

**دانشکده فنی و مهندسی**

**گروه مهندسی کامپیوتر و فناوری اطلاعات**

**گزارش سمینارتحقيق و تتبع نظري**

**كارشناسي ارشد رشته مهندسي كامپيوتر نرم‌افزار(M.Sc)**

**عنوان سمينار:**

**فن آوری بلاک چین در دنیای امروزی**

**استاد راهنما:**

**دکتر سيدعلي ابراهیمی رضوي**

**نگارنده:**

**مصطفی زارع دستنائی**

**990133173**

بهمن 1400



فهرست مطالب

[چکیده 1](#_Toc93164213)

[کلید واژه ها 1](#_Toc93164214)

[فصل 1 2](#_Toc93164215)

[مقدمه 2](#_Toc93164216)

[1.1 زمینه فعالیت 2](#_Toc93164217)

[1.2 مشکل 2](#_Toc93164218)

[1.3 هدف مورد نظر 3](#_Toc93164219)

[1.4 هدف مورد انتظار 4](#_Toc93164220)

[1.5 روش بررسی 4](#_Toc93164221)

[1.6 محدودیت ها 4](#_Toc93164222)

[1.7 پایداری و اخلاق 5](#_Toc93164223)

[1.8 رئوس مطالب 5](#_Toc93164224)

[فصل 2 7](#_Toc93164225)

[پیشینه و فعالیت های مرتبط 7](#_Toc93164226)

[2.1 معماری بلاک چین 8](#_Toc93164227)

[2.1.1 الگوریتم های اجماع 9](#_Toc93164228)

[2.2 کاربردهای بلاک چین 11](#_Toc93164229)

[2.3 اتریوم 12](#_Toc93164230)

[2.4 قراردادهای هوشمند 15](#_Toc93164231)

[2.5 کاربران مارکتینگ با بلاک چین 17](#_Toc93164232)

[2.6 فعالیت های مرتبط 18](#_Toc93164233)

[2.6.1 IndaHash 18](#_Toc93164234)

[2.6.2 APPICS 20](#_Toc93164235)

[2.6.3 PATRON 20](#_Toc93164236)

[فصل 3 22](#_Toc93164237)

[روش تحقیق 22](#_Toc93164238)

[3.1 فرآیند تحقیق 23](#_Toc93164239)

[3.1.1 بررسی مطالعات 23](#_Toc93164240)

[3.1.2 پیشنهاد مدل 23](#_Toc93164241)

[3.1.3 قرارداد هوشمند 24](#_Toc93164242)

[3.1.4 پیاده سازی 24](#_Toc93164243)

[3.1.5 موارد تحویلی 24](#_Toc93164244)

[فصل 4 27](#_Toc93164245)

[طراحی و پیاده سازی 28](#_Toc93164246)

[4.1 فن آوری ها و ابزارها 28](#_Toc93164247)

[4.2 معماری 29](#_Toc93164248)

[4.2.1 نمای کلی سطح بالا 29](#_Toc93164249)

[4.2.2 طراحی سیستم 30](#_Toc93164250)

[4.3 پیاده سازی 38](#_Toc93164251)

[4.3.1 درخواست برای کمپین 39](#_Toc93164252)

[4.3.2 برداشت 40](#_Toc93164253)

[4.3.3 انجام الزامات 41](#_Toc93164254)

[4.3.4 مطالبه دستمزد 43](#_Toc93164255)

[فصل 5 46](#_Toc93164256)

[تجزیه و تحلیل و نتایج 46](#_Toc93164257)

[5.1 نتایج تجربی 47](#_Toc93164258)

[5.2 ارزیابی 49](#_Toc93164259)

[فصل 6 50](#_Toc93164260)

[نتیجه گیری و کار آتی 50](#_Toc93164261)

[6.1 نتیجه گیری 50](#_Toc93164262)

[6.2 محدودیت 50](#_Toc93164263)

[فهرست کتب 51](#_Toc93164264)

# چکیده

بلاک چین، راه حلی برای گروه های مختلف برای رسیدن به اجماع در شبکه های همتا (P2P)، به ما امکان می دهد داده ها را در موجودیت های مختلف توزیع کنیم. بسیاری از زمینه ها، از جمله مالی، مراقبت های بهداشتی، تجارت الکترونیک، بازاریابی، می توانند از فناوری بلاک چین بهره مند شوند. علاوه بر این، برنامه‌های کاربردی موجود در کمپین‌هایی که برندها ایجاد کرده‌اند، ریز اینفلوئنسرها (10000 100000 فالوور) را شامل نمی‌شوند. به منظور مقابله با مشکلات ذکر شده، یک چارچوب کاربردی با اندازه توزیع شده و متناسب با بلاک چین در این پایان نامه پیشنهاد شده است. این چارچوب امکانی را برای اینفلوئنسرهای خرد فراهم می کند تا در کمپین های برندها شرکت کنند. با این حال، میکرو اینفلوئنسرها مستقیماً در ارتباط با برندها دخالت ندارند. در عوض، کلان اینفلوئنسرها (بیش از 100000 فالوور) با ایجاد کمپین های فرعی از کمپین های برندها، نقش پل ارتباطی بین میکرو اینفلوئنسرها و برندها را ایفا می کنند. با دخالت میکرو اینفلوئنسرها در چارچوب پیشنهادی، آنها همچنین تصاویر خود را با همان لباس (اندازه‌ها و شکل‌های مختلف بدن) به اشتراک می‌گذارند، که به خریداران بالقوه قبل از تصمیم به خرید، تصور بهتری از اینکه همان لباس چگونه به نظر می‌رسد را می دهد. راه حل پیشنهادی با قراردادهای هوشمند با استفاده از Solidity اجرا شده و در شبکه تست Ropsten آزمایش شده است. آزمایش قرارداد هوشمند در شبکه تست Ropsten نشان می دهد که راه حل پیشنهادی از نظر هزینه های مالی قابل اجرا است. چارچوب پیشنهادی محدود به ارائه این امکان به برندها برای تبلیغ محصولات نیست، بلکه به کلان اینفلوئنسرها و میکرواینفلوئنسرهای بالقوه فرصتی برای کسب دستمزد در ازای تبلیغ محصولات برندها ارائه می دهد. کل فرآیند از درخواست برای کمپین تا درخواست دستمزد بدون مداخله دستی انجام می شود.

# کلید واژه ها

بلاک چین[[1]](#footnote-1)، قرارداد هوشمند[[2]](#footnote-2)، برنامه توزیع شده[[3]](#footnote-3)، مد[[4]](#footnote-4)

# فصل 1

## مقدمه

بلاک چین اخیراً به دلیل پذیرش موفقیت آمیز ارزهای رمزپایه مانند اتریوم، بیت کوین محبوب شده است. همانطور که از نام آن مشخص است، بلاک چین دنباله ای از بلوک ها است که به هم متصل شده اند. ساختار غیرمتمرکز دارد. بلاک چین تاریخچه تراکنش ها را از طریق استفاده از غیرمتمرکزسازی و هش رمزنگاری ثبت می کند. فناوری بلاک چین راه حلی برای انتقال دارایی های دیجیتال بدون هیچ واسطه ای ارائه می دهد. شفافیت، تراکنش‌های سریع‌تر، نداشتن هزینه‌های واسطه‌ای در تراکنش‌ها و برخی دیگر از مزایای بلاک چین، آن را برای شرکت‌ها و مشاغل مناسب می‌کند. این یک دفتر کل غیرمتمرکز، مشترک و قابل اعتماد از تراکنش ها را ارائه می دهد که توسط هر گره در شبکه بلاک چین قابل قبول است. قراردادهای هوشمند مجموعه ای از قوانین تجاری هستند که توسط کد برنامه نویسی تعریف شده اند و می توانند در شبکه بلاک چین مستقر شوند. در این فصل مقدمه ای بر فناوری بلاک چین و ارتباط آن با پروژه ارائه می شود. ما مشکلی را که این پایان نامه به آن می پردازد، زمینه مشکل، اهداف این پروژه پایان نامه، و ساختار پایان نامه را شرح می دهیم.

## 1.1 زمینه فعالیت

فناوری‌های بلاک چین در حوزه‌های مختلفی مانند مالی، مراقبت‌های بهداشتی، بیمه، تجارت الکترونیک، بازاریابی و غیره به کار گرفته شده‌اند. از آنجایی که بلاک چین یک شبکه همتا را ارائه می‌کند که به اشخاص ثالث وابسته نیست، به ما اجازه می‌دهد تا یک پلتفرم قابل اعتماد و شفاف ایجاد کنیم. قراردادهای هوشمند خطوطی از کدهای برنامه نویسی هستند که بر روی بلاک چین مستقر می شوند. با کمک قراردادهای هوشمند در شبکه بلاک چین، می‌توانیم از قراردادهای دنیای واقعی در پلتفرم دیجیتال تقلید کنیم. مزیت اصلی استفاده از قراردادهای هوشمند، شفافیت و ارتباطات سریعتر است. هنگامی که قرارداد هوشمند ایجاد شد، نمی توان آن را تغییر داد. از آنجایی که قراردادهای هوشمند نسخه های دیجیتالی و برنامه ریزی شده قراردادهای سنتی هستند، زمانی که اجرا می شوند، تراکنش ها را بسیار سریعتر از پرداخت های معمولی پردازش می کنند.

## 1.2 مشکل

از آنجایی که پلتفرم های دیجیتال همه جا هستند، استراتژی های بازاریابی نیز در دهه گذشته تغییرات زیادی کرده است. در گذشته، شرکت‌ها بر روی تبلیغ محصولات خود فقط در تلویزیون یا روی بیلبوردها تمرکز داشتند. با این حال، با توجه به عصر دیجیتال، پلتفرم های رسانه های اجتماعی و کاربران رسانه های اجتماعی به شدت افزایش یافته اند. اکنون راه‌های جدیدی برای دسترسی به مصرف‌کنندگانی وجود دارد که بیشتر وقت خود را پشت صفحه نمایش می‌گذرانند. یکی از مدرن ترین روش های بازاریابی، اینفلوئنسر مارکتینگ است که در آن برندها از میکرواینفلوئنسرها و کلان اینفلوئنسرها در رسانه های اجتماعی برای تبلیغ محصولات خود استفاده می کنند. آنها به جای ایجاد تبلیغات سنتی، با کمک تأثیرگذاران رسانه های اجتماعی به مصرف کنندگان بالقوه می رسند. در این زمینه، فناوری بلاک چین می تواند به ایجاد پلتفرم های قابل اعتماد و شفاف بین برندها و اینفلوئنسرها و بین اینفلوئنسرها و طرفداران آنها کمک کند. با استفاده از فناوری بلاک چین، برندها می توانند بودجه و زمان صرف شده برای تبلیغات سنتی، ارتباطات و پردازش پرداخت را کاهش دهند. بیشتر اوقات، اینفلوئنسرهای رسانه‌های اجتماعی بدنی «ایده‌آل» دارند که بر ظاهر محصولی که تبلیغ می‌کنند تأثیر می‌گذارد. با این حال، از آنجایی که طرفداران فرم‌های بدنی متفاوتی دارند و آنچه ممکن است در یک اینفلوئنسر اینستاگرام دوست داشته باشند ممکن است برای آنها یکسان نباشد. منجر به مشکلاتی در خرید اینترنتی می شود. از آنجایی که لباس ها برای خریداران متفاوت به نظر می رسند، منجر به افزایش بازده در فروشگاه های آنلاین می شود که یک مشکل عمده برای خرده فروشان است [47]. در برنامه‌های موجود، طرفداران ماکرو اینفلوئنسرها یا میکرو اینفلوئنسرها در کمپین‌هایی که برندها ایجاد کرده‌اند درگیر نیستند. چارچوب پیشنهادی این امکان را برای میکرواینفلوئنسرها نیز فراهم می کند تا در کمپین های فرعی که کلان اینفلوئنسرها بر اساس کمپین هایی که برندها راه اندازی کرده اند، شرکت کنند. به این ترتیب، میکرو اینفلوئنسرها در اینستاگرام نیز تصاویر خود را با لباس هایی که در کمپین ها توضیح داده شده است به اشتراک می گذارند. دیدن لباس یکسان بر روی فردی به جای افرادی با اندام ایده آل، ممکن است به خریداران بالقوه ایده بهتری نسبت به ظاهر لباس در آنها بدهد. در این پایان نامه کارشناسی ارشد، به بررسی وضعیت کلی کاربرد فناوری های بلاک چین در مد می پردازیم و چارچوبی در بلاک چین برای رسیدگی به مشکلات ذکر شده توسعه و پیشنهاد می کنیم.

## 1.3 هدف مورد نظر

هدف از این پایان نامه شناسایی مشکل سایزبندی که باعث افزایش نرخ بازده در فروشگاه های آنلاین می شود و بررسی راه های ممکن برای غلبه بر آن می باشد. با کشاندن میکرو اینفلوئنسرها به فرآیند تبلیغ محصولات برندها، این هدف محقق خواهد شد. از آنجایی که میکرو اینفلوئنسرهای زیادی در شبکه های اجتماعی وجود دارد، به جای اینکه امکان ارتباط مستقیم با برندها را به آنها بدهند، اینفلوئنسرهای کلان می توانند به عنوان پل ارتباطی بین آنها ایفای نقش کنند. معماری توصیف‌شده راه‌حل پیشنهادی می‌تواند برای خوانندگانی که می‌خواهند قراردادهای هوشمند را روی بلاک چین پیاده‌سازی کنند، همراه با فن‌آوری‌های باطنی و فرانت‌اند مختلف مفید باشد.

## 1.4 هدف مورد انتظار

هدف اصلی این پروژه توسعه یک چارچوب بلاک چین توزیع شده است که می تواند برای تقویت نقش تأثیرگذاران دیجیتال در تبلیغات برای برندها و به حداقل رساندن تعداد بازگشت در فروشگاه های آنلاین مورد استفاده قرار گیرد. اهداف فرعی پروژه به شرح زیر است:

• بررسی وضعیت فن آوری های بلاک چین در برنامه های کاربردی تجارت الکترونیک.

• پیشنهاد چارچوبی متناسب با افزایش نرخ بازده در فروشگاه‌های آنلاین به دلیل مشکل اندازه‌بندی به‌عنوان بسط خدمات بلاک چین اینفلوئنسرهای اجتماعی در حال حاضر.

• بررسی معماری بلاک چین.

• بررسی روش های فنی امکان پذیر برای پیاده سازی چارچوب.

• توسعه رابط کاربری برای ارائه راه حل پیشنهادی.

• آزمایش با چارچوب پیشنهادی با تجزیه و تحلیل و ارزیابی در زمینه مد.

نتایج تحویل، گزارش پایان نامه و ارائه رابط کاربری چارچوب پیشنهادی خواهد بود.

## 1.5 روش بررسی

روش تحقیق کیفی فرآیند تجزیه و تحلیل داده های غیر عددی است، در حالی که روش تحقیق کمی از رویکرد قیاسی شکل گرفته و در مورد تجزیه و تحلیل داده های عددی است. در این پایان نامه برای استفاده از تکنیک های هر دو، از ترکیبی از روش های تحقیق کیفی و کمی استفاده شده است.

## 1.6 محدودیت ها

مدل پیشنهادی در شبکه بلاک چین Ropsten مستقر، آزمایش و تحلیل می‌شود که الگوریتم‌های مشابه شبکه اصلی اتریوم را اجرا می‌کند [29]. به دلیل هزینه های تراکنش، از شبکه اصلی بلاک چین برای استقرار قراردادهای هوشمند استفاده نمی شود.

## 1.7 پایداری و اخلاق

از آنجایی که چارچوب پیشنهادی به خریداران بالقوه ایده بهتری درباره نحوه قرار گرفتن لباس‌ها روی آن‌ها قبل از خرید آنها می‌دهد، منجر به کاهش بازده در خرید آنلاین می‌شود. نگرانی پایداری باید قبل از تصمیم مصرف کننده برای خرید ظاهر شود. پس از تصمیم گیری خرید، یافتن راه حل از جنبه پایداری آسان نیست [23]. بر اساس تحقیقات انجام شده، تفاوت فاحشی در مورد استفاده از روش بازگشت (بازگشت به فروشگاه فیزیکی، تحویل بسته و ...) وجود ندارد. همه آنها از نظر انتشار CO2 تأثیر بدی بر محیط زیست دارند [27]. با تأثیرگذاری بر رفتار مصرف‌کنندگان با کمک میکرواینفلوئنسرها، کاهش بازده مزایای زیادی بر پایداری خواهد داشت.

