UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

Proof-of-Attention: uma implementação em blockchain segura e confiável?

Nuno Gonçalo Gomes Silva de Loureiro Nelas

Mestrado em Engenharia Informática

Versão Pública

Trabalho de Projeto orientado por:
Prof. Doutor Diogo Miguel Ferreira Poças

2022

Agradecimentos

Ao meu orientador Professor Doutor Diogo Poças e ao meu chefe de equipa Fábio Costa, o meu enorme obrigado. A vossa orientação foi imprescindível para o sucesso deste trabalho. Aprendi imenso durante a investigação e desenvolvimento desta tese e sei que adquiri convosco um conjunto importante de ferramentas que certamente serão valiosas no decurso da minha vida profissional.

À Aptoide, com especial atenção ao Professor Doutor Paulo Trezentos, por continuarem a depositar a vossa confiança em mim e por disponibilizarem todos os recursos necessários para o meu desenvolvimento académico e profissional. Também não posso deixar em claro o meu agradecimento a todos os elementos, ativos e não ativos, desta incrível empresa que contribuíram para este projecto.

À Ana, por fazer de mim uma pessoa melhor, por dar-me força e amor para seguir em frente e nunca desistir. A toda a minha família, mesmo aos que já não cá estão, por todo o apoio incondicional e incentivo que sempre recebi. Aos meus amigos, que sem nunca terem pedido nada em troca, mostraram-se sempre disponíveis para me acompanhar durante esta viagem.

A todos vós, que directa ou indirectamente ajudaram-me a chegar até aqui, o meu obrigado. Olhar para trás e ver até onde cheguei graças a vocês é arrebatador.

“Hoje é o primeiro dia do resto da tua vida.”

Resumo

Em 2018, a Aptoide lançou a AppCoins, uma criptomoeda baseada em Ethereum. Esta tem por base um protocolo aberto e distribuído para todos os marketplaces de aplicações Android. Com esta divisa em mente, as AppCoins foram criadas para colmatar as duas principais falhas no modelo de negócio em aplicações Android, nomeadamente a falta de transparência nas transações, e consequente falta de confiança por todas as partes envolvidas, e a falta de reaproveitamento de valor no sistema [8].

Para resolver o segundo ponto, este protocolo implementa um conceito de "prémios" (*rewards*) chamado Proof-of-Attention (PoA) [8], que permite a qualquer utilizador receber AppCoins Tokens após utilizar qualquer aplicação durante 2 minutos. Em suma, um desenvolvedor ao criar uma campanha de PoA para a sua aplicação, estará a criar uma *pool* de AppCoins Tokens que depois serão distribuídas pelos seus utilizadores. Mais tarde, estes poderão utilizar os Tokens em compras dentro de qualquer aplicação (*In-App Purchases*), implementando assim o conceito de economia circular.

No primeiro trimestre de 2020, a Aptoide detectou que uma grande percentagem de PoA realizados eram provenientes de utilizadores fraudulentos, revelando assim falhas a nível de confiabilidade. Utilizadores maliciosos podem utilizar inúmeras técnicas para ultrapassar a segurança existente ao tentar converter um PoA, como ataques *Man-in-the-Middle* ou de *scripting*.

Como tal, o objetivo deste projeto é investigar o estado da arte e avanços nas técnicas associadas ao Proof-of-Attention em duas partes: (1) garantir que este serviço está disponível para todos os utilizadores da Aptoide, através da migração da lógica de negócio relativa ao Proof-of-Attention do AppCoins Advertisement SDK para a AppCoins Wallet; (2) prevenir ataques de Man-in-the-Middle e/ou scripting, através da implementação de técnicas que garantam a confiabilidade deste serviço.

No final desta investigação, espera-se poder responder à questão: "É possível desenvolver um sistema de "proof-of-attention" que seja fiável e seguro?"

Palavras-chave: Ethereum, Proof-of-Attention, ciberataques, fraude, Aptoide

Abstract

In 2018, Aptoide launched AppCoins, an Ethereum-based cryptocurrency. AppCoins is based on an open and distributed protocol for all Android application marketplaces. With this motto, AppCoins were created to address the two main flaws in the business model in Android applications, namely the lack of transparency in transactions and consequent lack of trust by all parties involved, and the lack of reusing value in the system. [8].

To solve the second point, this protocol implements a concept of ”rewards” called Proof-of-Attention (PoA) [8], which allows any user to receive AppCoins Tokens after using any application for 2 minutes. In short, when a developer creates a PoA campaign for his application, he will be creating a pool of AppCoins Tokens that will then be distributed by his users. They will then be able to use these Tokens for purchases within any application (In-App Purchases), thus implementing the concept of circular economy.

