

**网络安全通用原理论文报告**

**论文名称： Arbitrum: Scalable,Private smart contracts**

**教师姓名： 魏松杰**

**学生姓名： 林宇飞**

**学 号： 118106021939**

**成 绩：**

**学 期： 2018年下学期**

Arbitrum:一种具有可扩展性和隐私保护的智能合约技术

1. **研究背景**

智能合约的概念可以追溯到1994年，由Nick 提出，但直到2008年才出现采用智能合约所需的区块链技术，而最终于2013年，作为以太坊智能合约系统的一部分，智能合约首次出现。

什么是智能合约？智能合约作为区块链的一部分，允许我们在不需要第三方的情况下，执行可追溯、不可逆转和安全的交易。

以太坊则是目前为止最引人注目的智能合约框架，因为它是专门为支持智能合约的使用创建的。可以用Solidity语言编程，以太坊智能合约框架有助于促进去中心化网络，便于用智能合约处理交易。

1. **面临的问题**

以太坊是第一个支持图灵完备有状态智能合约的加密货币，但它在可扩展性和隐私方面存在限制。

* + 1. 验证者困境

工作量证明挖矿会对出矿的矿工给予奖励，而负责校验的矿工则没有任何收益。这在一般的交易场景下没有问题。但是如果涉及到比较复杂的智能合约，验证矿工就面临一个两难的选择：1.老老实实地完整执行脚本会白白浪费宝贵的算力，在下一区块的竞争中输在了起跑线上；2.不进行校验而直接将块加到链上，节省了算力，但是有站错队的可能，在后续的竞争选择了一个错误的起点。

* + 1. GAS限制

我们都知道以太坊上执行合约需要GAS，智能合约执行过程中所包含的计算资源和存储都是通过GAS来衡量。而每一个区块都有GAS大小的限制，因此在以太坊上无法执行大量计算和存储的算法。总之，以太坊的生产力被限制在单个挖矿机器在一个区块所能执行的代码步数上。

* + 1. 隐私问题

以太坊要求智能合约的执行需要每一个矿工验证，缺乏隐私特性。

* + 1. 孤块率问题

在非分片的基于工作证明的区块链中，更长的块执行时间会导致更高的孤块率，虚拟机的执行效率确实是一个瓶颈。在未来的系统中，复杂的运算也会继续使整个系统效率低下。

1. **Arbitrum介绍**

论文介绍了Arbitrum，这是一个执行智能合约的新平台,能够解决上述问题，t同时比以往的解决方案具有更好的可扩展性和隐私性。因为Arbitrum与底层的共识机制是无关的，所以对上述问题的解决方案可以在任何现有的共识机制中使用。

Arbitrum允许用户创建虚拟机，并指定管理者，同时将虚拟机的特征记录到智能合约上。虚拟机的参与者（包括用户和管理员），可以发送和接收资金和消息，以及执行计算，并根据代码离线存储数据。与执行智能合约的传统方法相比，仲裁vm更具有可扩展性和私密性。Arbitrum几乎完成了vm脱机的所有管理工作并确保了正确的执行。为了实现这一点，当有人创建一个Arbitrum的 VM时，他们会选择一组管理人员，他们将负责VM的执行。Arbitrum保证只要有一个诚实的管理人员就能确保VM正确执行(即使其他所有管理人员都密谋作弊)。而且由于几乎没有任何关于VM的数据被放到链上，Arbitrum VM比许多其他系统更加具有隐私性。

Arbitrum的大致流程与TrueBit相似，TrueBit是一种以太坊的链下扩展方案。流程如下：

1）用户（下文称为Task Giver）上传需要执行的代码（下文成为任务），并提供佣金。

2）链外第三方（下文称为Solver）发现这个任务，认为佣金可以接受，执行计算任务并答公示运算结果，同时提供一笔保证金。

3）另外的第三方验证者（下文称为 Verifier）重新执行任务，如果发现Solver造假，可以发起挑战，同样需要提供一笔保证金。

4）通过链上的智能合约让Solver和Verifier玩一个验证游戏（ verification game），通过Task Giver在链上提供的执行代码验证答案真伪，提供正确答案的一方获取佣金，造假的一方从保证金中支付整个验证过程所需的gas。

5）如果一段时间内没有人能提供证据证明Solver造假，Solver获得佣金。

相比于TrueBit，Arbitrum没有将代码和数据上传到链上，而是利于Arbitrum系统所设计的虚拟机，所需执行的代码全部上传到虚拟机上，对代码的每一步执行取hash值，最后以merkle树的形式将根节点的hash值存储于链上，以此保护数据的隐私性,当某一为虚拟机的管理员对其他管理员上传给verifier的hash有异议，则采用bisection协议来处理，对恶意上传虚假hash的一方进行处罚，而成功dispute的用户将得到奖励。

另外，Arbitrum所设计的虚拟机还有信息和收信箱的功能，VM可以通过两种途径收到信息。一种是用户可以通过一种特殊的通信格式的交易将消息上传到区块链上。虚拟机通过链读取信息。另一种是虚拟机可以通过send指令将消息发送给其他的虚拟机。任意一个虚拟机都包含有一个收件箱，同时收件箱的hash需要提交给verifier作为虚拟机的状态。

1. **背景和相关技术**
   * 1. Refereed Delegation

代理计算协议是指用户将需要大量计算资源的程序代码委托给代理服务器，代理服务器数量为两个以上，等服务器计算完成后将结果返回给用户，如果它们的计算结果不一致，则它们采用二分协议进行判断谁的结果才是正确的。

* + 1. Ethereum

以太坊是支持全状态和支持图灵完备编程语言的区块链平台。但是由于以太坊本身的共识算法和智能合约的设计上的限制，使得以太坊缺乏可扩展性和隐私性。

1. **以太坊上的其他解决方案**
   * 1. zkSNARKs

Hawk是一种使用zkSnarks来解决智能合约隐私性的系统。Hawk有很强的隐私保护能力，但是仍有一些缺陷，例如Hawk的隐私性依赖于可信的第三方，第三方能够看到隐私数据。

* + 1. Incentivised Verfication（TrueBit）

TrueBit使用流程与本文提出的Arbitrum类似，能够解决一些可扩展性的问题，但是缺乏隐私保护的功能。

* + 1. Plasma

Plasma是一种跨链技术，子链因为采用了不同的共识算法，相比于以太坊能够更快的实现共识，完成交易打包，再将每一个区块的hash作为一笔交易提交到以太坊的主链上。以此来提高交易的打包速度。但是当协议出现问题时，需要花费很多资源来解决。

* + 1. State Channels

状态通道能够使链下交易达成一致，但是当协议出现问题，需要花费很多资源来解决纠纷。

1. **总结**

目前以太坊上的大部分研究工作都是对共识层进行改进，本文所研究的对象是在智能合约层，通过对这一层的来进行改进。另外，目前以太坊的最大的瓶颈是交易速度问题，plasma和状态通道都是通过链下交易来提高以太坊的交易速度，侧重于解决TPS。本文所提出的Arbitrum的侧重点相对有点不同，Arbitrum是在TrueBit的基础上进行了创新，重点在于解决单笔交易gas限制问题和合约的隐私保护问题。本文在解决隐私保护的同时，也导致了一些问题，由于出于隐私保护的目的，合约数据存储于Arbitrum 的VM中，当VM的代理服务器出现问题，合约数据也会受到波及。

目前该项目仍在开发中，尚未公布开源代码及完整的方案。