DBAplus

数据库技术沙龙-上海站

资产交易：基于ripple的区块链落地应用

甘泉福

区块链介绍

IBM

什么是区块链？

区块链是一种共享账本技术，商业网络中的任何参与方都可以查看交易系统记录（账本）

交易（Transaction）
记录一笔资产转移的过程

区块（Block）
记录一段时间内全局最新交易的数据块

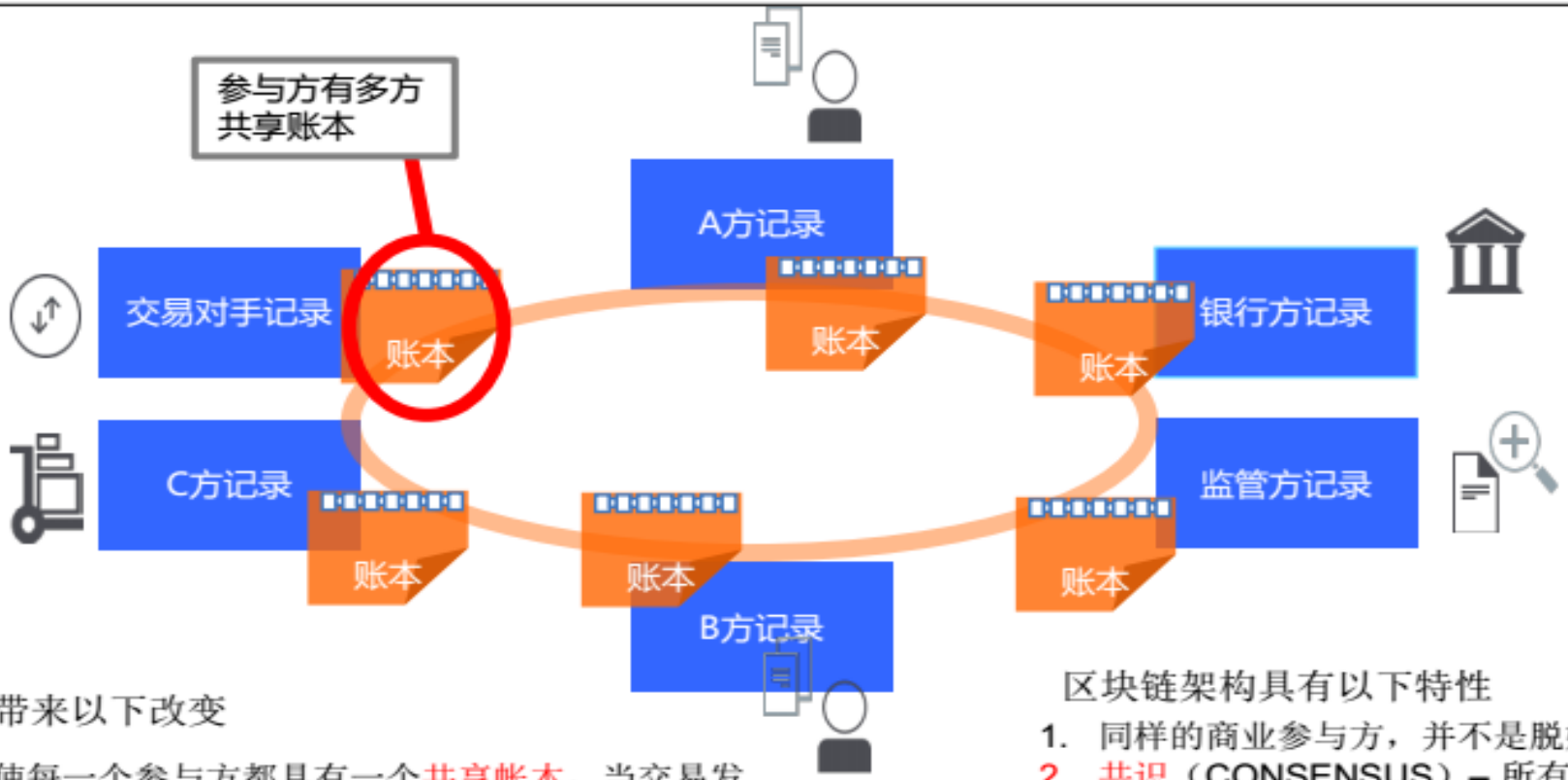
区块链（Blockchain）
通过竞争协商机制，确定全局认可的区块，把区块按时序串接在一起，形成全局公开账册

区块链技术（Blockchain Technology）
多方参与共同维护一个不断增长的分布式数据记录，这些数据通过密码学技术保护内容和时序，使得任何一方难以篡改、抵赖、造假

解决方案：共享的，复制的，授权的账本

IBM

什么是区块链？



区块链架构带来以下改变

1. 区块链架构使每一个参与方都具有一个共享帐本，当交易发生时，通过点对点的复制更改所有账本
2. 使用密码算法确保网路上的参与者仅仅可以看到和他们相关的账本内容，交易是安全的、授权的和验证的。
3. 区块链也将资产转移交易相关的合同条款嵌入交易数据库以做到满足商务条件下交易才发生
4. 网络参与者基于共识机制或类似的机制来保证交易是共同验证的。商业网络满足政府监管、合规及审计

