bitcoin vault

比特币 Vault 白皮书

Eyal Avramovich, Kacper Wiśniewski, Piotr Kozłowski, Radek Popiel et Anon 著

白皮书 v1.0

摘要

2009 年，一个匿名者或一个匿名开发团队创建了第一个基于区块链技术的点对点网络，该网络允许用户在匿名哈希地址之间转移资金。比特币革命就此开始。它产生了一系列原始概念的分叉。

其中之一就是促成了比特币 Vault 的概念。

作为开发者，我们的目标是用独特的功能升级现有的区块链，给用户更多的控制权，并通过管理钱包地址、存储私钥和公钥以及个人之间转移资产的方式提高其安全水平。我们希望创建一个币，它将提供比特币的所有优势，并提供额外的功能，让用户以简单方便的方式最大限度地控制他们的资产，同时不影响加密货币提供的灵活性。

以区块链的不变性为分布式账本的关键特征，我们不仅看到了优势，而且从我们自己的经验中也看到了与资金丢失，放错位置或被盗有关的危险。通过对代码进行一些更改以及在区块链生态系统中使用私钥和公钥的方式，我们想到了使不可逆交易可逆的想法，而又不影响区块链的不变性。

目录

简介 . . . **3**

问题陈述 . . . 3
宗旨与愿景 . . . 3

BTCV 途径 . . . **4**

三重密钥安全解决方案 . . . 4
比特币 Vault 生态系统 . . . 4

Gold Wallet . . . 5
Key Generator . . . 5
Electrum Vault . . . 5

技术概况 . . . **6**

工作量证明 . . . 8

合并挖矿 . . . 8
区块奖励 . . . 9

比特币 Vault 的发展 . . . **10**

比特币 Vault 的发展阶段 . . . 10
主网 . . . 10
路线图 . . . 10
工作流编号 1 ——发展升级 . . . 10
工作流编号 2 ——安全升级 . . . 11
工作流编号 3 ——用户体验升级 . . . 11
工作流编号 4 ——产品 . . . 11
工作流编号 5 ——营销活动 . . . 12
工作流编号 6 ——其他升级 . . . 12

量子计算与 DLT——我们的愿景 . . . **13**

量子计算的威胁 . . . 13
量子计算的机会 . . . 13

比特币 Vault 创造者 . . . **13**

相关作品 . . . **14**

BTCV 资源: . . . **14**

参考文献 . . . **14**

简介

比特币 Vault（BTCV）于 2019 年作为 alpha 链推出。它在 2019 年 12 月至 2020 年 11 月期间取得重大发展，其中发布了实现区块链上可逆交易的关键功能。

比特币 Vault 是世界上第一个允许用户在交易发布到区块链后取消交易的加密货币。这种革命性的方法是通过定制的区块链协议实现的，该协议在 144 个区块内（或 24 小时左右）确认支付。这一功能可以保护用户在常见的密钥盗窃、用户错误或操作失误以及系统错误的情况下不会损失他们的资金。

比特币 Vault 是 Bitcoin Royale 的硬分叉，在该过程中添加了一个私钥，从而使总数增加到三个。自 2019 年底推出以来，我们已经根据延伸到 2022 年及以后的雄心勃勃的路线图，扩大了技术和市场基础。

问题陈述

根据 CipherTrace 的《2020 年春季加密货币犯罪和反洗钱报告》，在 2020 年前 5 个月，密码盗窃、黑客攻击和欺诈总计 13.6 亿美元。

加密货币交易所每天都需要追回被误发到错误地址的用户资金。这既耗费了他们的时间和金钱，也不能保证用户资金能被追回。

每天有多少加密资产、币、代币被转移到知名的诈骗地址、黑客手中，或者因为中间人类型的攻击而丢失，目前没有可靠的消息来源。

我们认为，如果用户有可能在意识到自己犯了错误、资产被盗或有人未经授权访问加密货币钱包时，立即简单地取消和反转流出的交易，那么上述情况有很大一部分是可以避免的。

宗旨与愿景

BTCV 的开发是为了在三重密钥安全解决方案的基础上提供更高级别的安全性，允许用户在区块链上逆转某些类型的交易。它具有比特币的所有便利性，同时增加了重要功能，允许用户透明和自由。比特币 Vault 是我们对过去十年来加密社区所面临的问题的回答，这些问题主要是。