In the first quarter of 2020, Aptoide detected that a large percentage of PoA came from fraudulent users, thus revealing flaws in reliability. Malicious users can use numerous techniques to overcome existing security when trying to convert a PoA, such as Man-in-the-Middle or scripting attacks.

As such, the objective of this project is to investigate the state of the art and advances in techniques associated with Proof-of-Attention in two parts: (1) ensure that this service is available to all Aptoide users by migrating the Proof-of-Attention business logic from the AppCoins Advertisement SDK to the AppCoins Wallet; (2) prevent Man-in-the-Middle attacks and / or scripting, through the implementation of techniques that guarantee the reliability of this service.

At the end of this investigation, we hope to be able to answer the question: ”Is it possible to develop a ”proof-of-attention” system that is reliable and safe?”

Keywords: Ethereum, Proof-of-Attention, cyberattacks, fraud, Aptoide

Conteúdo

Lista de Figuras

Capítulo 1

Introdução

A seguinte tese, realizada no âmbito do Mestrado em Engenharia Informática da Faculdade de Ciências da Universidade de Lisboa em conjunto com a Aptoide S.A., ambiciona responder à pergunta se é de facto possível implementar um Proof-of-Attention em *blockchain* de forma segura e confiável.

Existem dois grandes problemas, previamente identificados pela instituição de acolhimento, na implementação atual do Proof-of-Attention no protocolo das AppCoins.

O primeiro problema refere-se à fraca propagação desta característica a todos os utilizadores da Aptoide, devido a questões como a resistência por parte dos desenvolvedores de jogos em integrar o AppCoins Advertisement SDK, ou como a preferência pelo método de integração One Step Payment, que não inclui o Proof-of-Attention.

Por outro lado, o segundo problema leva-nos à fraude e como utilizadores maliciosos utilizam técnicas para ultrapassar a segurança existente ao tentar converter um Proof-of-Attention. Essas técnicas, como ataques *Man-in-the-Middle* ou de *scripting*, impossibilitam ter alguma garantia de que os utilizadores que submetem provas são, de facto, utilizadores legítimos.

No contexto do projecto descrito neste relatório foi desenvolvido um sistema que, primeiramente, está disponível para todos os utilizadores da Aptoide, através da migração da lógica de negócio relativa ao Proof-of-Attention do AppCoins Advertisement SDK para a AppCoins Wallet e que, para além disso, também previne ataques de *Man-in-the-Middle* e/ou *scripting*, através da implementação de técnicas que dificultam a engenharia reversa, mais propriamente, a análise estática e dinâmica do código.

1.1 Motivação

A Aptoide é um *marketplace* de aplicações Android, alternativo ao Google Play. Diferencia-se pelo seu conteúdo ser submetido, não só pelos desenvolvedores, mas por todos os utilizadores, permitindo assim que cada utilizador crie o seu repositório (loja) e faça *upload* de aplicações. Adicionalmente, a Aptoide segue uma filosofia focada no empoderamento

dos seus utilizadores por oposição ao controlo/limitação adotada por outros *marketplaces* tal como a Google Play.

Em 2018, a Aptoide lançou a AppCoins, uma criptomoeda baseada em Ethereum.

Atualmente, existem duas implementações para o protocolo das AppCoins:

1. Totalmente descentralizado, onde qualquer desenvolvedor pode integrá-lo e utilizá-lo, mas a sua aplicação comunica diretamente com a *blockchain*.

2. Modelo híbrido, onde a Aptoide serve como intermediário, reduzindo assim os custos de operação (como por exemplo, o gás necessário numa transacção) e alguns problemas de escalabilidade.

A primeira tem o cunho da App Store Foundation [2], uma organização subsidiária da Aptoide, que tem como objetivo apoiar o desenvolvimento das AppCoins, após a distribuição inicial realizada pela Aptoide. A presente tese irá focar-se na segunda solução. Independentemente da implementação, estas representam um protocolo aberto e distribuído para todos os marketplaces de aplicações Android. Com esta divisa em mente, as AppCoins foram criadas para colmatar as duas principais falhas no modelo de negócio em aplicações Android, nomeadamente a falta de transparência nas transações e consequente falta de confiança por todas as partes envolvidas, e a falta de reaproveitamento de valor no sistema [8].

