

<div><div>Compact Block 方案</div><div><div>Alice</div><div>Bob</div><div><div>inv</div><div>req</div><div>Header TxIDs 一些全交易txs</div><div>我缺少 txs 2,3,112...</div><div>全交易txs 2,3,112...</div></div></div></div>	<div><div>Xthin 方案</div><div><div>Alice</div><div>Bob</div><div><div>inv</div><div>Ib = Bloom(pool) req</div><div>Header TxIDs Bob没有的txs</div><div>组装完整区块 如果仍然有缺少的交易 则进行一下两步</div><div>我缺少 txs 2,3...</div><div>全交易 txs 2,3...</div><div>组装完整区块</div></div></div></div>	<div><div>石墨烯方案</div><div><div>Alice</div><div>Bob</div><div><div>inv</div><div>tx pool counts m req</div><div>Header S=Bloom(TxIDs) I=IBLT(TxIDs)</div><div>区块池经过S过滤， 得到TxPool， I' = IBLT(TxPool) I - I' 得到A的独有交易</div><div>我缺少 txs 2,3,112...</div><div>全交易 txs 2,3,112...</div><div>组装完整区块</div></div></div></div>	<div><div>ChainStack方案</div><div><div>Alice</div><div>Bob</div><div><div>block hash S=Bloom(TxIDs)</div><div>区块池经过S过滤， 得到TxPool， 使用TxPool计算Estimate</div><div>Estimate</div><div>Header S=Bloom(TxIDs) I=IBLT(Txs)</div><div>区块池经过S过滤， 得到TxPool， I' = IBLT(TxPool) I - I' 得到A的独有交易 反解A独有交易</div><div>组装完整区块</div></div></div></div>
<div><div>数据传输量</div><div>( 区块中有2000笔交易，Bob的交易池有4000笔交易，区块中有1800个交易与Bob的交易池重合， 每笔交易长100B, 交易ID截取5B就够了 ) (我们设定Bloom过滤器的容错率f = 0.01)</div><div>Header ( 忽略 ) 所有TxID ( 2000 × 5 = 10KB ) 缺少的交易ID ( 200 × 5 = 1KB ) 缺少的全交易 ( 200 × 100 = 20KB )</div><div>总量：31KB ( 区块200KB )</div></div>	<div><div>数据传输量</div><div>( 区块中有2000笔交易，Bob的交易池有4000笔交易，区块中有1800个交易与Bob的交易池重合， 每笔交易长100B, 交易ID截取5B就够了 ) (我们设定Bloom过滤器的容错率f = 0.01)577, 套用公式，布隆过滤器的大小为x = y × (-ln(f))/ln(2)^2 × 1/8) = y * 1.079618</div><div>Header ( 忽略 ) 布隆Ib (4000 × 1.079 = 4.3KB) 所有TxID ( 2000 × 5 = 10KB ) 缺少的全交易 ( 200 × 100 = 20KB ) 忽略最后的缺少交易ID传输</div><div>总量：34.3KB</div></div>	<div><div>数据传输量</div><div>( 区块中有2000笔交易，Bob的交易池有4000笔交易，区块中有1800个交易与Bob的交易池重合， 每笔交易长100B, 交易ID截取5B就够了 ) (我们设定Bloom过滤器的容错率f = 0.01)577, 套用公式，布隆过滤器的大小为x = y × (-ln(f))/ln(2)^2 × 1/8) = y * 1.079618</div><div>Header ( 忽略 ) 布隆S ( 2000× 1.079 = 2.1KB) IBLT I ( 1.5 ( 2+4+5 ) × 预期差异 = 16.5 × 200 = 3.3KB ) 缺少的交易ID ( 200 × 5 = 1KB ) 缺少的全交易 ( 200 × 100 = 20KB )</div><div>总量：26.4KB</div></div>	<div><div>数据传输量</div><div>( 区块中有2000笔交易，Bob的交易池有4000笔交易，区块中有1800个交易与Bob的交易池重合， 每笔交易长100B, 交易ID截取5B就够了 ) (我们设定Bloom过滤器的容错率f = 0.01)577, 套用公式，布隆过滤器的大小为x = y × (-ln(f))/ln(2)^2 × 1/8) = y * 1.079618</div><div>Header ( 忽略 ) 布隆S两次 ( 2000× 1.079 × 2 = 4.2KB) Estimate ( 80×7×32+1800/128×32=18.3K ) IBLT ( Txs ) ( 1.5 ( 2+4+100 ) × 预期差异 = 159 × 200 = 31.8KB/47.7KB )</div><div>总量：54.2KB</div></div>
<div><div>Hash次数</div><div>总Hash次数：0</div></div>	<div><div>Hash次数</div><div>Bob 产生区块Bloom,Ib ( 4000 ) Alice 区块交易过滤Ib ( 2000 ) 总Hash次数：6,000 次</div></div>	<div><div>Hash次数</div><div>Alice 产生区块Bloom, S ( 2000 ) Alice 产生区块IBLT, I ( 2000 ) Bob 区块池过滤S ( 4000 ) Bob 产生剩余交易的IBLT ( 1800 ) 总Hash次数：9,800 次</div></div>	<div><div>Hash次数</div><div>Alice 产生区块Bloom, S ( 2000 ) Bob 区块池过滤1次S ( 4000 ) Bob Estimate ( 1800 × 2 = 3600 ) Alice 计算差异 ( 2000 × 2 = 4000 ) Alice 产生区块IBLT ( 2000 × 3 = 6000 ) Bob 区块池过滤1次S ( 4000 ) Bob 产生剩余交易的IBLT ( 1800 × 3 = 5400 ) 总Hash次数：29,000 次</div></div>

总结：  
推测慢的原因在于：1. 两次遍历交易池，交易池有锁，遍历和等待锁释放都需要时间。  
2. Hash计算量大  
建议：1. 考虑只遍历一次交易池，优化协议  
2. 改用石墨烯的方法，或者区块压缩的方法。