



# Bitcoin Vault Whitepaper

Eyal Avramovich, Kacper Wiśniewski, Piotr Kozłowski, Radek Popiel et Anon  
**Whitepaper v1.0**

## Resumo

Em 2009 um indivíduo anónimo ou uma equipa de programadores anónimos criou a primeira rede peer-to-peer baseada na tecnologia blockchain que permitia aos utilizadores transferir fundos entre endereços hash anónimos. A revolução Bitcoin tinha começado. O resultado foi uma série de ramificações do conceito original.

Uma delas levou ao conceito da Bitcoin Vault.

O nosso objetivo como criadores era atualizar o blockchain existente com funcionalidades únicas que dessem aos utilizadores mais controlo e elevassem o seu nível de segurança relativamente à forma como os endereços das carteiras são geridos, como as chaves privadas e públicas são armazenadas e os activos são transferidos entre indivíduos. Queríamos criar uma moeda que oferecesse todas as vantagens da Bitcoin com funcionalidades adicionais para os utilizadores terem o máximo controlo dos seus activos de uma forma fácil, conveniente e sem comprometer a flexibilidade que as criptomoedas oferecem.

Com a imutabilidade do blockchain como característica chave por detrás dos ledgers “livros de registos” distribuídos, vimos não só vantagens mas também – a partir das nossas próprias experiências – perigos relacionados com activos perdidos, mal colocados ou roubados. Com várias alterações no código e na forma como as chaves privadas e públicas são utilizadas no ecossistema do blockchain, chegámos à ideia de tornar transações irreversíveis em reversíveis sem comprometer a imutabilidade do blockchain.

## Conteúdos

<b>Introdução</b>	<b>3</b>
Declaração de Problema	3
Missão e Visão	3
<b>A Abordagem da BTCV</b>	<b>4</b>
Solução de Segurança 3-Keys	4
O Ecossistema da Bitcoin Vault	5
Gold Wallet	5
Key Generator	5
Electrum Vault	6
<b>Perspectiva Técnica</b>	<b>6</b>
Prova de Trabalho	8
Mineração Combinada	8
Recompensas por Bloco	9
<b>Desenvolvimento da Bitcoin Vault</b>	<b>11</b>
Etapas do desenvolvimento da BTCV:	11
Mainnet	11
Objetivos	11
Etapa de trabalho N.º 1 – Atualizações de desenvolvimento	11
Etapa de trabalho N.º 2 – Atualizações de Segurança	12
Etapa de trabalho N.º 3 – Atualizações da experiência do utilizador	12
Etapa de trabalho N.º 4 – Produtos	13
Etapa de trabalho N.º 5 – Atividades de Marketing	13
Etapa de trabalho N.º 6 – Outras atualizações	13
<b>Computação Quântica e DLT – A Nossa Visão</b>	<b>14</b>
Ameaça da Computação Quântica	14
Oportunidade da Computação Quântica	14
<b>Fundador da Bitcoin Vault</b>	<b>15</b>
<b>Trabalhos Relacionados</b>	<b>15</b>
<b>Referências BTCV:</b>	<b>15</b>
<b>Referências</b>	<b>16</b>

## Introdução

A Bitcoin Vault (BTCV) foi lançada em 2019 como corrente alfa. Foi altamente desenvolvida entre Dezembro de 2019 e Novembro de 2020, o que permitiu o lançamento da funcionalidade chave que permite transações reversíveis no blockchain

Bitcoin Vault é a primeira criptomoeda do mundo que permite aos utilizadores cancelar transações depois de serem colocadas no blockchain. Esta abordagem revolucionária é possível com um blockchain de protocolo personalizado que confirmo em finais de 2019, expandimos as bases técnicas e de mercado, em conformidade com um objetivo ambicioso que se estende até 2022 e mais além.

## Declaração de Problema

De acordo com o Relatório da CipherTrace na Primavera de 2020, sobre Crime e Anti-Lavagem de Dinheiro no mundo das criptomoedas, nos primeiros cinco meses de 2020, os roubos, pirataria e fraudes cripto totalizaram 1,36 mil milhões de dólares.

As empresas de câmbio de criptomoedas precisam de recuperar diariamente activos de utilizadores que foram enviados por engano para endereços errados. Isto custa-lhes tanto tempo como dinheiro e não garante que os activos dos utilizadores sejam recuperados.

Não existem fontes fiáveis sobre quantos activos cripto, moedas, tokens estão a ser transferidos todos os dias para endereços fraudulentos bem conhecidos, piratas informáticos ou estão a ser perdidos devido a ataques do tipo “Man-In-The-Middle”.

Acreditamos que uma parte significativa do acima descrito poderia ser evitado se o utilizador tivesse a possibilidade de simplesmente cancelar e reverter as transações de saída, assim que se apercebesse que cometeu um erro, que os activos foram roubados ou que alguém obteve acesso não autorizado à carteira de criptomoedas.

