比特币分叉

Blockseed - Jamie Cheng 2017.10.29

Agenda

- 什么是软硬分叉
- 什么是重放攻击
- BT1与BT2
- Bitcoin Cash
- Bitcoin Gold
- 扩容的其他解决方案

什么是软硬分叉

- 分叉是对比特币协议的改变
- 软分叉的改变向前兼容
- 硬分叉的改变不向前兼容
- 只有有争议的硬分叉才会带来不同的币种

比特币交易数据结构

字段		大小	意义
版本		4字节	明确这笔交易参照的规则
输入数量		1-9字节	被包含的输入的数量
输入	交易	32字节	指向交易包含的被花费的UTXO的哈希指针
	输出索引	4字节	被花费的UTXO的索引号
	解锁脚本尺寸	1－9字节	用字节表示的后面的解锁脚本长度
	解锁脚本	变长	这是签名数据，是隔离见证要移走的东西
	序列号	4字节	目前未被使用的交易替换功能
输出数量		1-9字节	被包含的输出的数量
输出	总量	8字节	用聪表示的比特币值（10-8比特币）
	锁定脚本尺寸	1－9字节	用字节表示的后面的锁定脚本长度
	锁定脚本	变长	一个定义了支付输出所需条件的脚本
时钟时间		4字节	一个UNIX时间戳或区块高度

表1：比特币交易数据结构

比特币区块数据结构

字段		大小	意义
区块大小		4字节	用字节表示的该字段之后的区块大小
区块头	版本	4字节	版本号，用于跟踪软件/协议的更新
	父区块哈希值	32字节	引用区块链中父区块的哈希值
	Merkle根	32字节	该区块中交易的merkle树根的哈希值
	时间戳	4字节	该区块产生的近似时间（Unix时间戳）
	难度目标	4字节	该区块工作量证明算法的难度目标
	Nonce	4字节	用于工作量证明算法的计数器
交易计数器		1-9 字节	交易的数量
交易		可变	记录在区块里的交易信息

表5：区块数据结构

硬分叉实例

- 在2013年3月12日，当时是bitcoin qt 0.8.0版本软件发布了，0.8版本采用了一种新的数据库level db。有的矿工节点升级了bitcoin qt 0.8版本，有的矿工还继续使用bitcoin qt0.7版本的软件。双方各自生产区块，但bitcoin qt 0.8采用的新数据库生产出的区块被被qt0.7版本节点拒绝掉。具体的原因是旧的数据库对超过800Kb的区块有时不接受。因此在区块高度225430比特币区块链分成了两条链，结果导致了比特币区块链产生两条链，一条是包含大于800kb区块的链，另一条是拒绝承认这些包含更大区块的链，这就发生了硬分叉。

硬分叉实例

- 在2015年7月4日比特币区块链在区块高度363731发生一次硬分叉。当时是Bitcoin Core 开发者往新版本的Bitcoin Core 0.10.0添加了BIP 66。这本来是一起软分叉的修改，在比特币网络上主要矿池都使用了0.10版本的软件时，但有一个矿池BTC Nuggets没有升级，导致BTC Nuggets挖出来的两个区块其他矿工拒绝掉，然后双方就各自挖矿延续自己认为是正确的区块链，由此产生硬分叉，分成了两条链。

比特币扩容问题

- Current:
- Average Block Interval: 600 Seconds / Block
- Max Block Size: 1 MB / Block
- Basic Transaction Size (1 input, 2 output) : 250 Bytes

比特币扩容问题

- Max Transaction Rate
  - BlockSize / BasicTxnSize / BlockInterval
  - 1024*1024 / 250 / 600 ~= 6.9905066667 ~= 7 TPS
- Solution
  - Add Block Size
  - Reduce Transaction Size
  - Reduce Block Interval (Not Recommend)

什么是重放攻击

- 重放攻击(Replay Attacks)发生在分叉后的两条链上
- 私钥和地址生成算法相同
- 交易格式相同

防止重放攻击

- 在交易中加入分叉后的UTXO
- 分叉链应该加入防重放攻击的机制

Segwit 2X

- 香港共识
- 纽约共识

Bitcoin Cash

- Website: https://www.bitcoinabc.org/
- Github: https://github.com/Bitcoin-ABC/bitcoin-abc

BCC Features

- Scalability: 8M
- Replay Attack Protection
- EDA(Emergency Difficulty Adjustment)

BCC防止重放攻击

- use a new signature hashing algorithm

Bitcoin Gold

- Website: https://bitcoingold.org/
- Github: https://github.com/BTCGPU/BTCGPU

Bitcoin Gold

- 1. Change Pow Algorithm
- 2. Replay Protection
- 3. Unique Address Format
- 4. Change Difficulty Adjustment Algorithm

Bitcoin Gold

- 难度调整算法
  - 1.每个区块做调整
  - 2. 根据前17个区块的平均难度决定下一个区块难度

BTG

- 1. 分叉后有8000个预挖区块，包含10万个BTG
- 2. 预挖矿难度最低
- 3. 本质上是一种ICO，可能带来监管风险

扩容的其他解决方案

- 无论是BT1，BT2，BCC，BTG中的哪一种，其可承载的交易量都不大
- 需要依赖二层支付网络：
  - 侧链（sidechain)
  - 闪电网络（lightning network)
- 关注产品：
  - Liquid
  - 根链（RSK）

分叉数据比较

Comparison BTC/BTG/BCH/B2X	BITCOIN BTC	**BITCOIN GOLD** BTG	BITCOIN CASH BCH	SEGWIT 2X B2X
Supply	21 Million	21 Million	21 Million	21 Million
PoW algorithm	SHA256	**Equihash**	SHA256	SHA256
Mining Hardware	ASIC	**GPU**	ASIC	ASIC
Block Interval	10 Minutes	**10 Minutes**	10 Minutes	10 Minutes
Block size (actual)	1M (2-4M)	**1M (2-4M)**	8M (8M)	2M (4-8M)
Difficulty adjustment	2 Weeks	**Every block**	2 Weeks + EDA	2 Weeks
Segwit	✓	✓	⊖	✓
Replay protection	●	✓	✓	⊖
Unique address format	●	✓	⊖	⊖