区块链架构具有以下特性

1. 同样的商业参与方，并不是脱媒的游戏
2. 共识（CONSENSUS）– 所有的参与方认同交易的有效性
3. 可证明性（PROVENANCE）– 每个参与方了解资产从哪里来，其所有权是如何改变的。
4. 永恒性（IMMUTABILITY）– 每个参与方一旦交易被同意发生则无法篡改。 如果交易是错误的，必须由新交易冲正并全可跟踪
5. 权威性（FINALITY）– 交易方决定资产的归属权及交易的完整性，全网确认记账

区块链——适合的场景

IBM

为什么与业务相关？

- 解决两类问题
  - –不信任网络中，信息隔断后造成信任不连续
    - 看见价值链全过程后，原本高风险交易变得不再可怕，而没有上下文的交易变得可疑
  - –传统合同执行过程中定义模糊，价值转移过程风险高，易争议
    - 在智能合约中，合同自动执行，条件触发，无法反悔，减少争议
    - 必须明确条和结果，不能有“视XX情况而定，XX方具有最终解释权”

- 适合的应用场景
  - –行业平台，成员分级，核心成员数量有限（少于100个），需要监管
    - 互联网+主要在消费侧（个人）野蛮生长
    - 区块链应该在供给侧（企业）有序发展
  - –低频交易，价值转移，多方参与，共同监管

区块链的广泛应用

IBM

为什么与业务相关？

- **金融**
  - 电子货币
  - 股权（私募、公募）、债券
  - 金融衍生品（期货、期权、次贷、票据）
  - 选举权、商品所有权、抵押品权属
  - 交易记录、服务记录
  - 众筹、小额信贷、小额捐赠
- **公共记录**
  - 地契、房地产权证、车辆登记证、营业许可证
  - 公司产权关系变更记录
  - 监管记录、犯罪记录、电子护照、出生死亡证
  - 选民登记、选举记录、体检记录、安全记录
  - 法院记录、法医证据、持枪证、建筑许可证
- **私人记录**
  - 合同、签名、遗嘱、信托、契约（附条件）、仲裁
  - 证书、学位、成绩、账号
  - 医疗记录、染色体、基因序列
- **有形资产**
  - 钥匙、酒店门卡、车钥匙、公共储物柜钥匙
  - 银行保险柜钥匙
  - 特殊包裹递送（发送方接收方钥匙一起打开）
  - 彩票、球票、电影票
- **无形资产**
  - 打折券、抵用券、付款凭单、发票、预订
  - 专利、商标、版权、软件许可、游戏许可、数字媒体（音乐、电影、照片、电子书）许可
  - 网络身份
- **其他**
  - 垃圾邮箱防范（每次发送需要一点工作量证明）
  - 武器发射密码（多个密码共用）

区块链的银行业务场景及考虑

IBM

- 哪些银行业务最适合应用区块链技术
  - 多方参与，但由于缺乏共信机制，存在过程冗长、信息不透明、易产生摩擦或纠纷
  - 银行需要强可信度控制的资本、资产相关的业务交易
- 一些典型的银行场景
  - 数字货币
  - 支付清算
  - 数字票据
  - 银行征信
  - 资产证券化
  - 供应链金融
  - 银行贷款
  - P2P理财
  - ……
- 区块链还处于很早期的发展阶段，银行应用区块链可以考虑下面一些指导原则
  - 选对应用领域，包括多方参与但不能太多（如比特币），自动合约执行解决摩擦而带来实质性效益，必须与金融机构的主要风险一起考虑等。
  - 充分保证技术的可行性，避免引入新的风险。如共识算法完备性、性能等。
  - 兼顾开放创新性与可监管性的平衡。
  - 区块链在银行的应用推广必须兼顾多个参与方的利益及时间表。

区块链——并非万能

IBM

不适用场景

1. 高性能（毫秒级）交易
2. 小型组织（无商业网络）
3. 寻找数据库的替代方案
4. 寻找消息传递的解决方案
5. 寻找交易处理的替代方案

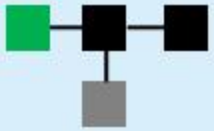
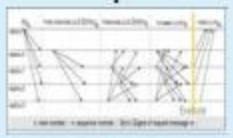
Bitcoin/Ethereum/Ripple/IBM OBC的区块链技术比较

IBM

	Bitcoin (比特币)	Ethereum (以太坊)	Ripple (瑞波)	IBM区块链(OBC)
架构设计	• 以电子加密货币为主 • 智能合约支持弱 • 没有图灵完备的智能合约开发语言	• 电子加密货币 • 智能合约 • 图灵完备的智能合约开发语言 • 自己独特的语言和GO	• 电子加密货币 • 特定场景应用 • 暂无智能合约支持	• 以智能合约为主的通用平台 • 可插入式共识算法框架 • 可以构建电子货币 • 满足商业需求 • 通用商业开发语言的支持
区块链的支持（共享帐本）	• 公有链 • 无限制进入 • 公开帐本 • 匿名制 • 无法审计	• 公有链 • 无限制进入 • 公开帐本 • 匿名制 • 无法审计	• 联邦链 • 准许制 • 即将支持金融机构各自交易的私密性	• 联邦链 • 准许制 • 加密的帐本 • 强身份认证 • 强私密性 • 可审计
帐本扩展性	• 差 • 需要全帐本 • 会导致挖矿集中	• 好 • 不完全需要全帐本		

