比特币保险库：点对点防盗电子黄金

Eyal Avramovich
github.com/bitcoinvault

摘要。中本聪原始版本的比特币是要创建点对点版本的电子现金。该协议的大多数成功分叉均试图对该版本做出进一步改进，提供更具伸缩性和更高效的支付系统。我们认为，比特币最有前途的未来不是作为交换媒介，而是作为价值储藏手段 – 一种更好形式的黄金（而非现金）。我们建议对原始协议做出一系列修改，目标是通过创建最终的电子价值储藏手段来实现这一未来。通过将比特币有效交易确认时间从 10 分钟增加到 24 小时，我们有能力处理比特币作为一种形式的黄金容易被盗的这一最大缺陷。一个并非着眼于为咖啡进行支付，而是着眼于完全放心地持有毕生积蓄的系统，其中，每一笔交易都被链上提醒的 144 个区块，并且可以用以前未曾用过的，因此无懈可击的恢复密钥将其紧急取消。该系统的初始启动不是通过硬分叉进行，而是通过更公平的加快采矿机制来进行，使系统能在短时间内识别比特币。我们在此向 Bitcoin Royale 白皮书[1]的创作者致以诚挚的谢意，他们创建了完全防盗电子黄金的愿景。作为一个团队，我们希望进一步推进这一想法，并开始实施下文所述的全部关键特性，使其成为甚至更先进的第三方私钥解决方案（第 6.2 款介绍该解决方案的其他特性）。

1. 序言

比特币 [2] 是于 2009 年诞生的一种去中心化的支付系统，通过该系统，各方可直接交易，无需通过受信任的金融机构。该系统依赖于工作量证明来维持没有受信任运营商的分布式账本，只要最诚实的节点控制的 CPU 算力比配合在一起的攻击者团队节点多，该系统就是安全的。比特币最初被其创造者中本聪描述为“电子现金系统”。

数年来对原始协议进行了多次成功修改，并以比特币代码库分叉的方式予以发布。其中包括于 2011 年面世的莱特币[3]，缩短了交易确认时间，更改了工作量证明算法以有利于消费级硬件（比如 GPU）；比特币现金[4]，于 2017 年面世，通过增加区块大小来增减原始协议的交易吞吐量；和比特币黄金[5]，也于 2017 年面世，通过改变哈希算法，使专业挖矿设备过时。

与原始版本一致，这些分叉和其他分叉的着眼点仍是使比特币成为更好的现金系统。原始版本的限制，比如高交易费用，10 分钟确认时间和每秒仅 4 笔交易左右的吞吐量，限制了比特币与目前占主导的中心化在线支付系统相竞争的能力。

2. 电子现金或电子黄金

尽管比特币作为电子现金，在消费者采用上没有取得多大成功，但它作为电子黄金却明显更为成功。比特币更适合作为交换媒介，还是更适合作为价值储藏手段，业内长期存在争论。黄金不是日常商品和服务的有效支付手段。消费者投资于黄金主要是为了对冲通胀和保持以后的购买力。与国家法定货币不同，比特币的固定货币政策和有限供应使其在这一方面尤其有吸引力。

历史表明，在设计制度时，很少会着眼于同时满足数个竞争性目标。为使其成为更好的交换媒介而对比特币进行优化，削弱了比特币作为价值储藏手段的潜力。同样地，通过进一步弱化作为有用电子现金所需的属性，我们可以大幅改进其作为电子黄金的功能。本文着眼于单一目标–创建最终的价值储藏手段，建议对原始比特币协议做出一系列修改。

如果我们不再将在线支付系统置于优先考虑，则我们无需看重交易费用或交易吞吐量。毕竟，黄金的价值比运输费要高得多，通常买来是进行长期投资的。与我们的努力尤其相关的是交易确认时间。在这一方面的权衡，例如将比特币平均 10 分钟的确认时间大幅增加，会带来很大的益处。因为我们预期 10 分钟内无法完成黄金在不同位置间的搬运，因此这种牺牲看起来是很自然的。

