
AMOP支持更多业务场景的通信协议	<ul style="list-style-type: none">• 高效、可靠、基于区块链网络的信息通信协议• 支持跨机构间点对点的实时消息通信• 为链外系统和区块链之间的交互提供标准化接口
CNS合约命名服务	<ul style="list-style-type: none">• 对耗时较高，有次数冗余的计算过程进行精简，在系统没有交易流量的时候，共识机制进入“心跳”状态，不需要产生无效记账，避免不必要的存储浪费• 记账者与跟随者同时并行计算• 当记账节点的互相检测异常时，可快速切换到下一个记账者



3

PART 3

其他领域的应用

电力能源

共享经济

信息证明

网络社交

慈善公益

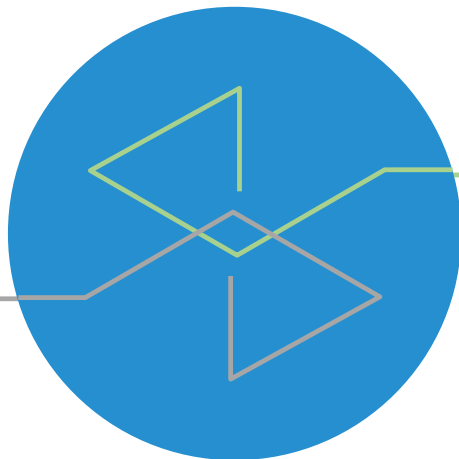
BLOCKCH

区块链分布式技术可促进能源的本地化生产和消费，降低线路损耗，节省运输成本

被中心化的电力生产机制和远程输电基础设施主宰：

- 远程运输造成高线路损耗。据高盛2016年《区块链：从理论到实践》的研究报告，预计美国每年有8%~9%的电能线路损耗。
- 小面积损坏会导致大面积瘫痪和停电。据美国国会研究服务处的报告，每年断电带来的损失达250~750亿美元。

现有电网面临的问题



区块链可以带来的改变

区块链技术建立的分布式账本透明、可追踪、点对点交易，使私人生产的小规模电力交易成为可能。

- 区块链可以建立一个去中心化的能源市场，实现电力的就近生产和消费，从而避免线路损耗。
- 在分布式技术支持下，小面积电网损坏不会造成电网的大面积瘫痪。

区块链应用于电力能源系统的概念证明与实践

概念证明

- 2016年4月，Transactive Grid举行了一个活动，使用他们的技术完成了发生在布鲁克林的两位老朋友家的第一次交易。这次活动中，退休的美国环境保护协会主管Bob Sauchelli使用以太坊的区块链从他家邻居Eric Frumin处购买了195个信用的电能，这些电能是由Eric Frumin家屋顶的太阳能板生产的。

- 纽约州正在把能源网重建为分布式平台，鼓励公用事业单位和创新者合作，而不是和他们竞争。纽约州能源与财政部主席理查德·考夫曼说：“我们建造的网络应该是混合系统。这套系统具有可靠性和传统中心站点的成本收益，有产品和分布式系统。而且，应用分布式方案的灵活性，电流的传输不止一个方向。”
- 为了给新的分布式电网奠定基础，2013年，纽约州州长Cuomo指派考夫曼制定了一系列名为改进能源愿景（REV）的政策，旨在使现存的能源构架更加实惠、可修复和清洁。作为REV项目的一部分，纽约州为有兴趣建造去中心化电网的潜在伙伴预留出4000万美元资金。有150个申请者，其中包括LO3，83位申请者分别收到了大约10万美元来从事他们的可行性研究。

实践

LO3 Energy通过区块链革命重塑未来能源行业

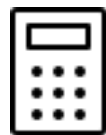
LO3 ENERGY

- LO3 Energy致力于通过区块链革命改变能源的生产、存储、买卖和使用方式，重塑未来能源行业。
- 其创始人Lawrence Orsini过去一直在能源行业工作，专注于提高能源效率，其他几个合伙人也都有能源方面的背景。合作伙伴有Braemar Energy Ventures、西门子、Centrica和Peci。

LO3 Energy和区块链技术开发商ConsenSys合资成立了一家公司TransActive Grid，该公司在纽约的布鲁克林地区运行着一个微网项目，并且已经完成概念证明。该项目通过智能仪表硬件层及使用区块链智能合约的软件层——在以太坊区块链上自动执行的合约，使街坊邻居可以在区块链上用智能合约来选择他们需要的能源来源、能源种类，甚至决定把能源出售给谁，追踪记录家庭使用的电量以及管理邻居之间的电力交易。

