众链

保障可信交易的基础技术设施





交易的发展需要支持可信交易的、数据安全的、多边合作高效的交易系统

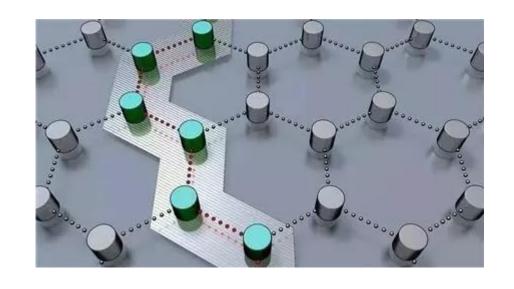


交易发展的四大阶段





可信交易系统与区块链技术有天然的契合



健全的身份管理机制

参与交易的每一方都应该有相关的角色 授权以及角色相关的权限划分

释放智能合约的自动化能力

交易多方应充分利用智能合约的自动化能 力缩短多边交易的达成时间

数据安全与隐私保护机制

只有被授权方才可以通过其数字身份证 明查看数据明文

保证网络化多边合作效率

可信交易应该使得多边的信息交换可信, 进而促成交易达成效率的提高

可审计、可追踪

必须保证交易的相关信息是可以审计, 可以追踪的

完备的可信交易协作机制

在交易的过程中使得相关方均可以对交易的状态进行认可,以确保交易的协作是有效的





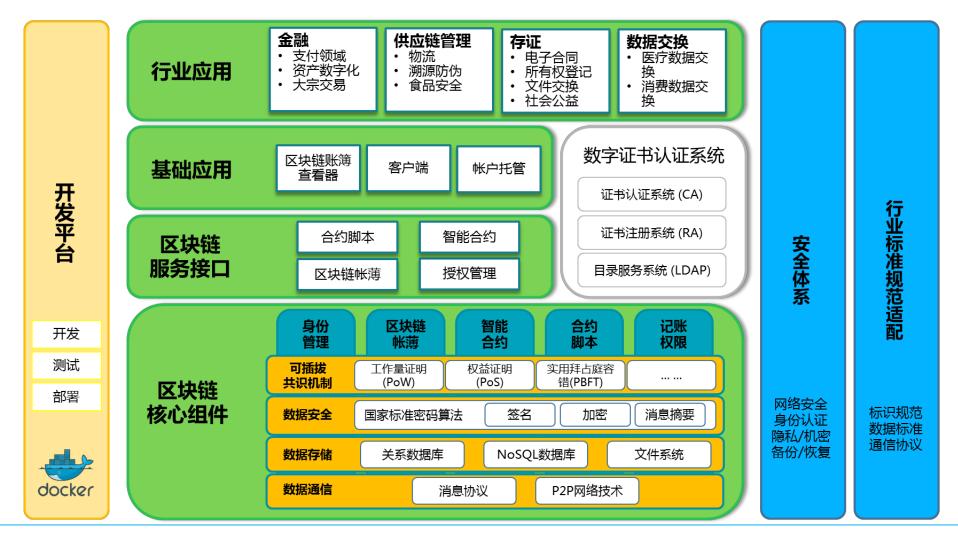
众链——保障可信交易的基础技术设施

• 成熟的、已支撑多个落地行业应用的区块链技术基础设施

- 定位
 - 可溯的参与人员注册
 - 可信的交易执行过程
 - 。 可靠的共享数据方式
 - 可见的证据保存系统



众链技术架构





众链特色技术



可拔插智能合约框架

非侵入式扩展业务

内嵌常见数字货币合约

以容器技术 封装智能合约



国密证书颁发

权限体系配置

数据按需加密

国密级权限管 理与数据加密



毫秒级交易支持

可拔插共识算法

内嵌多种共识算法

高性能交易校验 与共识框架



冷钱包机制代管

实时触发交易委托

密钥找回机制

安全的 密钥代管服务

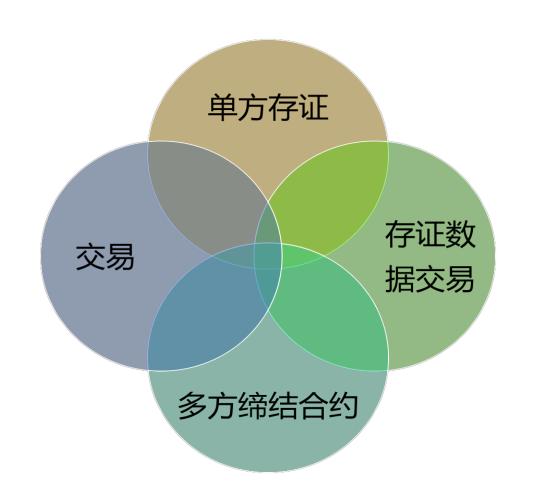
众链核心技术优势

架构层级	模块	技术优势	带来的业务优势
基础平台	密码服务	适配国家标准密码算法和国际标准密码算法	国密算法是由中国国家密码局认定的国产密码算法。适配国密算法,可以使区块链解决方案符合国家x信息安全标准。
	高性能	并行化执行提高交易的吞吐性能	私有链 TPS > 1000
	模块化共识机制	适配不同共识机制,包括实用拜占庭容错共识、 投票共识;	满足多种业务场景、联盟链的共识要求,实现快速适配和部署。
	内嵌式合约脚本	基于容器技术的合约脚本执行	1. 实现合约脚本的隔离验证; 2. Docker容器技术提高开发和部署生产力;
标准驱动	身份管理	支持主流第三方数字证书支持	1. 将对参与方的认证由线下转移到线上; 2. 通过身份认证,确保交易数据的安全;