هنگام انجام تحقیق، هیچ شرکت کننده یا اطلاعات کاربری درگیر نبود. ابزارهای فنی مورد استفاده در حین اجرا برای استفاده عمومی باز هستند. تمامی نتایج و ایده هایی که در طول تحقیق ظاهر شده اند به صورت شفاف در گزارش پایان نامه گنجانده شده است

## 1.8 رئوس مطالب

ساختار گزارش به شرح زیر است. فصل 2 اطلاعات زمینه ای درباره بلاک چین، معماری بلاک چین، قراردادهای هوشمند و بازاریابی تأثیرگذار ارائه می‌کند که برای دنبال کردن بقیه گزارش ضروری است. فصل 3 به تشریح نظری روش مورد استفاده در مطالعه می پردازد. فصل 4 طراحی سیستم مدل پیشنهادی و پیاده سازی آن را تشریح می کند. در فصل 5، نتایج و تجزیه و تحلیل ارائه شده است. فصل 6 نتیجه گیری های گزارش را خلاصه می کند و کارهای احتمالی آینده را تشریح می کند.

# فصل 2

## پیشینه و فعالیت های مرتبط

بلاک چین یک دفتر کل غیرمتمرکز از تمام تراکنش ها در یک شبکه همتا است که امکان انتقال همتا به همتا دارایی های دیجیتال را بدون واسطه فراهم می کند. بلاک چین به عنوان یک کلمه فنی توسط نویسنده و مخترع ناشناس بیت کوین، ساتوشی ناکاموتو، در وایت پیپر [30] اولین ارز دیجیتال، بیت کوین، اختراع شد. بیت کوین معروف ترین نمونه ای است که بر اساس فناوری بلاک چین ساخته شده است. امروزه بلاک چین فراتر از بیت کوین است زیرا کاربرد بلاک چین تنها به بخش مالی محدود نمی شود. تعریف بلاک چین که توسط ملانی سوان در کتاب خود [39] پیشنهاد شده است، نه تنها بیانگر آن چیزی است که بلاک چین است، بلکه قدرت آن را نیز بیان می کند: «ما باید در مورد بلاک چین به عنوان طبقه دیگری از چیزهایی مانند اینترنت فکر کنیم - یک فناوری اطلاعات جامع با سطوح فنی لایه‌بندی و کلاس‌های چندگانه برنامه‌های کاربردی برای هر شکلی از ثبت دارایی، موجودی، و مبادله، از جمله هر حوزه مالی، اقتصادی، و پول؛ دارایی‌های سخت (اموال فیزیکی، خانه‌ها، اتومبیل) و دارایی‌های نامشهود (رای، ایده‌ها، شهرت، قصد، داده های سلامت، اطلاعات و غیره). اما مفهوم بلاک چین از این هم بیشتر است؛ این یک الگوی سازمان‌دهی جدید برای کشف، ارزش‌گذاری و انتقال همه کوانتوم‌ها (واحدهای گسسته) هر چیزی است، و به طور بالقوه برای هماهنگی تمام فعالیت‌های انسانی در مقیاسی بسیار بزرگ‌تر از آنچه ممکن است. قبل از". [39] در حال حاضر، اقتصاد دیجیتال مبتنی بر برخی مقامات مورد اعتماد (به عنوان مثال، یک بانک مرکزی) است. مردم برای امنیت و حریم خصوصی دارایی های دیجیتال خود از خدمات مالی دیجیتال با اتکا به آن اشخاص مورد اعتماد استفاده می کنند. کاربرد بلاک چین در بخش مالی مزایای زیادی نسبت به بانکداری سنتی دارد:

• شفافیت: کل زنجیره جریان می تواند توسط هر کسی حسابرسی شود، به همین دلیل است که بلاک چین یک دفتر کل توزیع شده غیرمتمرکز است. این به دلیل امکان دسترسی آسان به تراکنش های تاریخی است، زیرا شفافیت بسیار بیشتری نسبت به بانکداری سنتی ارائه می دهد.

• هزینه های تراکنش کمتر: با استفاده از رویکرد دفتر کل توزیع شده برای تشکیل سیستمی که هر کسی می تواند برای تراکنش های همتا، بدون احراز هویت آژانس مرکزی استفاده کند، بلاک چین به طور قابل توجهی به کاهش هزینه های توسعه و عملیات کمک می کند [50]. از آنجایی که هیچ آژانس مرکزی وجود ندارد، هیچ هزینه ای از طرف اشخاص ثالث برای تراکنش اعمال نمی شود، بنابراین کارمزد تراکنش بسیار کمتر از بانکداری سنتی است.

• تراکنش های سریع تر: این واقعیت که تراکنش از طریق اشخاص ثالث انجام نمی شود، نه تنها منجر به کاهش کارمزد تراکنش ها، بلکه به تراکنش های سریع تر نیز می شود.

بسته به دسترسی به زنجیره ها، سه نوع بلاک چین وجود دارد. بلاک چین های عمومی منبع باز هستند، جایی که هر کسی می تواند به عنوان کاربر تراکنش ارسال کند یا می تواند ماینر باشد. بیت کوین، اتریوم نمونه هایی از بلاک چین عمومی هستند. از طرف دیگر، بلاک چین های خصوصی محدودتر هستند و معمولاً توسط سازمان ها استفاده می شوند. بنابراین، بلاک چین های خصوصی در مقایسه با بلاک چین های عمومی متمرکز تر هستند. سازمانی که مالک بلاک چین خصوصی است، عملیات نوشتن را مدیریت می کند. با این حال، مجوزهای خواندن می تواند عمومی یا محدود به برخی از شرکت کنندگان باشد [17]. بلاک چین های کنسرسیومی نوع خاصی از بلاک چین خصوصی هستند. تفاوت اصلی این است که بلاک چین کنسرسیوم توسط گروهی از نهادها به جای یک سازمان واحد در مورد بلاک چین خصوصی مدیریت می شود. از آنجایی که بلاک چین های کنسرسیوم به نهادهای مختلف اجازه می دهند زنجیره را کنترل کنند، به چندین سازمان کمک می کند تا در فرآیند کسب و کار همکاری کنند [11]. بلاک چین های ترکیبی ترکیبی از بلاک چین خصوصی و عمومی هستند. در سیستم های بلاک چین هیبریدی، هر گرهی می تواند در فرآیند اجماع شرکت کند. با این حال، تولید بلوک بعدی فقط برای برخی از گره ها مجاز است [18].

## 2.1 معماری بلاک چین

بلاک چین دنباله‌ای از بلوک‌ها است که برای ذخیره اطلاعات مربوط به تراکنش‌هایی که در شبکه بلاک‌چین اتفاق می‌افتد، به هم متصل می‌شوند. یک بلوک از سربرگ بلوک و بدنه بلوک [48] تشکیل شده است. هدر بلوک برای شناسایی یک بلوک خاص در بلاک چین استفاده می شود و دارای چندین فیلد است:

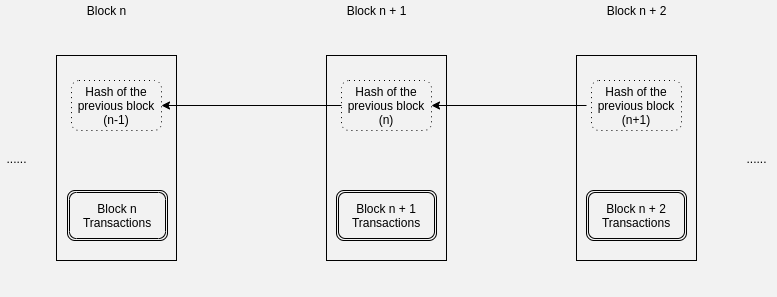
1. نسخه: شماره نسخه بلوک چهار بایت است که نشان می دهد از کدام مجموعه قوانین اعتبارسنجی بلوک پیروی کنید [8].

2. زمان: زمان یونیکس زمانی که ماینر شروع به هش کردن هدر کرد [8].

3. Nonce: یک عدد 4 بایتی که نتیجه فرآیند استخراج است. Nonce عددی است که برای تولید بلوک استفاده می شود که به بلاک چین اضافه می شود. ماینرها برای یافتن یک nonce با هم رقابت می کنند. برای حل پازل هش توسط گره انتشار دستکاری می شود [45]. اگر یک ماینر چنین nonce را پیدا کند، پاداش بلاک را دریافت می کند.

4. هش ریشه مرکل: از هش‌های تمام تراکنش‌های موجود در بلوک مشتق می‌شود و تأیید سریع داده‌های زنجیره بلوکی را تضمین می‌کند [8].

5. مقدار هش بلوک قبلی: زنجیره را ایمن می کند. یکی از مهمترین مفاهیم در بلاک چین است. برای تغییر این مقادیر، تمام مقادیر هش قبلی باید تغییر کنند. (شکل 2.1.1 را ببینید)

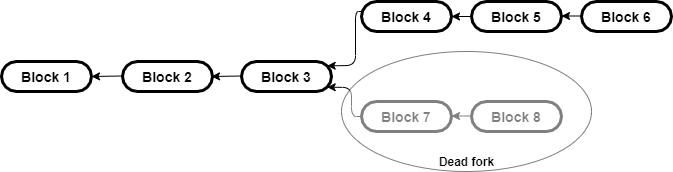
6. nbits: به عنوان هدف دشواری نامیده می شود و از 4 بایت تشکیل شده است. هدف‌گیری مشکل نسخه کدگذاری شده آستانه هدف، هش سرصفحه بلوک باید کمتر یا مساوی با [8] باشد.

شکل 2.1.1: هر بلوک دارای هش بلوک قبلی است، بلوک قبلی یک بلوک والد برای هر بلوک است.

### 2.1.1 الگوریتم های اجماع

بلاک چین از مکانیسم اجماع غیرمتمرکز برای دستیابی به قابلیت اطمینان در شبکه بلاک چین استفاده می کند. چندین الگوریتم اجماع مورد استفاده در بلاک چین وجود دارد، به طور عمده، PoW (اثبات کار)، PoS (اثبات سهام)، DPoS (اثبات واگذاری سهام)، و PBFT (تحمل عملی خطای بیزانسی) [28].

دوبرابر کردن یکی از مشکلات اصلی تراکنش های دیجیتال است. خرج مضاعف یعنی مالک دوباره همان سکه ها را خرج می کند. بیت کوین مشکل دو برابری را که تا رمزنگاری بلاک چین مشکل بود، حل کرد. این یک مشکل برای انواع دارایی های دیجیتال بود زیرا امکان کپی و خرج کردن آنها بیش از یک بار وجود داشت. مشکل اصلی این بود که هیچ راهی برای تایید هزینه مضاعف بدون شخص ثالث وجود نداشت [39]. بنابراین، یک راه حل رایج برای این مشکل، داشتن یک مقام مرکزی است که آن را کنترل کند. با این حال، این راه حل منجر به سیستمی مانند بانکداری سنتی می شود. راه حلی که در کاغذ سفید بیت کوین توضیح داده شد، پیاده سازی کار اثبات [30] بود، که یک معمای ریاضی برای یافتن مقداری به نام nonce است که پخش بلوک بعدی را به شبکه تولید می کند. اثبات کار یک الگوریتم اجماع است. الگوریتم‌های اجماع در هسته معماری بلاک چین قرار دارند که مکانیسم‌هایی هستند که باعث می‌شوند همه گره‌های بلاک چین توافق مشترکی داشته باشند و تضمین می‌کنند که آخرین بلوک به زنجیره اضافه شده است [25]. وجود پروتکل اجماع در بلاک چین نیز نقش مهمی در امنیت آن دارد. ایده اصلی اثبات کار، تخصیص پاداش از طریق رقابت قدرت هش بین گره ها است. اولین گره ای که مسئله ریاضی را حل می کند، بلوک بعدی را ایجاد می کند و پاداش می گیرد [28]. گره هایی که سعی می کنند هش ها را بیابند ماینر نامیده می شوند و فرآیند کلی اثبات کار استخراج نامیده می شود. ممکن است موردی وجود داشته باشد که دو ماینر به طور همزمان راه حلی پیدا کنند که منجر به واگرایی زنجیره به دو مسیر بالقوه شود. به آن چنگال می گویند. برای حل فورک ها، این پروتکل تعریف می کند که چگونه ماینرها باید زنجیره ای را برای استخراج انتخاب کنند و یک بلوک به آن اضافه کنند. معیار این است که زنجیره ای که برای تولید به بیشترین قدرت استخراج نیاز دارد، برنده است. این بدان معنی است که طولانی ترین زنجیره (نگاه کنید به شکل 2.1.2) مسیر بعدی برای ادامه است.



شکل 2.1.2: از آنجایی که شاخه بالایی بلندتر است، برنده است یک چنگال اتفاق می افتد

بنابراین برای اینکه بتواند تولید بلاک چین را کنترل کند، نهاد باید حداقل نیمی از قدرت هش جهان را کنترل کند تا اولین کسی باشد که آخرین بلاک را تولید می کند و بر طولانی ترین زنجیره تسلط پیدا می کند. بنابراین هزینه دستیابی به این امر بسیار بیشتر از سود است. [28].

بیشتر سیستم‌های بلاک چین موجود از مکانیسم PoW برای ایجاد اجماع استفاده می‌کنند. با این حال، از آنجایی که استخراج به انرژی زیادی در مکانیزم PoW نیاز دارد، الگوریتم Proof of Stake یکی از جایگزین‌های Proof of Work است. در Proof of Stake، سن هر سکه در نظر گرفته می شود. وقتی سکه در هر معامله ای خرج می شود، سن آن صفر می شود. در حالی که در PoW، طولانی ترین زنجیره برنده است، سیستم اثبات سهام از زنجیره ای با بالاترین سن مصرف سکه استفاده می کند. [6] Peercoin از روش سن سکه استفاده می کند، بنابراین در Peercoin، استخراج بلوک بعدی به کسی بستگی دارد که مجموعه قدیمی و بزرگتر سکه ها را داشته باشد. بنابراین در مقایسه با PoW، در PoS، انتخاب گره هیچ ارتباطی با منابع محاسباتی گره ندارد. به همین دلیل است که PoS در مصرف انرژی صرفه جویی می کند و موثرتر است [48]. TPS (تراکنش در ثانیه) نیز در PoS بالاتر از PoW است، زیرا PoS به سهامی که گره ها در اختیار دارند، متکی است، نه به قدرت محاسباتی [24]. در نتیجه، تراکنش ها سریعتر پردازش می شوند، که به معنای TPS بالاتر است.

## 2.2 کاربردهای بلاک چین

بلاک چین فقط مربوط به بیت کوین نیست. امروزه اپلیکیشن های بلاک چین در حوزه های مختلفی پیاده سازی شده اند.

برخی از شهودها و دانشگاه ها از فناوری بلاک چین در حل مشکلات آموزش استفاده کرده اند. یک مثال می تواند ذخیره اعتبارات، رونوشت نمرات و گواهینامه ها در بلاک چین باشد. یکی از دانشگاه هایی که قبلاً این را اجرا کرده است، دانشگاه نیکوزیا است. این اولین مدرسه ای است که از فناوری بلاک چین برای مدیریت گواهینامه های دانش آموزان استفاده می کند [37]. پروژه ای توسط Media Lab Learning Initiative و Learning Machine می تواند نمونه دیگری از کاربردهای بلاک چین در آموزش باشد. این یک اکوسیستم برای ایجاد، اشتراک گذاری و تأیید گواهی های آموزشی مبتنی بر بلاک چین است. همه گواهی‌های دیجیتال به صورت رمزنگاری در زنجیره بلاک بیت کوین امضا و ثبت می‌شوند [13].

برخی از کاربردهای بلاک چین موجود در حوزه پزشکی نیز وجود دارد. اکثر برنامه ها معمولاً در مورد رسیدگی به پرونده بیماران هستند. به عنوان مثال پروژه "MedRec" از فناوری بلاک چین برای به اشتراک گذاری سوابق استفاده می کند و به محرمانه بودن و یکپارچگی دست می یابد. همچنین اطلاعات دقیقی را در مورد سوابق بیماران ارائه می دهد و نه تنها به خود بیماران بلکه به ارائه دهندگان و موسسات درمانی مختلف نیز دسترسی دارند. [5]

فناوری بلاک چین در صنعت بیمه نیز کاربرد دارد. یکی از نمونه‌های کاربرد بلاک چین در صنعت بیمه InsureX است که هدف آن حل چالش‌های موجود در بازار سنتی بیمه است [10]. بر اساس گزارشی که توسط Deloitte [9] انجام شده است، چندین نقطه درد در بیمه سنتی وجود دارد که پیاده‌سازی بلاک چین آنها را حل می‌کند: به عنوان مثال، استفاده از واسطه در فرآیند، تبادل ناکافی اطلاعات، کلاهبرداری، بررسی و پردازش دستی ادعاها و غیره.