## Missão e Visão

A BTCV foi desenvolvida para fornecer um nível extra de segurança baseado numa Solução de Segurança de 3-Key que permite aos utilizadores reverter certos tipos de transações no blockchain. Apresenta toda a conveniência da Bitcoin, ao mesmo tempo que acrescenta funcionalidades importantes que permitem ao utilizador transparência e liberdade. Bitcoin Vault é a nossa resposta aos problemas enfrentados pela comunidade cripto durante a última década, que são principalmente:

1. Acesso não autorizado a carteiras por piratas informáticos ou acesso às chaves privadas do utilizador.
2. Erros humanos no envio de activos cripto para endereços de carteiras errados, erros ao escrever os montantes transferidos ou com a mistura do montante transferido com o montante a enviar.
3. Erros, bugs e outros problemas relacionados com o software de criptomoedas.

O desenvolvimento da BTCV está centrado nas funcionalidades de segurança e proteção, conveniência para o utilizador e experiência do utilizador. Também acreditamos que estes são os principais obstáculos que impedem que uma parte significativa da sociedade se torne parte da comunidade cripto global.

## A Abordagem da BTCV

As criptomoedas deram aos utilizadores liberdade e responsabilidade sobre a forma como armazenam, gerem e transferem activos através de redes P2P. Neste “white paper”, assumimos que todos os utilizadores de criptomoedas devem estar familiarizados com os conceitos de chave privada e pública, e saber como armazenar e proteger em segurança as chaves. Com base neste pressuposto, nós desenvolvemos uma nova abordagem à gestão de chaves e à sua utilização para vários tipos de transações.

### Solução de Segurança 3-Keys

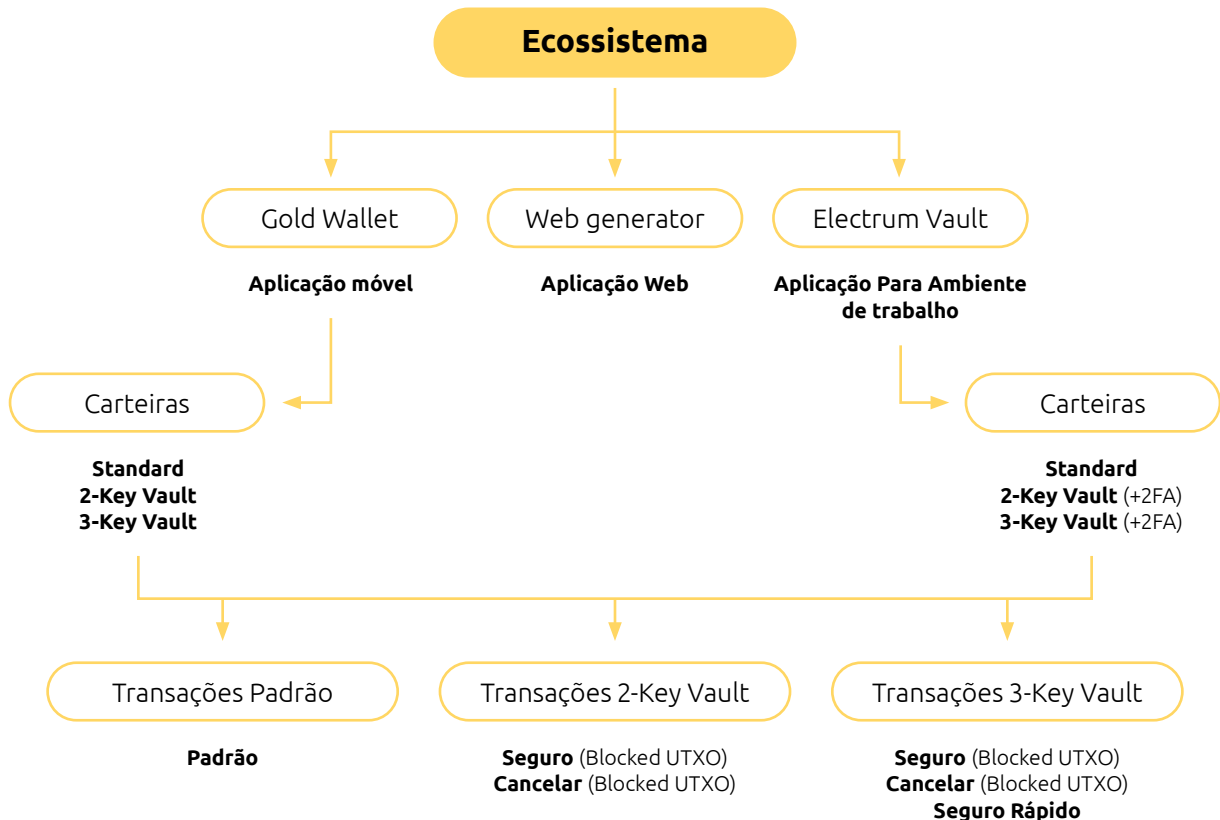
Bitcoin Vault desenvolveu uma Solução de Segurança 3-Key, que requer que os utilizadores criem três chaves Elliptic Curve Digital Signature Algorithm (ECDSA) – uma é armazenada automaticamente dentro da aplicação e as outras duas precisam de ser geridas pelo utilizador. A configuração atual da Bitcoin Vault permite aos utilizadores cancelar a transação iniciada e inverter a mesma para um endereço de carteira existente ou para um novo endereço de carteira.