	内容授权管理	支持对数据读取内容进行授权,实现公共帐薄 的全程可审计	1. 对交易数据进行访问授权,确保数据隐私; 2. 运行对数据权限进行授权的智能合约,随时为加入的监管机构进行历史数据访问授权,从而保证公开帐薄的被审计性和信任度;
	主侧链数据交换	通过主侧链的方式进行可信互信的数据交换	1. 便于参与方进行分类帐(子链)之间的数据交换; 2. 保护参与方的商业机密;
区块链基础应用	帐户托管	实现对用户公钥私钥或者数字证书的托管	对用户帐户进行安全、便利的管理





众链典型应用场景分类



场景分类	参与方数目	场景举例
单方存证	单方	音乐、文学著作等版权存证 专利存证 私人合约上传
存证数据交易	无限的多方	健康数据存证交易 信用数据存证交易
多方缔结合约	有限的多方	信用证 食品/贵重物品追踪追溯 资产数字化 资产证券化
交易	无限的多方	大宗交易流转 证券流转 代币流转





众链典型应用场景 – 单方存证



业务目的	证明某项数据归某人所有;
业务需求	存证时间真实; 存证不可篡改; 数据不可销毁; 数据可验证所有权;
区块链关键支撑技术	非对称加密算法签名确保所有存证时间真实; 非对称加密算法签名确保存证内容不可篡改; 分布式账簿确保数据不可销毁; 私钥签名公钥验证机制保证数据可验证所有权。
成功案例	某电子合同服务平台电子合同第三方证据保全 :提 升电子合同签约存证、取证效率,打造去中心化的 可信数据存证生态。





众链典型应用场景 - 食品供应链追踪追溯



业务目的	传统食品体系中,从食品生产者到加工企业,再到仓库或配送,最后送达零售商的整个过程中存在很多漏洞。每个环节信息由纸张记录,如果要追溯购买食品的生产地等情况,需要耗费几天时间。一旦食品出现问题,想要查明问题来源并作出决定都需要长时间的调查取证。
业务需求	快速实现多方数据的可信同步 流程环节透明化,全程可追溯 无纸化
区块链关键支撑技术	私钥签名公钥验证机制保证数据可验证写入人的可信性 以天然的分布式系统提供低成本的统一信息化系统,具 有天然的系统可拓展性。
成功案例	某零售企业基于区块链技术的可信食品溯源平台。





众链典型应用场景 - 资产证券化



业务目的	确保资产根据公众认可的流程形成证券;
业务需求	可回溯资产证券化各方角色(包括特殊目的机构、增信机构、信用评级机构、销售机构等)认证; 可检查资产证券化过程相关流程是否合法合规; 确保证券化资产的唯一性;
区块链关键支撑技术	将证券化资产进行密码学变换后生成唯一的ID,同样的资产再次证券化系统将预警;以智能合约约定资产证券化流程,避免出现不符合流程的证券化; 以私钥签名确保合约由相关方签署。
成功案例	某互联网金融公司区块链资产管理系统 :通过区块链技术,保证底层资产数据真实性,有效解决机构间对账清算问题。





谢谢!