Bitcoin/Ethereum/Ripple/OBC的Blockchain共识算法对比

IBM

	Bitcoin (比特币)	Ethereum (以太坊)	Ripple (瑞波)	IBM区块链(OBC)
共识算法对比	• PoW：计算密集型工作量证明机制(PoW) 	• Dagger一种内存消耗型PoW 	• RPCA瑞波共识算法 	• PBFT：可插入式共识算法框架 • 现在支持classic PBFT, batch PBFT, SIEVE, Noops 
Block Latency	• 10分钟 • 交易的最终确认可能需要60分钟	• 15秒	• 3-6秒	• 4次单程到最远验证节点的网络延迟 • 1000KM延迟20毫秒
Throughput（交易率）	• 现在3~7TPS • 通过参数调优的理论扩展性可达247TPS		• 可能上千	• 可能上千

Bitcoin/Ethereum/Ripple/OBC的Blockchain共识算法对比

IBM

	Bitcoin (比特币)	Ethereum (以太坊)	Ripple (瑞波)	IBM区块链(OBC)
网络容错能力	• 49% 故障	• 49% 故障	• (n-1)/5 故障	• f/(3f+1) 故障
网络带宽需求	• 较高		• 一般	• 较高
网络拓扑的有效性	 • 避免分叉		 • 避免分叉	 • 不会分叉
计算资源的消耗	• CPU密集型 • 大量专用硬件加速 • 会导致挖矿集中	• 内存密集型 • 潜在的可能性通过硬件加速 • 通过算法优化达到即使出现挖矿集中，也不能造假	• 很少CPU • UNL里的节点都是信任节点，且随机	• 很少CPU
新加节点或再同步	• 需要下载并验证整个帐本 • 现在需要耗时4天以上		• 动态 • 要注意是否会影响UNL	• 动态 • 可以断点恢复