A solução suporta três chaves ECDSA, com funções diferentes no ecossistema:

- A Chave de Transação Padrão é criada automaticamente e funciona em segundo plano. É necessária para iniciar todas as transações e para recuperar uma carteira no caso de pirataria informática ou problema técnico.
- Chave de Cancelamento de Transação permite aos utilizadores realizar o cancelamento de transações no prazo de aproximadamente 24 horas, depois de 144 blocos serem criados.
- A Chave de Transação Rápida dá aos utilizadores a possibilidade de fazer transações rápidas seguras e transferir BTCV numa questão de minutos.

## O Ecossistema da Bitcoin Vault

O ecossistema da Bitcoin Vault inclui três aplicações, que foram criadas na empresa exclusivamente com o objetivo de armazenar e gerir a BTCV. Juntas, formam uma ferramenta poderosa que garante um padrão mais elevado de segurança, transparência e liberdade.



### Gold Wallet

Gold Wallet é uma aplicação para dispositivos móveis concebida para armazenar, enviar e receber a BTCV. Permite aos utilizadores criar três tipos de carteiras e realizar vários tipos de transações: Segura e Rápida, Segura e de Cancelamento. A Gold Wallet também pode ser usada como autenticador para a autenticação de dois fatores (2FA) da aplicação Electrum Vault versão para o ambiente de trabalho do seu computador.

### Key Generator

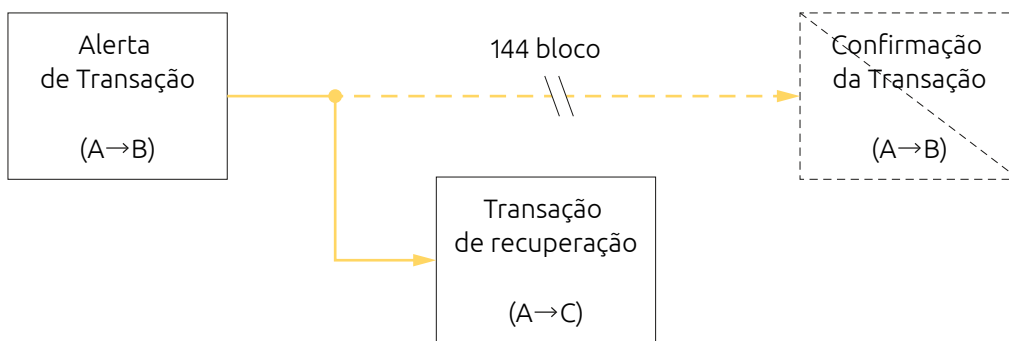
O Key Generator é uma aplicação baseada na web, que cria chaves individuais públicas e privadas necessárias para criar carteiras e realizar transações. Utiliza apenas recursos locais, o que significa que o processo de criação de chaves, bem como as próprias chaves, nunca deixam o dispositivo do utilizador. Não são armazenadas em lugar algum e não podem ser acedidas online. As chaves são armazenadas offline, proporcionando o máximo nível de segurança.

### Electrum Vault

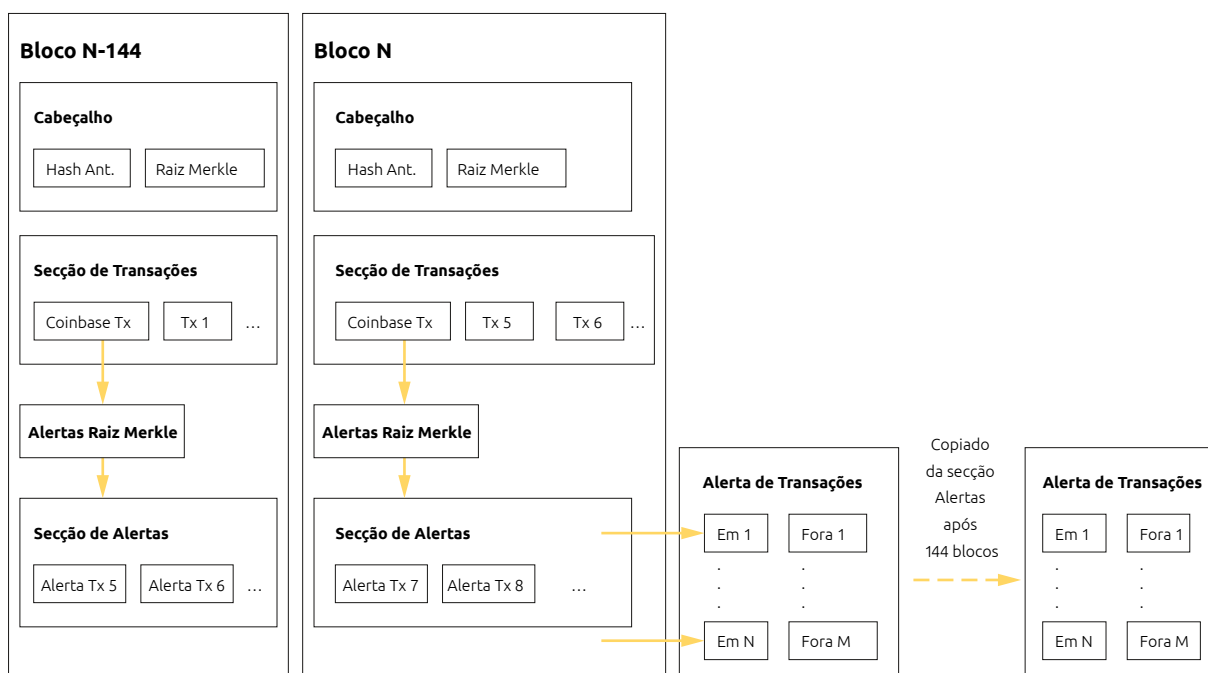
Electrum Vault é uma aplicação “desktop” para o ambiente de trabalho do seu computador, baseada numa Carteira Electrum de código aberto. Tem todas as funcionalidades da Gold Wallet, o que significa que pode ser utilizada para armazenar, enviar e receber BTCV, criar carteiras e realizar transações que incluem: Transação Segura e Rápida, Segura e Cancelamento.

