一种满足私密、量子安全、零费用的高TPS智能合约公有链系统

邹远春

2017年12月17日

目录

摘要

从比特币发布以来，去中心化、去信任化、数据无法篡改等等理念开始深入人心，以区块链为核心的加密货币得到快速发展。区块链技术是对社会几千年的社会生产关系的巨大颠覆，但目前被本身的一些特性所限制，应用领域还比较少，加上比特币和以太坊网络经常发生交易堵塞的情况，一旦突破这些限制，区块链价值传输的特性将迎来巨大的爆发机会。今年年中整个加密货币总市值在1千亿左右，短短几个月突破到3千亿，又半个月突破到5800亿，说明加密货币在经历高速发展，不过相对于全球几十万亿的量还有巨大的成长空间。虽然现在加密货币已经得到全球的认可，但是在商业应用落地上明显落后，谁能大面积的商业应用落地，谁就是未来的王者，比特币的数字货币和以太坊的ICO就是最好的明证。

区块链系统包含数据层、网络层、共识层、激励层、合约层、应用层。数据层封装了底层数据区块的链式结构，以及相关的非对称公私钥数据加密技术和时间戳等技术；网络层包括分布式组网机制、数据传播机制和数据验证机制等，主要采用完全P2P的组网技术；共识层主要封装网络节点的各类共识机制算法，影响整个系统的安全性和可靠性，目前最为知名的有工作量证明机制（Proof of Work，PoW）、权益证明机制（Proof of Stake，PoS）、股份授权证明机制（Delegated Proof of Stake，DPos）和各种BFT拜占庭容错算法；激励层将经济因素集成到区块链技术体系中，因为在公有链中必须激励遵守规则参与记账的节点，并且惩罚不遵守规则的节点，才能让整个系统朝着良性循环的方向发展。合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；应用层封装了区块链的各种应用场景和案例。

目前区块链公有链系统主要有比特币和以太坊，比特币基于UTXO模型、PoW共识算法、共识间隔10分钟左右、吞吐率（TPS）在7 10左右、具有弱匿名性；以太坊基于Account模型、PoW+PoS（Casper）共识算法、共识间隔15s左右、吞吐率（TPS）在15左右。TPS相对于传统传统应用领域偏低，这极大的限制了应用的落地推广。

本系统就是基于原有的这些区块链公有链系统来初步改善其中一些环节的瓶颈，打造一款满足私密性、量子安全、零交易成本、高TPS的智能合约公有链系统。

1 私密性

在区块链公有链中，每一个节点都能够获得完整的数据备份，所有交

易数据都是公开和透明的，这是区块链的优势，但另一方面，很多时候，不仅仅用户希望他的账户隐私和交易信息被保护，对商业机构来讲，很多账户和交易信息更是这些机构的重要资产和商业机密，不希望公开分享给同行。

对于私密性，我们统一用两点来描述：交易双方的匿名性、交易数据的机密性。匿名性是体现在虽然能看到每一笔交易的发送方和接收方的地址，但是无法对应到现实世界中的具体某个人；机密性是体现在根据公开的交易信息，除当事双方外，其它任何人不能明确确定交易的数据。

比特币BTC和以太坊具有弱匿名性，但交易数据公开，不具有机密交易性。为了解决区块链的隐私保护问题，目前主要有混币、环签名（Ring Signature）、同态加密、零知识证明等几种方式。混币是割裂输入地址和输出地址之间的关系；环签名方案中，一个成员利用他的私钥和其他成员的公钥进行签名，而且不需要征得其他成员的允许，而验证者只知道签名来自于这个环，但不知道谁是真正的签名者;同态加密是一种无需对加密树进行提前解密就可以执行计算的方法；零知识证明是一种密码学技术，无需泄露数据本身情况下证明某些数据运算的一种零知识证明，允许两方（证明者和验证者）来证明某个提议是真实的，而且无需泄露除了它是真实的之外的任何信息。

在这过程中，涌现了CoinJoin、Mimblewimble、Tumblebit、隐身地址（Stealth Addresses）、zk-SNARKS等等解决方案。DASH采用的混币CoinJoin的方案，把一些交易混合在一起，增加追踪的难度；门罗币是通过交易发送方环签名+交易接收方隐身地址来实现私密性的加密货币；Zcash和Zcoin是两个使用非交互式零知识证明而达到零知识级私密性的加密货币。

zk-SNARKS虽然具有极高的私密性，但是需要一个可信任的依赖装置来初始化配置参数。Bulletproofs就是一个非交互式零知识证明，其证明简短，同时无需可信任依赖装置的支持机密交易的工具。我们可以基于Bulletproofs来实现虽弱匿名但强机密交易的私密性系统，而且因为证明内容更简短，可以节约更大的存储空间。