Bitcoin/Ethereum/Ripple/OBC的Blockchain对比总结

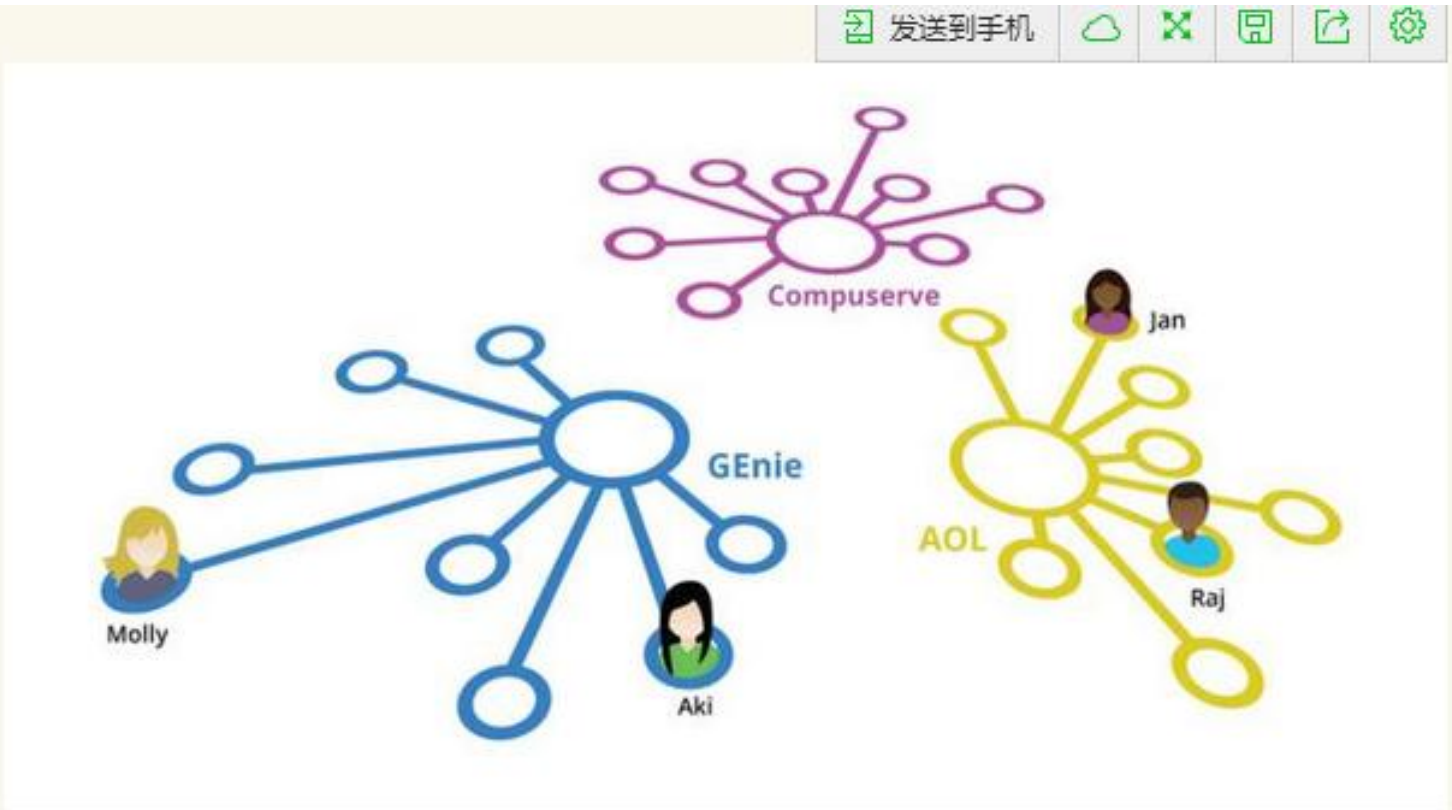
IBM

- Ethereum继承Bitcoin的设计思路，在算法、智能合约和帐本扩展性的方面做了较大改善；两者都是以公有链为设计出发点的。
- Ripple的设计思路是瞄准非常细分的应用场景，外汇兑换和跨境结算，暂时没有智能合约的支持和更详细的隐私及监管支持。
- IBM Blockchain（OBC）是一个平台化设计，支持插件式共识算法的更换，以智能合约设计为中心，对商用情形考虑比较周到。

Ripple简单介绍

Foreword·前言

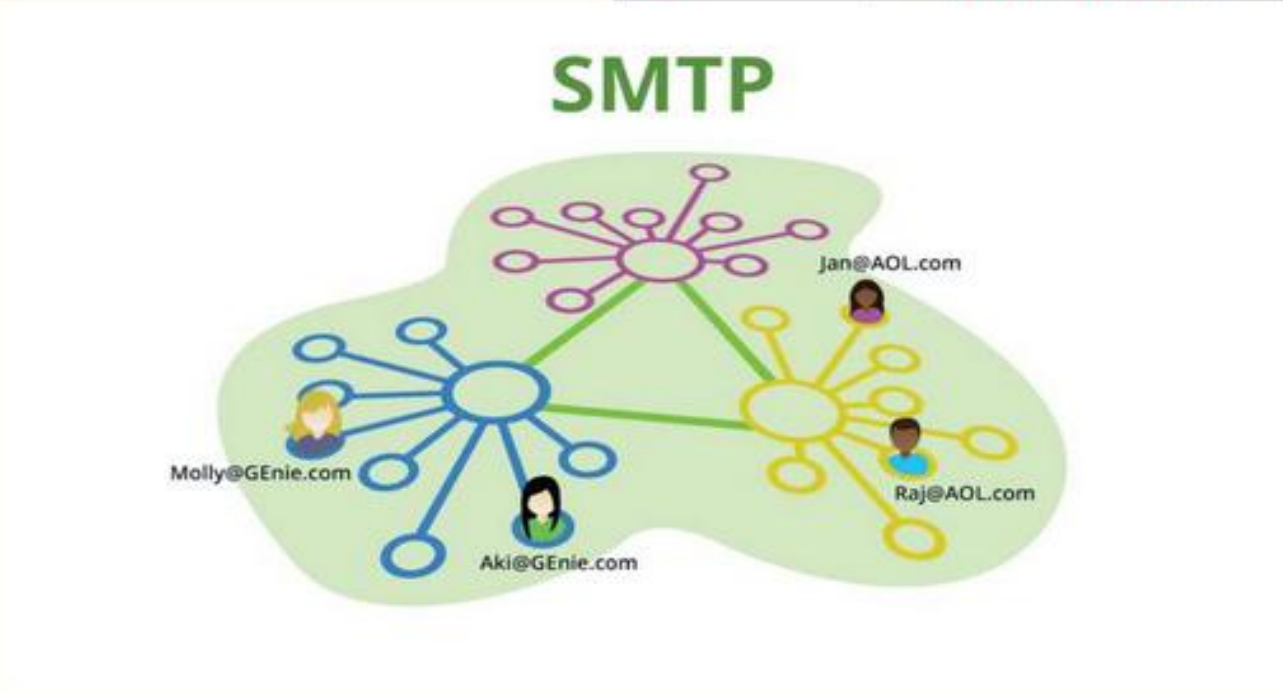
在互联网早期，人们只能在有限的、封闭的网络中发送信息。如果你在1989年之前使用CompuServe，那么你只能向其他CompuServe用户发送邮件。如果使用Genie，那就只能向其他Genie用户发送信息。在那个时代，电子邮件还没有诞生，也没有标准化的协议来将每个互联网运营商的邮件系统连接起来。



早期的电子邮件运营商仿佛在各自的围墙里运作

当被普通人称作“电子邮件”的SMTP（简单邮件传输协议）诞生的时候，它就可以把许多不同的邮件系统连接成一个单一而又相互连接的系统。SMTP协议的

作用在于将独立的系统连接起来——而这正是设计互联网的目的。互相连接起来的邮件系统的优势明显、势头强劲，因此SMTP便迅速成为了邮件的标准协议。今天，不互联的邮件系统已经成了无稽之谈。