Assente nos alicerces da blockchain, o protocolo permitiu entregar uma solução mais transparente, e consequentemente mais confiável, onde todas as partes envolvidas: utilizadores, desenvolvedores, lojas e *Original Equipment Manufacturer* (OEMs) - sabem exactamente que transações foram efetuadas e qual a sua quota-parte a receber. Para agilizar, a Aptoide também desenvolveu uma aplicação Android: AppCoins Wallet, uma carteira virtual para a moeda AppCoins, por onde um utilizador pode comprar itens integrados numa aplicação ou jogo (ex.: gemas, personagens).

A economia atual das aplicações tem falhas. Um desenvolvedor que queira lançar a sua primeira aplicação precisa, logo desde início, de um bom orçamento para alavancar a sua exposição aos utilizadores. Por exemplo, o custo por instalação (CPI) em média ronda os 1,06€ para dispositivos iOS e 0,45€ para dispositivos Android [5]. Se utilizarmos o Sensor Tower [7] (ferramenta para analisar estatísticas de uma aplicação) como guia, percebemos que uma aplicação para ter algum valor tem que ter no mínimo 5 mil downloads em qualquer uma destas lojas.

Por sua vez, se aplicarmos esses 5 mil downloads mínimos aos preços médios de CPI ficamos a saber que um desenvolvedor em início de carreira precisa de investir pelo menos, 5300€ para dispositivos iOS e 2250€ para dispositivos Android para aumentar a sua exposição a potenciais utilizadores. Estes números são ainda mais desmotivadores se soubermos que, de todos os utilizadores que instalam uma aplicação, apenas 5.2% gastam dinheiro nas mesmas [1].

Muito pouco valor é trazido para os principais participantes da economia: utilizadores e desenvolvedores. Para além disso, não há forma, através das principais lojas de aplicações, de reutilizar recursos de forma a aumentar a resiliência do sistema.

Por estas razões, este protocolo implementa um conceito de "prémios" (*rewards*) chamado Proof-of-Attention (PoA) [8], que permite a qualquer utilizador receber AppCoins Tokens após utilizar qualquer aplicação durante 2 minutos. Em suma, um desenvolvedor ao criar uma campanha de PoA para a sua aplicação, estará a criar uma *pool* de AppCoins Tokens que depois serão distribuídas pelos seus utilizadores. Estes depois poderão utilizar estes Tokens em compras dentro de qualquer aplicação (In-App Purchases), implementando assim o conceito de economia circular.

Tal como podemos ver pela imagem seguinte, um desenvolvedor que invista 1€ numa campanha de PoA, graças às margens reduzidas cobradas pelas lojas e pelos OEMs, consegue reaver 85% desse investimento inicial através dos seus novos utilizadores que efectuam compras dentro da sua aplicação. Isto também se deve devido aos AppCoins Tokens não poderem ser convertidos em AppCoins. Tal significa que estes Tokens só existem dentro do ecossistema e não podem ser convertidos para moeda fiduciária, tal como o Euro ou o Dólar.

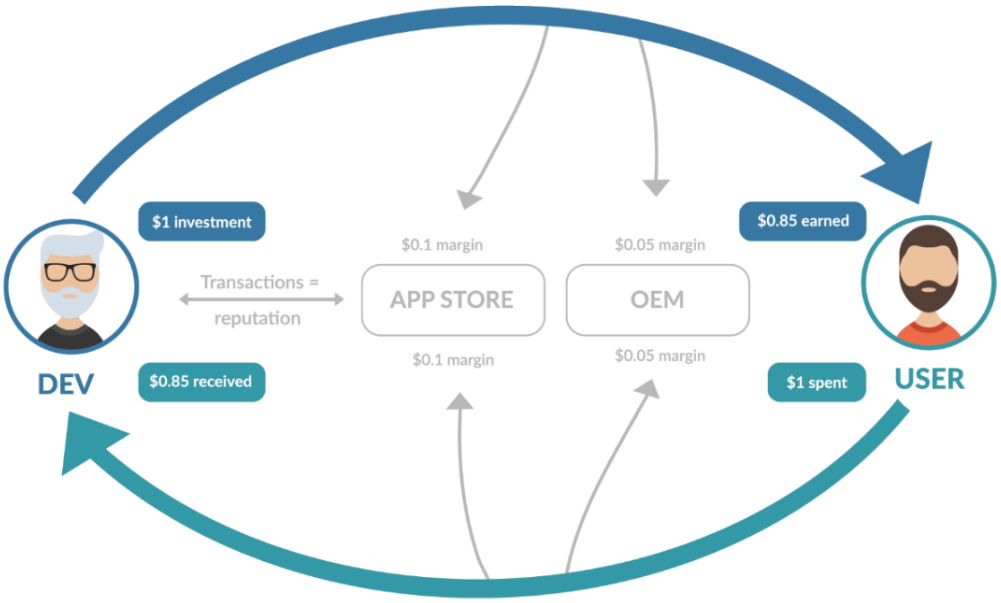

Figura 1.1: Economia circular no protocolo AppCoins [8]

