Bitcoin Vault: Entre Pares (Peer-to-Peer) Ouro Eletrónico Anti-Roubo

Eyal Avramovich
github.com/bitcoinvault

Abstrato. A visão original de Satoshi Nakamoto para a Bitcoin era a de criar uma versão peer-to-peer de dinheiro eletrónico. A maioria dos "forks" (bifurcações) de sucesso do protocolo tentam melhorar esta visão e proporcionar um sistema de pagamentos mais escalável e eficiente. Vemos a maior promessa da Bitcoin não enquanto meio de troca mas enquanto reserva de valor – uma melhor forma de ouro, não de dinheiro. Propomos um conjunto de modificações ao protocolo original com o objetivo de cumprir esta promessa através da criação da derradeira reserva eletrónica de valor. Através do aumento do tempo de confirmação efetiva de transações da Bitcoin de 10 minutos para 24 horas, somos capazes de enfrentar a maior falha da Bitcoin enquanto forma de ouro – a susceptibilidade ao roubo. Um sistema concebido não tanto para o pagamento de um café, mas para a manutenção das poupanças de uma pessoa com total paz de espírito, onde cada transação é alertada na cadeia por 144 blocos, podendo ser cancelada em caso de emergência com uma chave de recuperação que nunca foi utilizada anteriormente e que é, portanto, invulnerável. O bootstrap deste sistema não é através de um hard fork, mas através de um mecanismo mais justo de mineração acelerada, permitindo ao sistema alcançar a Bitcoin num curto período de tempo. Gostávamos de dar todo o crédito ao criador do papel branco da Bitcoin Royale [1] , que criou a visão do ouro eletrónico sem furto. Como equipa, gostaríamos de avançar com esta ideia e começar a implementar todas as características cruciais mencionadas abaixo e torná-la ainda mais avançada através da solução da 3ª chave privada que é revelada como uma característica adicional no parágrafo 6.2.

1. Introdução

A Bitcoin [2] é um sistema de pagamentos descentralizado e inovador lançado em 2009 que permite às partes transacionarem diretamente sem passar por uma instituição financeira confiável. O sistema depende da prova de trabalho para manter um livro razão distribuído sem um operador de confiança, que é seguro desde que os nós honestos controlem mais potência de CPU do que qualquer grupo cooperante de nós atacantes. Originalmente, a Bitcoin foi descrita pelo seu criador, Satoshi Nakamoto, como um "sistema de dinheiro eletrónico".

Ao longo dos anos, foram lançadas várias modificações bem sucedidas do protocolo original sob a forma de forks da base de códigos da Bitcoin. Estas incluem a Litecoin [3] lançada em 2011 para reduzir o tempo de confirmação da transação e alterar o algoritmo de prova de trabalho para favorecer o hardware de grau de consumidor tal como GPU; a Bitcoin Cash [4], lançada em 2017 para escalar o rendimento da transação do protocolo original através do aumento do tamanho dos blocos; e a Bitcoin Gold [5], que

também foi lançada em 2017 para tornar obsoleto o equipamento especializado de mineração através da alteração do algoritmo de hash.

Fiel à visão original, o foco principal nestes e noutros forks é fazer da Bitcoin um melhor sistema de dinheiro. As limitações do protocolo original, tais como as elevadas taxas de transação, os tempos de confirmação de 10 minutos e a produção aproximada de apenas 4 transações por segundo, dificultam a capacidade da Bitcoin para competir com os sistemas de pagamento online centralizados dominantes hoje em dia.

2. Dinheiro Eletrónico ou Ouro Eletrónico

Enquanto que a Bitcoin como dinheiro eletrónico não alcançou grande sucesso com a adesão do consumidor, tem sido significativamente mais bem sucedido como uma forma de ouro eletrónico. Existe um debate de longa duração na indústria sobre se a Bitcoin é superior como meio de câmbio ou, de facto, como reserva de valor. O ouro não é um meio eficaz de pagamento de bens e serviços no dia-a-dia. Os consumidores investem principalmente em ouro para se protegerem contra a inflação e para preservar o poder de compra futuro. Ao contrário das moedas nacionais, é a política monetária da Bitcoin e a sua oferta limitada que a tornam particularmente atrativa a este respeito.