1. 由于黑客攻击或获取用户私钥而导致钱包被擅自使用，
2. 人为失误，将加密资产发送至错误的钱包地址，或其他类型的错误，与错误输入转账金额或将转账金额与加油金额混合有关，
3. 与加密货币软件有关的错误、失误和其他问题。

BTCV 的开发专注于安保和安全功能，用户的便利性和用户体验，因为我们也相信这些是阻止社会上相当一部分人成为全球加密社区的关键挑战。

BTCV 途径

加密货币为用户提供了在 P2P 网络上存储、管理和转移资金的自由和责任。在本白皮书中，我们假设每个加密货币用户都应该熟悉私钥和公钥的概念，并知道如何安全地存储和保护密钥。

基于这一假设，我们开发了一种新的密钥管理方法及其在各类交易中的使用。

三重密钥安全解决方案

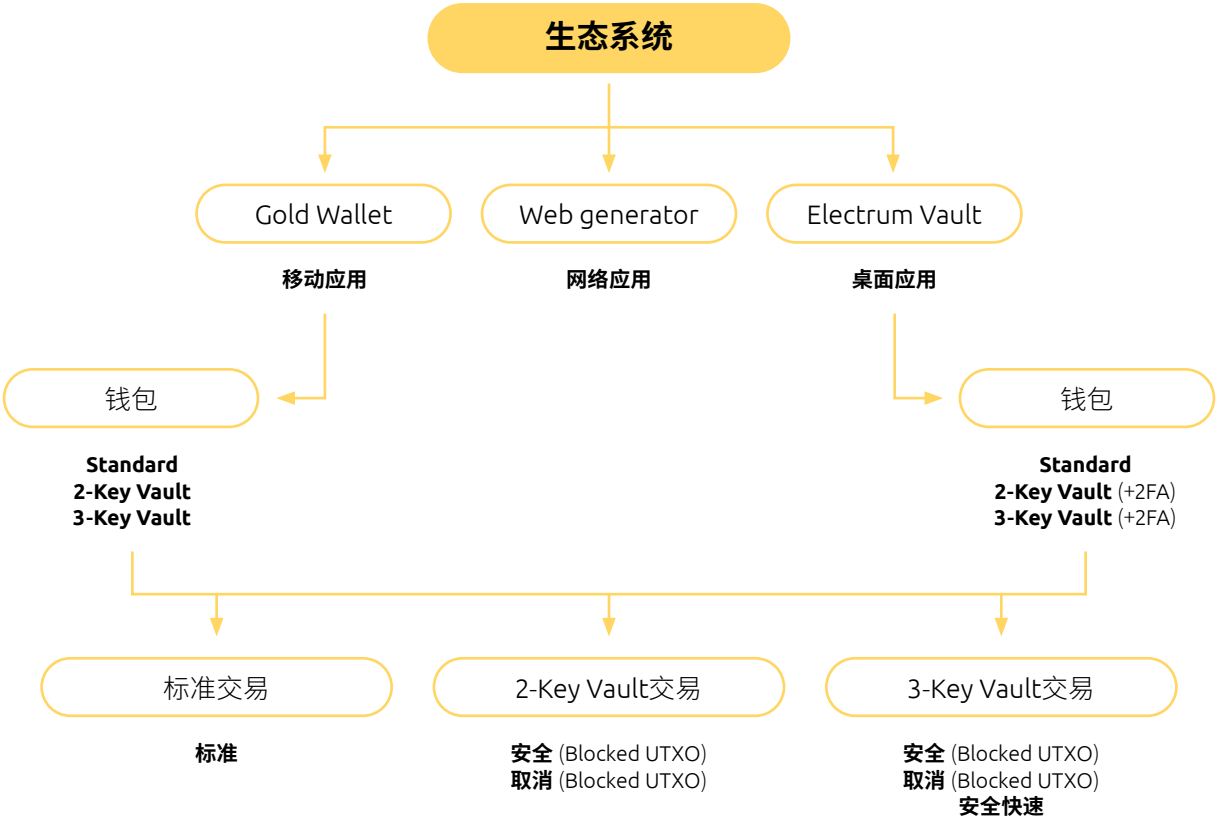
比特币 Vault 开发了三重密钥安全解决方案，需要用户生成三个椭圆曲线数字签名算法（ECDSA）密钥——其中一个在应用内自动存储，另外两个需要由用户管理。目前在比特币 Vault 中的设置允许用户取消发起的交易，并将其反转到现有或新的钱包地址。

