Walltime Zero

negociação de criptoativos sem criptocustódia.

Felipe Micaroni Lalli <micaroni@gmail.com>
Igor Hjelmstron Vinhas Ribeiro <igorhvr@iasylum.net>

v 1.0, Campinas, 1º de abril de 2020

Abstract

Walltime Zero se define por uma "observadora de Blockchain" que valida transações públicas e realiza determinadas ações caso essa transação tenha ocorrido de fato. Este documento propõe um modelo para a negociação de criptoativos (e.g. Bitcoin, Litecoin) envolvendo moeda fiduciária (e.g. Real, Dólar) sem a necessidade de custódia centralizada desses ativos, através do conceito de "Oráculo de saída" (*Outbound Oracle*), eliminando por completo todos os riscos envolvidos com essa custódia, tanto para os usuários do serviço como para o custodiador. A ausência de custódia em criptoativos traz inúmeras vantagens para todas as partes envolvidas bem como para todo o ecossistema. Diferentemente de uma *exchange* tradicional, ao invés de receber criptoativos e moedas fiduciárias de ambas as partes interessadas, e guardá-las durante o período de troca (que pode se prolongar por meses ou anos), esse intermediário receberia apenas moedas fiduciárias de uma das partes. A parte que deseja trocar criptoativos por moedas fiduciárias (parte "vendedora") enviaria o criptoativo diretamente para a outra parte interessada em trocar moeda fiduciária por criptoativos (parte "compradora"). Seria verificada então se a transferência foi efetuada no Blockchain e, em caso positivo, seria efetuada uma transferência de moeda fiduciária de sua conta bancária para a conta da parte vendedora.

1 Motivação

Desde a criação do Bitcoin, a custódia centralizada de criptoativos tem se mostrado um fiasco completo por diversos motivos [10]. Não é a toa que o Bitcoin tem um lema bastante conhecido: "Be Your Own Bank" (Seja Seu Próprio Banco). A proposta da **Walltime Zero** segue alinhada com esse princípio do Bitcoin, evitando a terceirização de sua tutela.

1.1 Risco de criptocustódia

Há um risco muito grande no processo de delegação de custódia. Há o risco de perda simplesmente [8], de morte dos gerenciadores das chaves privadas [7], fraude, roubo, insolvência, *hacking* ou mal gerenciamento dos fundos. No ano de 2019 tivemos inúmeros casos desse tipo no Brasil [9]. O risco se aplica tanto para o usuário que terá seus fundos custodiados perdidos de forma irreversível como para o custodiador que — a não ser que ele mesmo seja o fraudador — poderá sofrer ameaças ou ter sua reputação destruída para sempre. Há muitos riscos a serem considerados mesmo com técnicas de segurança para mitigá-los, como por exemplo, o uso de *cold wallet*, multi-assinaturas, *timelock* entre outros, principalmente no caso do próprio custodiador ser desonesto. O roubo de criptoativos é muito atraente ao criminoso por ser irreversível e deixar pouco ou nenhum rastro. Num caso de quebra do custodiador, dificilmente se saberá com certeza se o real motivo foi incompetência em gerenciar os fundos, se ele foi vítima de um atacante virtual ou físico, ou então se ele mesmo aplicou um golpe.

Figure 1: Revista Bitcoin de agosto de 2012 mostrando um dos primeiros desastres resultante de criptocustódia centralizada, causando um grande *crash* no preço na época por conta da quebra da Bitcoinica.

Outro problema é que é quase impossível provar solvência de um criptoativo. Mesmo as técnicas mais sofisticadas desenhadas para isso tem limitações significativas [13]. Exemplo: o custoadiador sempre tem a opção de emprestar criptoativos para apresentá-los durante uma auditoria.

1.2 Centralização e inflação artificial

A centralização de criptoativos é danosa para o próprio criptoativo em si, resultando em uma espécie de "inflação artificial" a partir do momento que os custodiadores se tornam grandes e insolventes, desvalorizando o seu preço. Imagine uma *exchange* quase totalmente insolvente operando milhares de criptoativos: para o mercado, esses criptoativos existem enquanto eles não forem sacados da plataforma. Imagine agora várias *exchanges* grandes fazendo o mesmo: isso pode fazer facilmente com que o total de criptoativos "virtuais" (inexistentes) circulando seja muito maior que o real (aumento de oferta artificial). É claro que isso pode ser exposto quando esses custodiadores colapsarem, mas nesse meio tempo o ativo pode sofrer grande desvalorização.

