连载｜侧链白皮书终篇：用楔入式侧链实现区块链的创新— 附录B 高效SPV证明、附录C 元互换（原子交换）、参考文献

[**chehw**](http://www.8btc.com/author/326)**2014-11-05 18:19 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**3**](http://www.8btc.com/enabling-blockchain-innovations-with-pegged-sidechains-appendix-b-efficient-spv-proofs-appendix-c-atomic-swaps-references#comment)**3705**

 我们提出一种新技术，“楔入式侧链”，使用户能用已有资产使用新的和创新的加密货币系统。本文阐述楔入式侧链及实施要求，及为能从将来区块链间的互联中充分受益所需的工作。全文见附。

－－－－

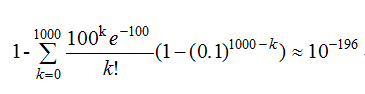
[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2014/10/sidechain1.png)

**附录B 高效SPV证明**

为了将币从一个侧链转移回比特币系统，我们需要嵌入侧链币已锁定于比特币区块链的证明。这些证明应包含（a）一个输出已经在侧链中被创建的记录，以及（b）一个证明足够的工作量已加于该输出之上的DMMS。因为比特币系统的区块链是共享的，并被所有的参与者验证，这些证明必须不能给网络强加大量负担。输出可以很容易地紧凑记录，但让DMMS做到并非是显而易见的事。

紧凑型SPV安全。SPV证明的置信度可以通过将一个攻击者和诚实网络模拟为随机处理过程[MLJ14]来证明。这些随机过程有一个实用的统计特征：由于每个哈希值必须小于目标值才能合法，用一半的时间将得到小于目标值一半的值；用1/3的时间将得到小于目标值1/3的值；用1/4的时间将得到小于目标值1/4的值；依此类推。当哈希值本身不再改变计作一个区块所需的工作量时，低于必要量(lower-than-necessary)的哈希值的存在实际上是链上做了过多工作的统计上的证据。，我们可以利用这一事实证明仅用几个区块眉就可以达到等同的工作量[Fri14]。因而，极大地压缩区块眉列表并提供仍能证明有相同的工作量是有可能的。我们称这样一个压缩的列表为紧凑型SPV证明或压缩的DMMS。

然而，制造一个欺骗性紧凑型SPV证明与一个非紧凑型SPV证明在预期上所需的工作量是相同的，造假者成功的可能性不再随被证明的工作量而指数衰减：机会上较弱的攻击者会有更高的可能性“偶然”成功；即，早期就发现低哈希值。为了说明这一点，假设攻击者有10%的网络哈希算力，并尝试在网络能产生同样多的证明之前，创建一个1000个区块的SPV证明。按照[Nak09]中的公式，我们看到他成功的可能性为：

[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2014/11/side-1.jpg)

作为对比，同样的攻击者在相同时间里生成一个单一区块，且该区块的价值相当于证明1000个区块的工作量的可能性大致为10%，这是一个相当高的数字。

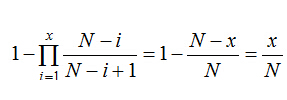
对这一问题的详细分析及其可能的解决方案超出了本文的范围。现在我们将介绍一种紧凑型SPV证明的实现，同时提供一些潜在解决方案，在阻止此类攻击的同时，仍保持证明的压缩效果显著。

需要注意的是，我们假定了一个常量难度值。我们观察到比特币系统中的难度值，虽然不是常量，但变化得足够慢以抗拒已知的攻击（Bah13）。因此，我们预期根据难度调整进行校正是可以做到的。

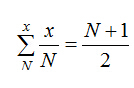
实现。紧凑型SPV证明的灵感来自于跳跃表（skiplist）[Pug90]，一个概率性数据结构，无需再平衡即可提供对数复杂度的检索（这很有用，因为对于一种仅追加式结构，比如区块链，是无法进行再平衡的）。