3. 被盗问题

价值储藏方式的关键要求是不易损坏。在交易任何有价值物时，被盗都是主要丢失风险之一。黄金在这方面表现得相当不错。与对电子资产进行虚拟攻击相比，盗窃实物黄金的风险要大得多。此外，盗贼很难对尺寸可观的被盗黄金进行藏匿，尤其是在跨境时。并且匿名对大量被盗黄金进行洗钱和清算也不是简单的事。

很不幸，相比之下，比特币的表现不佳。资金受设置了数组加密私钥的协议保护。但黑客在线上取得该等私钥后即可以远程方式立即并且不可撤销地占有全部资金。对被盗资金进行洗钱也要容易得多，因为交易是匿名进行的，可使用混合器对可追溯性进行干扰[6]，可批量创建 Sybil 身份。因此，加密货币被盗现象在增多，2018 年被盗超过 10 亿美元[7]。按照团体统计的重大事故列表[8]表明，即使实施了最新安全措施的专业机构也容易被攻击。

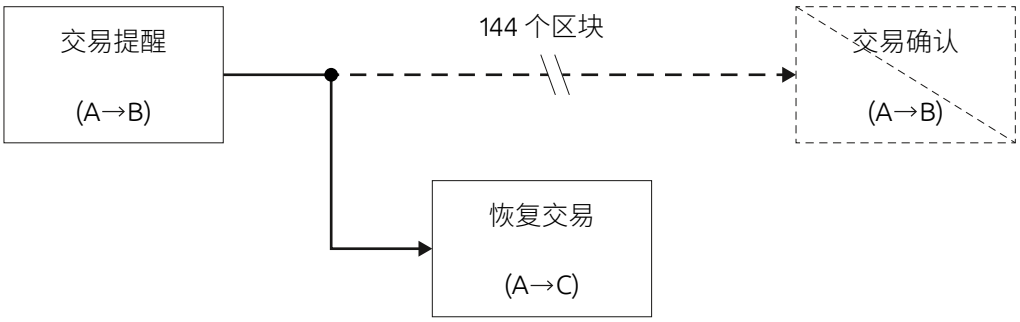
终端用户私钥的安全管理被证明也是比特币的重大挑战之一。因为密钥必须被定期用于与资金互动，签字交易必须在互联网上传输，因此每一密钥均易受攻击。重视安全的做法，比如将资金在“热”钱包和“冷”钱包中分开存放，比较繁琐，不能从根本上解决问题。事故表明，热钱包最终会持有大量资金[9, 10]，使用冷钱包仅减少了与密钥的互动，不能完全消除互动[11]。

4. 防盗解决方案

为消除被盗问题，我们基于新的、先进的锁定脚本和协议修改提出了解决方案。默认将利用新锁定脚本进行的交易延迟 24 小时。矿工将交易加入到新区块时，交易不再立即进行。取而代之的是，它将作为提醒在 144 个区块期间（假定区块时间是 10 分钟）内在链上加入。如果在 144 个区块期间内未被干扰，则交易将从提醒状态变更为“经确认”。

链上提醒的优点是，加密货币所有者在其加密货币被转移时，一律会收到事先通知。所有者有 24 小时时间依据提醒采取行动，取消转账（如果未经授权）。在托管钱包和传统银行系统中，延迟提款是久经验证的防盗行业标准。例如，Coinbase Vault [12]，等待时间是 48 小时。我们提出的解决方案，在没有被信任的第三方的情况下，提供了同等保护。

紧急取消处在提醒状态的交易，需要进行特别恢复交易，并且立即实施，不受 24 小时延迟的约束。进行恢复交易需要提供特别恢复密钥，特别恢复密钥必须在创建钱包时加入到锁定脚本。一旦为给定钱包注册了恢复密钥，恢复密钥就不可更改。



在设计上，用于紧急取消交易的私人恢复密钥是以前从未用过的新钥。该密钥可在线下生成，切勿接入互联网或输入到任一设备中。注册流程仅需要输入该密钥的公开部分，确定该私钥仍未用过。与必须不定期使用，因此容易被盗的冷钱包密钥不同，恢复密钥将仅在紧急取消交易时首次使用，因此完全防盗。恢复密钥在使用后，被认定为已损坏，全部资金应被立即转移至受新的未使用恢复密钥保护的新钱包。