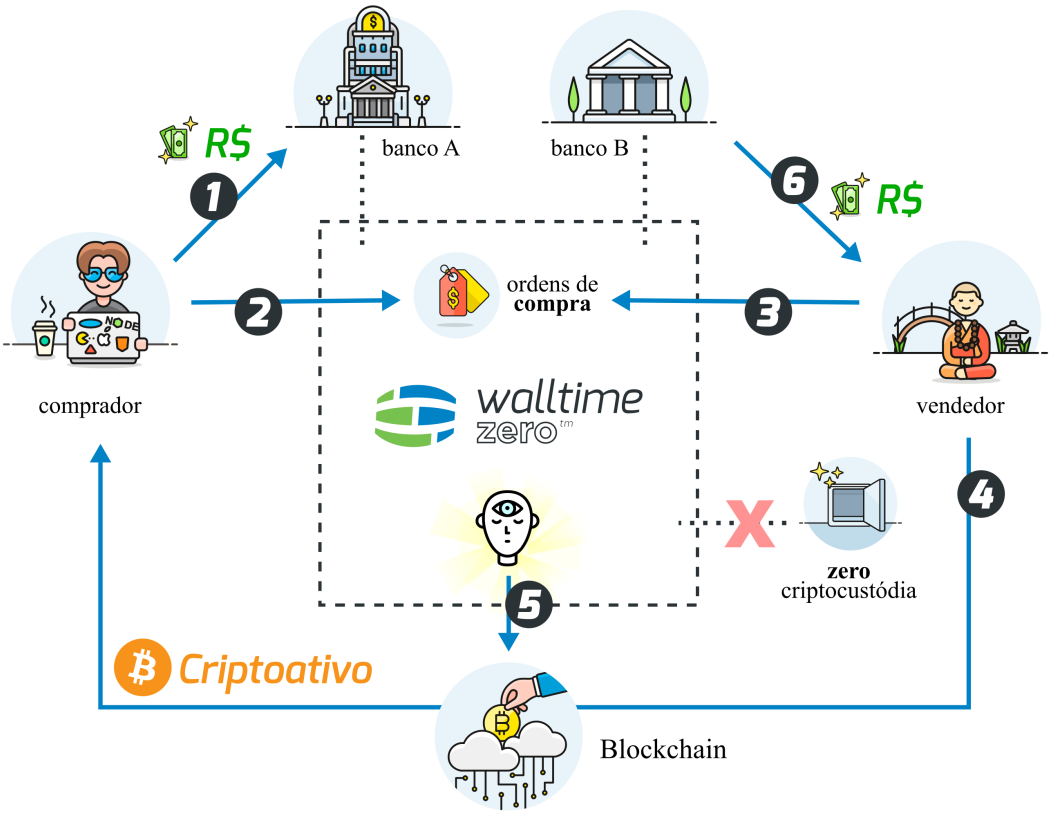
A existência de "papéis falsos" no mercado acontece bastante com metais como o ouro [11], principalmente por ele ser pouco *portável*, o que exige a centralização em grandes cofres do seu metal físico. Já os criptoativos tem a vantagem de serem bastante portáveis e também de terem a característica de "Plausible Deniability" [12], portanto muito mais propícios a serem custodiados de forma individual e descentralizada — diferente de metais preciosos como o ouro. Por que não então aproveitar essas características dos criptoativos e evitar ao máximo a custódia centralizada?

1.3 Conclusão

Por esses motivos apresentados, visando eliminar os riscos de criptocustódia e também evitar a centralização do criptoativo, os autores desta proposta criaram a **Walltime Zero**, um mecanismo inovador e enxuto para a negociação de criptoativos sem a necessidade de custodiá-los.

2 Especificação

Resumindo e generalizando o conceito, a **Walltime Zero** é uma "observadora de Blockchain" (Oráculo de saída ou *Outbound Oracle* [6]) que valida transações públicas e realiza determinadas ações caso essa transação tenha ocorrido de fato.