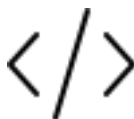
LO3 Energy将区块链应用于电力
能源的实践案例：
TransActive Grid

LO3 Energy的产品特点



Smart Meter

- 测量能源产量
- 将生产的能源连接到网络，收集管理能源



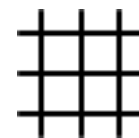
API

- 应用程序接口促进用户参与合作，使用户参与更加便捷



Blockchain

- 分布式数字账本允许私人电脑自动验证交易
- 交易验证后，加入账本



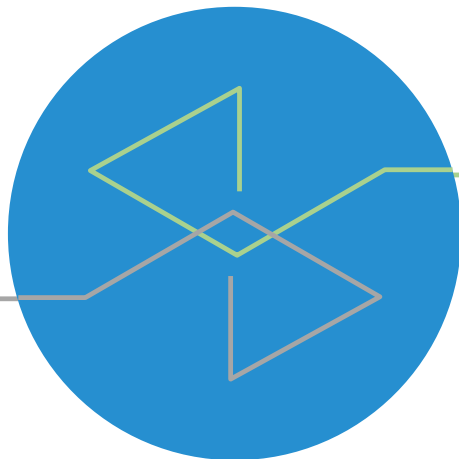
Grid

- 为区域性生产、存储和交易能源的场所建立社区网络
- 将建立的上述网络连接到现在能源网络上

出于对隐私的保护需求，基于区块链的去中心化社交平台将更受欢迎

- 平台用户隐私都集中在平台管理者手中，用户没有话语权。
- 中心化组织对流量价值、注意力价值进行剥削，用户交出了个人信息却没有获得任何利益。有些信息的使用甚至不经用户授权，如基于用户画像推荐产品，获得广告收益。
- 用户的价值观可能被潜移默化地影响。如通过推荐侧重某一倾向的信息影响用户决策。

中心化社交平台存在的问题



区块链可以带来的改变

- 分布式账本中，每个节点都有投票权，在全网中占有一定话语权。
- 每个节点拥有全网交易信息，用户可能获得有选择地向交易对手方公布信息的权利。
- 点对点交易，用户可以自由选择获取的信息。

基于区块链的去中心化社交平台ONO：重构所有权经济模型，用ONOT回报用户创造的注意力价值和内容价值

- 重构“所有权”经济模型，提出建立在区块链技术基础之上的流通通证ONOT，以平衡内容创造者、注意力价值提供者、平台提供方的经济利益
- 用户创造的注意力价值与优质内容知识产权，将获得ONOT作为回报
- 主要用户定位为95后乃至00后
- 目前，ONO社交网络已经吸引了来自中国、美国、英国、德国、韩国、日本、尼日利亚、巴基斯坦等多个国家的过百万用户



- 2017年，获得来自华创资本、松禾资本、InBlockchain的数百万人民币投资
- 2018年1月，徐可对外宣布其公司诺舟科技已并购了Jeff Ma所带领的资深硅谷区块链团队
- 2018年4月，竞选EOS全球21个超级节点
- ONOT是ONO原生通证的基本单位，是社交网络内用户创造价值的价值标记
- 用户创造注意力价值与优质内容知识产权，可与ONO共享权益。
- 用户可以用ONOT购买广告分发权、第三方应用

区块链可帮助共享经济体节省取信时间成本，避免押金造成的信用成本和交易成本

- 近年来，共享经济火爆，如共享单车、民宿、带宽、衣服等。预计未来几年，中国共享经济仍将保持年均40%左右的高速增长，到2020年，中国共享经济规模占GDP比重将超过10%。但共享经济面临着挑战，如信任问题、流转问题、价值计算问题。

用区块链解决共享经济中存在的问题

降低双方取信时间成本

在共享民宿经济中，租户和户主为了安全和避免损失，会花费很多时间询问对方信息，取信的时间成本高。区块链技术不可篡改的特性，使双方可对过往交易记录进行查询，大大降低取信时间成本

杜绝虚假交易评价

在中心化平台中，虚假交易和评价盛行，区块链技术不可篡改的特点可以杜绝虚假交易和评价

降低信用担保成本

押金是一种信用制约机制，但押金机制本身更有利于平台商家，提高了消费者消费的信用成本，使得共同的信用风险制约具有不平等性。如果使用区块链技术证明用户的信用，避免押金，则可以降低信用担保成本