解决方案支持在生态系统中具有不同角色的三个 ECDSA 密钥：

- 标准交易密钥自动生成并在后台工作。它需要启动所有交易，并在遭受黑客入侵或技术问题时恢复钱包。
- 取消交易密钥允许用户在生成 144 个区块约 24 小时内执行取消交易。
- 快速交易密钥使用户可以在几分钟内进行安全的快速交易和转移 BTCV。

比特币 Vault 生态系统

比特币 Vault 的生态系统包括三个内部创建的应用程序，它们完全是为了存储和管理 BTCV。它们共同构成了一个强大的工具，保证了安全、透明和自由的更高标准。



Gold Wallet

Gold Wallet 是一款用于移动设备的应用程序，旨在存储，发送和接收 BTCV。它允许用户创建三种类型的钱包并执行各种类型的交易，包括安全快速，安全和取消交易。Gold Wallet 还可以用作 Electrum Vault 桌面应用程序的双重身份验证（2FA）的身份验证器。

Key Generator

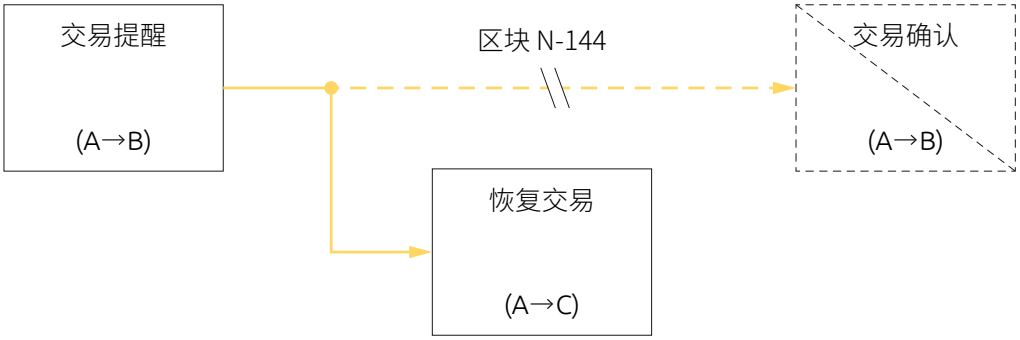
Key Generator 是一个基于网络的应用程序，可生成设置钱包和执行交易所需的单个公钥和私钥。它仅使用本地资源，这意味着密钥生成过程以及密钥本身永远不会离开用户的设备。它们不存储在任何地方，也不能在线访问。钥匙离线存储，提供最大程度的安全。

Electrum Vault

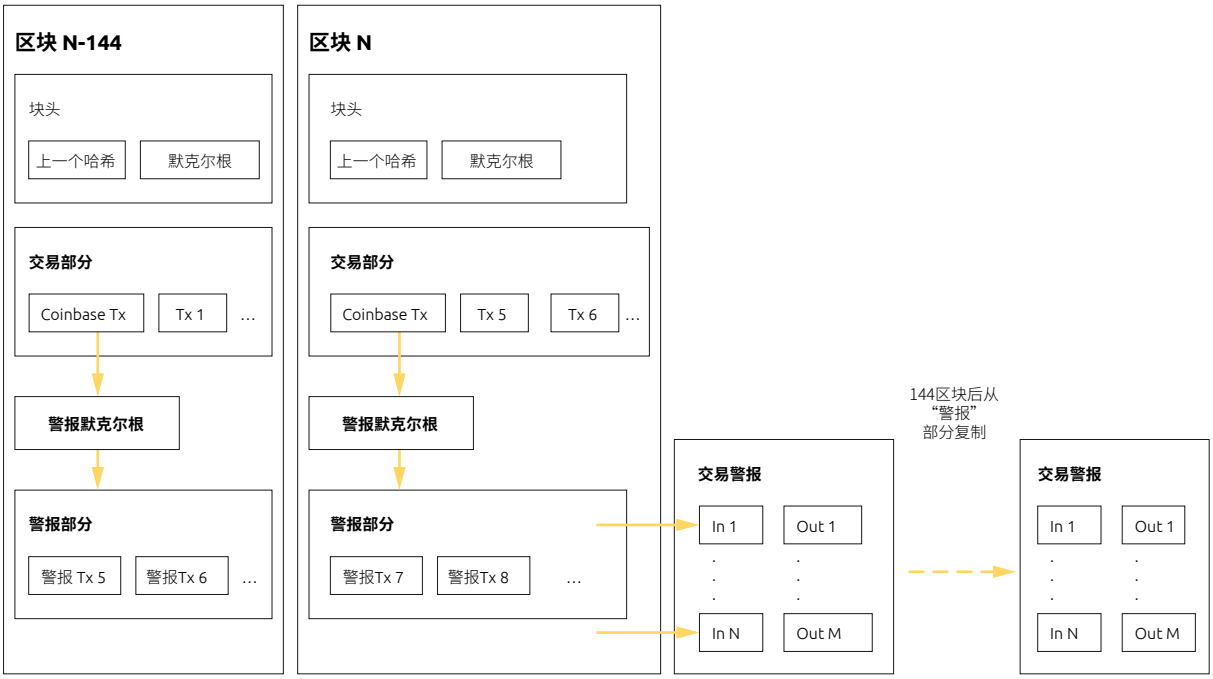
Electrum Vault 是一款基于开源 Electrum Wallet 的桌面应用。它具有 Gold Wallet 的所有功能，这意味着它可以用来存储，发送和接收 BTCV，创建钱包和执行交易，包括安全快速，安全和取消交易。