برنامه های بلاک چین همچنین امکانات جدیدی را برای محافظت از حقوق موجودات مختلف به ویژه در اینترنت به ارمغان می آورند. یک مثال می تواند حق چاپ فایل باشد. اگر در نظر بگیریم که یک فایل که دارای حق چاپ است را می توان به راحتی کپی کرد و چندین بار در سراسر شبکه کپی کرد. با این حال، پیاده سازی بلاک چین در این زمینه، برخی از این چالش ها را قابل حل می کند. علاوه بر این، این واقعیت که تمام تغییرات اضافه شده به دفتر کل توزیع شده هرگز قابل تغییر نیستند، اطلاعات مالک فایل را قابل اعتماد و به راحتی قابل تأیید می کند [10].

## 2.3 اتریوم

اتریوم یک شبکه بلاک چین توزیع شده برای شبکه های غیرمتمرکز و قراردادهای هوشمند است. اتریوم توسط ویتالیک بوترین معرفی شد و مزایایی نسبت به فناوری بیت کوین دارد. تفاوت اصلی بین اتریوم و بیت کوین در کامل بودن تورینگ است. این بدان معناست که اتریوم از انواع محاسبات پشتیبانی می کند. بلاک چین های اتریوم را می توان نه تنها در بخش مالی، بلکه در انواع مختلف مفاهیم نیز به کار برد. قراردادهای هوشمند خطوط کدی هستند که با رعایت برخی شرایط و ضوابط اجرا می شوند. جزئیات بیشتر در مورد قراردادهای هوشمند در قسمت بعدی توضیح داده خواهد شد. واحد پول اتریوم اتر نام دارد. همانطور که در وایت پیپر اتریوم [1] آمده است، «اتر سوخت رمزنگاری داخلی اصلی اتریوم است و برای پرداخت هزینه تراکنش استفاده می‌شود». وی کوچکترین واحد اتر است. یک اتر 1018 وی است. به جز Wei، سایر زیرمجموعه های مختلف اتر نیز وجود دارد (جدول 2.3.1 را ببینید).

با کمک قراردادهای هوشمند، هر توسعه‌دهنده بلاک چین می‌تواند شرایط و ضوابط خود را برای جریان کسب‌وکار خود ایجاد کند و آنها را در شبکه عمومی اتریوم مستقر کند. بنابراین با قراردادهای هوشمند، اتریوم همه را قادر می‌سازد تا قوانین خاص خود را برای برخی جریان‌های خاص داشته باشند [42].

دو نوع حساب در شبکه اتریوم امکان پذیر است. یکی از آنها حساب های خارجی است که توسط کلیدهای خصوصی کنترل می شوند. یکی دیگر حساب های قراردادی است. برخلاف حساب‌های دارای مالکیت خارجی، حساب‌های قرارداد با کد قرارداد خود کنترل می‌شوند [1].

|  |  |
| --- | --- |
| Multiplier | Name |
| 100 | Wei |
| 1012 | Szabo |
| 1015 | Finney |
| 1018 | Ether |

جدول 2.3.1: زیرمجموعه های مختلف اتر (بازچاپ شده از مقاله Ethereum: A Secure Decentralized Generalized Transaction Ledger [14]).

در اتریوم، حساب ها نشان دهنده حالت ها هستند. آنها از 4 جزء تشکیل شده اند [7]:

1. nonce: اگر حساب یک حساب قراردادی باشد اختصاص داده می شود. نشان دهنده تعداد قراردادهای ایجاد شده توسط آن حساب است. در غیر این صورت، اگر حساب یک حساب تحت مالکیت خارجی باشد، تعداد تراکنش‌های ارسال شده از حساب غیر یکسان است.

2. تعادل: این فیلد نشان دهنده مقدار Wei حساب است.

3. ذخیره سازی ریشه: هش 256 بیتی از گره ریشه درخت Merkle Particia. درخت محتویات ذخیره سازی حساب را رمزگذاری می کند. به طور پیش فرض خالی است.

4. کد هش: این جزء نشان دهنده هش کد EVM (ماشین مجازی اتریوم) حساب است. هش کد زمانی اجرا می شود که آدرس حساب یک تماس پیامی دریافت کند. آنها تغییر ناپذیر هستند.

بلوک ها از تراکنش ها تشکیل شده اند و همه بلوک ها توسط یک هش رمزنگاری به هم متصل می شوند. می‌توانیم بلوک‌ها را به‌عنوان یک مجله یا دفتر کل در نظر بگیریم. این یک سری از تراکنش ها را ثبت می کند، و همچنین حاوی یک شناسه برای وضعیت نهایی است [14]. تمام بلوک ها به همراه توابع هش رمزنگاری زنجیر شده اند.

دو نوع تراکنش در اتریوم وجود دارد. یکی از آنها تراکنش هایی است که منجر به تماس پیام می شود و دیگری تراکنش هایی است که برای تعامل با قرارداد هوشمند ارسال می شود.

هر دو نوع تراکنش یک ساختار داده مشترک دارند و حاوی فیلدهای داده مشترک هستند [14]:

1. nonce: مقداری برابر با تعداد تراکنش های ارسال شده توسط فرستنده. هر بار که یک فرستنده تراکنش جدیدی ارسال می کند، nonce یک افزایش می یابد.

2. gasLimit: حداکثر تعداد گازی که می توان برای انجام معامله پرداخت کرد.

3. به: آدرس گیرنده ای که پیام با او تماس گرفته است.

4. ارزش: ارزشی است که در نتیجه یک معامله به گیرنده منتقل می شود.

5. v, r, s: مقادیری که امضای تماس پیام را مشخص می کنند و برای تعیین فرستنده استفاده می شوند.

در شبکه اتریوم، اندازه گیری خاصی برای اندازه گیری کار محاسباتی برای اجرای هر تراکنش وجود دارد که به آن گاز می گویند. گاز یک مکانیسم کنترلی برای منابعی است که یک معامله می تواند مصرف کند. در شبکه اتریوم، زمانی که کاربر یک تراکنش جدید ایجاد می کند، برای اجرای تراکنش توسط کاربر هزینه ای برای شبکه پرداخت می شود. بخش‌هایی از این کارمزد که همانطور که در بالا گفته شد گاز نامیده می‌شود، برای هزینه‌های محاسباتی و همچنین ذخیره‌سازی انجام یک تراکنش است [46]. مقدار گاز درگیر در پردازش تراکنش ها همچنین به جلوگیری از حملات انکار سرویس کمک می کند. قیمت گاز اصطلاح دیگری است که هنگام صحبت در مورد این مکانیسم در شبکه اتریوم استفاده می شود. این فقط تعداد Wei در واحد گاز را نشان می دهد.

همانطور که از نام آن پیداست، محدودیت گاز حد یا حداکثر قیمتی است که کاربر حاضر است هنگام ایجاد یک تراکنش جدید یا حتی انجام یک تابع از یک قرارداد هوشمند بپردازد. ما می توانیم محدودیت گاز را به عنوان حداکثر بودجه برای استخراج کننده در شبکه اتریوم برای پردازش تراکنش در نظر بگیریم. هنگامی که ماینر هر عملیات محاسباتی را انجام می دهد، گاز از آن بودجه کم می شود. در صورتی که گاز پرداخت شده برای اجرای کل تراکنش کافی نباشد، یک استثناء OutofGas توسط EVM ایجاد خواهد شد. با این حال، همچنان در زنجیره گنجانده خواهد شد. در غیر این صورت، زمانی که گاز پرداختی بیش از نیاز برای انجام معامله باشد، مابقی گاز به کاربر بازپرداخت خواهد شد [46]. استخراج‌کنندگانی که یک تراکنش را تأیید و پردازش می‌کنند، این کارمزد را برای کاری که انجام داده‌اند دریافت می‌کنند. با تعیین یک آستانه، ماینرها می توانند تصمیم بگیرند که در صورت کم بودن کارمزد، تراکنش ها را انجام ندهند. کارمزد گاز بیشتر به این معنی است که معامله سریعتر از هزینه گاز کمتر انجام می شود. کل هزینه ای که کاربر مایل است برای انجام یک تراکنش جدید بپردازد، ضرب محدودیت گاز و قیمت گاز است.

totalCostOf Transaction = gasPrice ∗ gasLimit

## 2.4 قراردادهای هوشمند

قرارداد هوشمند برنامه ای است که بر روی بلاک چین اتریوم اجرا می شود. این فراتر از انتقال دارایی های ارز دیجیتال است. می توان آن را در بسیاری از زمینه ها و برنامه ها اعمال کرد. یک قرارداد هوشمند برای اولین بار در مقاله [40] توسط نیک سابو ذکر شد. نیک سابو پیشنهاد کرد که دارایی‌های مصنوعی ممکن است در قراردادهای هوشمند به کار روند: «یکی دیگر از حوزه‌هایی که ممکن است در قراردادهای هوشمند در نظر گرفته شود، دارایی‌های مصنوعی است. این اوراق بهادار جدید با ترکیب اوراق بهادار و مشتقات به طرق مختلف شکل می گیرد. ساختارهای مدت بسیار پیچیده برای پرداخت‌ها اکنون می‌توانند در قراردادهای استاندارد ساخته شده و با هزینه‌های مبادله‌ای کم معامله شوند، به دلیل تجزیه و تحلیل رایانه‌ای این ساختارهای مدت پیچیده».

برخی از انواع قراردادهای هوشمند در زمینه بلاک چین وجود دارد. شناخته شده ترین و پر استفاده ترین پیاده سازی در سراسر جهان در اتریوم است. قراردادهای هوشمند قوانین تجاری هستند که توسط برخی از خطوط کد تعریف شده‌اند و در صورت برآورده شدن شرایط از پیش تعریف شده به طور خودکار اجرا می‌شوند.

مزایای قراردادهای هوشمند را می توان به شرح زیر خلاصه کرد:

• آنها فرآیند پیچیده یا جریان های تجاری را که بسیاری از واسطه های میانی را به دلیل عدم اعتماد در میان شرکت کنندگان در معامله درگیر می کند، ساده می کنند [16]. بنابراین می توان آنها را بدون دخالت انسانی اعدام کرد.

• پس از برآورده شدن شرایط از پیش تعریف شده، تسویه مالی به طور خودکار اجرا می شود. در نتیجه، زمان چرخش را می توان به طور قابل توجهی کاهش داد [49].

• قراردادهای هوشمند را نمی توان در مقایسه با قراردادهای سنتی تغییر داد. بنابراین پس از ایجاد و استقرار آن، هر طرفی که در قرارداد هوشمند مشارکت داشته است، مطمئن است که در صورت تحقق شرایط از پیش تعریف شده، قرارداد هوشمند اجرا خواهد شد.

• قراردادهای هوشمند هرگز از بین نمی روند. آنها همیشه روی بلاک چین هستند. از سوی دیگر، قراردادهای سنتی می توانند از بین بروند.

• قراردادهای هوشمند هزینه های مبادله را کاهش می دهد. برخلاف قراردادهای معمولی، در قراردادهای هوشمند، هیچ هزینه ای با تضمین عملکرد قرارداد (به عنوان مثال، هزینه های دادرسی یا هزینه های مرتبط با ارائه وثیقه) وجود ندارد [36].

با این حال، آنها دارای معایب زیر هستند:

• اگرچه قراردادهای هوشمند هزینه را در مقایسه با قراردادهای سنتی کاهش می دهد، اما زیرساخت های لازم برای اجرای قراردادهای هوشمند و هزینه های مرتبط با توسعه همچنان بالا است [36].

• تغییرناپذیری قراردادهای هوشمند را می توان در برخی موارد به عنوان یک نقطه ضعف در نظر گرفت. به عنوان مثال، اگر یک اشکال در قرارداد قبلاً مستقر شده وجود داشته باشد، تغییر قرارداد غیرممکن است.

• وضعیت حقوقی قراردادهای هوشمند هنوز مشخص نیست.

کدهای قرارداد هوشمند بر روی EVM (ماشین مجازی اتریوم) اجرا می شوند. هر کسی که مهارت های لازم را داشته باشد می تواند یک قرارداد هوشمند بنویسد و آن را در شبکه مستقر کند. قراردادهای هوشمند را می توان با استفاده از زبان های برنامه نویسی سطح بالا مانند Solidity، C++، Java، JavaScript و غیره پیاده سازی کرد. Solidity اصلی ترین و پرکاربردترین زبان برنامه نویسی قرارداد هوشمند است. هر قرارداد هوشمند در بلاک چین دارای یک آدرس قرارداد منحصر به فرد است و همانطور که در بخش بالا ذکر شد، یک سکه مجازی به نام اتر در اختیار دارند.

[26] یک قرارداد هوشمند با ارسال یک تراکنش به آن آغاز می شود. یک تراکنش شامل پرداخت برای آن تراکنش و داده هایی است که برای عملکرد قرارداد ضروری است. برای پردازش هر تراکنش به قراردادهای هوشمند، هزینه ای برای اجرای قرارداد هوشمند به ماینرها پرداخت می شود. این کارمزد از ضرب قیمت بنزین و سقف بنزینی که توسط کاربر ارسال کننده تراکنش مشخص شده کم می شود.

یک قرارداد هوشمند اتریوم دارای حالتی است که شامل موارد زیر است:

• یک انبار خصوصی

• مقدار سکه های مجازی (اتر) [26]

آنها تغییر ناپذیر هستند. پس از ایجاد آنها، تغییر کد یک قرارداد غیرممکن است. قرارداد هوشمند مانند یک کد نرم افزار نرم افزار سنتی نیست که بتوان آن را تغییر داد و در همان مکان یا آدرس مستقر کرد. هنگامی که یک قرارداد هوشمند تغییر می کند تا دوباره مستقر شود، به عنوان یک قرارداد هوشمند کاملاً جدید مستقر می شود. به همین دلیل است که قراردادهای هوشمند غیرقابل تغییر در نظر گرفته می شوند.

## 2.5 کاربران مارکتینگ با بلاک چین

از آنجایی که استفاده از رسانه های اجتماعی در حال افزایش است، بازاریابی شبکه های اجتماعی در حال حاضر یکی از موثرترین راه های بازاریابی است. بر اساس گزارش دیجیتال 2019 [12] ارائه شده توسط آژانس "We are Social"، 57 درصد (4.388 میلیارد) از جمعیت جهان به اینترنت متصل هستند. تقریباً 80 درصد از افرادی که به اینترنت متصل هستند، کاربران فعال رسانه های اجتماعی هستند. میزان زمان صرف شده آنلاین برای هر کاربر نیز قابل توجه است و به طور میانگین بیش از 6.5 ساعت در روز است. این آمار برندها و شرکت ها را تشویق می کند تا از روش های بازاریابی رسانه های اجتماعی بیشتر از بازاریابی سنتی استفاده کنند. در عصر دیجیتال، رویکردهای مختلفی برای دستیابی به بسیاری از مصرف کنندگان بالقوه به روشی موثر وجود دارد. یکی از موثرترین روش ها پیروی از برخی توصیه های اینفلوئنسرها است. اینفلوئنسرها کاربران محبوب رسانه های اجتماعی هستند که ثابت کرده اند قدرت تاثیرگذاری بر تصمیمات خرید مشتریان دارند. با استفاده از این قدرت، آنها می توانند محصولات برندها را تبلیغ کنند و تعامل واقعی با محتوا داشته باشند. امروزه بازاریابی محصولات به دلیل رقابتی بودن تولیدکنندگان و فروشندگان در این بازی یک چالش واقعی است [32] . در بازاریابی سنتی، تبلیغات دهان به دهان برای کسب و کار بسیار مهم است. می توان گفت که اینفلوئنسر مارکتینگ نیز یکی از راه های تبلیغات دهان به دهان است. مقدار قابل توجهی از استفاده از اینترنت، گزینه های مصرف کنندگان بالقوه را برای دستیابی به اطلاعات محصولات بی طرف از سایر مصرف کنندگان گسترش داده است. همچنین این فرصت را برای مصرف کنندگان فراهم می کند تا توصیه های مربوط به مصرف خود را در مورد محصولات در wordofmouth الکترونیکی (eWOM) ارائه دهند [19].

