NEW

① 风险提示: 防范以"虚拟货币""区块链"名义进行非法集资的风险 —银保监会等五部门

你好,UJ216FBL退出登录

答讯▼

快讯

视频 ~

学院 ▼

产业区块链

海盗号

更多 图市日

搜索...

Q

命 学院首页 > 区块链教程 > 技术讲阶 > 深入浅出比特币签名 (1)

深入浅出比特币签名(1)

等一轮残月 管理员 船龄 **7.1年** 2016-03-02 09:59:00 来源 巴比特论坛 ⊚ 31169 ⊙ 0

在上次的帖子 http://8btc.com/thread-29595-1-1.html

里大概说过,比特币的交易就是如下形式的汇款单,一半是付款信息,给出付款签名和公章,另一半是收款信 息,给出金额,目标地址和兑现方式

对各个会计(全节点)来说,接收到这张汇款单时,有两个最重要的安全问题:

第一, 如何保证这张汇款单不是假的?

第二,如何保证汇款单上的签名不是假的?

事实上,比特币里第一个问题是保证不了的,也即如果两张不同的汇款单的签名都符合要求,你不知道哪个是真 的,这就是大名鼎鼎的据说导致了MTGOX倒闭的交易延展性问题 (transaction malleability)

不过,交易一旦确认,也就是记录到账簿以后,付款账户就是空的了(比特币每次都是将一个地址中所有的币都 花掉),所以从已确认交易的角度来说,不可能出现重复花一个地址的币的交易,这两张汇款单中必然有一张最 后要报废

为什么会出现两张不同的汇款单都有效的情况?这是比特币目前设计上的一个缺陷,是一个历史遗留问题,在我 下一篇文章中进一步讨论到签名细节的时候,就可以明白为什么了。但现在先看第二个问题,也即签名的安全保 证,只有先搞明白这个,才可以回答第一个问题

签名简单比喻来说就是盖章

比特币中用了一种方法:刻一个章摔成两半,一半私用,一半公用,私用的一半自己留着用于交易的时候盖,而 公用的那一半章(公钥)则在交易时付款信息里盖在空白处并随汇款单发送。公章里暗含有我要花的币的地址 (下面有述)。这样,收到汇款单的人只要看到我发布的那一半公章(公钥),就可以验证是否符合我要花的币 的地址,并且可以用来和我盖的那一半私章对比,如果中间的裂缝在显微镜下也完美吻合,就证明私章是我盖的 无疑,但他们却拿不到我的那一半私章(私章盖在文字上以后有很多部分和文字重叠而无法辨认了,无法仿造出 来),这样我不担心有人会拿着我发布的那一半公章来假冒我授权的交易

当然,也可能会有解密高手(量子计算机)试图就我发布的公章而假造一个每个裂缝都与之完美吻合的私章(也 就是通常所说的破解ECDSA椭圆曲线加密)。但如果我不花币,也就不用发送交易,那么别人光知道我的地址, 却不知道公章是什么样子的,也就无从破解(公钥可以推出地址,有地址却不能推出公钥)

为什么知道地址却算不出公章呢?因为地址是通过计算公章里所有字的总笔画数产生(哈希算法)。可以想象: 假设一个公章包含几百个字,光知道所有笔画的总数是完全无法知道公章是什么样子的,而有了公章却可以轻松 验证这个总数是否符合。而这个总数就是比特币中的地址(这只是个简化的例子,实际的哈希算法要复杂的多, 不是算总长度,但原理类似,都是对某串文字算出一个唯一的数)

之前说过,比特市转账每次都是彻底把原来账户中的市全部转走,因此只要我不重复使用同一个章,用完就扔 就不用拍小别人拿到我的公音后能干啥,如里高手不能很快的在我发布交易后根据里面的公音管出私音

凸点赞0

☆3次收藏 ペ分享 推荐教程

什么是DAC (简版)

DAC也许是自比特币诞生以来, 出现的一 的概念,而且在未来,我们相信DAC将会3

比特币搬砖常用充值工具及交易网站

如何使用比特币交易平台OKCoin的

怎样保护与备份比特币钱包?

Bitshares X的市场操作和交易引擎

科普 | 简介不同类型的以太坊钱包

比特币的交易过程是怎样的?

Hyperledger Fabric Chaincode 3

精通比特币 - 第8章 区块链分叉、矿

喵懂区块链18期 | 中心化魔鬼or 扩彩



下一篇: 深入浅出比特币签名 (2)

这就是为什么资深比特币玩家总是建议大家不要重复用同一地址,这是系统安全的最高级保障,有了这一点,即使量子计算机出现,比特币的交易也是安全的

了解盖章和数总笔画数这两个概念后,就能理解比特币如何保证签名的正确性了:首先,地址就是公章里包含的总笔画数,如果总笔画数和公章对不上,公章就是无效的,通过这个办法可以保证公章的有效性。其次,公章只是一个章的一半,如果公章和私章的合缝对不上,仍然是无效的

联系上面那幅图, 再看交易就好理解多了

交易甲

付款信息: 签名 + 公钥A

收款信息: 0.9999 + 59 (地址B) + 兑现条件

交易乙

付款信息: 签名 + 公钥B

收款信息: 0.9998 + 地址C + 兑现条件

整个过程是: 乙自己刻一个章B, 摔成两半, 一半是私章(私钥)B, 一半是公章(公钥)B, 然后他数了数公章B里包含的总笔画数, 得出个数字59, 也就是地址B, 然后他把这个数字告诉甲, 让甲给他发0.9999个币

于是甲发布了交易甲,收款信息里按照乙给他的地址59填入,兑现条件里写明按标准盖章方式验证。随后交易甲被会计审核通过,比特币总账簿里就记录了这笔交易,大家都可以查区块链看到,地址59包含0.9999个币的余额

可见,要查地址B有多少币,是通过查交易甲的收款信息而查到的。含有币的地址叫UTXO,也即unspent output (未花交易)。在比特币中凡见到UTXO,就知道是指含有资金的地址信息,也是一串交易的最终一站

随后, 乙想要花这个币的时候(交易乙), 他就在交易乙的付款信息里空白处盖上地址B的公章, 并另外写一串数(这串数后面解释), 并在这串数上盖上他的私章

交易乙

付款信息: 一串数上盖私章 (签名) + 公章B (公钥B)

收款信息: 0.9998 + 地址C + 兑现条件

公章B里的总笔画长度是59,和地址B相同,可证明乙是地址B的公章拥有者,然后乙在那串数上盖的私章的裂缝和公章又完全吻合(会计通过把他发布的公章盖回到那串数上,以验证两者之间的裂缝是否完全吻合),证明他的公章是他自己的,这样比特币中的付款安全验证就完整了

总结一下:由地址不能得到公章,而由公章也无法得到私章(现有技术下),因此用私章盖章,用公章验证私章的有效性,同时数公章中的总笔画数可验证和地址相符,这就完全保证了用私章盖章者是该地址的所有者,也就是签名的有效性

上面说到,盖章的时候是盖在一串数上(图中的12345),这是串什么数?这是整个比特币交易中最复杂的部分,下次再说



△ 点赞 0

☆3次收藏 ペ分享

下一篇:深入浅出比特币签名(2)

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



Copyright © 2011-2020 · 巴比特 · 署名-非商业性使用-相同方式共享(BY-NC-SA 3.0 CN) · 浙ICP备14013035号-8 · 🚇 浙公网安备 33010602002085号 · 站长统计 · 文章存档



凸 点赞 0

☆ 3 次收藏 ペ分享

下一篇: 深入浅出比特币签名 (2)