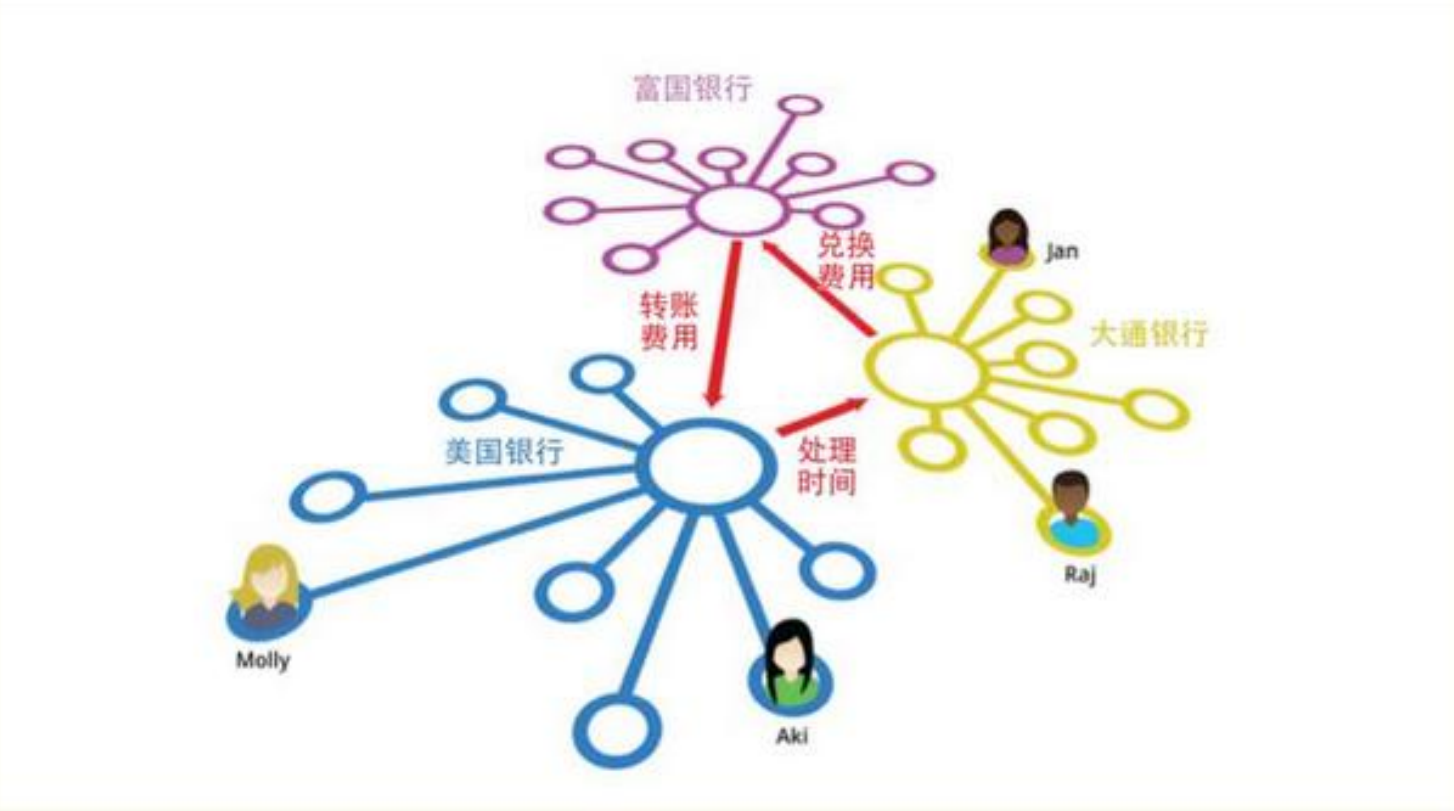


SMTP使得Molly@GEnie.com可以向Jane@AOL.com发送邮件

但是，今天的支付系统还和20世纪80年代的邮件系统一样——依然封闭而没有互联。

如果你是富国银行的客户，那么你只能够轻易、免费地向其他富国银行的客户转账。如果你有一张美国运通卡，那么你也只能在接受运通卡的商家购买商品。

为了把这些孤立的支付系统连接起来，我们就需要增设许多结算中心。你怎样才能把钱从富国银行的网络转账到大通银行或是PayPal（贝宝）的网络呢?你可以使用SWIFT（电汇的方式）。但是这种方式不但需要第三方支持，而且还需要为这笔交易支付费用。



现在的金融系统还类似于早期的电子邮件系统

当大部分的信息传输已经免费了的时候，金钱的转账依然有不少阻碍。电汇一

次的手续费要15美金，而汇款的费用则大约是7%。信用卡公司也对每一笔网上交易收取2%的费用。亚马逊每年都需要支付数十亿美元的交易费用。

互联网已经有了40年的历史，而在互联网通讯和互联网金融之间已经有了巨大的差距。

互联网通讯已经通过点对点的分布式网络被扁平化了，但是交易结算与交割在本质上需要集中化，这就使得金融交易仍然运行在20世纪50年代到70年代（前互联网时代）的基础之上。

在电子时代，金钱实际上只是另一种信息：存储在电子总账中的借贷信息。那么为什么在计算机转账和传递信息的方式之间会有如此大的差距呢?