اگر اینفلوئنسر مارکتینگ با فناوری بلاک چین ادغام شود، می تواند موثرتر باشد. با برنامه بلاک چین، dApps (برنامه های غیرمتمرکز) را می توان پیاده سازی کرد که شفاف، توزیع شده، انعطاف پذیر و منبع باز هستند. به دلیل منبع باز بودن، dApp در حال جلب اعتماد کاربران بالقوه است، بنابراین اگر برنامه منبع باز باشد، شفافیت مورد نیاز برای بهبود برنامه را با کمک مشارکت های توسعه دهندگان دیگر به ارمغان می آورد [33]. یک dApp متعلق به هیچ گره ای در شبکه نیست. با استفاده از قراردادهای هوشمند در بلاک چین dApp، اعتماد و شفافیت بیشتری به بسیاری از حوزه‌های کاربردی ممکن و همچنین بازاریابی تأثیرگذار می‌رسد.

استفاده از بلاک چین dApp با اینفلوئنسر مارکتینگ مزایای متعددی را برای برندها و اینفلوئنسرها به ارمغان می آورد که به طور خلاصه به شرح زیر است:

• سطح اعتماد بالاتر: از آنجایی که بلاک چین dApp شفافیت بیشتری را فراهم می کند، اعتماد به راحتی بین تأثیرگذاران و برندها ایجاد می شود.

• پردازش آسان‌تر پرداخت‌ها: با کمک قراردادهای هوشمند و ارزهای رمزنگاری شده، پس از برآورده شدن پیش‌شرط‌های خاص، به اینفلوئنسرها فوراً پرداخت می‌شود.

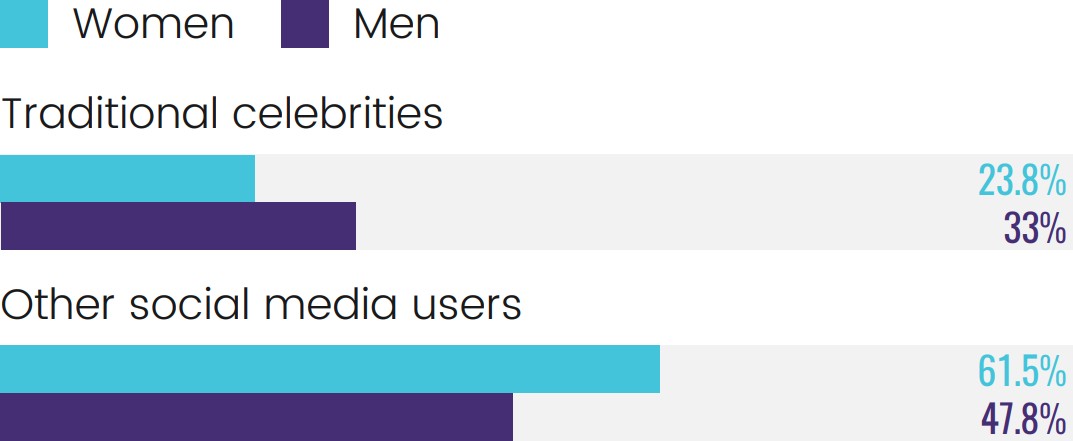
• فرآیند سریعتر و ارتباط سریعتر: نیازی به قرارداد کاغذی نیست و علاوه بر آن، اینفلوئنسرها نیازی به صرف وقت خود برای مذاکره با برندها و شرکتهای مختلف ندارند. در عوض، آنها همه چیز را در یک پلتفرم مدیریت می کنند. سرمایه گذاران و شرکت های برند نیز در ارتباط سریع تر با سرمایه گذاران با اشخاص ثالث و امضای قرارداد درگیر هستند.

## 2.6 فعالیت های مرتبط

در حال حاضر پلتفرم‌های بلاک چینی وجود دارد که تأثیرگذاران رسانه‌های اجتماعی را دربرمی‌گیرد. در این بخش به نمونه هایی از این پلتفرم ها اشاره می کنیم.

### 2.6.1 IndaHash

IndaHash [21] یکی از پلتفرم‌های پیشرو است که برندها را با تأثیرگذاران در رسانه‌های اجتماعی مرتبط می‌کند. در سال 2016 راه اندازی شد. IndaHash یک راه حل مبتنی بر وب و برنامه تلفن همراه خود دارد. IndaHash فرآیند مذاکره را خودکار می کند، جایی که برندها با تنظیم بودجه و جزئیات کمپین مانند شرایط برای تکمیل تکلیف (هشتگ ها، محتوایی که قرار است پست شود، و غیره) وظیفه ای را ایجاد می کنند. اینفلوئنسرها با اعمال وظایف ایجاد شده به کمپین آغاز شده توسط برندها می پیوندند. پس از درخواست اینفلوئنسرها برای کمپین، آنها محتوای مورد نیاز را با هشتگ های لازم در پلتفرم های رسانه های اجتماعی منتشر می کنند.



شکل 2.6.1: چه چیزی یا چه کسی بیشترین نظر را برای شما ایجاد می کند؟ (برگرفته از مطالعه بین المللی انجام شده توسط IndaHash Lab [44]).

IndaHash یک مطالعه بین المللی [44] با بیش از 2200 اینفلوئنسر دیجیتال در سال 2017 انجام داده است که بینش بسیار خوبی را با آمارهای مرتبط با اینفلوئنسر مارکتینگ به ارمغان آورد.

طبق نتایج، 83 درصد از اینفلوئنسرها محصولی را که در شبکه های اجتماعی دیده بودند در ماه گذشته خریداری کردند. این نشان دهنده قدرت واقعی بازاریابی رسانه های اجتماعی است. می تواند حتی به اینفلوئنسرها نیز بفروشد. نتیجه در شکل 2 نشان می دهد که اینفلوئنسرهای زن بیشتر از مردان به کاربران رسانه های اجتماعی اعتماد دارند. در مقابل، مردان بیشتر به افراد مشهور قدیمی اعتماد دارند.

همانطور که در کاغذ سفید [22] IndaHash توضیح داده شده است، مدل کسب و کار به شرح زیر است:

1. اینفلوئنسرها در پلتفرم ثبت نام می کنند.

2. ثبت نام پس از بررسی دستی اکانت اینستاگرام تایید می شود.

3. اینفلوئنسرها برای پیوستن به کمپین ها درخواست می دهند.

4. اینفلوئنسرها پیشنهاد ارائه می کنند.

5. پیشنهاد توسط مجری و مشتری بررسی می شود.

6. پس از تایید، مطالب منتشر می شود.

### 2.6.2 APPICS

APPICS [4] یک پلت فرم رسانه اجتماعی مبتنی بر بلاک چین و پاداش است که در بالای بلاک چین Steem اجرا می شود. هدف آن پاداش دادن به افراد با تبدیل لایک به ارز است. با APPICS، کاربران پلتفرم می توانند محتوای خود را پست کنند و به عنوان لایک در پست ها پاداش دریافت کنند. بنابراین، طرفداران رسانه های اجتماعی برای زمانی که در شبکه های اجتماعی می گذرانند پاداش دریافت می کنند. برخلاف هر سایت رسانه اجتماعی محبوب دیگری که ارزش و درآمد کل پلتفرم به سهامداران می رسد، پلتفرم APPICS به همه کاربران این امکان را می دهد که از طریق نماد پاداش "APX" درآمد کسب کنند. از آنجایی که امکان دریافت لایک های زیاد با دریافت پاداش بیشتر است، تولیدکنندگان محتوا انگیزه بیشتری برای به اشتراک گذاشتن پست هایی با کیفیت بهتر دارند. همچنین امکان ارسال تراکنش های مستقیم به حساب کاربر دیگر بدون کارمزد یا تاخیر اضافی وجود دارد. سکه مورد استفاده در این پلتفرم سکه APPICS (XAP) نام دارد. بعداً آن XAPهای به دست آمده را می توان به کارت اعتباری اضافه کرد. با مبلغ موجود در حساب کاربر، آنها می توانند اقلام انتخابی را نیز خریداری کنند. کاربران فعال می توانند توسط کاربران به عنوان تأثیرگذار در یکی از 15 دسته مانند مد، ورزش و غیره رأی دهند.

### 2.6.3 PATRON

یکی از پلتفرم‌های موجود مبتنی بر بلاک چین که شامل تأثیرگذاران رسانه‌های اجتماعی است، PATRON است. PATRON یک پلت فرم اقتصاد اشتراک گذاری مبتنی بر بلاک چین است که ارزش آن را به اشتراک می گذارد [31]. هدف این پروژه ایجاد یک اکوسیستم کامل است که در آن تأثیرگذاران و برندها بتوانند به طور مستقیم با هم ارتباط برقرار کنند. به این ترتیب، پروژه PATRON با هدف جایگزینی مدل کسب‌وکار موجود با سیستمی که برای برندها و تأثیرگذاران رسانه‌های اجتماعی به طور یکسان با هزینه‌های کمتر بدون دخالت هیچ واسطه‌ای بهتر عمل می‌کند [3]. با کمک پلتفرم Patron، برندها می‌توانند تأثیرگذاران رسانه‌های اجتماعی را بدون نگرانی در مورد کارگزار یا سایر واسطه‌ها رزرو کنند [3]. پلتفرم PATRON از توکن PAT استفاده می کند. آرزوی یک توکن ERC20 است که بر روی بلاک چین اتریوم پیاده سازی شده است.

مفهوم PATRON بسیار شبیه به مفهوم Airbnb است. در حالی که کاربران در Airbnb اتاق را به اشتراک می گذارند، در PATRON، اینفلوئنسرها "محل پست رسانه های اجتماعی" خود را با شرکت ها و برندها و همچنین طرفداران و دنبال کنندگان به اشتراک می گذارند [31]. بنابراین آنها برای جایگاه پست رسانه های اجتماعی خود که یک شرکت بدون واسطه آن را رزرو می کند، پول می گیرند.

در پلتفرم PATRON، اینفلوئنسرها به چهار دسته Micro Celebrity، Influencer، MicroInfluencer، NanoCelebrity طبقه بندی می شوند. برای اندازه گیری سطح تأثیرگذار از سه دسته استفاده می شود: [31]

1. قدرت ارسال پیام (قابلیت دسترسی)

2. کشش (درگیری)

3. قابلیت اطمینان (ارزیابی توسط شخص ثالث)

هر کسی که تحت یکی از دسته بندی ها قرار می گیرد می تواند از این پلت فرم استفاده کند. به عنوان مثال استفاده از اینفلوئنسر که خواننده و معروف در اینستاگرام است را می‌توان مثال زد. و در پلتفرم، برای آن اینفلوئنسر، نوع پست اسلات در اسلات موجود است (به عنوان مثال، اشتراک گذاری پست زنده، وضعیت، یا معمولی)، و همچنین قیمت آن اسلات. قابلیت جستجو به کاربران اجازه می دهد تا بر اساس نیازهای خود به جستجوی تأثیرگذاران در سراسر جهان بپردازند. [31]

# فصل 3

## روش تحقیق

**در این فصل روش تحقیق و روش های مورد استفاده در این پایان نامه شرح داده شده است. بخش 3.1 فرآیند تحقیق را تشریح می کند. بخش 3.2 تنظیمات آزمایشی را برای آزمایش چارچوب پیشنهادی شرح می دهد.**

## 3.1 فرآیند تحقیق

**در این تحقیق به منظور استفاده از تکنیک های مختلف در دو روش تحقیق کیفی و کمی، ترکیبی از هر دو رویکرد را دنبال می کنیم.**

**تحقیق کیفی عمدتاً در مورد جمع آوری داده های غیر عددی و درک مفهوم از طریق تجزیه و تحلیل داده ها است. از سوی دیگر، روش تحقیق کمی شامل جمع آوری داده ها به صورت عددی و تجزیه و تحلیل داده ها با محاسبات آماری است. روش تحقیق ترکیبی مفید است زیرا داده های کمی به جنبه کیفی یک مطالعه در طول طراحی با یافتن یک نمونه معرف کمک می کند. در مقابل، داده های کیفی با کمک به توسعه مفهومی به جنبه کمی مطالعه در طول طراحی کمک می کند [2].**

### 3.1.1 بررسی مطالعات

**به عنوان اولین گام از فرآیند تحقیق، یک مرور ادبیات کاملاً گسترده انجام شد. در ابتدا دانش حوزه بلاک چین کسب شد. در مرحله بعدی بررسی ادبیات، برنامه های کاربردی مشابه بلاک چین مورد مطالعه قرار گرفت. پس از بررسی ادبیات، دانش در مورد معماری شبکه بلاک چین اتریوم و اجرای dApp در بلاک چین اتریوم درک شد. از آنجا که دامنه بلاک چین به دانش فنی گسترده ای برای توسعه برنامه ها نیاز دارد که به عنوان بخشی از این مرحله نیز انجام می شود.**

### 3.1.2 پیشنهاد مدل

**در مرحله بعد، روش‌های ممکن برای غلبه بر مشکل افزایش بازدهی در فروشگاه‌های اینترنتی به دلیل مشکل تناسب لباس‌های آگهی‌شده، بررسی می‌شود. این مرحله با پیشنهاد چارچوبی برای نه تنها برندها، بلکه برای کلان اینفلوئنسرها نیز نهایی شد تا کمپین های خود را ایجاد کنند، کمپین هایی که برای طرفداران یا میکرو اینفلوئنسرها در دسترس است.**

### 3.1.3 قرارداد هوشمند

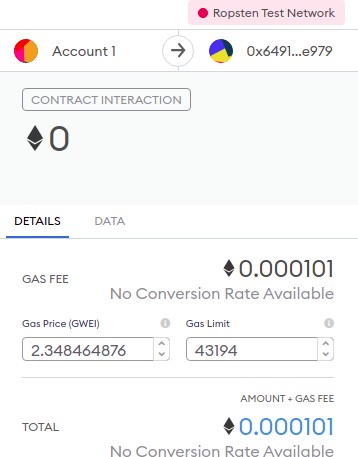
**پس از نهایی شدن راه حل پیشنهادی، قرارداد هوشمند طراحی می شود. در این مرحله اطلاعات لازم برای ایجاد کمپین مورد بحث قرار می گیرد. پس از فرآیند طراحی، پیاده سازی قرارداد هوشمند در Remix انجام می شود که یک کامپایلر مبتنی بر وب و IDE است [34]. ساختن و اشکال‌زدایی قراردادهای هوشمند در Remix آسان‌تر است، زیرا دارای ویژگی‌های داخلی برای استفاده برای توسعه است.**

### 3.1.4 پیاده سازی

**پس از طراحی و پیاده سازی قرارداد هوشمند، بستر وب برای ارائه راهکار پیشنهادی پیاده سازی شد. پیاده سازی وب شامل توسعه رابط کاربری و REST API برای شبیه سازی عملکردهای اساسی اینستاگرام لازم برای راه حل پیشنهادی ما است. REST API در چارچوب Spring با استفاده از Hibernate و Java پیاده سازی شده است. رابط کاربری با استفاده از next.js پیاده سازی می شود. به عنوان آخرین مرحله از این مرحله، web3js برای اتصال پلت فرم وب به شبکه محلی بلاک چین که از طریق اتریوم گاناش در دسترس است، استفاده می شود.**

### 3.1.5 موارد تحویلی

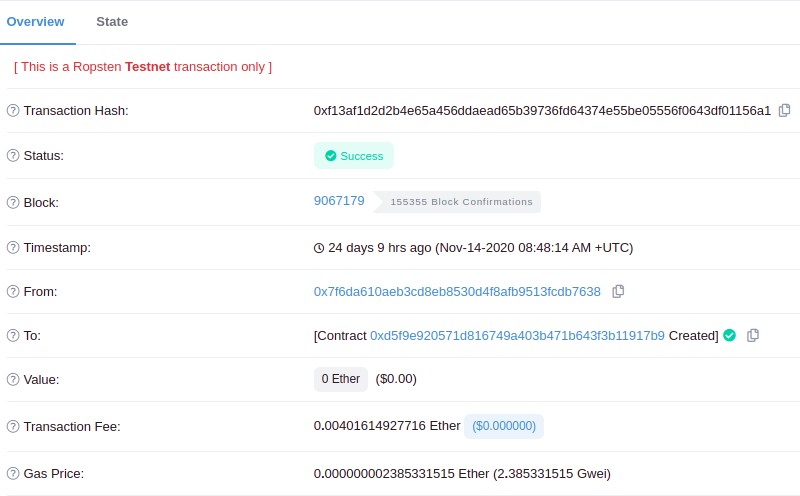
**موارد قابل تحویل، گزارش پایان نامه و اجرای ساده رابط کاربری از نحوه کار چارچوب پیشنهادی است.**



شکل 3.1.1: اعلان در Metamask قیمت گاز، محدودیت گاز و هزینه گاز برای اجرای تراکنش در شبکه آزمایشی Ropsten را نشان می دهد.