## Perspectiva Técnica

Script “códigos” de bloqueio, atraso predefinido de 144 blocos, transações de alerta na cadeia “Blockchain”:



BTCV Estrutura de bloco com secção de alerta (como é armazenada, o que acontece quando a transação muda de estado de alerta para confirmado, como os mineradores verificam quando a transação muda de estado)



Alertas de Transações alteram o ciclo de vida dos UTXOs.

Na versão padrão, o UTXO tem dois estados: não utilizado e utilizado (o que basicamente significa que é removido). Uma nova versão da Bitcoin Vault introduz um novo estado – confirmado. Isto altera a forma como os UTXOs são armazenados na base de dados. A partir de agora, o estado “confirmado” é o momento em que o UTXO é removido da base de dados e o estado utilizado bloqueia o UTXO e armazena a informação sobre a altura do bloco em que foi utilizado. Desta forma, o sistema aguarda que o Alerta de Transação seja confirmado antes de remover o UTXO.

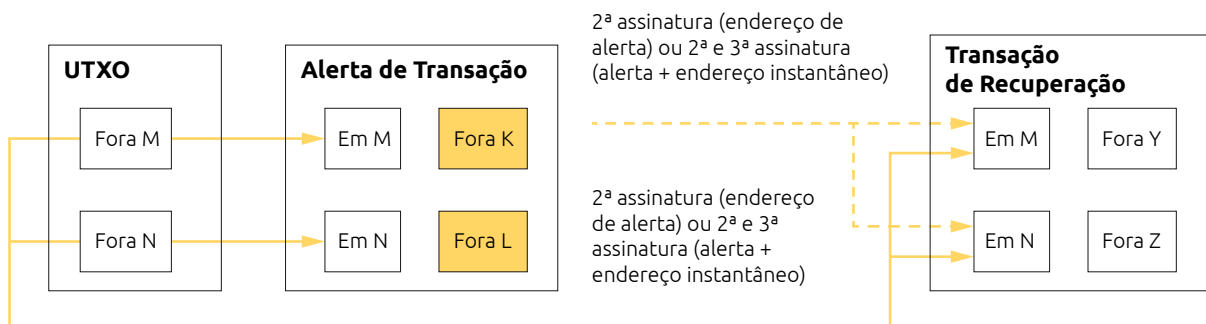
Esta é uma abordagem necessária porque, até à recepção da confirmação, o Alerta de Transação poderá ser recuperado com a Transação de Recuperação (utiliza apenas UTXO bloqueado como inputs). A melhor forma de alterar o ciclo de vida do UTXO na aplicação, seria armazenar informações sobre a altura em que foram utilizados – altura de utilização. Esta nova informação determinará em que estado se encontra o UTXO:

- 0 quando não utilizado.
- >0 quando utilizado.

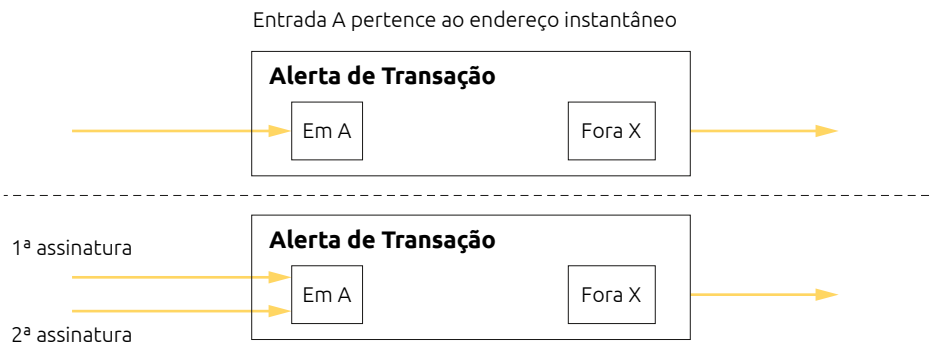
Além disso, a mesma informação deve ser considerada na estrutura “Undo”. A lista Undo armazena a informação dos estados anteriores dos UTXOs em diferentes alturas e utiliza essa informação quando a reorganização da cadeia ocorre.

