大家好，今天来为大家分享比特币 商家支付的一些知识点，和比特币支付功能的问题解析，大家要是都明白，那么可以忽略，如果不太清楚的话可以看看本篇文章，相信很大概率可以解决您的问题，接下来我们就一起来看看吧！

本文目录

1. 比特币如何解决“双花”问题？
2. 比特币要怎么交易
3. 比特币成为萨尔瓦多法定货币之一，它能满足这个国家的日常支付需求吗？
4. 什么是比特币收款账户

比特币如何解决“双花”问题？

什么是双花

双花就是同一枚比特币被使用两次，但是无论在比特币网络中还是现实世界都不可能发生，就像在现实中你不能用1块钱买个苹果，又用同一张1块钱买橙子。如果这都可以的话，钱就变得毫无价值了，因为这样每个人都会拥有无数多的钱，用也用不完，货币价值也就没有了。比特币核心网络在比特币区块链中验证每笔交易来防止双花。

那比特币网络如何防止双花呢？

假如你有1个比特币，你想要花两次。于是你向商家买了价值1个比特币的商品。然后，你再在另一个比特币地址上签名，并发送相同的1个比特币。

两笔交易都进入了还未进行验证的交易池。你的第一笔交易得到了确认，并在下一个区块中得到了矿工的工作量验证。但是矿工会认为第二笔交易是无效的，这样就没办法获得足够的确认，就会被撤出网络。

但是如果这两笔交易是由矿工同时操作呢？

当矿工同时从池中提取交易时，获得网络中确认数量最大的交易将会保留在区块链中，而另一个将被撤出。也有可能真实的那笔交易无法获得确认。这就需要6次确认机制。“6次确认”就是在这笔交易被添加到区块链之后，另外6个包含多个其他交易的区块就会被添加到这个区块之后。每一个都需要“6次确认”，且都和前一个区块有关联。所有这些确认和交易都在加上了时间戳，这就使得区块不可逆转，而且无法篡改。

而当你掌握的算力超过50%时，就可以无限逆转区块。但是有些区块链网络已经非常之大，想要和它对半抗衡是不可能的，但有一些区块链网络比较小，节点比较少，也有可能遭遇51%算力攻击，今天的BTG就是一个例子。

那名矿工为了实施双花攻击，获得了至少51%的BTG网络算力，就能够临时控制BTG区块链。像BTG这样的小型网络上，获得这么大的哈希算力也是非常费钱费力的，但是无利不讨好嘛，实施双花之后就有钱可赚了。

控制了网络之后，攻击者开始往加密货币交易所充值比如1000个BTG，让其进入市场，或者提现出来。再运用手中的算力，从自己对外付款交易之前的区块开始，忽略自己所有对外的付款交易，重新构造后面的区块，利用算力优势与全网赛跑，当最终创建的区块长度超过原主分支区块，成为新的主分支，至此，攻击完成；结果就是，由于撤销了所有对外付款交易，等于收回来所以已卖掉的BTG。就这样，他们能够向交易所充值后再迅速收回资金。

比特币黄金开发人员建议交易所在用户交易时通过确认交易数量来应对攻击。区块链数据表明，攻击者成功逆转了22个区块，这导致开发者建议将需要确认的区块提高到50个。

比特币要怎么交易

在交易平台上进行比特币的交易，你需要在交易平台上注册一个账户，完成实名认证，绑定银行卡即可进行比特币的买卖活动，国内比较知名比特币交易平台有easybtc、比特币中国、火币网。当然，还有一种就是使用比特币购买商品或服务，全球有许多接受比特币付款的商家，例如巨头公司戴尔和微软。比特币之家有关于接受比特币付款公司和商家的更多报道。

比特币成为萨尔瓦多法定货币之一，它能满足这个国家的日常支付需求吗？

每天会有一群人蹲超市里面，一个个盯着手机，什么时候比特币上涨了，赶紧买东西付款，一旦下跌不停就回家里蹲着，等下一波。如果崩盘了就一起换个政府

什么是比特币收款账户

比特币收款账户一般就是比特币钱包地址。比特币地址就像一个物理地址或者电子邮件地址。这是别人付给你比特币时你唯一需要提供的信息。然而一个重要的区别是，每个地址应该只用于单笔交易。比特币钱包大致实体钱包在比特币网络中的等同物。钱包中实际上包含了你的私钥，可以让你消费块链中分配给钱包的比特币。

和真正的钱包一样，每个比特币钱包都可以显示它所控制的所有比特币的总余额，并允许你将一定金额的比特币付给某人。

这与商家进行扣款的信用卡不同。

END，本文到此结束，如果可以帮助到大家，还望关注本站哦！