金钱转账缓慢、昂贵、复杂。原因是运行集中化专有软件的独立网络和独立支付系统过多。集中化的网络都很昂贵——他们不但需要钱来雇佣员工，购买服务器，而且还需要盈利。

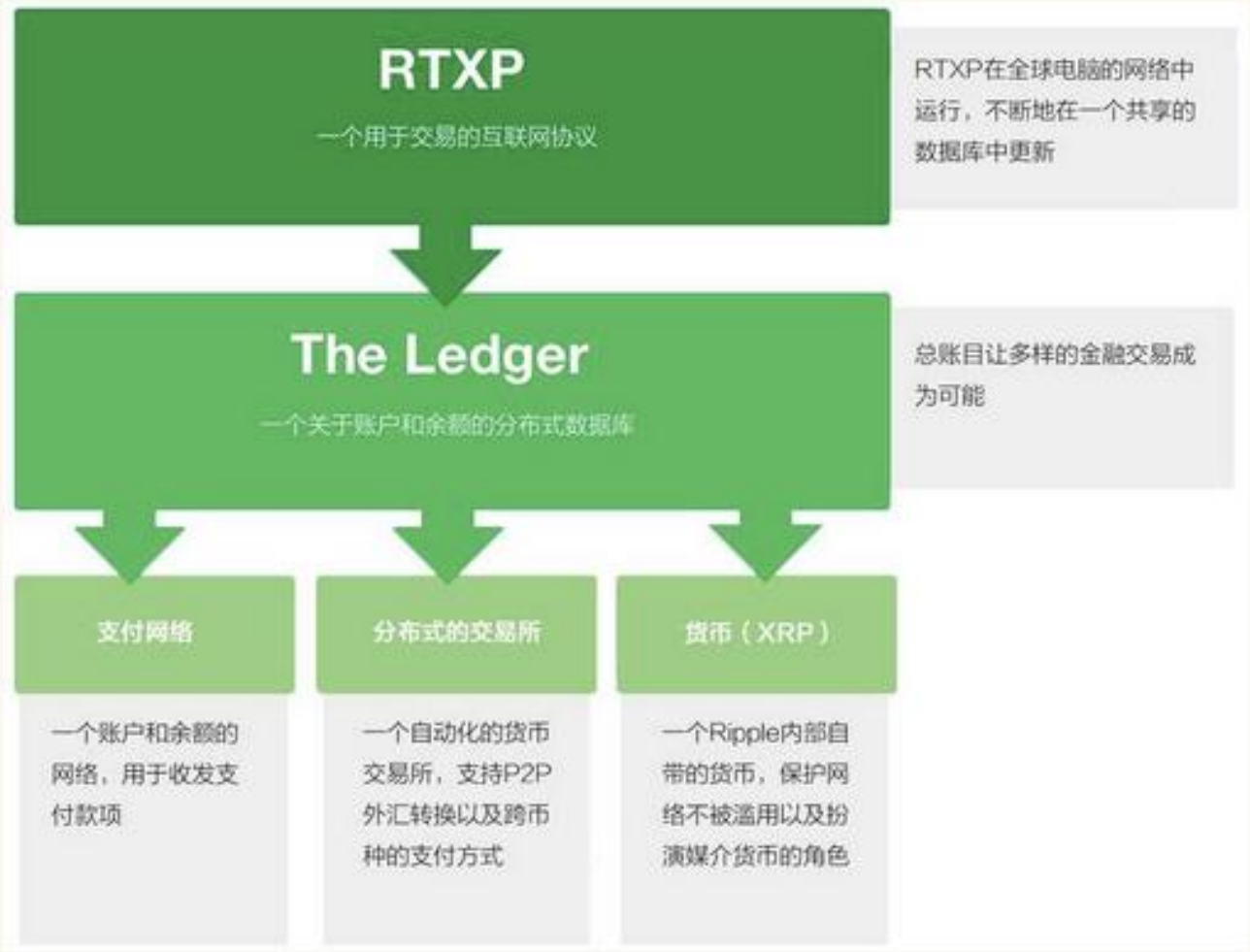
Ripple的诞生正是为了解决这一问题。

1.Ripple简介

什么是Ripple

Ripple是一种用来进行金融交易的互联网协议，该协议可以用来即时、免费的以任何币种向世界的任何角落转账。Ripple的核心部分是一个分布式数据库，记录了所有用户的账户、余额和交易情况的信息。这个数据库中的记录被称作Ripple账本（ledger）。

1.Ripple简介 10%



Radar介绍

目录：

Part-1 RADAR的技术背景

RADR系统是一个大型分布式的货币交易网络，这个网络由许多被称为节点的服务器组成，客户端通过签名并发送交易到节点，节点接收后，在节点网络中转发并处理交易，交易被一致共识结束并验证后，记入总账中，客户端发送的交易便完成。

RADR系统是一个大型分布式的货币交易网络，这个网络由许多被称为节点的服务器组成，客户端通过签名并发送交易到节点，节点接收后，在节点网络中转发并处理交易，交易被一致共识结束并验证后，记入总账中，客户端发送的交易便完成。