Os novos estados e tipos de transação UTXO, têm também um impacto nos saldos visíveis para os utilizadores. Os UTXO que estão no estado utilizado devem ser contados como um novo saldo que será visível no saldo confirmado. Não pode ser contado como saldo não confirmado, porque esse saldo está relacionado com transações não processadas e passíveis de serem utilizadas. A ideia é criar saldos que são não utilizáveis mas informativos:

- alertas enviados – contados dos UTXOs no estado utilizado, que são bloqueados por Alertas das Transações,
- alertas recebidos – contados dos UTXOs que vão estar disponíveis após a confirmação dos Alertas das Transações..



Como funciona a Transação Rápida (explicação do “by-pass” de 24h de atraso, o que o torna possível – multi-assinaturas):



## Prova de Trabalho

Bitcoin Vault é uma moeda de “Proof-of-Work” prova de trabalho baseada no código fonte aberto Bitcoin Royale. Com o Hardfork realizado a 17 de Novembro de 2020, foi implementada uma mineração combinada com a Bitcoin (BTCV).

## Mineração Combinada

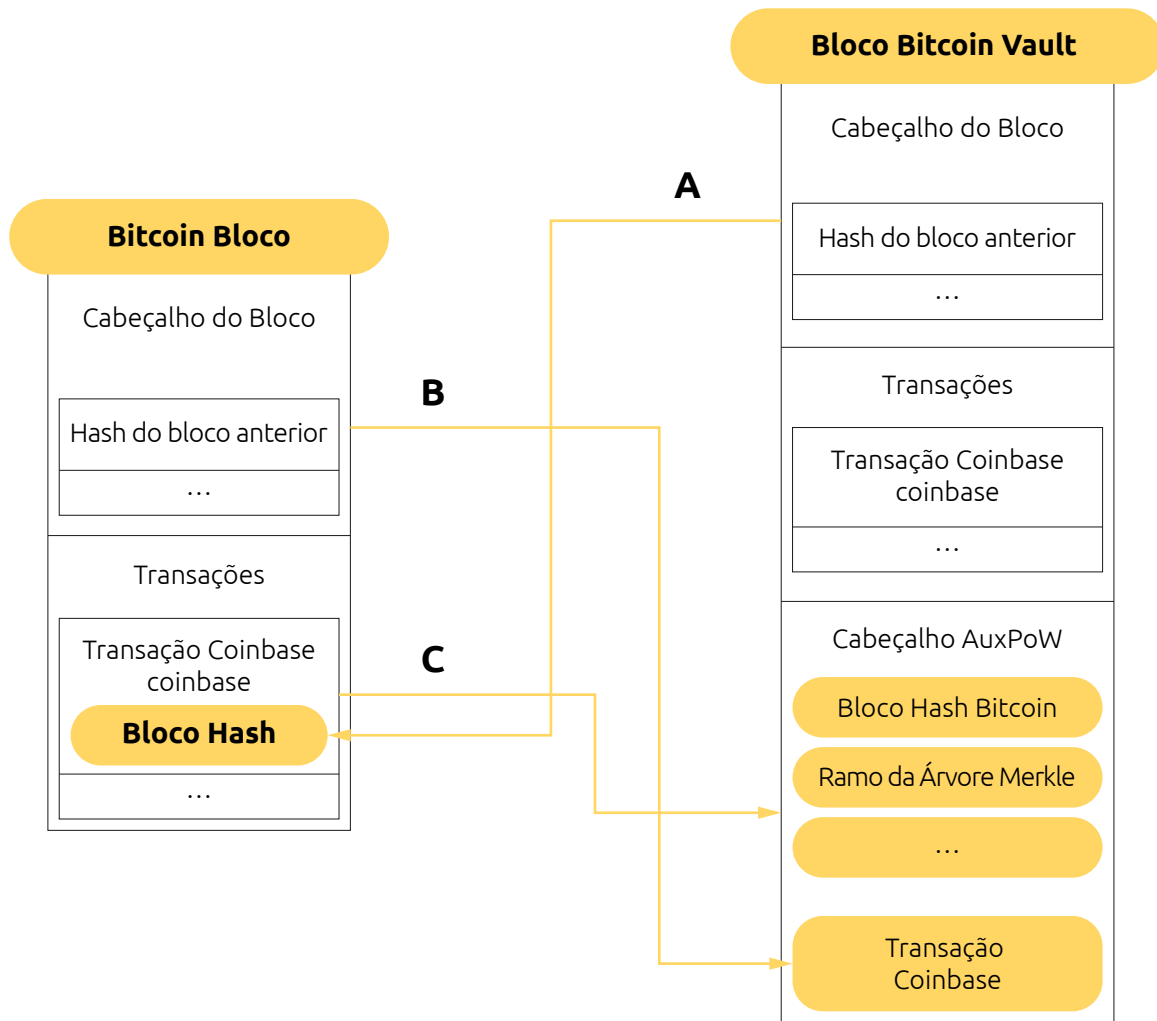
Juntamente com uma grande atualização do protocolo BTCV no bloco número 58.420, a Bitcoin Vault foi também ajustada para aceitar a mineração combinada. A Mineração Combinada, também conhecida como Prova de Trabalho Auxiliar, é um processo em que os mineradores estão simultaneamente à procura de “PoW” para pelo menos duas criptomoedas separadas com o mesmo poder computacional. Contudo, para construir uma tal relação entre os blockchains – parente e auxiliar – é mais fácil quando a cadeia auxiliar está preparada para a mudança.