技术概况

锁定脚本，默认延迟 144 区块，链上警报交易：



具有警报部分的 BTCV 区块结构（如何存储，交易状态从警报更改为确认时会发生什么，矿机如何在交易更改状态时进行验证）



交易预警改变了 UTXOs 的生命周期。

在标准版本中，UTXO 具有两种状态：未使用和已使用（基本上意味着已被删除）。确认新版本的比特币 Vault 引入了新状态。这改变了 UTXO 在数据库中的存储方式。从现在开始，”确认 “状态是 UTXO 从数据库中移除的时间，而状态已使用则锁定 UTXO，并存储其已使用的区块高度信息。这样一来，系统就会等待交易提醒确认后再删除 UTXO。

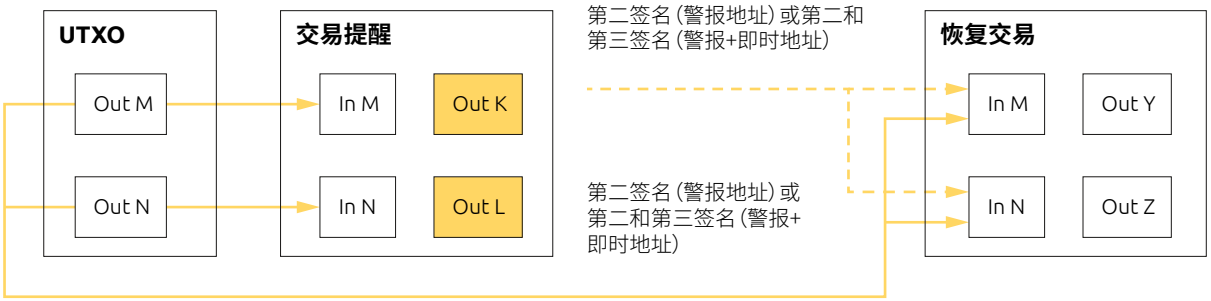
这是一种必要的方法，因为在收到确认之前，交易警报可能会用恢复交易来恢复（它只使用锁定的 UTXO 作为输入）。在应用程序中改变 UTXO 的生命周期的最好方法是存储它们被使用的高度——已使用的高度的信息。这个新信息将决定 UTXO 处于什么状态。

- 当已使用为 0。
- 当已使用 >0。

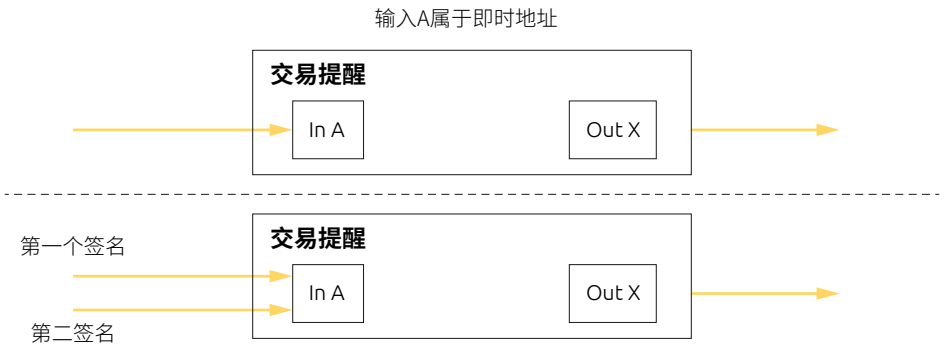
另外，在撤消结构中应该考虑相同的信息。撤销列表以不同的高度存储 UTXOs 先前状态的信息，并在链重组发生时利用这些信息。