智能合约提高交易速度

现有中心化平台中，为避免商家违约风险，商家收款时间和用户付款时间有较长的时间间隔，使用基于区块链的智能合约可以优化现有支付流程



- 2016年3月，Airbnb在伦敦金融城早报访谈中表示，正在考虑使用区块链技术管理声誉信息。
- 2016年4月，Airbnb收购了区块链技术公司ChangeCoin。

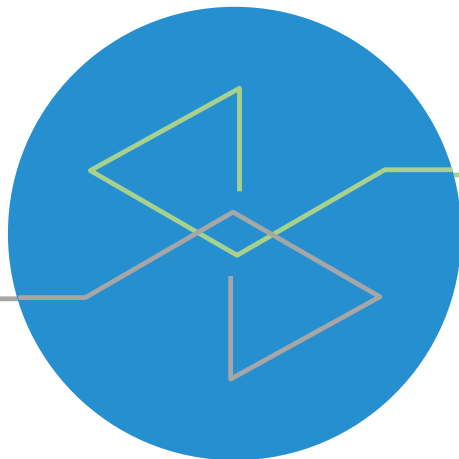
- 2017年，迅雷旗下网心科技开创的“共享计算”借势共享经济，收集闲置计算资源，将闲置资源转化为云计算服务，以更低的价格出售给企业。对参与共享计算、贡献自己闲置资源的玩客云用户奖励“链克”，迅雷成功实现了对共享资源的量化与追溯，保证用户的权益和共享的计算资源对等。



区块链分布式技术可以使公益资金去向更加透明化，促进商业和公益融合发展

- 信息不透明和真实性难以保证，平台如果不能取得捐款人的信任，则面临生存危机。
- 国内无偿救助平台发起公益筹款的主体多数是个人，虽然操作流程简单，但相对于具有成熟信用体系的机构而言，这种“共享”公益平台的风控难度较大，容易引发个人道德风险问题。
- 商业与公益结合中，商业目的与公益目的的平衡问题是个难点。





公益事业中存在的问题



区块链可以带来的改变

- 区块链信息不可篡改的特性可以使公益资金的去向真实性得到保证。
- 分布式技术可以使捐赠人了解整个项目的过程和参与的相关人员信息，不再担忧项目的真假和暗箱操作。
- 网络互助平台可以借助区块链技术提高平台的公信力，促进互助行业更好地发展。

众多知名公益平台试水区块链

公益平台	区块链实践
	2016年12月初，网络互助平台众托帮在上海举行了“心链”发布会，“心链”是众托帮依托区块链技术，专门针对公益行业开发的产品
	2016年底，蚂蚁金服旗下支付宝爱心捐赠平台宣布全面引入区块链技术，并向公益机构开放，公益项目发起人可以自主选择是否将项目发布在区块链上。签约机构经审核后均可自主发布基于区块链的公益项目。中国红十字基金会的首个区块链公益项目“和再障说分手”顺利上线，并实现实时账目公示
	2017年5月，腾讯利用区块链技术建立“公益寻人链”，把多个寻人平台的数据链接，使得各大公益平台能够实现信息共享
	2018年4月，大病社交筹款平台“水滴筹”创始人沈鹏在接受采访时表示，目前水滴筹正在联合腾讯探讨如何将区块链与公益结合起来

需注意的问题：区块链可以实现资金去向透明化，但是资金去向透明并不一定保证公益资金能对受益人产生最大化效用，能否实现受益人受益最大化，还需要很多后续工作。

区块链的可追溯性使得特定领域的信息证明成为可能

证明领域	应用简介
身份验证	区块链的可追溯性使得身份信息从采集、交易、流通以及计算分析的每一步都可以记录在区块链上，使得数据的质量获得前所未有的强信任背书，保证数据分析结果的正确性。区块链的身份信息不再由组织（政府机构或公司等）单方面确定，而需要参与方多方验证，区块链身份ID不可改变、移除、编辑、伪造
投票	区块链技术可以被运用到选民投票，通过电子统计确保只有正当的投票被记录，并且投票不会被篡改或移除，创建一个不可更改、公开的投票记录账本，让选举更加公平和民主化
食品溯源	通过区块链把食品所有环节的信息连接在一起。沃尔玛食品安全协作中心通过区块链技术将过去通过纸质形式进行食品信息确认的时间从6天缩短到2.2秒。但应该注意到区块链是一个更好的数据容器，其作用有一定的局限性，食品质量的核心还是食品本身。区块链的使用也会增加产品成本
药品防伪	区块链技术可用于药品防伪验证，比如在药品包装盒上有刮刮层，下面有验证标签，与区块链对照，查看药品真伪及来源，以杜绝非法生产的假药。2016年4月，埃森哲发起了一个用区块链技术记录跟踪药物的项目
电子病历	建立全球化的电子病历区块链，把所有病人包含本地医院和医生记录的信息统一到个人病历中。通用的个人病历能够减少患者诊断过程中的医疗错误，节省医生了解病人过往病史的时间
艺术品鉴定	通过区块链分布式技术将交易过程、鉴定评估过程、资金流转过程记录在各个节点中，保证各个参与环节都在一个公平、公开的环境中进行。下游机构或二次交易者可以随时付费查询，节约鉴定评估师的人力成本，提高鉴定评估效率，降低人为因素错误和道德风险