A história mostra que os sistemas raramente podem ser concebidos para satisfazer vários objetivos concorrentes ao mesmo tempo. Optimização Para se tornar um melhor meio de câmbio, a Bitcoin diminui o seu potencial como reserva de valor. Da mesma forma, ao sacrificar mais nas propriedades necessárias para o dinheiro eletrónico útil, podemos melhorar substancialmente a sua utilidade como ouro eletrónico. Neste artigo, propomos uma série de modificações ao protocolo original da Bitcoin com foco num único objetivo – criar a derradeira reserva de valor.

Se deixarmos de dar prioridade à concorrência enquanto sistema de pagamento online, não precisamos de nos focar nas taxas ou rendimentos da transação. Afinal de contas, o ouro é caro no transporte e normalmente é adquirido como investimento a longo prazo. Uma propriedade que é particularmente relevante para os nossos esforços é o tempo de confirmação da transação. Soluções nesta frente, tais como o aumento substancial do tempo médio de confirmação de 10 minutos da Bitcoin, podem levar a vantagens fundamentais. Uma vez que não seria mesmo de esperar transportar um carregamento de ouro em menos de 10 minutos, este sacrifício parece natural.

3. O Problema do Roubo

A condição chave de uma reserva de valor é a de não ser perecível. O roubo é um dos principais riscos de perda quando se lida com algo de valor. O ouro tem um desempenho muito bom a este respeito. O roubo físico do ouro é significativamente mais arriscado na execução do que qualquer ataque virtual a um bem eletrónico. Além disso, seria difícil para um ladrão esconder uma carga considerável de ouro roubado das autoridades, principalmente nas fronteiras. Também não é tarefa fácil lavar e liquidar ouro roubado em grandes quantidades, mantendo-se anónimo.

Infelizmente, em termos comparativos, a Bitcoin não se sai muito bem. Os fundos são protegidos pelo protocolo com conjuntos de cripto chaves privadas. Obter acesso eletrónico a estas chaves permite a um atacante apoderar-se de todos os fundos à distância, de forma imediata e irrevogável. A lavagem de fundos roubados é também significativamente mais fácil, uma vez que as transações são pseudónimas, podendo a rastreabilidade ser perturbada pela utilização de misturadores [6] e identidades Sybil que podem ser criadas a granel. Como resultado, o roubo de criptomoedas está a aumentar, com mais de mil milhões de dólares roubados em 2018 [7]. As listas comunitárias de incidentes graves [8] mostram que mesmo as instituições profissionais bem versadas nas mais recentes práticas de segurança são propensas a ataques.

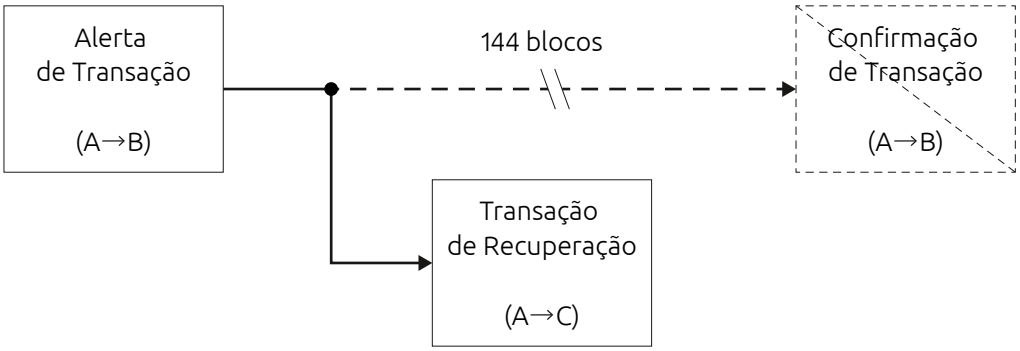
A gestão segura das chaves privadas por parte dos utilizadores finais está a revelar-se ser um dos maiores desafios da Bitcoin. Uma vez que as chaves devem ser utilizadas de forma regular para interagir com os fundos e as transações aprovadas devem ser transmitidas através da Internet, cada chave acaba eventualmente por se tornar vulnerável. Práticas conscientes de segurança, como a divisão dos fundos entre carteiras "quentes" e "frias", são complexas e não conseguem resolver o problema de raiz. Os incidentes mostram que as carteiras quentes contêm inevitavelmente quantidades significantes [9, 10] e a utilização de carteiras frias apenas reduz a interação com chaves mas não elimina completamente [11].