新的 UTXO 状态和交易类型对用户可见的余额也有影响。处于已使用状态的 UTXO 应算作新的余额，在确认的余额中可见。它不能算作未确认的余额，因为该余额与未开采和可使用的交易有关。这样做的目的是为了建立不可使用但信息量大的余额。

- 传出警报——计数为已使用状态的 UTXO，已被交易警报锁定，
- 传入警报——交易确认确认后将可使用的 UTXO 计数在内。



快速交易是如何工作的（解释 24 小时延迟的旁路，使之成为可能的——多重签名）。



工作量证明

比特币 Vault 是基于 Bitcoin Royale 开源代码的工作量证明货币。随着 2020 年 11 月 17 日进行的硬分叉，实施了与比特币（BTCV）的合并挖矿。

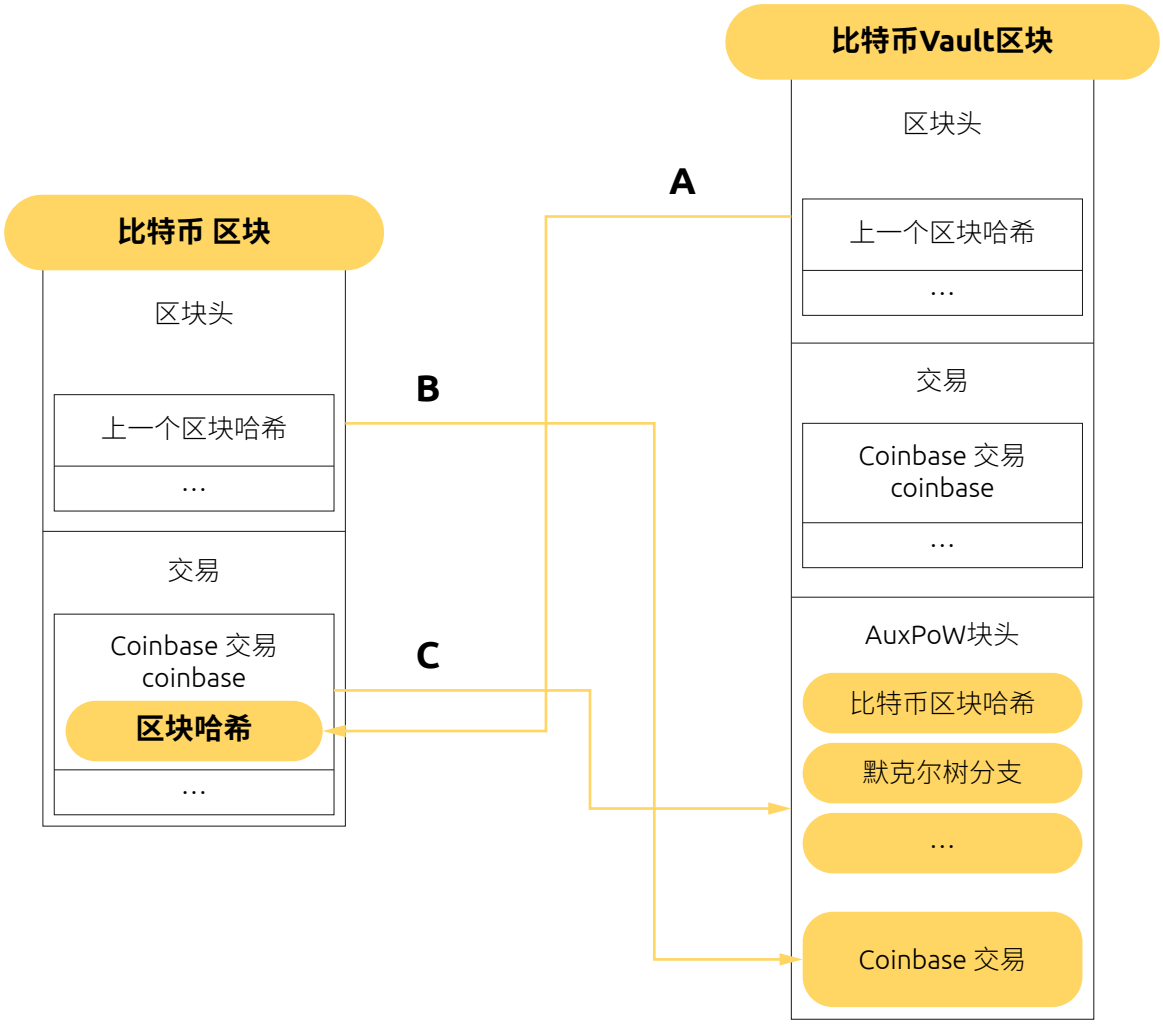
合并挖矿

在对区块数为 58,420 的 BTCV 协议进行重大更新的同时，比特币 Vault 也进行了调整以接受合并挖矿。合并挖矿（也称为辅助工作量证明）是一个过程，是指矿机同时为至少两种具有相同计算能力的独立加密货币寻找 PoW 的过程。但是，父链和辅链之间建立这样的关系，最容易的是辅链做好了改变的准备。

在比特币 Vault 中，由于两种加密货币都使用 SHA-256 哈希函数，因此采用比特币实现了合并挖矿。在这种情况下，BTC 是父链，而 BTCV 是辅链。

因此，比特币的（父）工作量证明解决方案可用于验证比特币 Vault（辅链）作为辅助的工作量证明（AuxPoW）共识机制。

BTC 和 BTCV 区块之间的区块结构及其关系的图形示例的技术说明：



随着对协议的合并挖矿的实现，BTCV 矿机受到激励，可以同时从 BTC 和 BTCV 区块链中获得两个区块奖励。另一个激励因素是，由于通过搭载比特币网络的更高哈希率，给网络增加了额外的哈希能力，网络安全性得到了提高。

区块奖励

比特币 Vault 的总供应量为 2100 万枚币，预计一个区块的开采时间为 10 分钟。

比特币 Vault 区块奖励旨在消除在加密货币开发的早期阶段出现的某些问题。确定了两个主要问题：