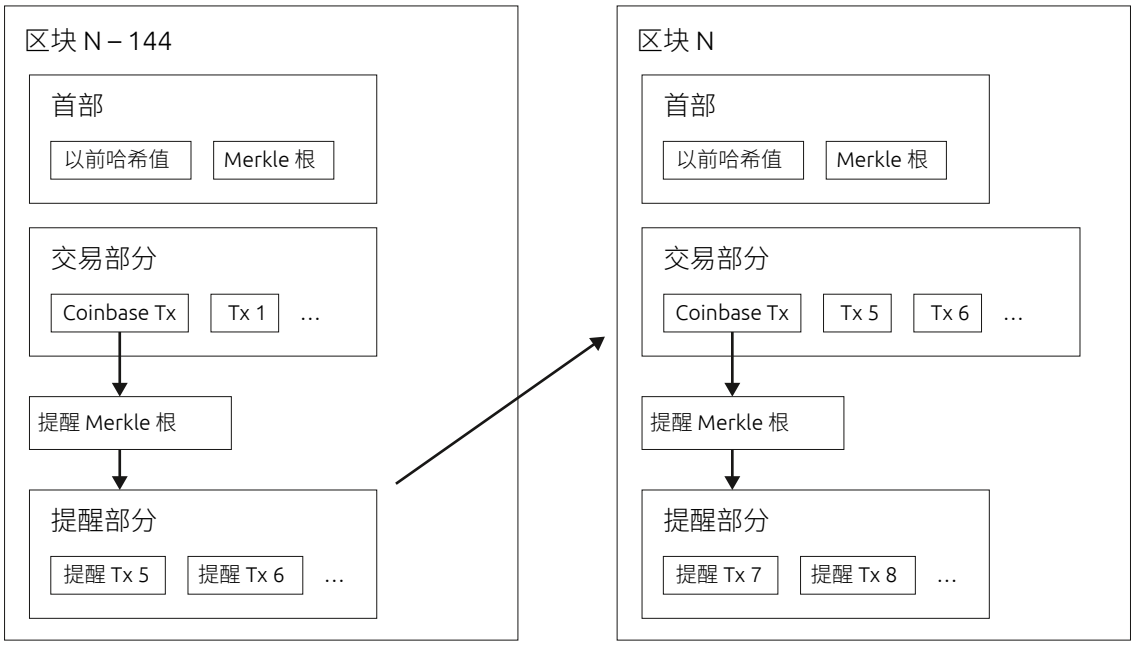
由 Bitcoin Royale 最先提出的数字黄金概念，假定将系统中的全部交易延迟 24 小时，使加密货币成为安全、缓慢转移的价值储藏方式。我们利用两个概念 – 数字黄金和数字现金 – 对这一概念进行了扩充，并且没有对安全造成损害。

在提出缓慢转移提醒的同时，我们有条件地保留了快速转移、“立即”交易。为提供最高安全性，发送该交易将需要用户使用在创建钱包期间由第三方提供的密钥进行基于区块链的 2FA。

5. 区块

与原始比特币协议类似，每一区块均含有经确认交易列表，并在其首部持有该等交易的 Merkle 根哈希值。因为一些交易必须在链上等待 24 小时，因此它们不能被立即加到交易部分中。取而代之的是，它们被加到原始比特币协议没有的一个新的特设部分 – 提醒部分 – 中。提醒部分的 Merkle 根哈希值储存在 coinbase 交易的输入值中，与原始比特币的区块首部兼容。

新区块被挖出时，矿工回看 144 个字节，并检查区块 N-144 提醒部分。确认时，交易的所有提醒仍有效，并进入新区块的交易部分。



开采区块 N 的步骤如下：

1) 将新常规交易加入到区块 N 提醒部分（未确认）。
2) 将新立即交易加入到区块 N 交易部分（经确认）。
3) 将新恢复交易加入到区块 N 交易部分（经确认）。
4) 检查区块 N-144 交易部分，将有效交易加入到区块 N 交易部分（经确认）。