我们需要比特币系统有一个改变，让每个区块眉不是仅指代它之前的一个区块眉，而是可以指明它的每一个前代。为了提高空间使用效率，这些指代可以存储于一个梅克尔树中：通过在每一个区块只包含一个根哈希值，我们就可得到一个对树中的每个元素的指代。其次，提取SPV证明时，允许证明者使用这些指代来跳转回某一区块，链上回指的链接不再只有一个，假使该区块眉实际证明的工作超过了仅那些跟从直接前驱链接所证明的总目标工作量。结果是一个短的DMMS证明了与原始区块链一样多的工作量。

这能小多少呢？假设我们尝试为一个高度为N的完整区块链生成SPV证明。为简单起见，假定该链的难度值是一个常量；即，每个区块的目标值是相同的。考虑在x个区块内找出一个可完全跳回到创世块的足够大的证明的概率；也就是说，在区块N-x和区块N之间（找到）。这等于1减去我们找不到时的概率，或写成

[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2014/11/side-2.jpg)

在跳过链上剩余区块前需要向回扫描的区块数预期为

[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2014/11/side-3.jpg)

因此，如果我们想用一次跳跃来跳过整个剩余链，我们预期只需检索半程即可；用同样的方法，我们只需检索1/4即可跳过这半程，1/8即可跳过这1/4的路程。结果是预期的总证明长度是该链原始长度的对数。

对于一个100万区块的链，对整条链预期的证明大小仅为log2 1000000 ≈ 20个区块眉。这使DMMS的大小下降为10千字节左右的范围。

然而，正如上面所观察到的情况，如果攻击者能在仅实际开采了对外展示的区块眉时就可生成紧凑性证明，那么他就能在证明总工作量时以一个不能被忽略的概率也做到这一点。攻击者可以利用这样一个策略，生成无效区块，这些区块每个反向链接点指向最近的区块。当提取一个紧凑型证明时，攻击者只需每次都跟从最高权重的链接即可。

我们可以调整方案，用以下几种方法之一来防止这种情况发生：

l  通过限制最大的跳跃尺寸，我们可以回归到比特币系统的性能，令攻击可能发生的概率随被证明的工作量大小呈指数衰减。利用一个常量（与最大跳跃大小成正比）因子，使预期的证明小于完整区块眉列表的大小。

l  通过使用一个随着工作量证明数量而增加的最大跳跃尺寸，有可能用攻击成功概率次指数衰减的代价换得次线性证明的尺寸。这能更大地节省空间，同时还令攻击者的成功概率低到足以忽略不计。

l  交互处理或一个切选机制（cut-and-choose）可以使紧凑性证明在安全性上只有少量削减。例如，要求证明者展示随机数指定的区块眉（以及它们在区块链中的连接），使用证明的一部分作为随机数种子。当仅用一个常量因子增加证明的尺寸时，这降低了攻击的可能性。

如果预期每条侧链会有很多交易，我们可以在父链中维护一个跟踪侧链末端的特殊输出。这一输出通过独立的SPV证明（可以是用上面提到的方法之一压缩的）来移动，使父链在任何时间都可以察知侧链的末端。

接下来，需要有一个总是以该末端为结束点的转移证明，可以只用一个输出查询即可验证。这保证了验证者验证的转移证明中没有“缺失的链接”，因而这些证明可以维持对数尺寸而不会使伪造的风险增加。

这使父链上的总开销与侧链的数量及长度成正比；没有这一输出，总开销还与链间的转移数量成正比。

这种讨论是没有穷尽的；优化这些取舍以及正规化安全保障超出了本文的范围，也超出了当前进行中的工作的主题。

**附录C 元互换（原子交换）**

一旦某侧链可运转，就有可能让用户无需使用楔入，自动在链间兑换币。实际上，现今用竞争币也可以做到，尽管独立的价格使其难于规划。这一功能很重要，因为正如我们所看到的，直接使用楔入需要相当大的交易（相应地带有高交易费）和长等待期。相比之下，元互换只需在每个网络上使用两笔交易即可完成，每个交易的大小与普通支付到地址（pay-to-address）的交易差不多。