获得新参与者的初期时间太短，无法达到项目可持续发展所需的适当社区成员数量。

初期之后，区块奖励急剧减少。这可能会阻碍矿工进一步参与采矿过程，并导致散列功率显著下降。

为了防止此类威胁，比特币 Vault 提出了以下解决方案：

- 将更高区块奖励的期限延长至46个月。
- 将这段时间分为 9 个较短的子期间，每半年进行一次，并逐步减少区块奖励。.

这使项目背后的团队有足够的时间进行开发。社区有机会成长为很多人，从早期开始激励矿工参与网络的时间更长，并且有足够的时间让硬币数量赶上比特币，同时又不会导致大幅的区块奖励减少 。

在此期间，区块奖励减少按以下方式安排：

日期	BTCV奖励减少	子期间编号	区块奖励	子期间时间	子期间区块
2020年5月	175 减至 150	1	175	6 months	29850
2020年11月	150 减至 125	2	150	6 months	26600
2021年5月	125 减至 100	3	125	6 months	26600
2021年11月	100 减至 75	4	100	6 months	26600
2022年5月	75 减至 50	5	75	6 months	26600
2022年11月	50 减至 25	6	50	6 months	26600
2023年5月	25 减至 12.5	7	25	6 months	26600
2023年11月	12.5 减至 6.25	8	12.5	6 months	26600
2024年5月	6.25 减至 3.125	9	6.25	6 months	26600

因此，在此期间将分发19,687,500枚硬币，赶上并达到其比特币第4次减半的数量（估计于2024年3月11日）。之后，BTCV区块奖励将遵循比特币减半时间表。

比特币 Vault 的发展

比特币 Vault 的发展阶段

2019 年五月至 2019 年十二月	Pre-Alpha
2019 年十二月至 2020 年九月	Alpha
2020 年九月至 2020 年十一月	Beta
2020 年 11 月 1 日	Mainnet