2.1 Passo a passo de uma negociação semi-descentralizada

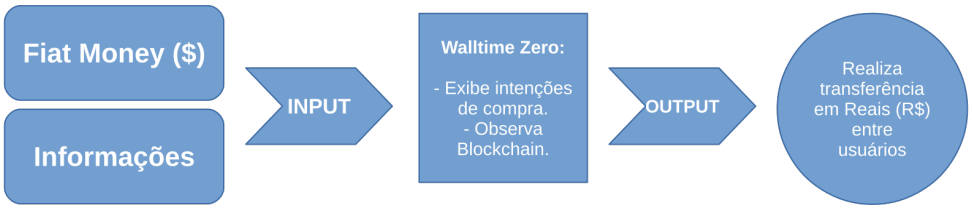
1. Comprador deposita moeda fiduciária em uma das contas bancárias da **WZ** (Walltime Zero), informando um endereço de criptoativo, o preço e volume.
2. A **WZ** mostra publicamente em seu site um **livro de ordens de compra**.
3. O vendedor escolhe uma ordem de compra disponível e faz uma reserva.
4. É exibido ao vendedor o endereço de criptoativo do comprador e o vendedor faz a transferência **diretamente** a ele sem passar pela **WZ**.
5. A **WZ** **observa** a transferência no Blockchain e valida que ela realmente aconteceu.
6. A **WZ** faz a transferência bancária do valor correspondente ao vendedor.

2.2 Algumas considerações importantes

- No processo de depósito de moeda fiduciária do comprador para a conta bancária da **Walltime Zero**, para grandes volumes deve ser verificada a licitude da origem do dinheiro, ou seja, se o comprador tem capacidade financeira compatível com o volume.
- Da mesma forma, a **Walltime Zero** só pode fazer a transferência bancária para o vendedor caso esse também comprove a sua capacidade financeira.
- Existem alguns riscos operacionais melhor descritos na seção 3.2.
- O conceito proposto pela **Walltime Zero** é possível somente em criptoativos em que se possa observar externamente a transferência.

- Existem somente **ordens de compra de criptoativos**. Isso pode ter um impacto negativo na experiência do usuário pois o comprador é sempre "*maker*" (não consegue fazer ordens *takers*) enquanto o vendedor só consegue fazer ordens *takers*, não conseguindo deixar expressa sua intenção de venda no livro de ordens.
- Toda ordem deve ser executada **por inteiro**. Não existe o conceito de ordens parciais e, caso o vendedor queira negociar um volume muito alto, seria necessário realizar diversas transferências para diversas *wallets*, prejudicando um pouco a experiência do usuário. Uma forma de otimizar tal procedimento seria criando algumas restrições de valores mínimos ou incrementais. Por exemplo: permitir apenas a criação de ordens com volumes pré-determinados como: 0.1, 0.5, 1 e 5 BTC. Se o usuário quiser comprar 4.6 BTC, por exemplo, seriam criadas 4 ordens de 1 BTC, 1 ordem de 0.5 BTC e outra ordem de 0.1 BTC. Por outro lado, se o comprador criar ordens com volumes muito altos (5 BTC, por exemplo) ele vai precisar aguardar um vendedor que queira executar a ordem como um todo. Para aumentar as chances de execução e diminuir o tempo de espera, o comprador deverá criar ordens com valores menores.
- O cancelamento de uma ordem por parte do comprador pode ser difícil, já que o vendedor poderia reservar uma ordem durante um intervalo de tempo em que ela ficaria indisponível para cancelamento. Lembrando que, apesar disso, o vendedor deve honrar com a venda no caso de reserva de ordem e, se não honrar, pode receber uma penalidade por isso. Uma forma de minimizar esse impacto negativo na experiência, seria fornecer a possibilidade de criação de "ordens dinâmicas", ou seja, que alteram o preço de compra automaticamente baseados em algum indicador externo. Exemplo: "preço da *exchange* XYZ + 5%". Dessa forma, o preço seria flutuante e valeria o preço do momento da consolidação da transferência em criptoativo.

2.3 Modelo de transformação



Note que não há passagem de criptoativos pela **Walltime Zero**.

3 Riscos

3.1 Riscos legais

Os riscos legais são de bloqueio judicial de conta, pedido da justiça para exposição de informações pessoais de algum usuário, e receber dinheiro ilícito de compradores. Todos esses riscos são comum a *exchanges* tradicionais e uma forma de minimizá-lo é fazendo um grande esforço de *compliance* e KYC.

3.2 Riscos operacionais

3.2.1 Possíveis conflitos e mediação

1. Transferência acidental por parte do vendedor

   Um dos maiores riscos para o vendedor é o de **transferência acidental** para o comprador. O vendedor pode cometer três tipos de erro:

   (a) transferir um valor *acima* do especificado na ordem.

   (b) transferir um valor *depois* que a janela de transferência fechou (expiração da transferência). Nesse caso a ordem poderia ser reaberta e ficar disponível para outro vendedor durante esse meio tempo.