Bulletproofs技术可以实现高效的保密的加密货币交易。对机密交易的有效范围证明是斯坦福大学应用密码学小组的一份工作报告。这个项目由Dan Boneh教授负责，还包括来自斯坦福大学、伦敦大学学院和Blockstream的博士生和研究人员。Bulletproofs设计是为了在比特币和其他加密货币交易中实现高效的机密交易而设计的。Bulletproofs基

于Pedersen承诺，为了量子安全，我们可以用ElGamal承诺代替Pedersen承诺，但验证Bulletproofs比验证一个SNARK证明更耗时，需要权衡。

2 共识算法安全

目前主流的共识算法:POW Proof of Work工作量证明，POS Proof of Stake股权证明，DPOS: Delegated Proof of Stake，委托权益证明，BFT Byzantine Fault Tolerance 拜占庭容错算法

2.1 PoW：Proof of Work，工作量证明

比特币在Block的生成过程中使用了POW机制，一个符合要求的Block Hash由N个前导零构成，零的个数取决于网络的难度值。要得到合理的Block Hash需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的Block Hash值，说明该节点确实经过了大量的尝试计算，当然，并不能得出计算次数的绝对值，因为寻找合理hash是一个概率事件。当节点拥有占全网n

2.2 PoS：Proof of Stake，股权证明

POS：也称股权证明，类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。简单来说，就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明POS模式下，有一个名词叫币龄，每个币每天产生1币龄，比如你持有100个币，总共持有了30天，那么，此时你的币龄就为3000，这个时候，如果你发现了一个POS区块，你的币龄就会被清空为0。你每被清空365币龄，你将会从区块中获得0.05个币的利息(假定利息可理解为年利率5

2.3 DPoS：delegated Proof of Stake，委托权益证明

比特股的DPoS机制，中文名叫做股份授权证明机制（又称受托人机制），它的原理是让每一个持有比特股的人进行投票，由此产生101位代表,我们可以将其理解为101个超级节点或者矿池，而这101个超级节点彼此的权利是完全相等的。从某种角度来看，DPOS有点像是议会制度或人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区

块），他们会被除名，网络会选出新的超级节点来取代他们。DPOS的出现最主要还是因为矿机的产生，大量的算力在不了解也不关心比特币的人身上，类似演唱会的黄牛，大量囤票而丝毫不关心演唱会的内容。

2.4 PBFT：Practical Byzantine Fault Tolerance，实用拜占庭容错算法

PBFT是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。将所有的副本组成的集合使用大写字母R表示，使用0到—R—-1的整数表示每一个副本。为了描述方便，假设R=3f+1，这里f是有可能失效的副本的最大个数。尽管可以存在多于3f+1个副本，但是额外的副本除了降低性能之外不能提高可靠性。

2.5 缠结网络Tangle+Pos

Tangle是IOTA的核心技术，基于定向非循环图(DAG)的分布式账本，交易零费用。

我们借鉴Tangle带来的高TPS和零费用特点，但是也要借鉴区块链的高稳定性、具有时间戳的特点，所以我们结合两者来实现我们的目标。

在整个共识角色中，包含交易的交易人、交易验证矿工、对交易验证矿工工作量记账的记账矿工，系统监督者。每个参与系统网络进行交易的用户都进行了PoW来发布交易，因为发布的任何交易都是零费用，所以我们要用户轻微的PoW来限制其突然发布大量的交易；交易验证矿工可以验证交易并提交工作量证明给记账矿工，不过要成为交易验证矿工必须要资产抵押，一旦证明其存在非法或者恶意操作后直接没收抵押的资产。记账矿工基于PoS分布式共识算法来记录交易验证矿工的工作量，采用区块链存储，默认是先提交验证证明的矿工会得到奖励，当然最多不会超过一定N（一个默认值）。当然我们还有监督者，他们时刻关注Tangle网络，如果有矿工恶意操作，就提交证明到记账矿工，一旦发现交易验证矿工恶意操作，就锁定其资产，同时奖励监督者，当然同时也要监督监督者。一个交易需要多少个工作量是可以事先计算出来的，包括智能合约交易，这样我们可以快速的记录矿工的工作量。

对于给矿工的奖励，我们可以在每个特定区块周期来释放一定量的加密货币，然后根据当前周期的总的工作量来统一分配这些加密货币，轻微的通货膨胀。采用这样的方式，我们不仅可以为Tangle网络引入区块高度或者时间戳的概念，同时也保持了Tangle高TPS的特性，而且零费用，又吸引大量的矿工来提升Tangle网络的稳定性和安全性。而且是两级验证，矿工的奖励存在滞后也不影响整个网络的共识。

3 智能合约安全

以太坊发生过硬分差，也发生过智能合约安全漏洞导致的安全事件，损失金额巨大。对于商业应用，智能合约安全性是重中之重。

我们考虑在智能合约中引入Bulletproofs，来提高合约的交易私密性，这对企业应用来说提高其数据的私密性。

同时我们为了避免硬分差，考虑可升级的智能合约模型。智能合约拥有者若需要升级智能合约，必须通过资产抵押来锁定智能合约，而且新的升级合约必须要通过审计才能有效，可以通过成立的基金会或者第三方权威机构来发布审计报告。