Na Bitcoin Vault, a mineração combinada foi implementada com a Bitcoin, uma vez que ambas as criptomoedas utilizam a função hash SHA-256. Neste caso, a BTC é a “corrente-mãe” e a BTCV a corrente auxiliar.

Como resultado, as soluções de prova de trabalho (parente) da Bitcoin podem ser utilizadas para validar a Bitcoin Vault (corrente auxiliar) como mecanismo de consenso da prova de trabalho auxiliar (AuxPoW).



Explicação técnica com exemplo do gráfico da estrutura dos blocos e da relação entre os blocos BTC e BTCV:



Com a implementação da mineração combinada ao protocolo, os mineradores da BTCV são incentivados pela possibilidade de obter duas recompensas de blocos tanto da BTC como das correntes de bloqueio “blockchains” da BTCV. Um incentivo adicional é que, graças à potência de hash adicional acrescentada à rede através do “piggybacking” da rede Bitcoin com uma percentagem de hash mais elevada, a segurança da rede é aumentada.

### Recompensas por Bloco

A Bitcoin Vault tem um fornecimento total de 21 milhões de moedas e um tempo estimado de mineração por um bloco de 10 minutos.

A recompensa por bloco Bitcoin Vault foi concebida para eliminar certos problemas que surgem nas fases iniciais de desenvolvimento da criptomoeda. Foram identificados dois problemas principais:

O período inicial para ganhar novos participantes é demasiado curto, para atingir o número certo de membros da comunidade necessários para o desenvolvimento sustentável do projeto.

As recompensas por bloco depois do período inicial diminuiriam drasticamente. Isto pode desencorajar os mineradores de participarem no processo de mineração e resultar em quedas significativas na potência de hash.

A fim de prevenir tais ameaças, a Bitcoin Vault propôs as seguintes soluções:

- Prolongar o período com prémios por bloco mais elevados, para 46 meses.
- Dividir este período em nove subperíodos mais curtos, de seis em seis meses, com uma redução mais lenta da recompensa por bloco.

Isto permite que a equipa por detrás do projeto tenha tempo suficiente para o desenvolvimento. A comunidade tem uma oportunidade de crescer para números significativos, os mineradores são incentivados a participar na rede desde os seus primeiros dias e por um período mais longo, e existe tempo suficiente para que o número de moedas possa alcançar a Bitcoin, sem causar uma redução drástica das recompensas por bloco.

Durante esse período, a redução das recompensas por bloco é programada da seguinte forma:

<b>Data</b>	<b>BTCV Redução de Recompensas</b>	<b>Número de sub-período</b>	<b>Recompensa por bloco</b>	<b>Tempo de Sub-período</b>	<b>Blocos de Sub-períodos</b>
Maio – 2020	175 a 150	1	175	6 meses	29850
Nov. – 2020	150 a 125	2	150	6 meses	26600
Maio – 2021	125 a 100	3	125	6 meses	26600
Nov. – 2021	100 a 75	4	100	6 meses	26600
Maio – 2022	75 a 50	5	75	6 meses	26600
Nov. – 2022	50 a 25	6	50	6 meses	26600
Maio – 2023	25 a 12,5	7	25	6 meses	26600
Nov. – 2023	12,5 a 6,25	8	12.5	6 meses	26600
Maio – 2024	6,25 a 3,125	9	6.25	6 meses	26600

Como resultado, 19.687.500 moedas vão ser distribuídas durante este período, recuperando e atingindo o mesmo número de Bitcoins no 4<sup>º</sup> halving (previsto para 11 de Março de 2024). Depois disso, a recompensa por bloco BTCV seguirá o calendário de halving da Bitcoin.

## Desenvolvimento da Bitcoin Vault

### Etapas do desenvolvimento da BTCV:

Maio 2019 – Dezembro 2019	Pre-Alpha
Dezembro 2019 – Setembro 2020	Alpha
Setembro de 2020 – Novembro de 2020	Beta
Novembro de 2020	Mainnet

### Mainnet

A Mainnet foi lançada com sucesso a 17 de Novembro de 2020 com o número 58.420 de altura de bloco.