主网

主网于 2020 年 11 月 17 日成功启动，区块高度为 58,420。

路线图

2020 年 12 月，BTCV 开发团队发布了涵盖 2021 至 2022 年的新路线图。BTCV 的进一步发展被分为六个工作流。

工作流编号 1 ——发展升级

开发工作流涉及所有将被添加到比特币 Vault 的区块链升级。该工作流的主要目标是参与围绕 Ethereum 2.0 的 Dapp 生态系统与 Wrapped BTCV（wBTCV），直到 2021 年底。

- 2021 年第一季度
  - wBTCV ERC-20 代币——wBTCV 背后的分析和代币经济学
- 2021 年第二季度
  - 账目整合
- 2021 年第三季度
  - wBTCV ERC-20 令牌 beta 测试阶段
- 2021 年第四季度
  - 发布 wBTCV
  - 开始与 DeFI 生态系统整合
- 2022 年第一季度
  - 与 DeFI 生态系统充分整合
  - Dapps 的开发
- 2022 年第二季度
  - Dapps 的开发

工作流编号 2 ——安全升级

比特币 Vault 拥有一支由区块链安全专家组成的内部团队。主网区块链的完整性已经得到了无数次验证，我们的主要目标是在 2021 年加强代码，并在外部合作伙伴的支持下发现任何漏洞和漏洞。经过内部和外部渗透测试之后，我们将为开发人员运行一个开放式赏金计划，并与“白帽”社区密切合作。

- 2021 年第一季度
  - 完整的代码审核（内部和外部）
- 2021 年第二季度
  - 渗透测试(内部)
- 2021 年第三季度
  - 渗透测试(外部)
- 2021 年第四季度
  - 安全审计CIS/20
  - 云安全矩阵
- 2022 年之后
  - 进一步的安全改进和审核
  - 黑客竞赛
  - 赏金计划

工作流编号 3 ——用户体验升级

用户体验是产品使用和采用背后的最重要因素之一。我们的目标是根据社区的反馈意见进一步开发和升级应用程序，并使它们适合各种用户的需求。

- 2021 年第一季度与第二季度
  - GoldWallet 移动应用的用户体验改进
  - Electric Vault 移动应用程序简易模式和专家模式切换
- 2021 年第三季度
  - GoldWallet 的用户通知
- 2021 年第四季度
  - GoldWallet 与第三方应用程序的整合
- 2022 年之后
  - 进一步改善用户体验

工作流编号 4 ——产品

随着 IT 的发展，我们一直致力于将新产品推向市场，以确保市场的接受度。在 2021 年，我们希望在 BTCV 合作伙伴的支持下推出质押产品，并将 BTCV 生态系统与 FIAT 货币联系起来。

- 2021 年第一季度
  - 通过第三方提供新的质押产品
  - 新的贸易产品
- 2021 年第二季度
  - 新的付款网关
  - FIAT 整合

- 2021 年第三季度
  - 数据分析平台（大数据）
- 2021 年第四季度
  - wBTCV 代币相关产品
- 2022 年之后
  - 新的三重密钥功能
  - dApps 产品

工作流编号 5 ——营销活动

2021 年，我们计划在全球范围内发起一场针对 BTCV 当前和未来用户以及全世界整个加密社区的宣传和参与活动。我们将寻求新的合作伙伴关系，以加强 BTCV 区块链的安全性，并使 BTCV 领先于量子研究。

- 2021 年第一季度
  - 启动新网站
- 2021 年第二季度与第三季度
  - 全球宣传和参与运动
- 2021 年第四季度
  - 战略安全伙伴关系
- 2022 年之后
  - 战略科学伙伴关系

工作流编号 6 ——其他升级

通过对 BTCV 生态系统进行一些其他升级，我们希望与社区建立联系并互动，并通过将于 2021 年第二季度初全面启动的新的空投机制为持有者提供新的选择。我们的长期重点还将围绕量子计算及其对区块链加密的潜在影响.

- 2021 年第一季度
  - 开发和启动新的空投机制
  - 空投钱包锁定
- 2021 年第二季度
  - 空投平台/应用程序
- 2021 年第三季度
  - 区块链分析平台
- 2021 年第四季度
  - 量子研究
  - 科学伙伴资助计划

量子计算与 DLT——我们的愿景

如大多数区块链开发者一样，我们对量子技术的进步非常感兴趣。研究像区块链这样的分布式账本技术（DLT）的研究人员和开发人员依赖于公钥加密和哈希函数，这对于所有区块链解决方案都是必不可少的。