   (c) transferir para um endereço antigo de comprador (fora de qualquer contexto de negociação).

   Nesses três casos acima, a única forma de recuperar o valor seria através da *boa vontade* do comprador. Dessa forma, se isso acontecer, o sistema da **Walltime Zero** se limitaria a detectar e confirmar que houve o acidente e tentaria mediar o caso, até onde fosse possível. A **Walltime Zero** daria um prazo para que

o comprador devolvesse o valor excedente ao vendedor e, caso não fosse cumprido, os seus dados seriam entregues ao vendedor para que esse pudesse fazer uma denúncia às autoridades competentes e processar o comprador desonesto. A *política de privacidade* já deixaria claro que em casos de conflitos assim, os dados poderiam ser entregues à outra parte para que ela pudesse tomar as medidas legais cabíveis.

O vendedor também poderia transferir um valor *abaixo* do especificado na ordem. Nesse caso, a **Walltime Zero** não tomaria nenhuma ação até que o vendedor transferisse o restante completando a totalidade. Por poder prejudicar o comprador temporariamente, poderia ser aplicado algum tipo de sanção ao vendedor, como uma *red flag* que o impediria de reservar ordens durante algum período de tempo ou por tempo indeterminado.

2. Transferência muito lenta (com taxa inadequada)

   Outro caso de conflito pode ocorrer caso o vendedor transfira o criptoativo ao comprador com uma taxa de rede inadequada (menor que a sugerida pelo sistema), fazendo com que seja ultrapassado um tempo máximo de espera aceitável para o comprador. Nesse caso, a **Walltime Zero** tentará mediar o conflito, sugerindo que alguma das partes utilize a técnica CPFP (caso seja Bitcoin ou outra técnica para outro criptoativo). Nesse caso o vendedor também receberia algum tipo de sanção.

3.2.2 Abuso do vendedor reservando inúmeras ordens de compra

Esse tipo de abuso é impactante pois uma ordem reservada ficaria invisível aos demais vendedores e indisponível para cancelamento durante todo o período de reserva (janela de transferência) que poderia durar alguns minutos. Num cenário de muita volatilidade, uma reserva não honrada poderia ser muito prejudicial ao comprador que teve sua ordem congelada durante esse período. Por esse motivo, assim como em alguns sistemas de compra e venda como Mercado Livre ou e-Bay, quando um vendedor reservar uma ordem, ele é obrigado a honrar o compromisso sob a pena de pagar uma multa pré-definida que seria dividida entre a **Walltime Zero** e o comprador como forma de compensação.

3.2.3 Risco de custódia em moeda fiduciária

Apesar de não ter o risco mais preocupante que é o de custódia de criptoativos, o modelo da **Walltime Zero** ainda possui os riscos de custódia em moeda fiduciária, assim como qualquer *exchange* tradicional. O risco é menor que o de criptoativos pois toda transferência em moeda fiduciária é controlada pelo sistema bancário tradicional, é nominal e também reversível, além de ter limites bem restritos, em contraste com criptoativos que são anônimos, irreversíveis e ilimitados, portanto muito mais atraentes para um atacante.

Outro ponto importante é que, assim que uma ordem é executada, o valor em moeda fiduciária pode ser automaticamente transferido para a outra parte, sem a necessidade da criação de um pedido de retirada por parte do vendedor. Isso faria com que a quantidade custodiada fosse reduzida na prática.