Part-1 RADAR的技术背景

- 雷达部署全球核心节点7个：Virginia, California, Seoul, Singapore, Tokyo, Sydney, London

Part-1 RADAR的技术背景

- 雷达底层及时使用的是基于Ripple改进的联盟链。
- 相比Ripple，雷达主要优化和增强的是：
  - 灵活性：支持更多的业务类型
  - 可扩展性：联盟节点、接入方式更多
  - 性能： 支持更高的交易频率
  - 存储方式：支撑海量数据

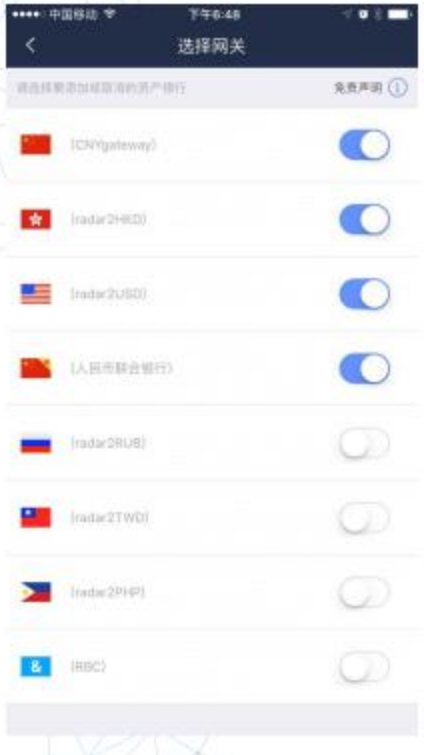
更详细资料见wik百科：https://cnwiki.radarlab.org/intro

注：联盟链而不是公有链，是保证系统具有更高容量和性能的商业级开发方案，同时也具有更高的安全性。
类似的，全球几十家银行合作的R3系统，IBM推出的超级账本，都是联盟链形式。

对于公众来说，RADR是开源且完全公开和透明的。
RADR的百科全书，包含最详尽的说明、源代码、分布式原理、共识交易机制、交易路径寻找算法、社交货币发行算法等等。全球的开发者可以使用RADR的API应用程序编程接口，开发相应的应用系统。

英文RADR百科： https://wiki.radarlab.org
中文RADR百科： https://cnwiki.radarlab.org
开源地址： https://github.com/radrbiz
RADR数据查询： https://info.radarlab.org/
API地址： https://radarlab.org/dev/radar-api-tool.html
开发者文档： https://radarlab.org/dev/

Part-2 RADAR的网关



网关简介

货币通过网关进入RADAR网络。网关是RADAR中用来描述货币进出点的专有词汇。网关是接收货币存储并相应地发行RADAR网络中的余额的公司。

就像一个传统银行的网络一样,RADAR中的每一笔交易和支付通过一个合法的账目变更来完成。不依赖于中心化的 网络运营者,RADAR网络中全世界的服务器对账目的变更达成一个共识,然后更新他们本地的数据库版本,这样, 所有人都同时达成共识。

在RADAR 网络中，每种货币（VBC和VRP除外）都有其对应的发行网关。当用户想从RADAR网络提取定额的线下币种时，原相应电子货币的发行网关有责任为用户兑换等值的线下资金。

Part-2 RADAR的网关分布

- 目前法币网关有：
  - USD 美元
  - CNY 人民币 (最大)
  - RUB 俄罗斯卢布
  - HKD 港币
  - TWD 新台币
  - PHP 菲律宾比索
  - GBY 英镑
  - JPY 日元
  - SGD 新加坡元
  - MYR 马来西亚令吉特

注意⚠：以上为雷达技术架构好的网关，部分网关目前并不存在交易量，其中人民币兑美金，港币的交易量最大。

Part-3RADAR的交易数据

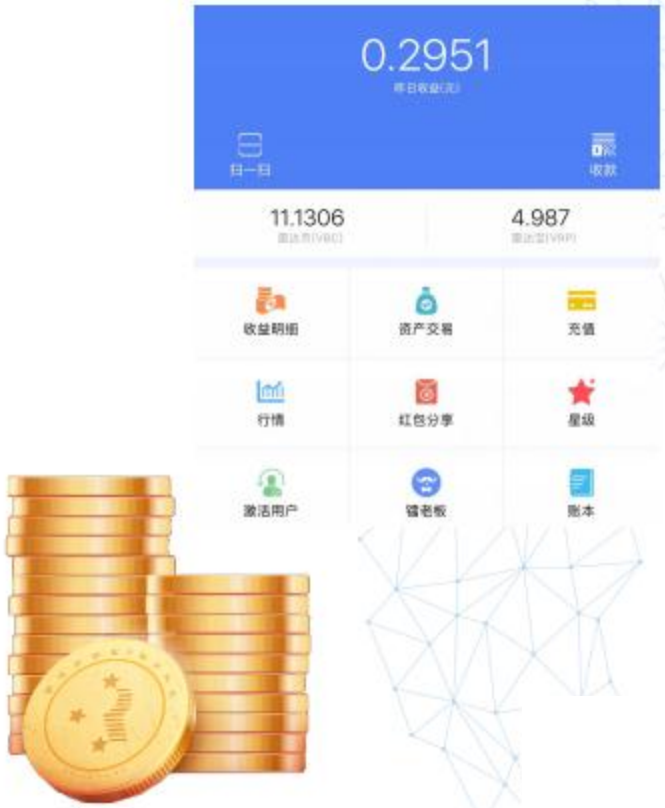
- 雷达的交易活跃度非常高，目前已经积累了900万个Ledger，平均Ledger交易数都在200~500不等。
- 详见：https://charts.radarlab.org/#/
- 雷达当前总账数据量达到1TB，已成为全球最大区块链系统（比特币，目前才60G数据；数据量是Ripple的5倍，值得一提的是，ripple于2015年已经下线了其在线钱包业务，主要业务变为b2c，主要服务于银行。而雷达的c端用户量增长稳定。
- 雷达日活跃用户在10(万)左右，高峰值达20万。
- 雷达的 TPS>1000 ，满足一般交易所需要（比特币TPS=7）
- 雷达上线了两年半，并稳定运行至今。