比特币Vault 区块链由功能强大的加密算法（例如 ECDSA 和 SHA-256）保护，这些算法也用在比特币以及许多其他加密货币中。当前使用的加密算法对于传统的计算方法已经足够强大。

量子计算的威胁

理论上讲，量子技术的计算能力指数级提升，可能会导致破解公钥计算私钥哈希，或者破解 SHA-256 算法，获得区块链上所需的一次性哈希值区块。根据该领域的许多专家的说法，我们距离开发稳定的量子计算机还有多年的研究时间。即便如此，这些计算机也需要进行适当的编码，以便破解特定加密算法。

量子计算的机会

与其把重点放在威胁上，不如把重点放在机遇上。

同样，在理论上，当量子计算机能够达到足够的稳定性来进行可靠的计算时，就有可能用它们来改进密码算法。这就是我们看到的区块链未来的机会。

目前，我们可以考虑采用多种方法来实现防量子货币的目标，即：

- 基于网格的加密系统，
- 基于多变量公共密钥加密系统，
- 超奇异的椭圆曲线同构加密系统，
- 基于哈希的数字签名加密系统
- 混合型解决方案，如谷歌测试的方案（CECPQ1和CECPQ2）
- 以及其他方法。

为了找到合适的反量子方案，为后量子时代的 BTCV 货币做好准备，我们的开发团队需要在必要的密钥压缩技术和特定代码和编码技术的使用上做更多的研究。

然而，目前还没有一种后量子区块链算法能够同时提供小型密钥、短型签名/哈希、快速执行、低计算复杂度和低能耗。这些因素对于资源受限的嵌入式设备（如物联网中使用的设备）尤为关键。

在未来的三到五年内，我们 BTCV 的开发者将专注于通过新的合作伙伴关系，尤其是与来自各行各业，初创企业和技术大学的专家，在量子抗性方面实现操作准备。

比特币 Vault 创造者

比特币 Vault 由 Minebest 的 CEO Eyal Avramovich 创立，Minebest 是世界领先的加密矿场运营商之一，位于亚洲和欧洲。

更多关于 Minebest 的信息可参见：https://minebest.com/

更多关于比特币 Vault 背后团队的信息可以参见其官网：https://bitcoinvault.global/

相关作品

我们要感谢 Bitcoin Royale 的创造者，因为他们的概念想法促成了比特币 Vault 的发展。

Bitcoin Royale 白皮书：https://bitcoinroyale.org/bitcoinroyale.pdf

BTCV 资源:

关于该项目的其他信息可参见：

https://bitcoinvault.global/
https://twitter.com/vaultbitcoin
https://medium.com/bitcoin-vault-btcv
https://t.me/Bitcoin_Vault
https://www.facebook.com/bitcoinvaultofficial
https://www.instagram.com/bitcoinvaultofficial
https://www.youtube.com/c/BitcoinVault

参考文献

1. Bitcoin Whitepaper, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf
2. Bitcoin Royale: Peer-to-Peer No-Theft Electronic Gold, Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
3. Cryptocurrency Anti-Money Laundering and Crime Report, Spring 2020, https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/
4. The Chainalysis 2020 Crypto Crime Report, https://go.chainalysis.com/2020-Crypto-Crime-Report.html
5. Bitcoin, crypto-coins, and global anti-money laundering governance, Malcolm Campbell-Verduyn, https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance
6. Namecoin project, https://www.namecoin.org/
7. Bitcoin Wiki, Merged Mining Specifications, https://en.bitcoin.it/wiki/Merged_mining_specification
8. Adam Back, Hashcash – A Denial of Service Counter-Measure, http://www.hashcash.org/papers/hashcash.pdf
9. Phil Daian, Rafael Pass, Elaine Shi; Snow White: Robustly Reconfigurable Consensus and Applications, https://eprint.iacr.org/2016/919.pdf
10. Wrapped Tokens A multi-institutional framework for tokenizing any asset https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf
11. Smart Contract Extensibility with Wrapped Tokens https://yos.io/2019/07/13/smart-contract-extensibility-wrapped-tokens/#:~:text=Wrapped%20Tokens%20is%20a%20design,two%20versions%20at%20any%20time.
12. Aleksei Pupyshev, Ilya Sapranidi, Elshan Dzhafarov, Shamil Khalilov, Ilya Teterin, Graviton: interchain swaps and wrapped tokens liquidity incentivisation solution, https://arxiv.org/ftp/arxiv/papers/2009/2009.05540.pdf