有一个归功于Tier Nolanr[Nol13]的方案，工作原理如下。

假设我们有两个成员方，A和B，在不同的区块链上持有币。假设他们在对方的链上分别有地址pkA和pkB，A有一个秘密数a。那么，A可以用下面的方法将币与B进行兑换：

1．在其中一条链上，A创建一笔交易，将币移动到一个输出O1，该输出的赎回条件限制为：（a）出示a以及B的签名，或（b）A和B双方的签名。A先不广播该交易。

A创建第二笔交易，将币从O1返还回A，带有48小时的时间锁定。A将此交易传递给B，让B来签名。

一旦B签名了这笔锁定的退款交易，A就可以安全地广播移动币至O1的那笔交易，A执行此操作。

2．类似地，B创建一笔交易，将币移至另一条链的一个输出O2上，该输出仅能在（a）出示a和A的签名，或（b）A和B双方的签名，时被赎回。B先不广播该交易。

Ｂ创建第二笔交易，将币从O2返还给B，带有一个24小时的时间锁定。B将该交易传递给A，让A来签名。

一旦A签名了这笔锁定的退款交易，B可以安全地广播移动币到O2的那笔交易，B执行此操作。

3．由于A知道a，A能够花费O2中的币，A执行此操作，取得B的币的所有权。

当A执行此操作后，a被暴露出来，B就可以花费O1中的币，B执行此操作，取得A的币的所有权。

**参考文献**

* [AJK05] J. Aspnes, C. Jackson, and A. Krishnamurthy, Exposing computationally-challenged Byzantine impostors, Tech. Report ALEU/DCS/TR-1332, Yale University, 2005,
* <http://www.cs.yale.edu/homes/aspnes/papers/tr1332.pdf>.
* [And12a] G. Andresen, BIP16: Pay to script hash, Bitcoin Improvement Proposal, 2012,
* <https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki>.
* [And12b] , BIP34: Block v2, height in coinbase, Bitcoin Improvement Proposal, 2012,
* <https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki>.
* [Bac02] A. Back, Hashcash — a denial of service counter-measure, 2002, <http://hashcash.org/papers/hashcash.pdf>.
* [Bac13a] , bitcoins with homomorphic value (validatable but encrypted), 2013,
* BitcoinTalk post, <https://bitcointalk.org/index.php?topic=305791.0>.
* [Bac13b] , Re: [Bitcoin-development] is there a way to do bitcoin-staging?, 2013,
* Mailing list post, <http://sourceforge.net/p/bitcoin/mailman/message/31519067/>.
* [Bah13] L. Bahack, Theoretical Bitcoin attacks with less than half of the computational power (draft), arXiv preprint arXiv:1312.7013 (2013).
* [BSCG+13] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, SNARKs for C: Verifying program executions succinctly and in zero knowledge, Cryptology ePrint Archive, Report 2013/507, 2013, <http://eprint.iacr.org/2013/507>.
* [Cal12] M. Caldwell, Sustainable nanopayment idea: Probabilistic payments, 2012,
* BitcoinTalk post, <https://bitcointalk.org/index.php?topic=62558.0>.
* [Cha83] D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology Proceedings of Crypto 82 (1983), no. 3, 199–203.
* [Fri14] M. Friedenbach, [Bitcoin-development] compact SPV proofs via block header
* commitments, 2014, Mailing list post, <http://sourceforge.net/p/bitcoin/mailman/message/32111357/>.
* [FT13] M. Friedenbach and J. Timón, Freimarkets: extending bitcoin protocol with
* user-specified bearer instruments, peer-to-peer exchange, off-chain accounting,
* auctions, derivatives and transitive transactions, 2013, <http://freico.in/docs/freimarkets-v0.0.1.pdf>.
* [Ges16] Silvio Gesell, The natural economic order, Peter Owen Ltd. 1958., London, 1916,
* <https://archive.org/details/TheNaturalEconomicOrder>.
* [GH12] I. Gerhardt and T. Hanke, Homomorphic payment addresses and the pay-to-contract protocol, CoRR abs/1212.3257 (2012).