4. Solução Anti-Roubo

Como forma de eliminar o roubo, propomos uma solução com base num novo e sofisticado roteiro de bloqueio e modificação do protocolo. Uma transação executada através do novo roteiro de bloqueio será, por defeito, colocada em espera durante 24 horas. Quando um mineiro adiciona uma transação a um novo bloco, a transação deixa de ser confirmada de forma imediata. Em vez disso, será acrescentada na cadeia como um alerta com uma duração de 144 blocos (assumindo o tempo de bloco de 10 minutos). Se não for perturbada durante 144 blocos, a transação passará do estado de alerta para "confirmado".

O benefício dos alertas na cadeia é que os proprietários de moedas irão receber notificações antecipadas não censuráveis sempre que as suas moedas são movimentadas. O proprietário terá 24 horas para agir em caso de alerta e será capaz de anular a transferência se não autorizada. Os levantamentos em espera são um padrão comprovado da indústria anti-roubo em carteiras de custódia e no sistema bancário tradicional. A Coinbase Vault [12], por exemplo, tem um tempo de espera de 48 horas. A nossa proposta de solução proporciona a mesma proteção sem um terceiro de confiança.

A anulação de emergência de uma transação em estado de alerta requer uma transação de recuperação especial e é executada de forma imediata, sem ser sujeita ao período de espera de 24 horas. A transação de recuperação requer uma chave de recuperação que deve ser incorporada no roteiro de fecho durante a criação da carteira. Uma vez registada a chave de recuperação para uma determinada carteira, não pode ser alterada.