## 3.2 راه اندازی آزمایشی

چندین شبکه آزمایشی مانند Ropsten، Rinkeby، Kovan برای آزمایش برنامه های بلاک چین در دسترس هستند. برای ارزیابی عملکرد راه حل قرارداد هوشمند پیشنهادی، قرارداد هوشمند در شبکه تست Ropsten مستقر شد. Ropsten Test Network یک محیط آزمایشی برای قراردادهای هوشمند است. این یکی از شبکه های آزمایشی است که بیشترین شباهت را به شبکه اصلی در اتریوم دارد. هم شبکه اصلی اتریوم و هم شبکه تست Ropsten از الگوریتم اجماع بسیار مشابهی استفاده می کنند. Ropsten Network رایگان است، که آن را برای ارزیابی های ما مناسب می کند زیرا هیچ هزینه مالی در استقرار قراردادهای هوشمند در Ropsten وجود ندارد. با توجه به هزینه های مالی، ارزیابی راه حل پیشنهادی تنها در شبکه آزمایشی به جای شبکه اصلی اتریوم انجام می شود. Metamask یک افزونه مرورگر است که امکان دسترسی به شبکه های محلی بلاک چین و همچنین آزمایش شبکه های بلاک چین از جمله Ropsten را فراهم می کند. با کمک Metamask، چند حساب اتریوم در شبکه آزمایشی Ropsten ایجاد شد. پس از داشتن تعدادی حساب در شبکه آزمایشی، با استفاده از Remix IDE مبتنی بر مرورگر، قرارداد هوشمند راه حل پیشنهادی در شبکه تست Ropsten مستقر می شود. با این تنظیمات آزمایشی، ما موفق می شویم توابع قرارداد هوشمند را از طریق Remix فراخوانی کنیم. و در Metamask، می‌توانیم قیمت اجرای تراکنش‌های خاص را ببینیم (شکل 3.1.1 را ببینید). به منظور تایید اجرای موفقیت آمیز تراکنش ها (نگاه کنید به شکل 3.2.1) از Etherscan (Ropsten Testnet Explorer) [35] استفاده می شود.

شکل 3.2.1: جزئیات تراکنش ایجاد قرارداد هوشمند در Etherscan.

# فصل 4

## طراحی و پیاده سازی

این فصل به شرح طراحی و اجرای پروژه می پردازد. طراحی سیستم به تفصیل شرح داده شده است. علاوه بر این، تعاملات بین اجزای مختلف سیستم نیز در این بخش توضیح داده شده است.

## 4.1 فن آوری ها و ابزارها

مدل پیشنهادی از چندین مؤلفه تشکیل شده است که فناوری های مختلفی را در توسعه شامل می شود.

Truffle: یک محیط توسعه که یک ابزار خط فرمان برای ساخت، کامپایل و استقرار اتریوم dApps با استفاده از EVM فراهم می کند.

Web3.js: Web3.js یک API جاوا اسکریپت اتریوم است. این مجموعه ای از کتابخانه ها است که دارای توابع داخلی برای تعامل با گره اتریوم است. آن توابع داخلی [43] به ما اجازه می دهند تا با استفاده از اتصال HTTP اقدامات لازم را انجام دهیم.

• web3.eth.Contract: این شیء امکان تعامل با قرارداد هوشمند در شبکه بلاک چین را فراهم می کند. اگر قرارداد جدید باید ایجاد شود، رابط JSON قرارداد هوشمند به عنوان یک پارامتر داده می شود. Web3 تماس را به یک تماس ABI سطح پایین از طریق RPC تبدیل می کند.

new web3 .eth. Contract( contract.abi)

.deploy({ data: contract.evm. bytecode})

.send({ gas: gasPrice , from: accountAddress});

• web3.eth.getAccounts: این تابع لیست حساب ها را برمی گرداند.

• web3.utils.fromWei: این تابع هر مقدار wei را به مقدار اتر تبدیل می کند.

• contract.methods.myMethod: زمانی که روش ها به سادگی فراخوانی می شوند، هرگز نمی توانند وضعیت قرارداد هوشمند را تغییر دهند. برای تغییر وضعیت قرارداد هوشمند، تراکنش باید به جای فراخوانی روش ارسال شود.

MetaMask: یک کیف پول اتریوم که با نصب افزونه مرورگر می توان از آن در توسعه استفاده کرد.

Solidity: یک زبان سطح بالا که برای پیاده سازی قراردادهای هوشمند در پلتفرم های مختلف بلاک چین استفاده می شود. [38]

Ganache: امکان ایجاد یک بلاک چین محلی برای توسعه در بلاک چین اتریوم را فراهم می کند. برای توسعه، آزمایش و استقرار قرارداد هوشمند استفاده می شود. [15]

React: Next.js برای ایجاد یک رابط کاربری استفاده می‌شود تا به کاربران اجازه دهد با قراردادهای هوشمند موجود تعامل داشته باشند یا قراردادهای هوشمند جدید در بلاک چین اتریوم ایجاد کنند.

Remix: Remix IDE برای توسعه قراردادهای هوشمند، اشکال زدایی و آزمایش مستقیم آنها در مرورگر استفاده می شود. این یک ابزار متن باز است که با جاوا اسکریپت نوشته شده است

## 4.2 معماری

در این بخش، معماری چارچوب پیشنهادی مورد بحث قرار می گیرد.

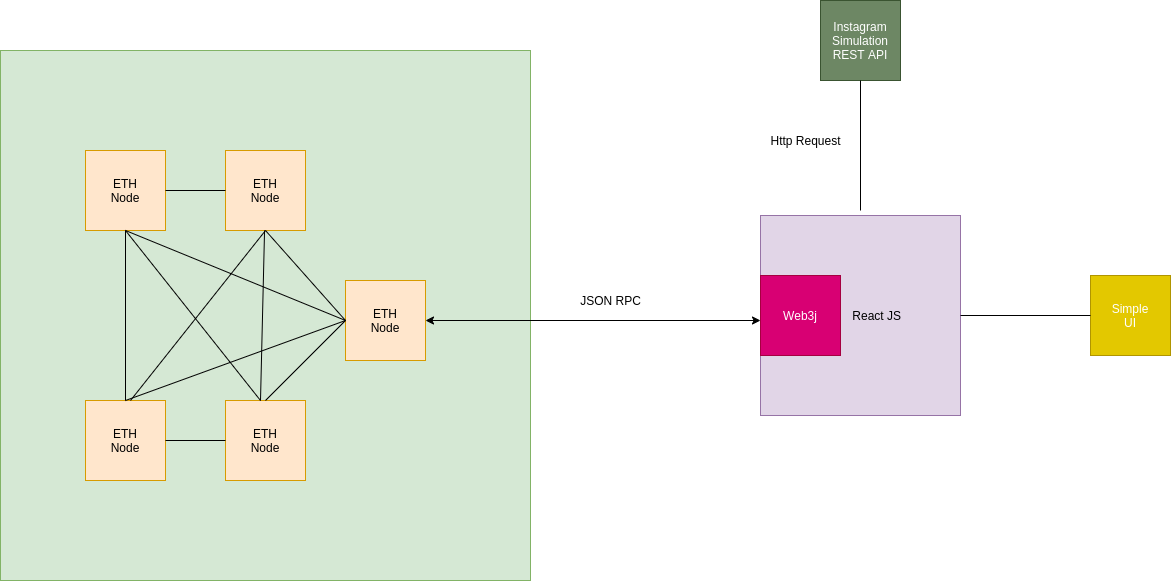
### 4.2.1 نمای کلی سطح بالا

سیستم پیشنهادی قرار است از شبکه های اجتماعی اینستاگرام استفاده کند. برای اینکه فرآیند توسعه را روان‌تر کنیم، یک REST API ساده ایجاد کرده‌ایم که اقدامات ساده اینستاگرام را با افشای چند نقطه پایانی شبیه‌سازی می‌کند.

• POST/users/username/posts/: این نقطه پایانی برای شبیه سازی اشتراک گذاری یک پست در اینستاگرام استفاده می شود.

• GETusers/username/posts/: این نقطه پایانی برای شبیه سازی واکشی تمام پست های یک کاربر استفاده می شود.

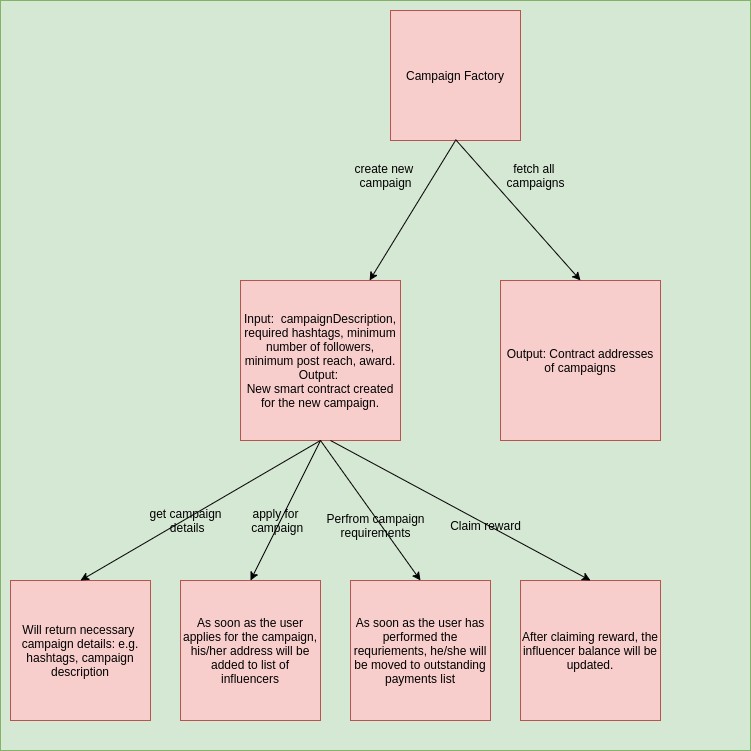
Next.js برای توسعه یک رابط کاربری برای مدل پیشنهادی استفاده می شود. در مدل پیشنهادی، یک جفت بالا بین نمونه قرارداد هوشمند و شبیه سازی اینستاگرام وجود دارد. Web3j در حال ارتباط با پلتفرم اتریوم است و توسط Fetch API، ما با REST API تعامل داریم. در نتیجه این تعاملات، ما تصمیم می‌گیریم که آیا کاربر مجاز است اقدامات مورد نظر خود را انجام دهد (به عنوان مثال، درخواست برای کمپین).

شکل 4.2.1: نمای سطح بالا از طراحی سیستم

### 4.2.2 طراحی سیستم

در مدل پیشنهادی، سه نوع حساب قابل ایجاد وجود دارد. حساب برند برای برندها و شرکت ها است که کمپین های خود را منتشر کنند. حساب ماکرو اینفلوئنسر برای ماکرو اینفلوئنسرها است که می توانند در کمپین ها درخواست دهند و در آن شرکت کنند. نوع اکانت میکرو اینفلوئنسر برای طرفداران ماکرو اینفلوئنسر است. از آنجایی که مجوز و مدیریت حساب مدل پیشنهادی خارج از محدوده است، Auth0 Authentication API [41] با پیاده سازی مدیریت حساب سخت کد شده استفاده می شود.

در مدل پیشنهادی از دو قرارداد هوشمند استفاده شده است. یکی از قراردادهای هوشمند CampaignCreaterFactory و دیگری Campaign نام دارد. دو نوع کمپین وجود دارد که می توان ایجاد کرد (شکل 4.2.3 را ببینید): کمپین، کمپین فرعی. نوع کمپین را فقط می توان با نام تجاری ایجاد کرد. از طرف دیگر، نوع SubCampaign را فقط می توان توسط ماکرو اینفلوئنسرها ایجاد کرد. بنابراین مخاطب مورد نظر برای نوع کمپین، کلان اینفلوئنسرها هستند. فقط آنها می توانند برای آن کمپین ها درخواست دهند. با این حال، نوع SubCampaign برای میکرو اینفلوئنسرها هدف گذاری شده است.



شکل 4.2.2: نمای سطح بالا از طراحی سیستم

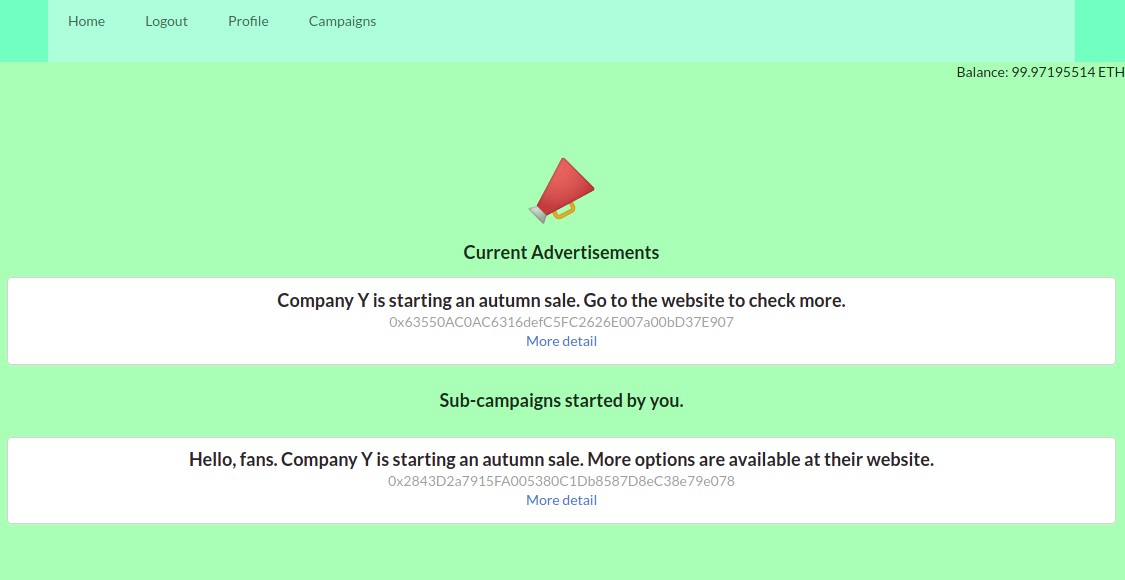
نقش CampaignCreaterFactory این است که کارخانه ای برای ایجاد همه کمپین های دیگر باشد. با داشتن CampaignCreaterFactory، هدف ما جمع‌آوری تمام کمپین‌ها در یک کارخانه است که به وسیله آن واکشی همه کمپین‌های موجود آسان‌تر می‌شود.

contract CampaignCreaterFactory { address[] public deployedCampaigns;

function createNewCampaign(uint minimumNoOfFollowers ,

string memory addDescription , string memory requiredHashtags , uint advertisementFee ,

uint advertisementReach ,



شکل 4.2.3: صفحه ای که در آن کلان اینفلوئنسرها می توانند کمپین ها و کمپین های فرعی را مشاهده کنند.