### Objetivos

Em Dezembro de 2020, a Equipa de Desenvolvimento da BTCV lançou novos objetivos que abrangem os anos 2021-2022. A continuação do desenvolvimento da BTCV foi dividida em seis etapas de trabalho:

### Etapa de trabalho N.º 1 – Atualizações de desenvolvimento

O trabalho de desenvolvimento diz respeito a todas as atualizações do blockchain que serão adicionadas à Bitcoin Vault. O principal objetivo desta etapa de trabalho é participar no ecossistema Dapp “Aplicações descentralizadas” em torno do Ethereum 2.0 com a BTCV Envolvida (wBTCV) até ao final de 2021.

- Primeiro Trimestre 2021
  - wBTCV ERC-20 token – análise e “tokenomics” por detrás do wBTCV
- Segundo Trimestre 2021
  - Integração do Ledger
- Terceiro Trimestre 2021
  - wBTCV ERC-20 token fase de testes beta
- Quarto Trimestre 2021
  - wBTCV lançamento
  - Início da integração com o ecossistema DeFi
- Primeiro Trimestre 2022
  - Integração total com o ecossistema DeFi
  - Desenvolvimento de DApps – Aplicações Descentralizadas
- Segundo Trimestre 2022+
  - Desenvolvimento de DApps – Aplicações Descentralizadas

## **Etapa de trabalho N.º 2 – Atualizações de Segurança**

Bitcoin Vault tem uma equipa interna de especialistas em segurança do blockchain. A Mainnet do Blockchain foi verificada inúmeras vezes e em 2021 o nosso principal objetivo será reforçar o código e identificar quaisquer erros e falhas deixadas, também com o apoio de parceiros externos. Após testes de penetração internos e externos, executaremos um programa de prémios aberto para programadores e trabalharemos em estreita colaboração com a comunidade 'white hat'.

- Primeiro Trimestre 2021
  - Auditoria de código completa (interna e externa)
- Segundo Trimestre 2021
  - Testes de Penetração (internos)
- Terceiro Trimestre 2021
  - Testes de Penetração (externos)
- Quarto Trimestre 2021
  - Auditoria de segurança CIS/20
  - Matriz de Segurança Cloud
- 2022+
  - Mais melhorias e auditorias de segurança
  - Hackathons
  - Programa de recompensa

## **Etapa de trabalho N.º 3 – Atualizações da experiência do utilizador**

A experiência do utilizador é um dos fatores mais importantes por detrás da utilização e adoção do produto. O nosso objetivo é continuar a desenvolver e actualizar aplicações e adaptá-las às necessidades de uma variedade de utilizadores, com base nas opiniões recebidas da comunidade.

- 1 Trim. E 2 Trim. de 2021
  - Aplicação móvel GoldWallet melhorias UX
  - Electric Vault aplicação móvel, troca de versão fácil e versão especialista
- Terceiro Trimestre 2021
  - GoldWallet Notificações para os utilizadores
- Quarto Trimestre 2021
  - GoldWallet Integração com aplicações de outras empresas
- 2022+
  - Outras melhorias UX

## **Etapa de trabalho N.º 4 – Produtos**

Juntamente com a equipa desenvolvimento das tecnologias de informação “IT”, estamos seriamente concentrados na adoção pelo mercado com a preparação do lançamento de novos produtos. Em 2021, queremos lançar produtos de “staking” com o apoio dos parceiros BTCV e ligar o ecossistema BTCV às moedas FIAT.

- Primeiro Trimestre 2021
  - Novos produtos de staking através de empresas terceiras
  - Novos produtos de Trading “negociação”
- Segundo Trimestre 2021
  - Novos gateways de pagamento
  - Integrações com moedas FIAT
- Terceiro Trimestre 2021
  - Plataforma de análise de dados (Big Data)
- Quarto Trimestre 2021
  - Produtos relacionados o token wBTCV
- 2022+
  - Novas funcionalidades 3-Keys
  - Aplicações descentralizadas – Produtos

## **Etapa de trabalho N.º 5 – Atividades de Marketing**

Em 2021, planeamos o lançamento de uma campanha global de consciencialização e envolvimento, destinada aos atuais e futuros utilizadores da BTCV, bem como a toda a comunidade cripto em todo o mundo. Vamos procurar novas parcerias que reforcem a segurança do blockchain da BTCV , bem como permitir que a BTCV esteja à frente da indústria de investigação quântica.

- Primeiro Trimestre 2021
  - Lançamento de um novo site
- 2 Trim. e 3 Trim. de 2021
  - Campanha de sensibilização e de envolvimento global
- Quarto Trimestre 2021
  - Parceria estratégica de segurança
- 2022+
  - Parceria científica estratégica

## **Etapa de trabalho N.º 6 – Outras atualizações**

Com algumas atualizações adicionais ao ecossistema da BTCV, queremos conectar e envolver-nos com a nossa comunidade e oferecer novas opções para os “hodlers” através de um novo mecanismo “airdrop”, que será totalmente lançado no início do segundo trimestre de 2021. O nosso objetivo a longo prazo será também a computação quântica e o seu potencial para influenciar a criptografia do blockchain.