我们也考虑兼容ERC20，当前以太坊网络上拥有大量的智能合约资产，可以让这些智能合约可以无缝迁移到当前系统，这也是为未来智能合约跨链做准备。

基金会发布智能合约编写规范，无偿审计智能合约等服务，加速应用部署，保障智能合约安全性。

4 高TPS

我们知道比特币和以太坊经常存在网络堵塞的情况,针对这个情况，比特币引入闪电网络（LightningNetwork）和隔离验证，以太坊也通过状态通道（State Channels）和分片处理（sharding）来解决。

闪电网络和状态通道这两种策略是保持底层的区块链协议不变，尽可能将交易放到链外执行，通过改变协议用法的方式来解决扩展性问题。在这种策略下，分布式账本只是记录粗粒度的账本，而真正细粒度的双边或有限多边交易明细，则不作为交易记录在分布式账本上。

分片处理，总体思路是每个节点只处理一部分交易，比如一部分账户发起的交易，从而减轻节点的计算和存储负担。

虽然通过这些机制可以提升吞吐量，但是真个交易的成本并没有降下来。而我们系统底层采用Tangle网络，理论上可以支持无限的交易。

5 Oracle预言机

当前社会通过数字证书来认证身份，这是一笔巨大的财富，这些通过身份认证的企业可以很方便的把数据发布到系统网络上，完成数据的上链。这对预测、博彩、保险等领域来说有巨大的需求，本系统的零费用+智能合约可以完美支持。后期系统可以考虑更灵活的方式，让系统本身就支持预言机共识(链上预言机共识)，类似Aeternity网络Oracle共识机制，到时候就不会局限于数字证书身份认证的第三方企业才能上链。

6 应用

6.1 电商+供应链

互联网电商冲击了传统零售业，带给大家购物更多的选择、物廉价美的产品、快捷物流体验，但是也带来了产品可能存在假冒伪劣等问题和消费者个人数据信息泄露风险。

源头厂家或企业可以通过智能合约把产品资产发布到本系统上，整个交易可以是私密交易，这样消费者可以通过该交易的合约来验证是不是源头厂家或企业发布的资产合约。通过这样，我们可以一定程度上避免假冒伪劣产品，但无法完全杜绝中间存在商家把真实产品替换为假冒伪劣产品的情况。但是如果一旦发现是假冒伪劣产品，我们可以通过一步一步的交易溯源找到不诚信的商家，而且源头厂家或企业在交易的时候，每个产品资产都具有惟一标识符或惟一产品批次，在每次交易流转中消费者可以要求商家必须提供该证明信息（该信息被商家和消费者共享），这样更容易溯源，甚至可以在智能合约交易中实现该功能，不过存在商家泄露交易数据的风险。

在整个交易过程中，如果采用私密性合约，则数据只有在商家和消费者共享，交易数据得到保护，这就是与现有电商平台的显著区别，而且费用成本低廉。如果有物流，为了保护消费者的个人信息，我们甚至可以考

虑通过每次交易的随机网络电话和随机门限密码来保证物流不会泄露电话和姓名等信息，不过会给物流人员和商家泄露收货地址信息。

我们可以提供应用系统，来帮助源头厂家或企业–代理商–中间商–零售门店或超市–消费者。基于本系统，实现电商+供应链一体化整合，对商家或消费者来讲，数据安全、可靠、便捷；对整个社会来讲，增加假冒伪劣成本，帮助消费者和做好产品的厂家或企业。

除此之外，因为系统是开放的，而且零费用，很多商家可以把本系统和商家自己的业务系统整合，提供更丰富的服务。

在电商中，特别是社区电商还有巨大的潜力可以挖，比如外卖或者就近的社区消费，对消费者来讲是高频消费；商家对这类系统也有很高的需求，评论等数据都在链上，无法篡改，杜绝缺少商业诚信商家。优惠券等。

6.2 企业级应用系统

现有商业社会的数字证书，权威的机构数据上链。

个人的所有数据都可以上链完成自我证明，比如身份信息，权威机构数据加密后上链，当验证的时候当事人只要出示数字身份，然后输入个人的助记词密码，就可以获取个人信息，验证。

公共服务都可以上链，减少公共服务支出，提升服务的便捷性和公共开支。

6.3 物联网

本系统具有零费用+智能合约特点，物联网、车联网等行业的应用很多场景。

智能终端嵌入微钱包应用可以微支付，车辆行程数据和维修数据可以记录到系统中，可以通过系统传递消息等等。

6.4 征信

证明数据的真实性，智能合约的安全多方计算、同态加密等技术来证明数据或者协助多方计算等等。

6.5 供应链应用

食品安全与溯源

供应链金融

7 攻击预防

8 项目更多规划

成立基金会，维护该项目，创造社区，打造生态链。
原子交换
哈希时间锁定
跨链
Oracle预言机

参考文献