CampaignType newCampaignType) public {

address newCampaign = address(new Campaign(

minimumNoOfFollowers , addDescription , requiredHashtags , advertisementFee ,

msg.sender , advertisementReach , newCampaignType));

deployedCampaigns.push( newCampaign);

}

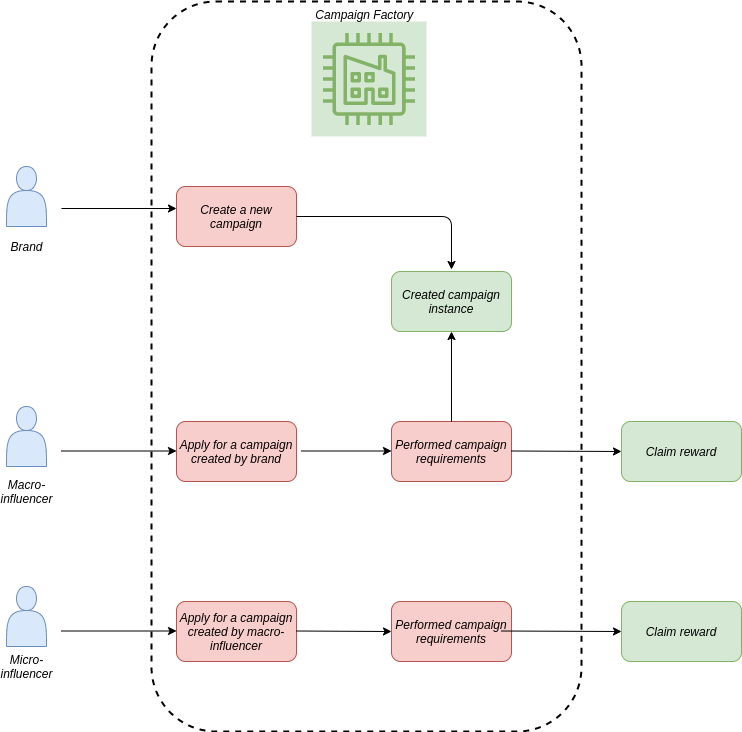
function getAllDeployedCampaigns() public view returns

( address[] memory) {

return deployedCampaigns;

}

}



شکل 4.2.4: خلاصه ای از تعاملات در سیستم

آرایه DeployedCampaigns تمام کمپین هایی را که ایجاد شده اند ذخیره می کند. آنها می توانند هر دو نوع Campaign و SubCampaign باشند. تمام آدرس های قرارداد کمپین ها به دلیل ذخیره در آرایه قابل پیگیری هستند. و نوع آرایه از نوع آدرس است زیرا تمام آنچه در آن وجود دارد آدرس قراردادها است. ما از یک آرایه روی نقشه استفاده کردیم زیرا در Solidity، اگر عملیات مورد نظر تکرار باشد، آرایه مناسب‌تر است. تابع اصلی که قرارداد کمپین را ایجاد می کند createNewCampaign است. تمام پارامترهای لازم را که با فراخوان قرارداد آمده است را می گیرد. پارامترهای ارسال شده به فراخوان ایجاد قرارداد به شرح زیر است:

• minimumNoOfFollowers: حداقل تعداد فالوورهای اینفلوئنسر که واجد شرایط شرکت در کمپین هستند.

• addDescription: بسته به اینکه چه کسی کمپین را ایجاد کرده است، توسط برند یا کلان اینفلوئنسر تنظیم می شود.

• مورد نیاز هشتگ ها: فیلدی برای هشتگ های مورد نیاز کمپین که اینفلوئنسر باید با پست در رسانه های اجتماعی به اشتراک بگذارد.

• هزینه تبلیغات: میزان پاداشی که اینفلوئنسر در درخواست و دستیابی به تعداد مورد نیاز مخاطب دریافت می کند.

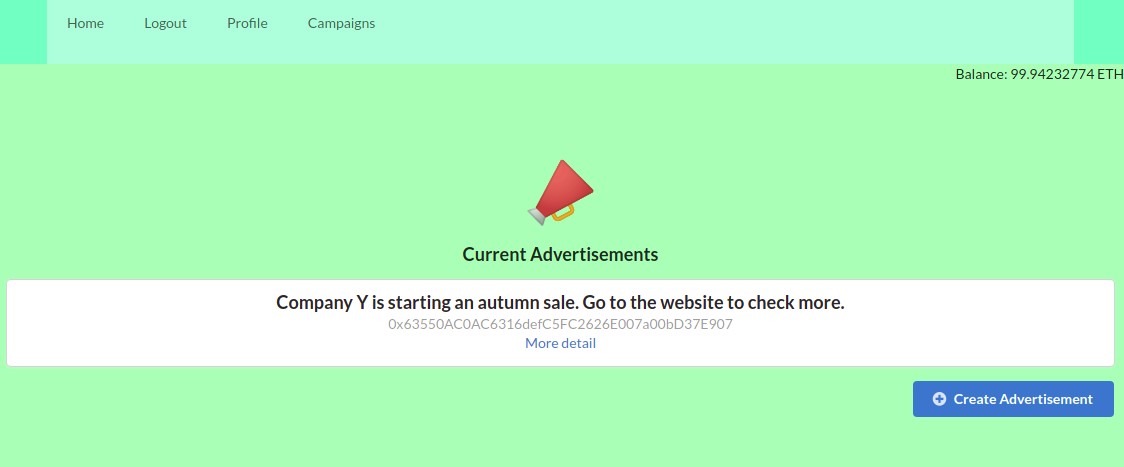
• msg.sender: این پارامتر برای ذخیره مالک قرارداد، آدرس نهادی که کمپین را ایجاد کرده است، استفاده می شود.

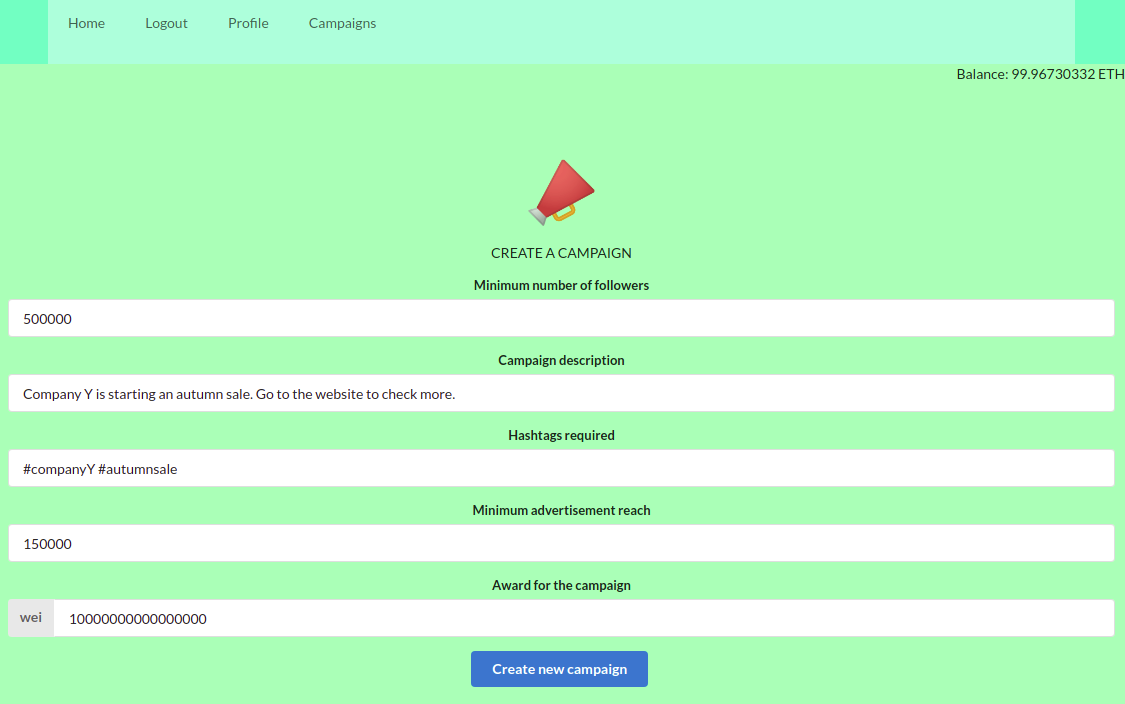
• advertisementReach: هدف مخاطبان تبلیغات (پست تعامل) که باید به آن رسید تا اجازه دریافت پاداش را داشته باشد. تا زمانی که به تعداد مشخصی از مخاطبان نرسیده باشد، اینفلوئنسرها قادر به دریافت پاداش نیستند.

• newCampaignType: نوع کمپین کمپین یا SubCampaign

بسته به اینکه چه کسی قرارداد کمپین را ایجاد کرده است.

قرارداد دیگر قرارداد Campaign است که توسط CampaignCreaterFactory نامیده می شود. هنگامی که یک نام تجاری بر روی دکمه ایجاد تبلیغات کلیک می کند (شکل 4.2.5 را ببینید)، صفحه ایجاد یک کمپین جدید بارگذاری می شود. در آن صفحه، تمام جزئیات لازم برای یک کمپین پر شده است (شکل 4.2.6 را ببینید). هنگامی که یک نام تجاری بر روی دکمه ایجاد یک کمپین جدید کلیک می کند، قرارداد CampaignCreaterFactory سازنده قرارداد Campaign را فرا می خواند که منجر به ایجاد کمپین جدید می شود. در قرارداد کمپین، ما یک ساختار تبلیغاتی ایجاد کرده‌ایم که جزئیات لازم قرارداد کمپین را ذخیره می‌کند. در Solidity، ساختار نوعی است که با هر تعداد فیلد قابل تعریف است.

 شکل 4.2.5: صفحه ای که برندها می توانند کمپین هایی را که ایجاد کرده اند مشاهده کنند. هنگامی که آنها بر روی ایجاد تبلیغات کلیک می کنند، برای ایجاد یک کمپین جدید به صفحه هدایت می شوند.



شکل 4.2.6: صفحه ای که برندها یک کمپین جدید ایجاد می کنند.

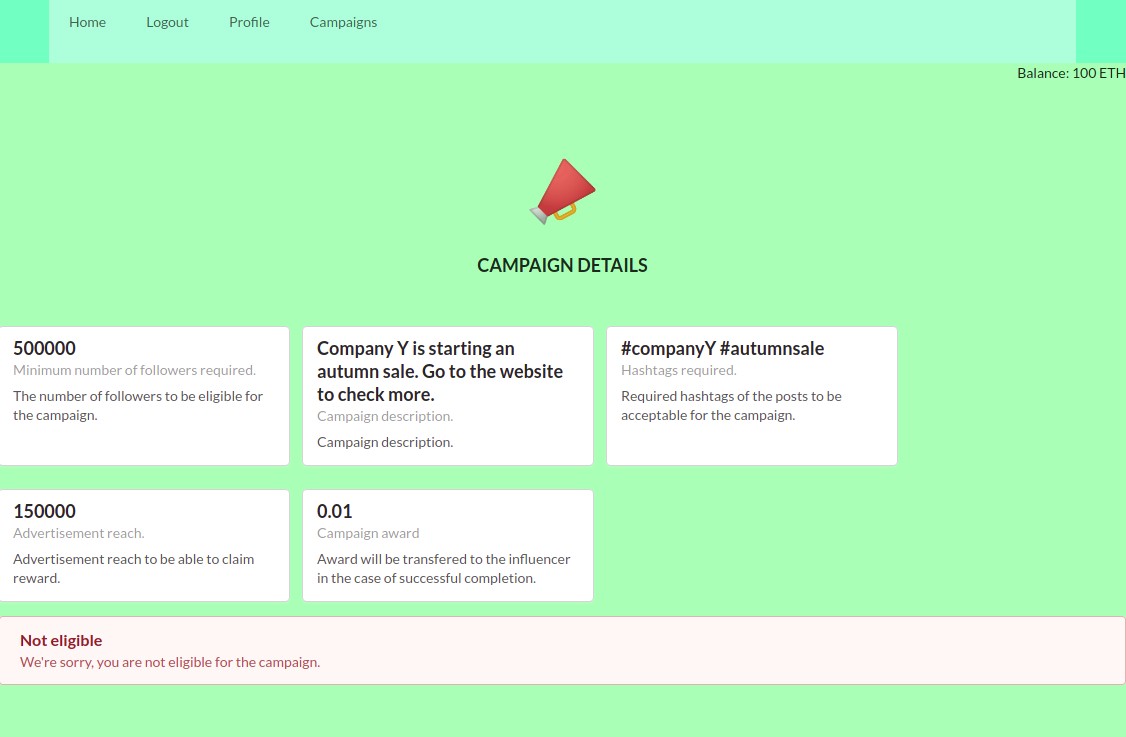
|  |  |  |
| --- | --- | --- |
| 1 | struct | Advertisement { |
| 2 |  | string description; |
| 3 |  | string hashtags; |
| 4 |  | uint payment; |
| 5 |  | uint addReach; |
| 6 | } |  |
| 7 |  |  |

صفحه مشاهده جزئیات کمپین خاص تقریباً برای هر سه نوع حساب یکسان است. جزئیات کمپین مانند حداقل تعداد فالوور، توضیحات کمپین، هشتگ های مورد نیاز، حداقل دسترسی به تبلیغات و جایزه کمپین در صفحه نمایش داده می شود. تنها تفاوت این است که دکمه‌های اعمال، انجام الزامات، و درخواست پاداش تنها در صورتی نشان داده می‌شوند که واجد شرایط کمپین باشید.

مهمترین چیزی که در قرارداد هوشمند کمپین باید به آن اشاره کرد، سه نقشه است که آدرس اینفلوئنسرها را ذخیره می کند.

mapping( address => bool) private alreadyAppliedInfluencers; mapping( address => bool) private currentInfluencers; mapping( address => bool) private outstandingPayments;

mapping( address => bool) private alreadyAppliedInfluencers; mapping( address => bool) private currentInfluencers; mapping( address => bool) private outstandingPayments;



شکل 4.2.7: پیام اطلاعاتی نشان می دهد که کلان اینفلوئنسر واجد شرایط کمپین نیست.

• alreadyAppliedInfluencers: این نقشه آدرس حساب افراد تأثیرگذار را که قبلاً در کمپین شرکت کرده اند ذخیره می کند. داشتن این نقشه برای پیگیری آدرس‌های حساب‌ها ضروری است تا از شرکت چندین بار اینفلوئنسر در کمپین جلوگیری شود.

• currentInfluencers: این نقشه آدرس های حساب اینفلوئنسرهای فعلی را ذخیره می کند. اینفلوئنسرهای کنونی اینفلوئنسرهایی هستند که برای کمپین درخواست داده اند، اما هنوز الزامات کمپین را انجام نداده اند تا واجد شرایط دریافت جایزه باشند.

• پرداخت‌های معوق: این نقشه آدرس‌های حساب افراد تأثیرگذار را ذخیره می‌کند که الزامات کمپین را انجام داده‌اند، اما آنها هنوز جایزه را دریافت نکرده‌اند. به محض اینکه اینفلوئنسر مدعی جایزه شد، از این نقشه حذف شده و به نقشه قبلاًAppliedInfluencers اضافه می شود.

## 4.3 پیاده سازی

در این بخش، وظایف قرارداد هوشمند به تفصیل شرح داده شده است.

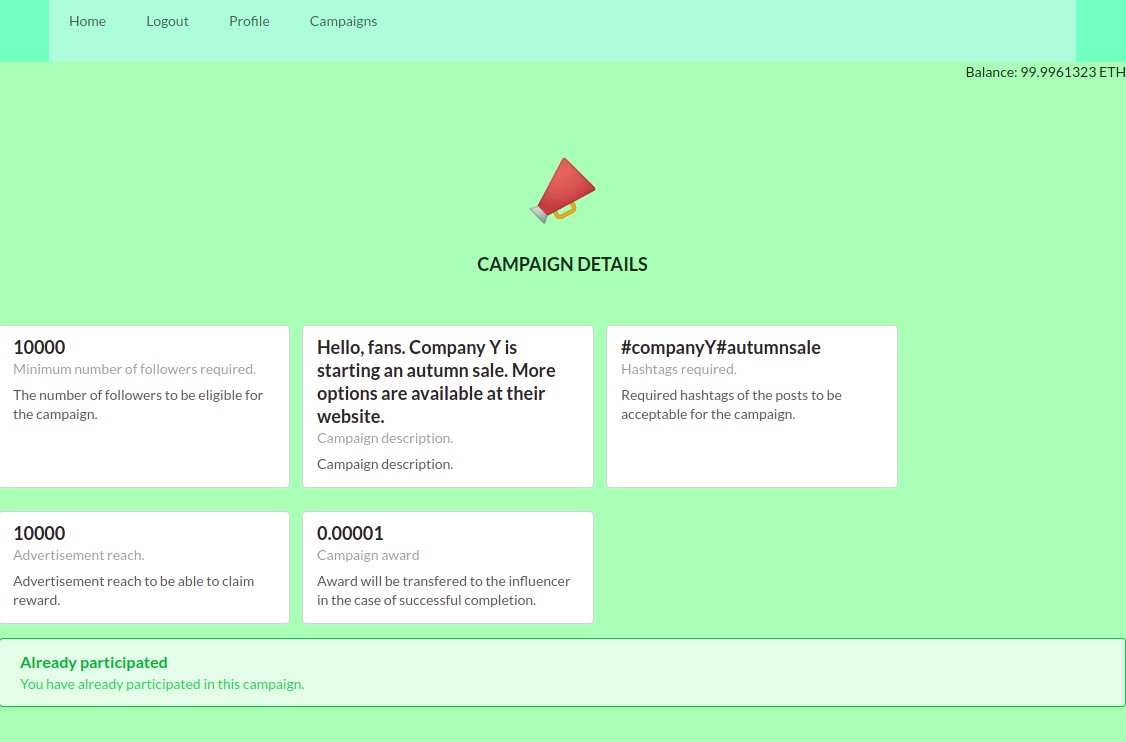
### 4.3.1 درخواست برای کمپین

نقش اصلی داشتن سه نقشه، بررسی های امنیتی قبل از درخواست اینفلوئنسرها برای کمپین یا ادعای جایزه کمپین است. وقتی اینفلوئنسر برای کمپین درخواست می‌کند، ابتدا بررسی می‌شود که آیا آدرس قرارداد اینفلوئنسر در نقشه قبلاًAppliedInfluencers وجود دارد یا خیر. اگر قبلاً در نقشه قبلاًAppliedInfluencers وجود نداشته باشد، درخواست برای کمپین موفقیت آمیز خواهد بود. در صورتی که آدرس حساب اینفلوئنسر در نقشه وجود داشته باشد، درخواست برای کمپین با موفقیت به پایان نمی رسد

function applyForCampaign() public payable {

require(!( alreadyAppliedInfluencers[msg.sender])); currentInfluencers[msg.sender] = true;

}



شکل 4.3.1: پیام اطلاعاتی نشان می دهد که ماکرو اینفلوئنسر یا میکرو اینفلوئنسر قبلاً در کمپین شرکت کرده است.

