

学院首页 > 区块链教程 > 新手入门 > 深入浅出比特币交易 (transaction)

深入浅出比特币交易 (transaction)

等一轮残月 管理员 船龄 7.1年

2016-03-02 09:55:00

来源 巴比特论坛

👁 19544

💬 0



如果你接触比特币够久，你一定听说过比特币是个区块链，一个区块里包含很多交易，而交易都是链在一起的。那么，具体交易的细节如何？通常的技术文档都充满了术语，即使是中本聪的白皮书也难以直接联系实际，我最近又仔细研究了一下，这里用一种简单的比喻来解释下

比方说你的钱包里有三个地址A，B，C。你在地址A有1个币，你在钱包软件里把币发送到地址B，可以在区块链上查到这笔交易，不妨叫做交易甲。然后你又做了一笔交易乙，把币从地址B发到地址C。假设手续费是0.0001个币，每次发送你都花了0.0001个币作为手续费，那交易甲被确认后地址B就是0.9999个币，而交易乙被确认后地址C里就是0.9998个币

交易甲：地址A 1BTC -> 地址B 0.9999 BTC，手续费 0.0001
交易乙：地址B 0.9999BTC -> 地址C 0.9998 BTC，手续费 0.0001

用账簿的比喻最好理解

账簿就是区块链，账簿的每页纸就是区块，这些纸依次装订在一起形成了一整个账簿。每页纸上贴满了一条又一条的汇款单（交易）

如果仔细观察汇款单交易乙（把0.9998个币从地址B转到地址C，并付0.0001手续费），你会发现交易乙是由两大部分组成，前一部分可称为付款信息(input)，后一部分可称为收款信息(output)

按一般在银行填汇款单的习惯，付款信息里该填支出账户名（也就是地址B）和账户所有人签名（授权交易），而收款信息里应该填金额和收款方账户名（也就是地址C）。事实上，比特币交易也大致是这么写的，只有细微差别

交易甲

付款信息： 签名 + 公钥A（签名相当于盖章，是用地址A的私章（私钥）产生，而地址A的公钥可用于让其他人验证这个章是否有效（私钥公钥加密原理到处都有））

收款信息： 0.9999（金额） + 地址B + 兑现条件（这里的兑现条件注明了未来要花地址B的币需要满足何种条件，下面有详述）

交易乙

推荐教程

BTSX新手教程三：给信任的受托人

1、点击“代理” 2、左边是工作中的受托、候选受托人，名单太多找不到你要投票的受

大地币TRC新手挖矿教程

比特币的相关名词解释

qtum量子链POS挖矿教程

什么是比特币脑钱包、纸钱包？

如何注册比特币网络钱包Blockchain

比特币交易网 - 转币提现指南

从零构建基于以太坊（Ethereum）

什么是“双重支付”问题，怎样解决

比特币交易平台BitStamp介绍

收款信息： 0.9998 + 地址C + 兑现条件

交易丙

付款信息： 签名 + 公钥C

收款信息： 0.9997 + 地址D + 兑现条件

有几点和银行汇款单不同的地方

- 第一，每个汇款单都是花前一个汇款单的收款地址里的币，这样所有交易就一个个链结在一起，而如果要彻底核实某笔交易丙是否有效，就要顺着这个链一直回溯到最原始的挖矿产出交易（在交易甲之前还有别的交易），这样保证了只要用户有区块链的完整拷贝（也就是目前全节点的那60G数据），就可以独立验证任何一笔交易的有效性
- 第二，每次汇款只能完全将支出账户里所有的币都花掉。以交易乙为例，汇款完成后原来的地址B就空了。如果只想转一半的资金到地址C，剩下的那一半就要在收款信息里另外填一个账户地址E，也就是所谓的找零地址
- 第三，总汇款金额小于地址B的部分就是手续费。如果地址B里有0.9999个币，汇款到地址C的金额是0.9998个币，那中间的差额0.0001就是矿工的手续费
- 第四，验证交易乙是否有效，是靠上一个交易即交易甲的收款信息中的兑现条件来保证的。可以有多种规则，目前最常见的两种就是提供收款地址的签名（P2PKH）以及提供一段程序的哈希值（P2SH，这个涉及到哈希，一种防伪的手段）


如果你完全看懂了，那你对比特币交易的功能理解，就接近于core程序员的水平了，以后碰到很多名词如scriptSig（签名+公钥）和scriptPubKey（兑现规则）之类你就很容易知道那都是汇款单上的哪个部分了

这里还有个较为复杂的概念即签名，我另外单独发文分析，这个签名和最近的火星文隔离见证有密切关系

全部 最佳

请发表你的真知灼见（不少于5个字）...

发表评论



巴比特学院是巴比特旗下的教育培训品牌，由巴比特主办，与专业培训机构合作，邀请业内区块链专家和实践者作为培训导师，通过导师现场授课、行业高端论坛、企业调研走访等方式，打造国内一流区块链培训品牌，推动区块链在中国的发展与创新。2018年，巴比特学院的品牌影响力将向杭州以外的北京、上海、南京、成都、深圳、广州等地辐射。

关于我们

关于巴比特

使用条款

版权声明

品牌素材

联系我们

联系人：学院课代表

微信：btczs001

地址：杭州市西湖区西溪首座

扫码咨询