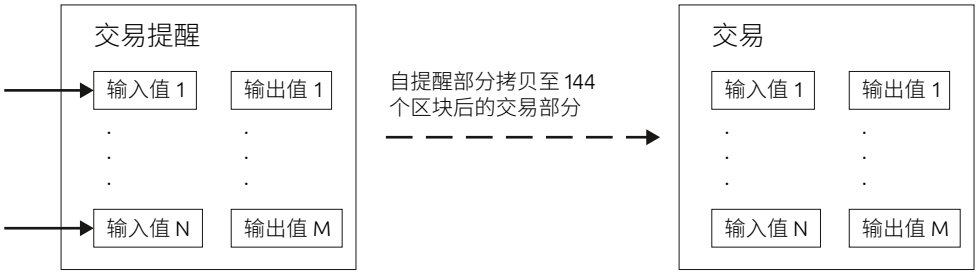
6. 脚本

比特币保险库的核心功能是通过先进的锁定脚本可访问，其行为与依据由非锁定脚本出示的签名数字而实施的行为不同。提供两个变体：

1. 提醒锁定脚本 – 需要一个或两个签名。如果出示了一个签名，则生成提醒交易。如果出示了两个签名，则生成恢复交易。
2. 提醒 + 立即锁定脚本 – 需要一个、两个或三个签名。如果出示了一个签名，则生成提醒交易。如果出示了两个签名，则生成立即交易。如果出示了全部三个签名，则生成恢复交易。

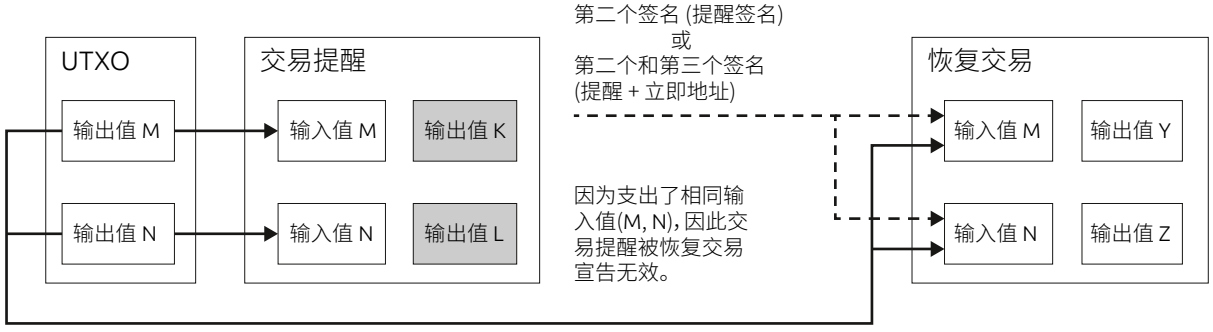
7. 交易

比特币转账通过与比特币协议中的交易相同的常规交易来进行。其格式不会随着其从提醒部分到交易部分而改变。



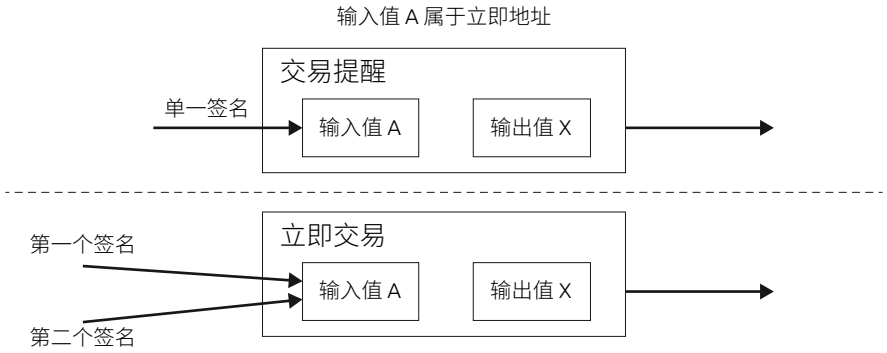
7.1. 恢复交易

恢复交易支出与被恢复提醒相同的 UTXO。区别是，它为同一 UTXO 出示了更多签名：2（如果是提醒锁定脚本）或 3（如果是提醒 + 立即锁定脚本）。如果恢复交易被处理，则被恢复 UTXO 被支出，因此依赖该 UTXO 的已有提醒被宣告无效，并使其在 24 小时延迟后不能被确认。