به همین دلیل است که برای بررسی اینکه آیا فرستنده پیام در نقشه قبلاًAppliedInfluencers وجود دارد یا خیر از require استفاده می کنیم. اگر وجود داشته باشد، یک مورد از استثنا ایجاد می کند و تراکنش برگردانده می شود. با این حال، در برنامه جلویی، ما نیز نیاز داریم

به همین دلیل است که برای بررسی اینکه آیا فرستنده پیام در نقشه قبلاًAppliedInfluencers وجود دارد یا خیر از require استفاده می کنیم. اگر وجود داشته باشد، یک مورد از استثنا ایجاد می کند و تراکنش برگردانده می شود. با این حال، در برنامه front end، ما همچنین باید بررسی کنیم که آیا آدرس حساب اینفلوئنسر در نقشه وجود دارد یا خیر. اگر اینطور شد، دکمه اعمال برای کمپین را پنهان می کنیم. در عوض، پیامی را نشان می‌دهیم که تأثیرگذار را در مورد مشارکت قبلی در کمپین مطلع می‌کند (شکل 4.3.1 را ببینید). این پیام تنها در صورتی نمایش داده می‌شود که اینفلوئنسر در کل فرآیند آن کمپین خاص، از جمله ادعای پاداش، مشارکت داشته باشد. بررسی وجود فرستنده پیام فقط در سمت مشتری برای امنیت کافی نیست. در صورت عدم استفاده از محدودیت الزامی، برخی از قراردادهای دیگر در بلاک چین می توانند قرارداد کمپین را فراخوانی کنند، اگرچه نباید مجاز به تماس باشند. بنابراین با کمک نیاز، از این نوع تماس ها جلوگیری می شود. لازمه درخواست برای کمپین داشتن فالوور کافی است. هنگامی که برند یا کلان اینفلوئنسر یک کمپین ایجاد می کند، حداقل تعداد دنبال کنندگان (minimumNoOfFollowers) را برای واجد شرایط بودن در کمپین مشخص می کند. اگر تعداد فالوورهای اینفلوئنسر کمتر از حداقل NoOfFollowers باشد، آنها نمی توانند برای کمپین درخواست دهند (شکل 4.2.7 را ببینید).

### 4.3.2 برداشت

اینفلوئنسرها می توانند از کمپین کنار بکشند. برای اینکه بتوانند از کمپین خارج شوند، باید قبلا برای کمپین درخواست داده باشند، به این معنی که اینفلوئنسر باید در نقشه فعلی اینفلوئنسرها وجود داشته باشد. در آن صورت، دکمه خروج از کمپین ظاهر می شود (شکل 4.3.2 را ببینید). اگر از کمپین خارج شوند، نقشه ها به روز می شوند، آدرس حساب اینفلوئنسر از نقشه تأثیرگذاران فعلی و پرداخت های معوق حذف می شود. وقتی از کمپین کنار می‌روند، با حذف آن‌ها از نقشه‌های موجود، به اینفلوئنسرها اجازه می‌دهیم تا در صورت تصمیم، مجدداً برای کمپین درخواست دهند.

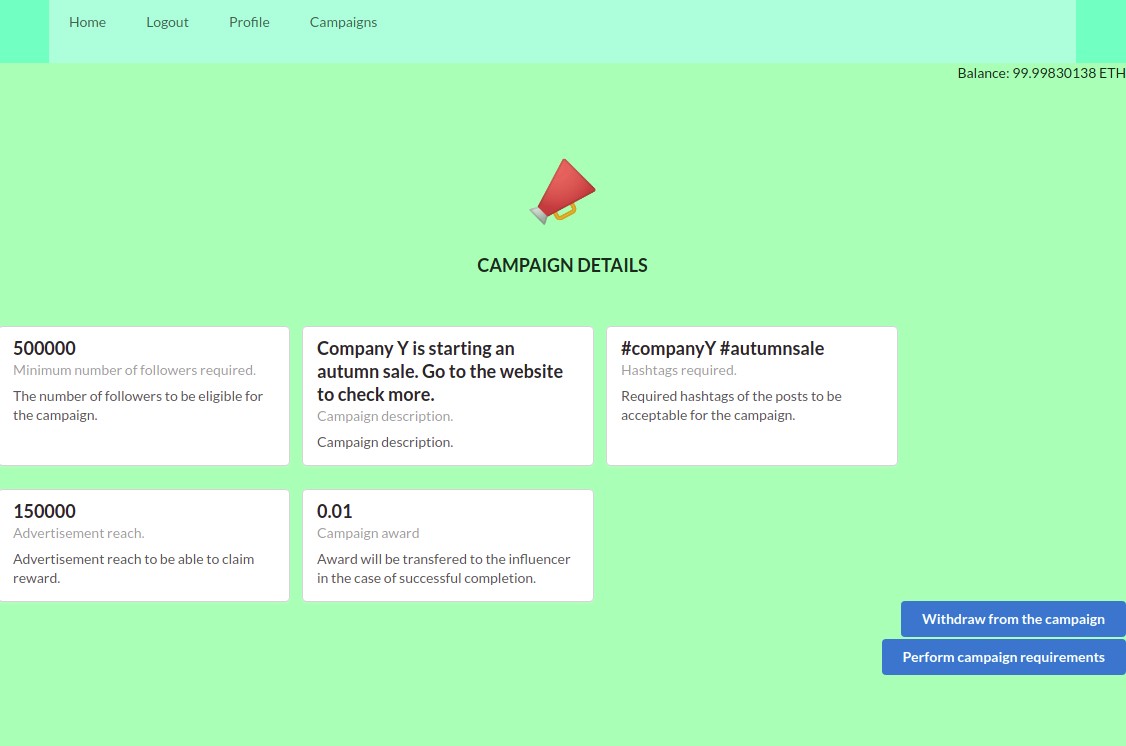
function withdrawFromCampaign() public payable { require( currentInfluencers[msg.sender]);

currentInfluencers[msg.sender] = false; outstandingPayments[msg.sender] = false;

}

### 4.3.3 انجام الزامات

پس از درخواست برای کمپین، آنها در نقشه اینفلوئنسرهای فعلی وجود دارند و می توانند الزامات کمپین را انجام دهند تا بتوانند پاداش کمپین را دریافت کنند. پس از انجام الزامات، دو فرآیند در حال انجام است. ابتدا پست در شبیه سازی اینستاگرام به اشتراک گذاشته می شود و سپس روش انجام شده CampaignRequirements قرارداد هوشمند فراخوانی می شود. برای اینکه این تابع منجر به تماس موفق شود، آدرس اینفلوئنسر باید در نقشه فعلی اینفلوئنسرها وجود داشته باشد. پس از بررسی این شرایط توسط نیاز، آدرس حساب اینفلوئنسر به پرداخت‌های معوق اضافه می‌شود



شکل 4.3.2: پس از درخواست برای هر کمپین، یک اینفلوئنسر می تواند بعداً از آن کمپین خارج شود.

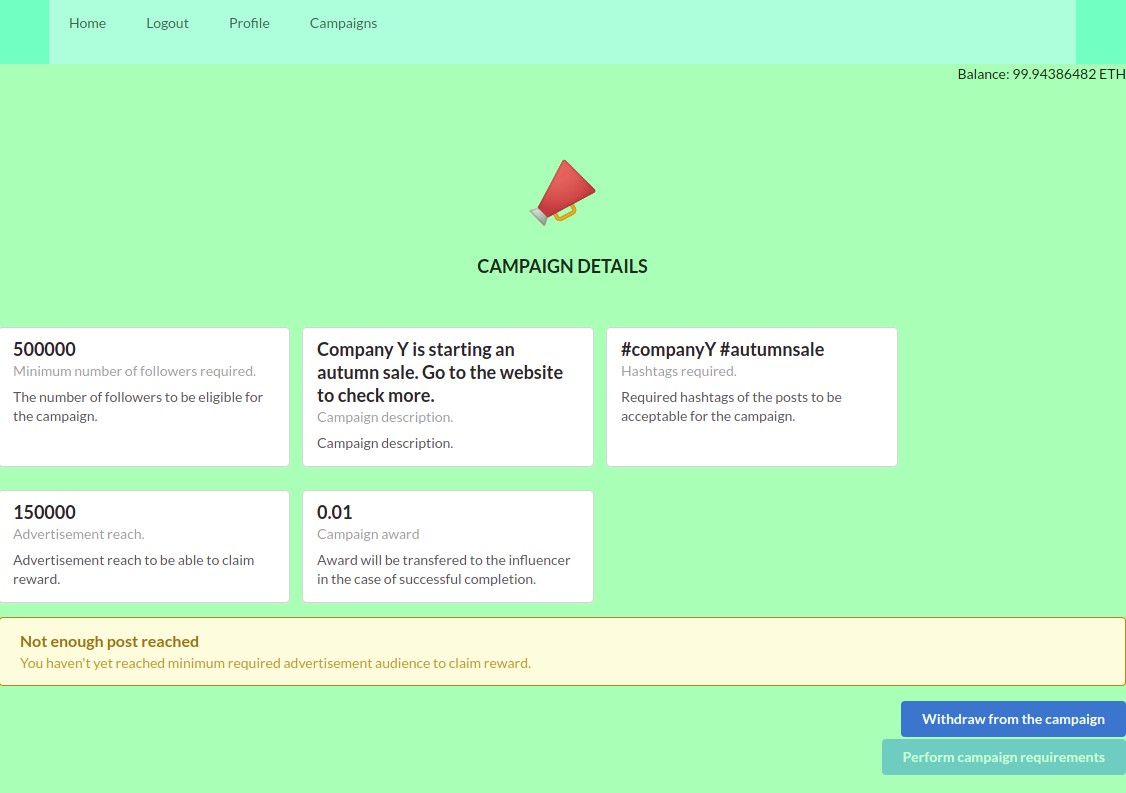
روش اجراشدهCampaignRequirements قرارداد هوشمند نامیده می شود. برای اینکه این تابع منجر به تماس موفق شود، آدرس اینفلوئنسر باید در نقشه فعلی اینفلوئنسرها وجود داشته باشد. پس از بررسی این شرایط توسط نیاز، آدرس حساب اینفلوئنسر به پرداخت‌های معوق اضافه می‌شود.

function performedCampaignRequirements() public { require( currentInfluencers[msg.sender]);

outstandingPayments[msg.sender] = true;

}

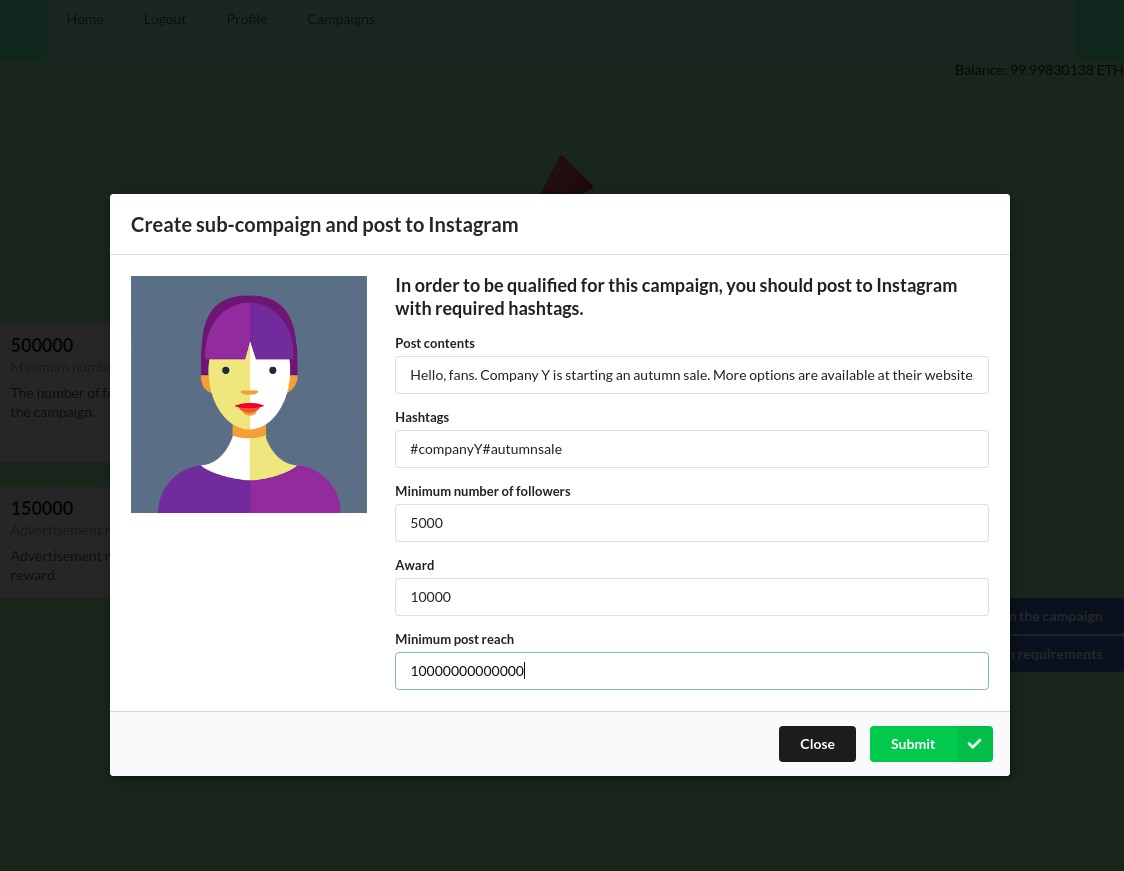
انجام الزامات برای ماکرو اینفلوئنسرها و میکرو اینفلوئنسرها رفتار متفاوتی دارد. هنگامی که یک ماکرو اینفلوئنسر الزامات کمپین ایجاد شده توسط یک برند را انجام می دهد، پست در شبیه سازی اینستاگرام به اشتراک گذاشته می شود. در همان زمان، یک کمپین فرعی توسط ماکرو اینفلوئنسر ایجاد می شود (شکل 4.3.4 را ببینید). این کمپین فرعی برای شرکت میکرو اینفلوئنسرها در دسترس است. برعکس، زمانی که یک میکرو اینفلوئنسر الزامات کمپین فرعی ایجاد شده توسط یک ماکرو اینفلوئنسر را انجام می دهد، پست در شبیه سازی اینستاگرام به اشتراک گذاشته می شود، هیچ قراردادی ایجاد نمی شود. به همین دلیل است که وقتی میکرو اینفلوئنسر الزامات کمپین را انجام می دهد، مانند کلان اینفلوئنسرها نیازی به تعیین جزئیات کمپین ندارند (شکل 4.3.5 را ببینید).



شکل 4.3.3: پیامی که به اینفلوئنسر اطلاع می دهد که مخاطب هدف به دست نیامده است.