- Primeiro Trimestre 2021
  - Desenvolvimento e lançamento do novo mecanismo de “airdrops”
  - Lock da carteira de Airdrops

- Segundo Trimestre 2021
  - Airdrops plataforma / aplicação
- Terceiro Trimestre 2021
  - Plataforma de análise do Blockchain
- Quarto Trimestre 2021+
  - Investigação Quântica
  - Programa de bolsas para parcerias científicas

## Computação Quântica e DLT – A Nossa Visão

Na qualidade de criadores de blockchains, estamos genuinamente interessados no progresso das tecnologias quânticas. Os investigadores e programadores que trabalham em tecnologias de ledger distribuído (DLTs), tal como as blockchains dependem da criptografia da chave pública e das funções de hash que são essenciais para todas as soluções do blockchain.

Bitcoin Vault blockchain é protegida por poderosos algoritmos criptográficos tais como ECDSA e SHA-256, também utilizados na Bitcoin, bem como em muitas outras criptomoedas. Os algoritmos de encriptação atualmente utilizados são suficientemente poderosos para os métodos computacionais tradicionais.

### Ameaça da Computação Quântica

Em teoria, a melhoria exponencial do desempenho informático com tecnologia quântica pode levar ao ponto de descodificar uma chave pública para calcular o hash da chave privada ou descodificar o algoritmo SHA-256 para obter o único bloco de valor de hash necessário no blockchain. De acordo com muitos especialistas na matéria, ainda estamos a anos de investigação do desenvolvimento de computadores quânticos estáveis. Mesmo assim, esses computadores teriam de ser devidamente codificados com o objetivo de descodificar certos algoritmos criptográficos.

### Oportunidade da Computação Quântica

Em vez de nos concentrarmos nas ameaças, gostaríamos de nos concentrar nas oportunidades.

Mais uma vez, em teoria, quando os computadores quânticos são capazes de alcançar estabilidade suficiente para realizar cálculos fiáveis, seria possível utilizá-los para melhorar os algoritmos criptográficos. Esta é a oportunidade que vemos para o futuro do blockchain.

Nos dias de hoje, podemos considerar diferentes abordagens para atingir o objetivo de uma moeda à prova de computação quântica, ou seja:

- Criptosistemas baseados em reticulados
- Criptosistemas de chave pública de base multi-variada.
- Criptosistemas super-singular elliptic-curve isogenies
- Criptosistemas de assinatura digital baseados em hash.
- Soluções híbridas como as testadas pelo Google (CECPQ1 e CECPQ2).
- E alguns outros.

Para encontrar uma solução anti-quântica adequada e preparar a moeda BTCV para uma era pós-quântica, a nossa equipa de desenvolvimento precisa de fazer mais investigação em termos das técnicas de compactação de chaves necessárias e sobre a utilização de certos tipos de códigos e técnicas de codificação.

No entanto, hoje em dia, não existem algoritmos do blockchain pós-quantum que forneçam chaves com um tamanho pequeno, assinaturas curtas/tamanhos de hash, execução rápida, baixa complexidade computacional e baixo consumo de energia, tudo ao mesmo tempo. Estes fatores são especialmente críticos para dispositivos incorporados com recursos limitados, como os utilizados na “Internet of Things” Internet das Coisas.

Durante os próximos 3 a 5 anos, nós os criadores da BTCV vamos concentrar-nos em atingir a prontidão operacional em resistência quântica através de novas parcerias, especialmente com peritos de várias empresas, start-ups e universidades técnicas.

## Fundador da Bitcoin Vault

Bitcoin Vault foi fundada por Eyal Avramovich, CEO da Minebest e um dos principais líderes mundiais em instalações de mineração cripto localizadas na Ásia e na Europa.

Mais informações sobre o Minebest podem ser encontradas aqui: <https://minebest.com/>

Mais informações sobre a equipa por detrás da Bitcoin Vault podem ser encontradas no site oficial: <https://bitcoinvault.global/>

## Trabalhos Relacionados

Gostaríamos de dar crédito aos criadores da Bitcoin Royale pela ideia conceptual que levou ao desenvolvimento da Bitcoin Vault.

Bitcoin Royale whitepaper: <https://bitcoinroyale.org/bitcoinroyale.pdf>

## Referências BTCV:

Podem ser encontradas informações adicionais sobre o projeto:

<https://bitcoinvault.global/>

<https://twitter.com/vaultbitcoin>

<https://medium.com/bitcoin-vault-btcv>

[https://t.me/Bitcoin\\_Vault](https://t.me/Bitcoin_Vault)

<https://www.facebook.com/bitcoinvaultofficial>

<https://www.instagram.com/bitcoinvaultofficial>

<https://www.youtube.com/c/BitcoinVault>

## Referências

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](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](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 Dzhabarov, Shamil Khalilov, Ilya Teterin, Graviton: interchain swaps and wrapped tokens liquidity incentivisation solution, <https://arxiv.org/ftp/arxiv/papers/2009/2009.05540.pdf>