



XXV Congresso de Iniciação Científica da Unicamp

18 a 20 Outubro Campinas | Brasil



Terminal de baixo custo para transações offline com Bitcoin

David Mao San Wei*, Marco Aurélio Amaral Henriques

Resumo

Bitcoin foi introduzido por Satoshi Nakamoto em 2009. Ele é um sistema de pagamento eletrônico baseado em prova matemática e algoritmos criptográficos. O Bitcoin é independente de qualquer autoridade central e tem taxas de transação muito baixas. Este sistema já é aceito por muitos estabelecimentos e indivíduos como opção de pagamento; no entanto, ambas as partes de uma transação devem estar online para transmitir os dados da transação para a rede do Bitcoin e confirmar sua aceitação. Este trabalho propõe e implementa um terminal de venda offline para transações Bitcoin de pequena monta, a fim de levar as vantagens da criptomoeda para pequenos negócios com um baixo custo, funcionalidade adequada e sem a necessidade de uma conexão permanente e custosa com a Internet.

Palavras-chave:

Bitcoin, terminal de vendas, transação offline

Introdução

Criptomoedas, tais como o *Bitcoin*, vêm tornando-se muito populares nos últimos anos. Segundo os dados de Coinmap¹, no mês de junho de 2017, o mundo já conta com mais de 9000 estabelecimentos que aceitam Bitcoin como forma de pagamento. O Brasil, por sua vez, tem um grande grupo de comerciantes que mantêm pequenos negócios. Seria interessante se eles pudessem usufruir das facilidades de *Bitcoin* para vender seus produtos. Entretanto, esses comerciantes podem não estar num ambiente onde existe uma conexão de Internet e a maioria dos aplicativos e terminais de *Bitcoin* exigem tal conexão. Além disso, o custo para manter o sistema online o tempo inteiro pode ser muito alto. Como não se pode verificar as assinaturas digitais no ambiente sem conexão com a rede, o modelo *offline* pode vir a sofrer possíveis fraudes. No entanto, considerando que as transações são de pequeno valor, este risco é compensado evitando-se o custo para ficar *online* permanentemente. O modelo é adequado para a situação de microempreendedores e comerciantes que não possuem uma infraestrutura para acesso barato e estável à Internet. Portanto, neste trabalho, propomos um modelo de terminal de baixo custo feito em sistema embarcado que aceita transações em *Bitcoin* sem a necessidade da conexão permanente à rede.

Resultados e Discussão

Depois de um estudo detalhado sobre o Bitcoin², especialmente sobre a parte de criação de pagamentos, descobrimos que para a construção de uma transação, não é preciso conexão à Internet. A construção de uma transação requer somente uma chave privada para fazer assinatura digital, o valor de hash das transações anteriores que serão utilizadas como entrada da transação e o endereço de destino do pagamento. A transmissão de tal transação pode ser feita mais tarde, totalmente separada da criação da transação (Figura 1). Ao chegar ao quiosque, o cliente se conecta ao ponto de acesso WiFi disponibilizado pelo comerciante, obtém o seu endereço de *Bitcoin* e faz a escolha de produtos, tudo isso por meio de um browser. Feito isto, o cliente abre o seu software de *wallet* no celular e cria uma transação de Bitcoin com o endereço do comerciante e com o valor da compra.



Figura 1. Modelo de uma transação offline

Ao finalizar a construção da transação, o cliente manda a transação para o terminal do comerciante via um formulário web. O terminal do comerciante faz uma verificação básica de consistência dos dados:

1. A estrutura de dados da transação está consistente?
2. O endereço de transferência é o do comerciante?
3. O valor transferido é igual ao valor da compra?
4. A transação já existe no terminal?

O terminal de venda foi prototipado e testado em uma placa *Intel Galileo Gen 2*³, funcionando satisfatoriamente. Mais detalhes como código fonte, documentação completa e vídeo de demonstração podem ser obtidas na página do projeto no github⁴.

Conclusões

Propusemos um método para realizar transações Bitcoin *offline* e implementamos um terminal de vendas que opera neste contexto. Esta solução é voltada para comerciantes que não querem ou podem manter uma conexão permanente com a internet e não exigem que todas as transações de baixo valor sejam totalmente confirmadas pelo Bitcoin antes de realizar novas vendas.

1. SatoshiLab. **Mapa dos estabelecimentos comerciais que aceitam Bitcoin**. Disponível em: <<https://coinmap.org>>. Acesso em: 28 de junho de 2017.

2. Andreas M. Antonopoulos. **Mastering Bitcoin**. O'Reilly Media. First Edition, December 2014.

3. Intel Developer Zone IoT. **Getting Started with the Intel Galileo Board on Linux**. Disponível em: <<https://software.intel.com/en-us/get-started-galileo-linux>>. Acesso em : 28 de junho de 2018.

4. ReGrAS. **Projeto btc_offline_pos**.

Disponível em: <https://github.com/regras/btc_offline_pos>. Acesso em: 28 de junho de 2017.