Part-4 Radar原生货币 - VBC VRP

雷达是基于Ripple的RTXP协议的金融网络产品。它促进和开发了全球化的、更快速、低成本的支付、清算系统，汇兑系统。它支持各种类型的货币，使得互联网支付就像Email一样简单便捷。

特别的，雷达宝、雷达币都是在RADR网络里的内置原生货币。 雷达宝主要用来作为交易费，防止垃圾交易；而雷达币是创新引入的“社交货币”。RADR核心程序会按照特定的持币量和推广关系算法，每日发行新货币，以促进RADR推广者的收益并产生动力。

详细发行算法请见
https://cnwiki.radarlab.org/dividend



Part-4 Radar原生货币 - VBC VRP

VRP 中文译名 - 雷达宝

VRP是雷达系统原生货币之一，和xrp在ripple网络中的作用一样，VRP的存在相当于Radar系统中的润滑剂和桥梁，为Radar系统的流动性提供了巨大的便利，从而带动了Radar系统的发展。

它有两个作用，一是防止垃圾请求攻击（由于Radar协议的开源性。恶意攻击者可以制造大量的“垃圾帐目”，导致网络瘫痪。为了避免这种情况，Radar要求每个用户在做任何操作时都需要消耗至少0.001个VRP）这一费用对于正常交易者来说成本几乎可以忽略，但对于恶意攻击者，就大大提高了作恶成本和门槛。

VRP的总量设定是1000万，根据持有VBC的数量每天获得对应0.1%的系统分配，可自由交易。

Part-4 Radar原生货币 - VBC VRP

VBC 中文译名 - 雷达币

- VBC是雷达系统新引进的一种社交数字货币。
- 数字加密货币的发行基本都依赖于矿机挖矿，即由P2P网络节点进行大量复杂的计算而产出新的货币。挖矿收获与矿机的配置成正比，且挖矿的过程需要消耗大量资源。
- 而radar开创了“社交数字货币”理念，将数字货币发行权分配给货币的持有者和推广者，以实现让价值创造者获得价值的公平的货币体系。

Part-4 Radar原生货币 - VBC VRP

VBC 中文译名 - 雷达币

- Radar的发行同样依靠挖矿，但是挖矿的规则与持有和分享有关。radar新产生的币，50%按投资额排名加权发行，另外50%按照推广力度加权发行，让持有者和推广者成为发行者，获得相应的利益，从而促进radar的快速成长。对于radar这样的全球化支付系统，体量越大，价值越高，也越稳定，持有者和分享者获得利润也越高，从而促使分享者更加努力的进行分享，使持有者愿意投入更多，形成良性循环。

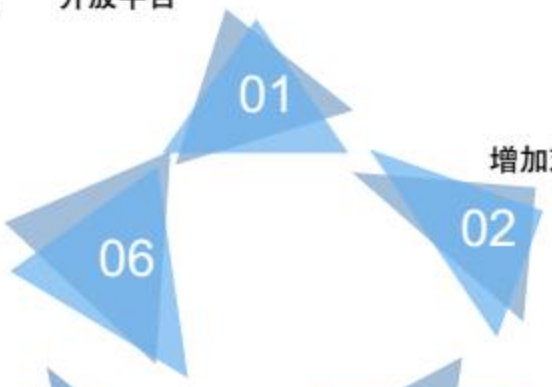
- **VBC总数10亿个，首期1000万个，前半年月增长10%，随后三年月增长5%，再三年月增长3%，最后保持月增长1%，直到10亿枚发行完毕。每次产出总数的50%用于用户的分红奖励，另外50%用于用户的推广奖励。**

- 更详细发行规则： http://mp.weixin.qq.com/s/eksFlQraDezWr-pS6KIwHA

Part-5 2016优化

雷达2016年的重要改进

Lorem ipsum dolor sit amet kolor



增加对移动端镭达钱包
以及开元通宝等雷达应用的
技术接口支持

海量数据稳定性优化

- 目前区块链数据规模已经超过1TB

安全性改进

- 异常登录风险识别
- 二步验证逻辑加强
- 网关层面的风险监控

关注了解更多

镭达钱包 RADAR WALLET　RADR trade

DBAplus

www.dbaplus.cn

THANK YOU