一种高性能智能合约系统

邹远春

归档于 2018 年 6 月 2 日

目录

1 摘要

区块链去信任化和价值传输的特性，让我们可以重构整个社会体系内的生产关系，从而促进生产力的发展。现阶段我们都还在完善基础设施，随着大量的优秀人才涌入，区块链底层技术在快速更新迭代，我们需要更安全可靠、更高吞吐交易性能的区块链系统来应对企业级市场的挑战。

Arsenal 是新型的区块链底层公有链，参考目前行业最前沿的技术方案，在安全性、私密性、共识算法、智能合约等方面微创新，以解决安全可靠与高吞吐量等核心问题。

2 密码学安全

现代公钥密码学算法的安全性建立在解决某些问题的困难性假设基础上的。比如 RSA 公开秘密算法是基于大数分解困难性假设设计的；ElGamal 加密算法是基于离散对数困难性假设设计的；还有现在在区块链密码学安全领域最流行的椭圆曲线密码学，依赖于被广泛承认的解决椭圆曲线离散对数问题的困难性上。但是随着量子计算机的出现，利用量子计算具有的天然并发性，使得原来在电子计算机环境下的一些困难问题，在量子计算机环境下却成为容易计算的。

目前可用于密码破译的量子计算算法主要有 Grover 算法和 Shor 算法。对于密码破译来说，Grover 算法的作用相当于把密码的密钥长度减少一半。而 Shor 算法则可以对目前广泛使用的 RSA、ElGamal、ECC 公钥密码和 DH 密钥协商协议进行有效攻击。

Arsenal 考虑到抗量子计算的迫切性，考虑引入基于格密码的抗量子计算密码及数字签名方案，比如 **NTRU**。NTRU 是来自 Security Innovation 的基于格的公钥密码系统，是 RSA 和椭圆曲线密码学（ECC）的领先替代品，因为它具有更高的性能和抗量子计算机攻击的能力。NTRU 于 1996 年发展成为二十一世纪网络安全挑战的远见解决方案。NTRU 基于一个称为“近似格向量问题”的数学问题，包含三种算法：NTRUEncrypt、NTRUMLS 和 PASS。它已在学术期刊上发表过，并在 Crypto、Eurocrypt 和 RSA 上发表过，并已被 IEEE 和 X9 标准采用。同时考虑到引入 NTRU，会导致存储膨胀，所以 Arsenal 考虑的是优先采用现有的椭圆曲线算法，但同时支持 NTRU，以便未来的合适时机完整迁移到 NTRU 解决方案上。另外，在加密散列算法方面，Arsenal 会采用第三代安全散列算法 SHA-3。

3 UTXO 与 Account 模型并存

智能合约大体可以分为三类：

- 数字或原子资产合约
- 存储状态的状态合约
- 其它的无存储状态的计算合约

UTXO 出自比特币，适合用来表达可以转移的数字或原子资产，我们采用 UTXO 模型来表达数字或原子资产合约，一是可以提高交易的并发度；二是可以让数字或原子资产更安全，杜绝以太防账户模型所存在的数据溢出或者其它各种漏洞导致的资产无故增发等情况。

Account 模型与以太坊一脉相传，参考以太坊的 MPT 树实现的链下存储，除了在世界状态处理上。因为以太防 Account 模型对每一笔交易都会改变世界状态，但是在现实世界中很多交易是没有相关性的，所以我们在共识算法中会有合约冲突的仲裁，实现分区，提高整个系统的吞吐量。

4 底层存储数据结构

为了实现分区，提高吞吐量，我们底层存储采用 DAG 存储结构，但每一个区块同链式存储结构主体保持一致。

5 共识算法

共识算法是区块链网络的核心，保证系统散布在网络各个参与节点的账本数据保持一致，通过多方博弈协作和有效的机制设计来构建一个安全可靠的点对点价值传输网络。

以太坊网络类似一台超级全球计算机，通过世界状态保持一致，就像一台单进程单线程的机器，为了提高性能与吞吐量，我们可以改变世界状态机制来改进单线程模型为多线程模型，因为在某一时刻很多交易是不冲突的。

Arsenal 把所有节点分为两层，下层是挖矿层，节点根据自己的工作量证明和身份信息分到特定的组里，这些信息会写入区块来年。每个组挖矿，然后提交到自己所属的上层的公证层。公证层有多个公证组，每个公正组对应于下层的一个挖矿组。系统在某一时刻会根据公证主链的参数 +VRF 选中某一公证组来对下一个区块链组签名，它在一个周期内收集其它公证组传来的区块，然后简单的验证有没有双花和状态冲突，然后根据优先顺序解决冲突，写入区块签名并广播给其他所有公证组。公证组再负责与各自的挖矿组交互，有必要通知下面的挖矿组哪一个块是无效的以及同步最新的区块信息。

挖矿组负责智能合约执行和简单的双花判断，公证层主要是负责双花

判断和冲突仲裁。虽然是 DAG 结构，但是其中有一分支链即公证链主要用于记录公证组的公证结果，同时基于 VRF 来选择下一个公证组。

整个设计符合 AFK 扩展立方体架构风格。

6 隐私

很多非常私人或者敏感的信息是不能公开存储在公有链上的，比如我们想保证交易的匿名性和保密交易，**匿名性**是隐藏交易双方的信息，**保密交易**是隐藏交易中的金额。**零知识证明**提供了可用于构建隐私保护机制的基础，证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。

目前在隐私保护方面主要是基于 zkSnarks 来实现，但它需要一个可信任设置过程。Arsenal 采用 Bulletproofs 来实现保密交易，它是斯坦福大学应用加密小组（ACG）最近发表的一篇论文，Bulletproofs 技术是不需要任何可信设置的简短非交互式零知识证明，实现对保密交易的有效范围证明，每笔保密交易都包含了一个验证交易有效性的加密证明，从而可以隐藏一笔交易中的金额。

Arsenal 关注区块链隐私技术的最新发展，zkStarks，一种更透明的零知识证明技术，解决了 zkSnarks 的主要弱点之一：需要可信设置过程，并且能更好抵御量子计算机的攻击。通过对它的支持，Arsenal 可以支持更多看重隐私的应用场景。

7 兼容 EVM

以太坊智能合约是图灵完备的，其上有大量的资产，通过考虑兼容 EVM，来方便迁移。但同时我们也要改进，一是改进浮点数计算；二是加入去中心化密码学安全的随机数生成协议，从而支持更丰富的应用场景。

8 企业级应用市场

在企业级应用市场，除了考虑高吞吐量，还考虑到合约安全与交易成本问题等等。

- 实现合约的形式化验证

- 链上合约可升级治理协议
- 考虑前期在交易手续费上实现“零费用”
- 支持 Cosmos 跨链协议，把区块链价值传输价值最大化，后期考虑实现基于 Cosmos 协议的跨智能合约调用
- 开发 Arsenal 的闪电网络，实现更快捷的微支付，可以应用于物联网、内容平台等更多支付场景中
- 对预言机 Oracle 支持，作为现实世界与区块链交互的入口，引入外部世界状态信息
- 实现去中心化的密码学安全的随机数生成协议