7.2. 立即交易

在立即交易中，可避开默认的 24 小时交易确认延迟，将交易确认时间缩短至大约 10 分钟。其机制类似于多重签名钱包。它需要来自独立私钥的额外签名，独立私钥应在独立地方安全储存。这就是为什么立即交易仅可自专用 P2SH 地址 – 由提醒 + 立即锁定脚本生成的立即地址 – 发送的原因。



8. 兼容性

我们的设计试图尽可能与标准比特币协议兼容。基本目标是尽可能减少对现有比特币全部节点、钱包、矿池和矿机的必要代码改变。但是，如果对已有的区块链做出了改变，则需要实施硬分叉。

为了避免改变区块首部的格式，使加密货币与比特币专用矿机不兼容，提醒部分的 Merkle 根哈希值储存在标准 coinbase 交易的输入值中。

如果需要实施硬分叉，则我们的目标是使过渡对现有加密货币用户而言尽可能容易。所有的现有脚本类别不改变其行为，因此在硬分叉实施前存在的全部加密货币均可以通常方式支出。但我们强烈建议切换到新的更安全的脚本。

9. 激励

系统借用了比特币的激励模型，该模型过去十年来被证明是成功的。 加入提醒，需要对该模型做出轻微改动。激励矿工将交易提醒加入区块，激励方式是对输出值和输入值之间的差值计费。对以后的区块交易计费，费用分配给包含交易提醒的原始矿工。

以后的矿工仍将为挖出新区块而获得区块奖励，奖励包括来自新的立即交易、注册交易和恢复交易的全部费用，和交易提醒的以后费用承诺。根据共识规则，以后的矿工有义务将 N-144 区块的全部提醒加到交易部分（不包括被恢复的交易）。

如果提醒被取消，则原始矿工的提醒费用不可恢复，并且总成本是原始提醒费用加恢复交易费用。

10. 相关工作

Malte Möser 等人关于比特币保险箱所做的工作[13]给我们留下了深刻印象。他们对比特币脚本语言所做的扩展使得以后可对加密货币的使用进行限制，从而可被用来实施多种安全措施。其中主要是保险库交易，这与我们提出的延迟提款机制类似。

我们已经选择了更简单的实施方式，这种方式不需要由钱包实施的定制脚本递归数组。我们的交易更多的是一个可选扩展，它是对协议的根本改变，从而对交易产生广泛的强制性影响。将实施负担转到矿工身上，带给终端用户与缺省设置相同的交易体验，这使我们能更好地实现创造真实电子黄金的使命。

参考文件

1. Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://www.bitcoin.org/bitcoin.pdf, 2008.
3. Litecoin Project, “Litecoin, open source P2P digital currency”, https://litecoin.org, 2014.
4. “Bitcoin Cash”, https://www.bitcoincash.org, 2018.
5. bitcoingold.org, “Bitcoin Gold”, https://bitcoingold.org, 2018.
6. J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “Coinparty: Secure multi-party mixing of bitcoins”, In: *CODASPY ’15*, 2015.
7. CipherTrace, “Cryptocurrency Anti-Money Laundering Report, 2018 Q4”, https://ciphertrace.com/crypto-aml-report-2018q4, 2019.
8. “BLOCKCHAIN GRAVEYARD”, https://magoo.github.io/Blockchain-Graveyard, 2019.
9. C. Zhao, “Binance Security Breach Update (May 7 2019)”, https://binance.zendesk.com/hc/en-us/articles/360028031711, 2019.
10. J. Buck, “Coincheck: Stolen $534M In NEM Were Stored On Low Security Hot Wallet“, https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet, 2018.
11. J. Preissler, “Important Notice: Only trade TIO on trade.io”, https://medium.com/@trade.io/important-notice-only-trade-tio-on-trade-io-823d59fd7104, 2018.
12. KM. Cutler, “Coinbase Launches A More Secure Bitcoin Storage Option Called ‘Vault’”, https://techcrunch.com/2014/07/02/coinbase-vault, 2014.
13. M. Möser, I. Eyal, E. Gün Sirer, “Bitcoin Covenants”, In: *Financial Cryptography and Data Security, FC 2016, Lecture Notes in Computer Science*, Vol. 9604. Springer, Berlin, Heidelberg.