Para um PoA ser convertido para o utilizador (e posteriormente adicionado à *blockchain*), os seguintes requisitos devem ser cumpridos:

1. A aplicação encontra-se em primeiro plano;
2. O dispositivo (ex.: telemóvel) não está bloqueado;

3. A aplicação é fidedigna (provém da Aptoide ou outro possível parceiro).

Toda a lógica inerente ao PoA, do lado do cliente, encontra-se dentro do AppCoins Advertisement Software Development Kit (SDK), uma biblioteca que qualquer desenvolvedor poderá incluir no seu jogo ou na sua aplicação. Por norma, um desenvolvedor que integre o SDK de Advertising, integra também o AppCoins Billing SDK, uma outra biblioteca utilizada para facilitar a comunicação entre o jogo ou aplicação e a AppCoins Wallet em compras integradas em aplicações.

Contudo, existe alguma resistência por parte dos desenvolvedores em implementar os SDKs de AppCoins. Primeiro, porque estes já integraram os SDKs da Google e da Apple, sendo que integrar um terceiro seria sempre mais trabalhoso. Segundo, porque como o protocolo ainda está numa fase bastante embrionária, a margem de lucro que podem vir a receber poderá não ser suficiente para o esforço extra.

Para colmatar este problema, a Aptoide resolveu criar o One Step Payment (OSP), uma forma acessível de iniciar uma compra com AppCoins através de um simples URL com a informação da mesma (ex.: *Stock Keeping Unit*). Esta nova forma de integração ganhou importância, sendo que, em maio de 2021, 11 das 20 aplicações mais lucrativas com AppCoins estão a utilizar OSP. Apesar do sucesso deste método de integração, este não inclui o SDK de Advertising, o que leva a que 55% das aplicações mais importantes na Aptoide não tenham a funcionalidade do PoA. Porém, se a lógica de negócio por detrás do PoA passar para a AppCoins Wallet, este problema será resolvido pois utilizadores que utilizem aplicações com AppCoins têm a aplicação AppCoins Wallet no seu dispositivo.

A fraude é outro grande problema apontado ao PoA. No primeiro trimestre de 2020, a Aptoide detectou que uma grande percentagem dos PoA realizados eram provenientes de utilizadores fraudulentos, revelando assim falhas a nível de confiabilidade. Este problema, também relacionado com a fraude na indústria de anúncios online [4] [9], é sempre complexo pois qualquer solução que seja executada do lado do cliente nunca será segura por si só [3]. Utilizadores maliciosos podem utilizar inúmeras técnicas para ultrapassar a segurança existente ao tentar converter um PoA. A mais conhecida é a de ataque *Man-in-the-Middle*, onde os dados trocados entre duas partes são de alguma forma interceptados e possivelmente alterados pelo atacante sem que as vítimas percebam que tal aconteceu. Outra também bastante utilizada consiste em utilizar *scripts* que se comunicam com o servidor das AppCoins diretamente, fingindo que converteram um PoA.

1.2 Objetivos

O objetivo deste projeto é investigar o estado da arte e avanços nas técnicas associadas ao Proof-of-Attention em duas partes:

1. Garantir que este serviço está disponível para todos os utilizadores da Aptoide,

através da migração da lógica de negócio relativa ao Proof-of-Attention do App-Coins Advertisement SDK para a AppCoins Wallet.

2. Prevenir ataques de *Man-in-the-Middle* e/ou *scripting*, através da implementação de técnicas que garantam a confiabilidade deste serviço.

No final desta investigação, espera-se poder responder à questão: "É possível desenvolver um sistema de "proof-of-attention" que seja confiável e seguro?"

1.3 Contribuições

A aposta por parte da Aptoide no One-Step Payment como forma de integração, embora seja bastante vantajosa pela simplicidade que a mesma representa para os desenvolvedores de aplicações que integram o sistema de pagamentos com AppCoins, também significa que todas estas aplicações não poderão usufruir do Proof-of-Attention, uma das principais funcionalidades do protocolo que permite implementar o conceito de economia circular. Este trabalho, ao incluir a migração da lógica de negócio por detrás do PoA para a AppCoins Wallet, representa uma grande contribuição tanto para o protocolo e moeda AppCoins, como para a Aptoide.