* [Gri99] Ian Grigg, Email correspondence, 1999, <http://cryptome.org/jya/digicrash.htm>.
* [jl213] jl2012, OP\_CHECKCOLORVERIFY: soft-fork for native color coin support, 2013, BitcoinTalk post,<https://bitcointalk.org/index.php?topic=253385.0>.
* [Lam79] L. Lamport, Constructing digital signatures from a one-way function, Tech. Report SRI-CSL-98, SRI International Computer Science Laboratory, October 1979.
* [Lie01] B. Lietear, The future of money, Random House, London, January 2001.
* [Max11] G. Maxwell, Deterministic wallets, 2011, BitcoinTalk post, <https://bitcointalk.org/index.php?topic=19137.0>.
* [Max14] , User:gmaxwell/alt ideas, https://en.bitcoin.it/wiki/User:
* Gmaxwell/alt\_ideas. Retrieved on 2014-10-09., 2014.
* [Mer88] R.C. Merkle, A digital signature based on a conventional encryption function, Lecture Notes in Computer Science, vol. 293, 1988, p. 369.
* [Mil12] A. Miller, The high-value-hash highway, 2012, BitcoinTalk post, <https://bitcointalk.org/index.php?topic=98986.0>.
* [MLJ14] A. Miller and J. J. LaViola Jr, Anonymous Byzantine consensus from moderately-hard puzzles: A model for Bitcoin, Tech. Report CS-TR-14-01, UCF, April 2014.
* [Mou13] Y. M. Mouton, Increasing anonymity in Bitcoin … (possible alternative to Zerocoin?), 2013, BitcoinTalk post, <https://bitcointalk.org/index.php?topic=290971>.
* [MP14] G. Maxwell and A. Poelstra, Output distribution obfuscation, <https://download.wpsoftware.net/bitcoin/wizardry/brs-arbitrary-output-sizes.txt>, 2014.
* [Nak09] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, <https://www.bitcoin.org/bitcoin.pdf>.
* [Nol13] T. Nolan, Re: Alt chains and atomic transfers, <https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949>,  2013.
* [Poe14a] A. Poelstra, ASICs and decentralization FAQ, 2014, <https://download.wpsoftware.net/bitcoin/asic-faq.pdf>.
* [Poe14b] , Is there any \_true\_ anonymous cryptocurrencies?, Bitcoin.SE, 2014, <http://bitcoin.stackexchange.com/a/29473>.
* [Poe14c] , A treatise on altcoins, 2014, Unfinished, <https://download.wpsoftware.net/bitcoin/alts.pdf>.
* [Pug90] W. Pugh, Skip lists: A probabilistic alternative to balanced trees, Communications of the ACM 33 (1990), no. 6, 668, <ftp://ftp.cs.umd.edu/pub/skipLists/skiplists.pdf>.
* [Sza97] N. Szabo, The idea of smart contracts, 1997, <http://szabo.best.vwh.net/idea.html>.
* [Tod13] P. Todd, Fidelity-bonded banks: decentralized, auditable, private, off-chain
* payments, 2013, BitcoinTalk post, <https://bitcointalk.org/index.php?topic=146307.0>.
* [vS13] N. van Saberhagen, Cryptonote v 2.0, <https://cryptonote.org/whitepaper.pdf>, 2013.
* [Wui14] P. Wuille, BIP62: Dealing with malleability, Bitcoin Improvement Proposal, 2014, <https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki>.

－－－－