**R3发布Vitalik Buterin以太坊报告（全文下载）**

2016-06-03 10:01



暴走时评：R3CEV最近发表了一篇以太坊创始人Vitalik Buterin的报告，40多页的文字详细分析了以太坊架构的技术构成和在金融业的应用，以及金融机构用它搭建私有区块链的方法和潜在问题。这份报告是以太坊创始人对初创企业咨询的回应，他承认目前以太坊还需要技术升级，因此开发团队还在完善相关技术，并为大家尤其关注的区块链扩展性和隐私性提供了两个可选的解决方案。

翻译：Annie\_Xu

R3CEV发布最新报告评估以太坊对银行成员和私有区块链倡议的意义。

该报告由以太坊创始人Vitalik Buterin执笔，40多页的文字详细分析了以太坊架构的技术构成和在金融业的应用，同时分析了金融机构用它搭建私有区块链的方法和潜在问题。

有些人可能不习惯白皮书一样的密集文字，R3首席科学家Richard Gendal Brown和战略主管Kathleen Breitman为他们提供了简洁的概述，介绍了该报告的目的，为非技术型读者提供了高水准的信息。

关注微信公众号“区块链铅笔Blockchain”，回复关键词“以太坊2”，即可查看下载本报告全文。

R3研究主管Tim Swanson描述，发表该报告是因为初创企业获得银行的大量信息咨询请求，是为了满足他们对以太坊和智能合约等新颖特性的好奇。

Swanson把这个报告看成R3深化共有区块链探索的标志，尽管它还是有智能合约平台Corda这样的不同解决方案。

“报告的想法是追踪平台的发展脉络，拨开肤浅的表象。这些平台不是为了受监管的金融机构而开发的，但那并不是说一定要一成不变。我们一直都是按部就班的”。

Swanson和Breitman纷纷表示该报告标志着R3的思想领袖地位，统领了一群致力于解决区块链技术应用潜在问题的团队。

Brown也表示认可，把以太坊描述成“骄人的成绩”，可以作为其他基于区块链的解决方案的榜样。

同时他警告，金融机构把这个用途广泛的以太坊技术融入传统金融的过程中可能会出现很多问题。

挑战升级

该报告的重要意义在于以太坊创始人Buterin为金融服务公司利用以太坊平台的方式提供了特殊注解。今年1月份R3在11家主要银行中主导了一项测试。

Buterin在报告中提出以太坊平台的可扩展性是主要问题，尽管很多创新者都在为之努力。因此他呼吁机构参与到以太坊的完善计划中。



Vitalik Buterin

Buterin在报告中重点建议各机构调查“state channels”——一种在主要区块链以外完成高容量以太坊交易的技术；在基于区块链的系统中分步骤实施数据库分片。

“关注可扩展性的机构有两个方案：一个是在state channels中搭建尽可能多的应用逻辑，无论是私有还是共有链；第二个是在私链版以太坊中实施EIP105，结合异步编程和分片机制，实现可并行性”。

但是只有Serenity发布后才能在以太坊区块链上实施这两者方案，之后紧接着发布Metropolis升级版。但是它们的具体发布日期没确定。

然而Buterin说机构可以在私有版技术中实施预设的特性，尽管以太坊开发团队还在完善这些特性。

Buterin进一步解释了为什么现代的区块链平台架构会有这些固有问题。

”区块链的独特之处在于它的去中心化有与众不同的特质；在不同参与方之间的分配意义上讲，它不是分布式的，而是复制的；该网络所有节点完成一笔交易，并共同维护区块链的状态“。

隐私性有所改善

Buterin还以隐私性为重点，金融业人士共同思考这个问题之后，它成为人们热烈争论的问题。

专家争论现在的区块链环境不符合联盟的探索需求，因为这种方式需要银行共享商业敏感数据。

然而Buterin指出私有区块链不是隐私性的解决办法，但是区块链天生就是数据共享和管理的理想系统；只是实际应用过程存在固有缺陷。

”如果你的首要信息安全焦点是隐私性，你对state channels这样的先进加密技术或较为复杂的加密经济机制不感兴趣，那与其用区块链，你还不如选择服务器“。

Buterin断言面临这个挑战的私有区块链开发者有两个选择；一是尽可能隐藏区块链中共享信息的链接，其二是开发提供数学可证隐私性的高级方案。

他接着表示积极探索解决方案的人可能面临创新思维的挑战。

但是Buterin对以太坊解决这些问题的潜力表示乐观，因此才向人们阐述以太坊的大容量和复杂性。

”以太坊2.0和3.0的长期目标是让该协议可以达到Visa那样的交易量，甚至用这个手提电脑端运行节点的庞大用户群来完成更高的交易量“。