Sendo a fraude um grande problema apontado a esta funcionalidade, mais concretamente com o facto de não ser possível ter garantia que os utilizadores que submetem provas são, de facto, utilizadores legítimos, uma segunda contribuição importante foi a investigação e posterior implementação de uma solução para prevenir ataques de *Man-in-the-Middle* e/ou *scripting* ao Proof-of-Attention.

1.4 Metodologia

A realização deste projecto dividiu-se em duas partes principais. Na primeira, ligada à propagação do Proof-of-Attention, foi realizada uma prova de conceito para demonstrar a viabilidade da migração da lógica de negócio relativa ao Proof-of-Attention do AppCoins Advertisement SDK para a AppCoins Wallet. Após esta prova de conceito, foi necessário o estudo do código-fonte do AppCoins SDK e da AppCoins Wallet. Estes artefactos têm um cariz público, pelo que se encontram disponíveis no GitHub da Aptoide. O AppCoins SDK tem por base a linguagem de programação Java. O AppCoins Wallet tem por base as linguagens de programação Java e Kotlin. Este estudo serviu para a familiarização com estes produtos, de forma a facilitar a posterior integração da prova de conceito nos mesmos.

A segunda fase, desta vez ligada à estratégia antifraude no Proof-of-Attention, foi onde existiu uma maior pesquisa e estudo para aprender sobre os possíveis vetores de ataque, assim como técnicas de mitigação para os mesmos, de forma a reduzir e/ou prevenir

utilizadores fraudulentos. Para a análise e seleção de artigos, escolheu-se como ponto de partida o *white paper* do Basic Attention Token [6], um Token criado pelo navegador Brave para troca de anúncios digitais descentralizada e transparente baseada em *blockchain*. Com base nos resultados obtidos, desenvolveu-se uma solução fiável que mitigou a possibilidade de utilizadores fraudulentos no Proof-of-Attention.

1.5 Estrutura do documento

O presente documento encontra-se estruturado em cinco capítulos, divididos em subcapítulos.

No primeiro capítulo é efetuado um enquadramento do tema do trabalho realizado, a sua motivação e a sua importância. Aqui descrever-se-ão as ferramentas e tecnologias utilizadas durante a realização deste trabalho.

O segundo capítulo destina-se ao estado da arte, referindo a realidade do conhecimento atual e contextualizando a metodologia implementada com literatura revista no âmbito do tema.

Nos capítulos três e quatro é feita uma apresentação em detalhe dos dois problemas que este trabalho pretende resolver. Será exposta também uma descrição pormenorizada da solução escolhida, que inclui o seu desenho e posterior implementação, assim como a sua avaliação.

Por fim, no quinto capítulo, serão apresentadas as conclusões retiradas com a realização desta tese, assim como a descrição do trabalho que pode vir a ser feito no futuro, dentro deste tema.

Bibliografia

[1] AppsFlyer. Asian consumers spend 40% more on in-app purchases. https://www.appsflyer.com/company/newsroom/pr/global-app-spending-habits-report/. Accessed: 2021-09-19.

[2] App Store Foundation. App store foundation. https://appstorefoundation.org/. Accessed: 2020-11-29.

[3] MITRE. Cwe-602: Client-side enforcement of server-side security. https://cwe.mitre.org/data/definitions/602.html. Accessed: 2020-11-29.

[4] Bob Mungamuru, Stephen Weis, and Hector Garcia-Molina. Should ad networks bother fighting click fraud?(yes, they should.). Technical report, Stanford, 2008.

[5] Appy Pie. App installs: An ultimate guide to mobile app install campaigns. https://www.appypie.com/an-ultimate-guide-to-mobile-app-install-campaigns. Accessed: 2021-09-19.

[6] Brave Software. Basic attention token (bat) - blockchain based digital advertising. Technical report, Brave Software, 2016.

[7] Sensor Tower. Sensor tower - mobile app store marketing intelligence. https://sensortower.com/. Accessed: 2021-09-19.

[8] Paulo Trezentos, Diogo Pires, and Aptoide Team. Appcoins: Distributed and trusted app-based transactions protocol. Technical report, ISCTE / Aptoide, 2017.

[9] L. Zhang and Y. Guan. Detecting click fraud in pay-per-click streams of online advertising networks. In *2008 The 28th International Conference on Distributed Computing Systems*, pages 77–84, 2008.