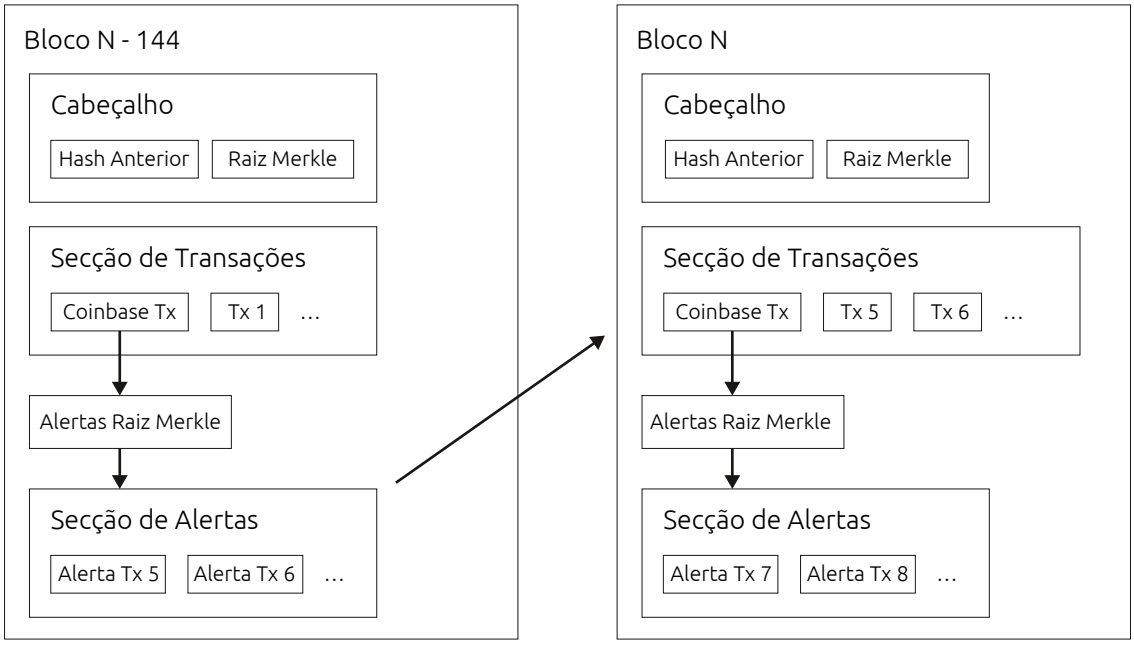
A chave de recuperação privada utilizada para a anulação de emergência destina-se a ser uma chave nova que nunca tenha sido utilizada anteriormente. Esta chave pode ser gerada offline e nunca deve ser ligada à Internet ou guardada em qualquer dispositivo. O processo de registo requer apenas a parte pública desta chave, assegurando que a chave privada pode permanecer intocada. Ao contrário das chaves da carteira fria, que devem ser utilizadas ocasionalmente e são assim vulneráveis ao roubo, a chave de recuperação será utilizada pela primeira vez apenas na anulação de emergência e, portanto, pode ser completamente resistente ao roubo. Uma vez utilizada a chave de recuperação, deve ser considerada comprometida e todos os fundos devem ser imediatamente transferidos para uma nova carteira protegida por uma nova chave de recuperação não utilizada.

O conceito original de ouro digital da Bitcoin Royale de adotou o tempo de espera de todas as transações no sistema por 24 horas, tornando a moeda numa reserva de valor segura e de movimentação lenta. Gostaríamos de expandir este conceito para obter o melhor de dois mundos – o ouro digital e o dinheiro digital, sem qualquer concessão de segurança. A par dos alertas de movimentação lenta, mantemos condicionalmente as transações rápidas e "instantâneas". Para fornecer a maior segurança, o envio de tal transação irá exigir que um utilizador efetue um 2FA com base na cadeia de blocos, utilizando a 3ª chave fornecida durante a criação da carteira.

5. Blocos

Tal como o protocolo original da Bitcoin, cada bloco contém uma lista de transações confirmadas e contém o hash de raiz Merkle destas transações no seu cabeçalho. Uma vez que algumas transações têm de esperar 24 horas na cadeia, não podem ser acrescentadas de forma imediata à secção de transações de um bloco. Em vez disso, são acrescentadas a uma nova secção especial que não existe no protocolo original da Bitcoin – a secção dos alertas. O hash de raiz Merkle para a secção de alertas é armazenado na entrada da transação coinbase mantendo o cabeçalho do bloco compatível com a Bitcoin original.

Quando um novo bloco é extraído, o mineiro olha para os 144 blocos anteriores e examina a secção de alerta do bloco N-144. Todos os alertas para transações que ainda são válidas tornam-se confirmados e povoam a secção de transações do novo bloco.



Os passos para minerar o bloco N são os seguintes:

1) Adicionar novas transações regulares à secção de alertas do bloco N (não confirmadas).
2) Acrescentar novas transções instantâneas à secção de transações do bloco N (confirmadas).
3) Adicionar novas transações de recuperação à secção de transações do bloco N (confirmadas).
4) Examine a secção de alertas do bloco N-144 de e adicione as transações válidas à secção de transações do bloco N (confirmadas).