4 Glossário

- **Blockchain** é uma tecnologia de registro distribuído imutável. Conceito que surgiu pela primeira vez no paper técnico do Bitcoin [3].
- **Comprador** se define por quem está interessado em trocar moeda fiduciária por criptoativos. Apesar do termo ser ambíguo (pois é possível que alguém queira "comprar" reais com bitcoin, por exemplo) — neste documento ele tem esse significado previamente especificado.
- **Criptoativo** é uma *commodity* puramente digital como o precursor Bitcoin [3].
- **Criptocustódia** se define pela custódia de criptoativos, ou seja, pelo armazenamento centralizado temporário de ativos digitais onde o usuário não possui a chave desses ativos, que ficam sob responsabilidade do custodiante.
- **Exchange** [1] é um serviço que funciona como um intermediário entre duas partes interessadas em trocar criptoativos por moedas fiduciárias e vice-versa. Essa terceira parte recebe os valores das outras duas partes e então, consolidada a transação, faz a troca entre elas. Dessa forma, nenhuma das partes precisa confiar entre si, mas apenas na *exchange* durante a troca. **Walltime Zero** não se define como uma "exchange" pois em nenhum momento recebe ou faz a custódia de criptoativos. O serviço limita-se a ficar observando se um determinado acordo entre as partes será cumprido e, em caso positivo, executa outra ação (no caso, a transferência de moeda fiduciária de uma parte para a outra).
- **KYC** (Know Your Customer) é a identificação e *due diligence* de clientes (também conhecido como exigências “Know Your Client (KYC)”, ou Conheça seu Cliente) implicam que empresas que são ativas no setor de serviços financeiros precisam fazer a *due diligence* dos clientes para conferir sua identidade e evitar roubo de identidade, fraude, lavagem de dinheiro e financiamento ao terrorismo. Leis e regulações rígidas impostas por governos do mundo inteiro forçaram empresas a olhar com mais atenção para suas operações e para as relações que promovem a fim de administrar proativamente sua exposição a riscos. Regulações nacionais e internacionais sobre lavagem de dinheiro (Anti-Money Laundering - AML), e exigências incluídas em outras regulações, como a Alternative Investment Fund Managers Directive (AIFMD), a Foreign Account Tax Compliance Act (FATCA) e o Common Reporting Standard (CRS), têm exigências de KYC que afetam empresas do mundo inteiro.
- **Moeda fiduciária** [2] é a moeda estatal, assim como o Real, Dólar, Euro etc. que são emitidas e controladas por órgãos governamentais e que geralmente não são lastreadas em nenhuma *commodity*.
- **Oráculo de saída** (ou *Outbound Oracle*) — Um "Oráculo" [4] conecta o "mundo real" e um "Blockchain". Geralmente esse *oráculo* é de entrada, ou seja, através de observações de eventos do mundo real (por exemplo: medição da temperatura ambiente, ou então o ganhador de uma eleição presidencial) ele alimenta algum *smart contract* [5] para que determinado comportamento pré-programado aconteça e o resultado seja consolidado em um Blockchain. Um "Oráculo de saída" [6] faz o oposto: usa como fonte de informações um Blockchain (pagamento para uma determinada *wallet*, por exemplo) e executa ações no mundo real. A **Walltime Zero** faz exatamente isso: ela confere se um determinado pagamento foi feito para uma determinada *wallet* e, em caso positivo, executa uma ação no mundo real que é a transferência de moeda fiduciária de uma conta bancária para outra como especificado em um contrato previamente assinado.
- **Ordem** representa a intenção de compra ou de venda de um usuário.
- **Ordem *maker*** representa uma ordem que fica parada no livro de ordens aguardando uma oferta.
- **Ordem *taker*** representa uma ordem que executará imediatamente sem ficar parada no livro de ofertas, por possuir um preço atraente.
- ***Socketpuppet*** é a criação de uma identidade falsa usada para fins fraudulentos na Internet.
- **Técnica CPFP** (Child Pays For Parent) do Bitcoin é um conceito elementar, o que significa que a transação filho está pagando e compensando a transação pai, para que ambos possam ser confirmados em breve.
- **Vendedor** se define por quem está interessado em trocar criptoativos por moeda fiduciária. Apesar do termo ser ambíguo (pois é possível que alguém queira "vender" reais por bitcoin, por exemplo) — neste documento ele tem esse significado previamente especificado.

5 Referências

- [1] J. Frankenfield, Bitcoin Exchange Investopedia Definition (archived), 2019.
- [2] L. Mises, The Theory of Money and Credit, 1912.
- [3] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (archived), 2008.
- [4] B. Curran, What are Oracles? Smart Contracts, Chainlink & "The Oracle Problem" (archived), 2019.
- [5] N. Szabo, Smart Contracts: Building Blocks for Digital Markets (archived), 1996.
- [6] S. Voshmgir, Blockchain Oracles (archived), 2019.
- [7] Quadriga: The cryptocurrency exchange that lost $135m (archived), 2019.
- [8] Cryptocurrency exchange CEO 'loses' private key to user funds — claims it doesn't really matter (archived), 2019.
- [9] Crypto and Blockchain News From Brazil: Oct. 6–12 in Review (archived), 2019.
- [10] The Bitcoinica Hack (archived), 2012.
- [11] B. Saelensminde, There's Something Fishy Going On In The Gold Market, 2014.
- [12] Plausible Deniability (archived).
- [13] Kraken Proof-of-Reserves Audit Process (archived), 2019.