区块链安全综述

林文海(11721018)

2018年06月10日

摘要

这是中文摘要。

Abstract

This is abstract in English.This is abstract in English.This is abstract in English. This is abstract in English.This is abstract in English.This is abstract in English. This is abstract in English.This is abstract in English.This is abstract in English.

1 前言

1.1 比特币基础

比特币[1]是第一个完全去中心化的电子货币系统。自从比特币在2009发行以来，它的价值已经获得巨大的提升，截止2018年6月10日，单个比特币的价值为7311.87美元，比特币总市值已经突破1249亿美元[2]。比特币的核心是基于区块链技术，区块链本质上是一种分布式账本，它记录着比特币系统的所有历史交易信息。为了保证分布式账本的内容不会被随意篡改，比特币系统需要网络中的P2P节点使用它们的算力去解决某种哈希计算题，以此来产生工作量证明PoW，想要产生一个区块同时将交易加入到区块中就必须要有PoW。我们将产生区块的过程称为“挖矿”，参与挖矿的P2P节点我们称之为“矿工”。当矿工挖出一个新的区块后会立即把新区块通过比特币网络进行广播并开始下一轮的挖矿，其他节点会对新区块进行校验，如果校验合法，那么新区块将被加入到原有的区块链的头，从而延长整个区块链。如果矿工挖出来的块获得网络上大多数节点的认可，那么矿工将获得一些比特币作为奖励。新的区块中的头保存着前一个区块的哈希值，如果前一个区块内容发生改变，那么将要重新进行PoW，并且导致后面的区块内容也发生变化，也要重新进行PoW。因此，随着区块链越来越长，篡改越早以前的区块的代价将越大，这就保证了区块链上数据具有不可篡改的特性。

截止2018年06月，每挖到一个新区块的矿工将获得最少12.5个比特币作为奖励，除此之外，新区块中包含的所有交易的手续费也将作为矿工的奖励。根据比特币的设计，新区块的产生速度需要保持在平均每10分钟一个，由于比特币网络的总的计算能力在不停的变化，因此挖矿的难度需要频繁进行调整，这个周期为两周，准确地说是产生2016个区块花费的时间。随着挖矿难度的提升，独立矿工挖到新区块的平均时间将变得更长，并且很不稳定。为了避免这种收入不稳定的问题，一些矿工就组织共同进行挖矿并根据算力分享收益，这被称为矿池。大部分矿池由矿池管理着和矿工构成。管理者作为比特币网络上的节点运行完整的比特币协议，而矿工是通过运行矿池协议[3] 加入矿池而不是直接连接到比特币网络上。矿池管理者将未解决的挖矿任务分成一个个子任务分给矿工，矿工解决这些子任务后将产生PPoW和FPoW，并将他们提交给矿池管理者。PPoW是指没有挖出新的区块但是验证了一部分答案是错误的，FPoW是指找到了正确答案，也就是挖到区块。如果一个矿池中的矿工产生了FPoW并将它提交给管理者，管理者会立即将FPoW产生的新区块广播到比特币网络中。如果区块经过了其他大部分节点的验证并被采纳，那么矿池管理者将受到奖励，同时按照矿工贡献的PoW的比例将奖励分给矿工。比特币网络（挖矿部分）当前由独立矿工、允许任何人加入的开放矿池以及需要认证才能加入的私人矿池构成。

1.2 比特币挖矿过程

区块链中的交易是以Merkle树[4]的结构存储在区块中。区块链中每一个区块的头都包含了当前区块Merkle树根的哈希值、前一个区块的头哈希值、难度目标以及nonce值。在比特币系统中，挖矿其实就是不断地尝试nonce值，然后计算加密问题以此产生PoW。具体来说，挖矿的目标就是找到一个有效的nonce值满足 $sha256(sha256(blkhdr)) < t$, 其中 $blkhdr$ 是区块完整的头信息， t是一个根据比特币协议计算出来的256位的数值，称为难度目标。因为哈希计算是不可逆的，因此矿工只能通过不断的尝试nonce值来计算区块头的哈希，很明显这个的难度是很高的。为了保证区块的平均产生速度在10分钟左右，比特币系统每产生2016个区块后都要重新调整难度目标 t 的值。当一个矿工发现一个有效的nonce值并且产生一个新的区块后会立即将新区块广播给比特币网络中的每个节点。当其他节点接收到新区块并通过验证后，会把新区块作为区块链的新的头。

1.3 区块链分叉

比特币系统中的区块链分叉分为由挖矿产生的分叉[5]和由版本升级产生的分叉[6]，而由版本升级产生的分叉又分为软分叉和硬分叉，我们这里提到的分叉特指由挖矿产生的分叉，当两个矿工在很短的时间内相继挖到了有效的新的区块并将新区块广播到比特币网络上，由于网络存在延时，因此有些节点先收到了区块 B_1, 而有些节点先收到了区块 B_2, 通常情况下，节点会将先收到的区块作为区块链的新的头。所以，整个网络中就存在着一部分节点以区块 B_1作为区块链的头而其他节点以区块 B_2作为区

块链的头，这就是由挖矿所产生的区块链分叉。在产生分叉后的新一轮挖矿中，会有一个分叉先算出来新的区块，那么这个分叉就是有效的，而另一个分叉是无效的。除了这种偶然产生的分叉外，分叉也可以认为地故意产生。当一个矿工先挖出了一个新区块但是不立即将其广播到网络上，知道矿工检测到网络中其他的节点也挖出了一个新的区块后才将自己的挖到的新区块广播出去，以此来故意产生分叉。这种故意产生的分叉可以被用于“双重支付”攻击[7]和“selfish mining”攻击[8, 9, 10]。

参考文献

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. (2008).

[2] CoinMarketCap. Bitcoin Market Info. https://coinmarketcap.com/currencies/bitcoin/. (2018). [Online; accessed 10-Jun-2018].

[3] Stratum Mining Protocol. https://en.bitcoin.it/wiki/Stratum_mining_protocol. (2018). [Online; accessed 10-Jun-2018].

[4] Ralph C Merkle. 1980. Protocols for Public Key Cryptosystems. In Symposium on Security and privacy. IEEE.

[5] Bitcoin.org. Bitcoin Developer Guide. https://bitcoin.org/en/developer-guide#block-height-and-forking. (2018). [Online; accessed 10-Jun-2018].

[6] Bitcoin.org. Bitcoin Developer Guide. https://bitcoin.org/en/developer-guide#detecting-forks. (2018). [Online; accessed 10-Jun-2018].

[7] Double Spending Risk Remains After July 4th Bitcoin Fork. https://www.coindesk.com/double-spending-risk-bitcoin-network-fork/. (2018). [Online; accessed 10-Jun-2018].

[8] Ittay Eyal and Emin Gun Sirer. 2014. Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In *International Conference on Financial Cryptography and Data Security*. Springer.

[9] Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. 2016. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. In *European Symposium on Security and Privacy*. IEEE.

[10] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. 2015. Optimal Selfish Mining Strategies in Bitcoin. *arXiv preprint arXiv:1507.06183* (2015).

[11] Author, F., Author, S., Author, T.: Book title. 2nd edn. Publisher, Location (1999)

[12] Author, A.-B.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010)