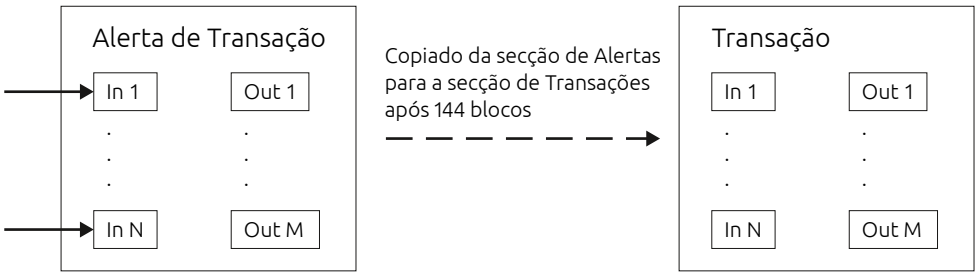
6. Roteiros

A funcionalidade central da Bitcoin Vault está disponível através do sofisticado roteiro de bloqueio, que se comporta de forma diferente, com base no número de assinaturas apresentadas no roteiro de desbloqueio. Estão disponíveis duas variantes:

1. Alerta de roteiro de bloqueio – exige ou uma ou duas assinaturas. Se for apresentada uma assinatura, é gerada uma transação de alerta. Se forem apresentadas duas assinaturas, é gerada uma transação de recuperação.
2. Alerta + roteiro de bloqueio instantâneo – requer uma, duas ou três assinaturas. Se for apresentada uma assinatura, é gerada uma transação de alerta. Se forem apresentadas duas assinaturas, é gerada uma transação instantânea. Se as três assinaturas forem apresentadas, é gerada uma transação de recuperação.

7. Transações

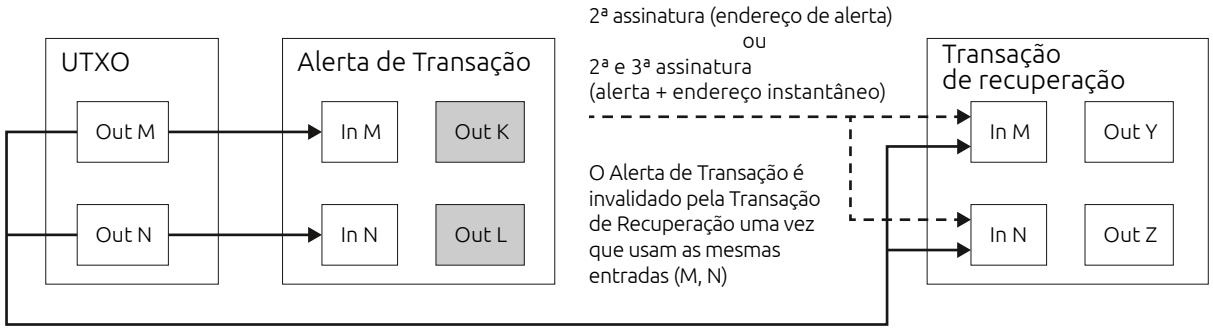
As transferências de moedas são realizadas utilizando transações regulares idênticas às do protocolo da Bitcoin. O seu formato não muda à medida que são movidos da secção de alertas para a secção de transações.



7.1. Transações de Recuperação

Uma transação de recuperação gasta o mesmo UTXO que o alerta recuperado. A diferença é que apresenta mais assinaturas para o mesmo UTXO: 2 em caso de roteiro de alerta de bloqueio, ou 3 em caso de roteiro de alerta + bloqueio instantâneo.

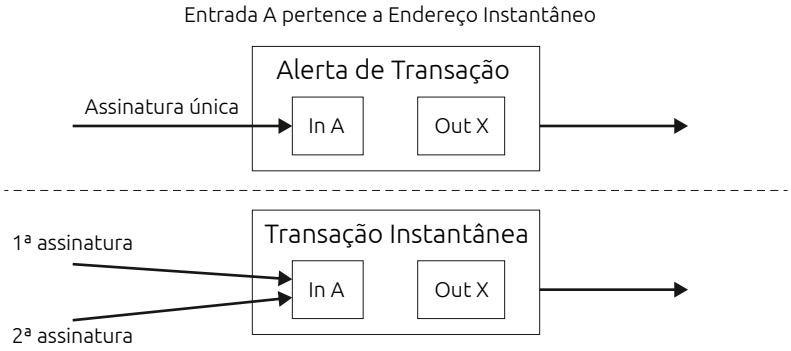
Quando uma transação de recuperação é processada, o UTXO recuperado é gasto, invalidando assim quaisquer alertas que se baseiem neste UTXO e impede que sejam confirmados após o seu tempo de espera de 24 horas.