4

PART 4

总结与展望

人们期待区块链可以解决更多问题，但实施中仍持谨慎态度
基于代币的区块链的发展速度远快于没有代币的区块链
区块链对传统体系的挑战是渐进式而非革命式的

BLOCKCH



各界对私人加密货币持谨慎态度，但对区块链技术非常乐观，并积极布局，寻求区块链的落地场景。

- 2018年1月，达沃斯世界经济论坛上，尽管部分人士对加密货币持谨慎态度，甚至斥责，但部分学者专家对区块链技术相当乐观。
- 商业巨头纷纷涌入，展现了对区块链的肯定： Azure 发布了区块链应用创建服务区块链工作台，亚马逊网络服务（AWS）CloudFormation模板工具支持用户创建自己的区块链应用程序，华为将比特币钱包置入手机内部，三星透露将利用区块链来管理其全球供应链。



区块链的应用范围极其广泛，人们对区块链的应用场景有很高期待。

- Gartner表示，由于对流程效率、供应链和物流解决问题机会的重视，运输、政府和公用事业部门也开始加大对区块链技术的投入。
- 目前人们寄希望于通过区块链解决更多问题，本报告中提到的应用仅为区块链的部分应用。
- AWS副总裁Jeff Barr表示，区块链是新货币体系的基础，也是促进国际支付的一种方式；很多人则将区块链视为分布式账本和不变数据源，可应用于物流、供应链、房地产、众筹和其他应用。



基于代币的区块链的发展速度远快于没有代币的区块链。

- 区块链孕育于比特币中，作为分布式账本技术，天然适合代币的交易和贸易体系。
- 目前，主流区块链中都发行了代币，用代币作为体系内价值交换的工具，支持系统发展。



区块链对现存体系的挑战是渐进式，而非革命式的。人们对区块链技术的实际作用仍持谨慎态度。

- 2018年3月12日，国际清算银行（BIS）发布报告，提醒各国央行对发行自己的数字货币持谨慎态度。
- 摩根士丹利公司表示：“区块链为目前的平台提供了一种成本有效的方式来添加额外的弹性层。目前，还需要做一些工作，才能解决客户界面的一些细节。”
- 很多机构虽然在尝试使用区块链，但没有用基于区块链的系统完全替代现有系统。如纳斯达克申请区块链专利“区块链交易记录的系统和方法”，用于备份交易所交易记录。摩根士丹利公布已在使用BDS360区块链平台备份交易结算和资产转账记录。纽约梅隆银行表示，目前使用区块链技术并不是来大幅度降低运营成本，然而大型银行可以利用区块链技术保护交易和结算历史数据，来解决自己网络的弹性问题。



信和研究院
CREDIT HARMONY RESEARCH

致力于打造金融科技领域高影响力的智库组织



长按识别，关注信和研究院

信和研究院正式成立于2017年3月1日，致力于打造金融科技领域高影响力的智库组织。对内成为公司科学决策、创新孵化和战略管控的引擎；对外成为公司理念发声、合作联盟和监管互动的枢纽。研究院旨在推动科技金融主业各体系胸怀全局，放眼未来，凝心聚力，科学管理和合规运营，不断强化公司在行业竞合中的优势地位。



信和研究院
CREDIT HARMONY RESEARCH

北京市丰台区南四环西路186号汉威国际广场3区3号楼3层305-308室 P.C 100070
Tel : 010-50808953 <http://research.creditharmony.cn>



蜜蜂学堂

Scholarship

超级年卡

让更多人享受到知识与成长的快乐

- ✓ HR全模块1000小时线上实战课程
- ✓ 50份超3000页可编辑PPT蜜蜂笔记
- ✓ 1000页PPT模板&图标集（每两周更新）
- ✓ 10本畅销书籍精美思维导图

~~原价3999元~~ 今限时团购**399元!!!**



【原价3999元限时团购399】 蜜蜂学堂学习年卡



扫描或长按识别二维码