7.2. Transações Instantâneas

Uma transação instantânea permite contornar o tempo de espera padrão de 24 horas para a confirmação da transação e acelerar a confirmação da mesma para cerca de 10 minutos. O seu mecanismo é semelhante ao da carteira multisig. Requer uma assinatura adicional de uma chave privada separada que deve ser guardada em segurança numa localização diferente. É por isso que as transações instantâneas só podem

ser enviadas a partir de endereços P2SH especiais – endereços instantâneos gerados a partir do alerta + roteiro de bloqueio instantâneo.



8. Compatibilidade

A nossa concepção tenta tornar o protocolo tão compatível quanto possível com o protocolo padrão da Bitcoin.

O objetivo subjacente é minimizar as alterações de código necessárias aos nós completos da Bitcoin existentes, carteiras, piscinas e mineiros. No entanto, se as alterações forem efetuadas numa cadeia de blocos já existente, vão requerer um hard fork, de forma a evitar a alteração do formato do cabeçalho do bloco, tornando assim a moeda incompatível com os mineiros ASIC da bitcoin, o hash de raiz Merkle para a secção de alertas é armazenado na entrada da transação de coinbase padrão.

Se o hard fork for necessário, o nosso objetivo é tornar a transição tão fácil quanto possível para os utilizadores de moedas existentes. Todos os tipos de roteiro existentes não alteram o seu comportamento, por isso todas as moedas existentes antes do hard fork são gastáveis de uma forma habitual. No entanto, aconselhamos vivamente a mudar para o novo, roteiros mais seguros.

9. Incentivo

O sistema toma emprestado o modelo de incentivo da Bitcoin, que se tem revelado bem sucedido ao longo da última década.

A incorporação de alertas requer pequenas modificações a este modelo. Os mineiros são incentivados a incluir os alertas de transações num bloco pela promessa de taxa calculada a partir da diferença entre valor das saídas e entradas. As taxas são calculadas a partir das futuras transações no bloco, e distribuídas para o mineiro original – o que inclui alertas de transações. O futuro mineiro irá ainda receber uma recompensa de bloco por extrair um novo bloco, todas as taxas a partir do novo instante, transações de registo e recuperação e a promessa de futuras taxas a partir de alertas de transações. O futuro mineiro

é obrigado, por regras de consenso, a incluir todos os alertas do bloco N-144 até às secções de transação, excluindo as que foram recuperadas.

Em caso de cancelamento do alerta, as taxas para o mineiro original do alerta são irrecuperáveis e o custo total é a taxa do alerta original mais a taxa para a transação de recuperação.

10. Trabalho Relacionado

Estamos particularmente impressionados com o trabalho de Malte Möser et al. sobre a Bitcoin Covenants [13]. A sua extensão da linguagem do roteiro da Bitcoin permite restrições na utilização futura de moedas, que podem ser utilizadas para implementar uma variedade de medidas de segurança. A principal das quais se refere às transações de vault, que se assemelham ao nosso mecanismo proposto de levantamento tardio.

Optamos por uma implementação mais simples que não requer um conjunto recorrente de roteiros personalizados para ser implementado por carteiras. A nossa proposta é mais do que uma extensão opcional, é uma alteração fundamental ao protocolo, com um amplo efeito obrigatório nas transacções. Transferir o peso da implementação para os mineiros e deixar a experiência de transação do utilizador final idêntica à padrão, permite-nos um melhor cumprimento da nossa missão de criar o verdadeiro ouro eletrónico.

References

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 ln 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.