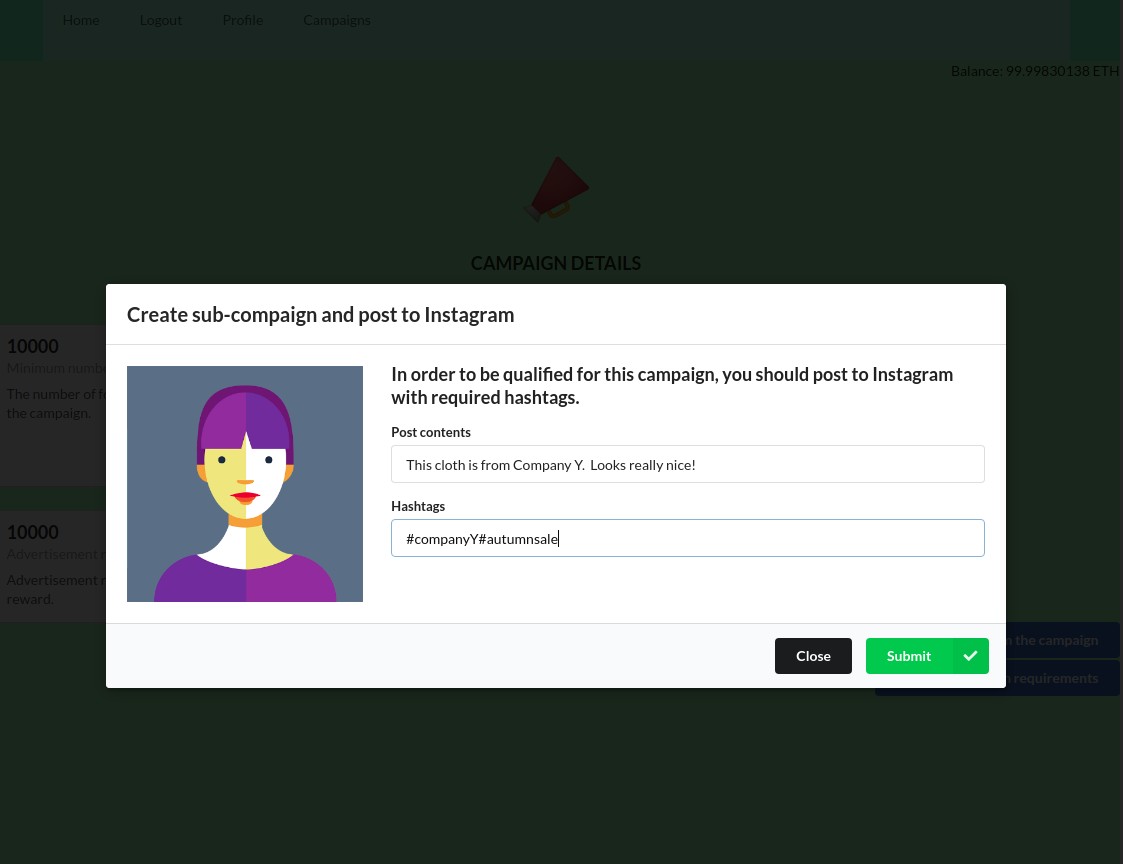
### 4.3.4 مطالبه دستمزد

برای اینکه بتوانید جایزه کمپین را دریافت کنید، دو شرط باید رعایت شود. اول، حساب اینفلوئنسر باید هم در نقشه فعلی اینفلوئنسرها و هم در نقشه پرداخت‌های معوق وجود داشته باشد. با استفاده از تابع نیازمندی Solidity، به آن رفتار دست پیدا می کنیم. شرط دوم رسیدن به تعداد مورد نیاز مخاطب است. این بدان معناست که پست به اشتراک گذاشته شده در رسانه های اجتماعی باید دارای حداقل دسترسی مخاطب (advertisementReach) باشد که توسط مالک کمپین در هنگام ایجاد قرارداد هوشمند مشخص شده است. اگر به هدف مورد نیاز مخاطب نرسیده باشند، نمی توانند پاداش را مطالبه کنند (شکل 4.3.3 را ببینید). میزان دسترسی مخاطب به اینفلوئنسر کلان و میکرو اینفلوئنسر متفاوت محاسبه می شود. برای یک کلان اینفلوئنسر، مجموع درگیری پست‌های یک کلان اینفلوئنسر و درگیری پست‌های یک میکرو اینفلوئنسر در نظر گرفته می‌شود که برای کمپین فرعی که ماکرو اینفلوئنسر ایجاد کرده است درخواست داده است. از سوی دیگر، از آنجایی که یک میکرو اینفلوئنسر نمی تواند کمپین فرعی ایجاد کند، دسترسی مخاطب صرفاً درگیر شدن پست هایی است که در رسانه های اجتماعی به اشتراک گذاشته اند. اگر این دو شرط برآورده شوند، دکمه درخواست پاداش در صفحه جزئیات کمپین در دسترس خواهد بود (شکل 4.3.6 را ببینید). پس از رسیدن به هدف مورد نیاز، هنگامی که تابع پاداش ادعا (claimTokens) با موفقیت فراخوانی شد، پاداش مشخص شده برای کمپین به حساب اینفلوئنسر منتقل می شود.

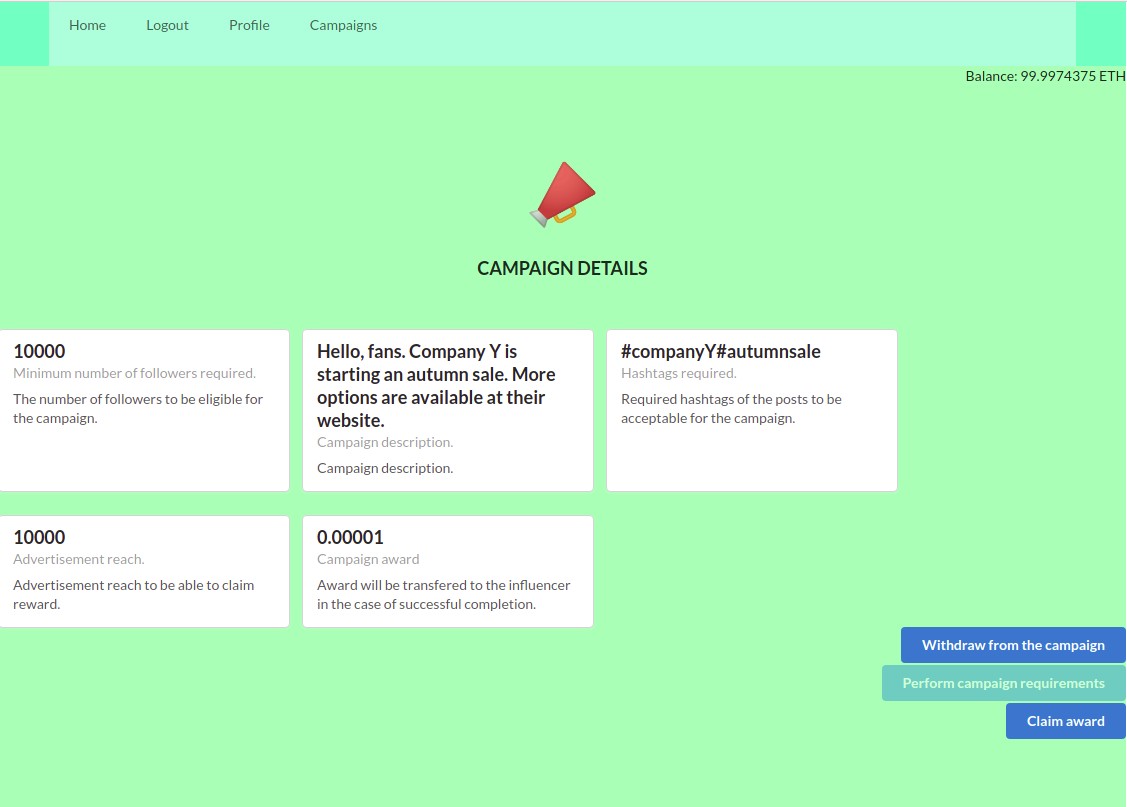


شکل 4.3.4: صفحه ای که یک اینفلوئنسر ماکرو یک کمپین فرعی ایجاد می کند و یک پست را در اینستاگرام به اشتراک می گذارد.

require( outstandingPayments[msg.sender]); require( currentInfluencers[msg.sender]);



شکل 4.3.5: صفحه ای که یک میکرو اینفلوئنسر پستی را در اینستاگرام به اشتراک می گذارد.



شکل 4.3.6: صفحه ای که در آن یک ماکرو اینفلوئنسر یا یک میکرو اینفلوئنسر ادعای پاداش می کند.

# فصل 5

## تجزیه و تحلیل و نتایج

این فصل نتایج تجربی و تجزیه و تحلیل نتایج را شرح می دهد.

## 5.1 نتایج تجربی

قرارداد هوشمند پیشنهادی برای ارزیابی در شبکه تست Ropsten مستقر شده است. برای اتصال به شبکه تست Ropsten ابتدا با کمک متامسک چند اکانت در Ropsten ایجاد شده است. و برای استقرار قرارداد هوشمند از Remix استفاده می شود. Remix IDE با Web3 تزریق شده به Metamask متصل می شود. معیارهای اصلی که می خواستیم اندازه گیری کنیم، هزینه تراکنش برای اقدامات قراردادهای هوشمند بود. این یک اندازه گیری مهم برای بررسی اینکه آیا هزینه قرارداد هوشمند بالاتر از هزینه های تبلیغات سنتی است یا خیر بود. به منظور جلوگیری از هزینه های مالی، تست ها بر روی شبکه آزمایشی انجام شده است.

استقرار کارخانه قرارداد اولین قدم برای ایجاد قراردادهای فردی بود. استقرار کارخانه قراردادی منجر به ایجاد قرارداد جدید برای کارخانه کمپین شد. کل هزینه استقرار کارخانه کمپین 0.004016 ETH بود (جدول 5.1.1 را ببینید). زمانی که پلتفرم برای تولید در دسترس باشد، این معامله تنها یک بار انجام می شود. بنابراین این هزینه در مرحله بعدی فرآیند اتفاق نخواهد افتاد. از آنجایی که ما فقط یک بار نیاز به استقرار کارخانه کمپین داریم، پس از استقرار کارخانه، از آن قرارداد کارخانه برای ایجاد کمپین های فردی جدید استفاده خواهیم کرد.

یک پلتفرم در دسترس (Etherscan) برای کاوش تراکنش ها وجود دارد. Etherscan بیشتر به عنوان یک موتور جستجو استفاده می شود. امکان جستجوی تراکنش ها و مشاهده جزئیات تراکنش مانند وضعیت، قیمت بنزین، سقف بنزین و کل هزینه ها وجود دارد.

|  |  |
| --- | --- |
| Contract Factory Deployment Costs | |
| Total price | 0.004016 ETH |
| Gas price | 2.385331515 |
| Gas limit | 1683686 |
| Processing time | 31s |

جدول 5.1.1: هزینه های استقرار قرارداد کارخانه کمپین در شبکه تست Ropsten

|  |  |
| --- | --- |
| Campaign creation costs | |
| Total price | 0.002847 ETH |
| Gas price | 2.348464876 |
| Gas limit | 1212433 |
| Processing time | 34s |

جدول 5.1.2: هزینه های ایجاد کمپین جدید

پس از ایجاد و استقرار کارخانه کمپین، ایجاد کمپین جدید برای اندازه گیری هزینه آزمایش شده است. این هزینه هر بار که یک برند یک کمپین جدید ایجاد می کند، اتفاق می افتد. این مبلغ از حساب برند در شبکه بلاک چین اتریوم شارژ می شود. کل هزینه ایجاد کمپین 0.002847 ETH است (جدول 5.1.2 را ببینید).

هزینه ای که از اینفلوئنسرها برای 4 اقدام زیر دریافت می شود:

• برای کمپین اقدام کنید

• از کمپین کناره گیری کنید

• الزامات کمپین را انجام دهید

• درخواست پاداش

کل هزینه درخواست برای کمپین 0.000199 ETH است (جدول 5.1.3 را ببینید). این مبلغ پس از درخواست اینفلوئنسر برای کمپین دریافت می شود. زمان پردازش تراکنش در شبکه تست Ropsten 32 ثانیه است.

|  |  |
| --- | --- |
| Costs of applying for campaign | |
| Total price | 0.000199 ETH |
| Gas price | 2.348464876 |
| Gas limit | 84931 |
| Processing time | 32s |

جدول 5.1.3: هزینه های درخواست برای کمپین

|  |  |
| --- | --- |
| Costs of withdrawing from a campaign | |
| Total price | 0.000035 ETH |
| Gas price | 0.00000000234 |
| Gas limit | 31,395 |
| Processing time | 17s |

جدول 5.1.4: هزینه های خروج از کمپین از قبل اعمال شده

|  |  |
| --- | --- |
| Costs of performing campaign requirements | |
| Total price | 0.000101 ETH |
| Gas price | 2.348464876 |
| Gas limit | 43194 |
| Processing time | 18s |

جدول 5.1.5: هزینه های مرتبط با اجرای الزامات کمپین

کل هزینه برداشت از یک کمپین 0.000035 ETH است (جدول 5.1.4 را ببینید). زمان پردازش تراکنش در شبکه تست Ropsten 17 ثانیه است.

هزینه کل برای اجرای الزامات کمپین 0.000101 ETH است که ارزان ترین اقدام در کل فرآیند است (جدول 5.1.5 را ببینید). مدت زمان پردازش تراکنش 18 ثانیه است که همچنین بسیار کمتر از زمان پردازش سایر اقدامات است.

برای دریافت پاداش کمپین، 0.000199 ETH از موجودی اینفلوئنسر کسر می شود. (به جدول 5.1.6 مراجعه کنید) زمان پردازش تراکنش تقریباً 18 ثانیه برای عمل بود.

## 5.2 ارزیابی

همانطور که در بخش قبل محاسبه شد، هزینه ای که یک برند برای ایجاد کمپین پرداخت می کند تقریباً 0.002847 ETH است. این مبلغ بسیار کمتر از هزینه های تبلیغاتی سنتی است که در آن برندها بیشتر از این برای کارهای اداری هزینه می کنند. کل هزینه مشارکت در برنامه کمپین از ابتدا تا پاداش ادعایی 0.000499 ETH است. هزینه خروج از یک کمپین در هزینه کل فرآیند محاسبه نمی شود زیرا خروج بخشی از سناریوی خوشحال کننده در راه حل پیشنهادی نیست.

|  |  |
| --- | --- |
| Costs of claiming reward | |
| Total price | 0.000199 ETH |
| Gas price | 2.348464876 |
| Gas limit | 64312 |
| Processing time | 18s |

جدول 5.1.6: هزینه های مربوط به ادعای توکن

totalCost = applicationCost + performRequirementsCost + claimRewardCost

با مقایسه کل مبلغ شرکت در کمپین با پاداشی که اینفلوئنسرها در ازای تبلیغ محصولات دریافت می کنند، هزینه شرکت در کمپین قابل قبول است. طبق گزارش فایننشال تایمز [20]، اینفلوئنسرهایی با حدود 100000 فالوور در اینستاگرام می توانند حدود 2000 پوند برای هر پست دریافت کنند، در حالی که اینفلوئنسرهای مشهور با بین 4 میلیون تا 20 میلیون دنبال کننده می توانند حدود 5000 پوند 13000 پوند دریافت کنند. در مقایسه با این ارقام، هزینه شرکت در کمپین مناسب است.

برخلاف راه حل های مشابه موجود، در چارچوب پیشنهادی، اینفلوئنسرهای خرد در فرآیند کمپین دخیل هستند. مشارکت میکرو اینفلوئنسرها نیازمند ارتباطات اضافی با قرارداد هوشمند است زیرا زمانی که اینفلوئنسرهای کلان نیازمندی ها را انجام می دهند، به منظور گنجاندن میکرو اینفلوئنسرها در کمپین ها، یک کمپین فرعی ایجاد می شود. نتایج آزمایش نشان می‌دهد که حتی با دخالت آن ارتباطات، با در نظر گرفتن زمان و هزینه، چارچوب پیشنهادی قابل اجرا است.

# فصل 6

## نتیجه گیری و کار آتی

این فصل نتایج و نتیجه گیری هایی را که می توان در رابطه با بیان مشکل گزارش گرفت، مورد بحث قرار می دهد. محدودیت های مطالعه و کار احتمالی آینده نیز در این فصل توضیح داده شده است.

## 6.1 نتیجه گیری

بر اساس نتیجه آزمایش بر روی شبکه Ropsten می توان نتیجه گرفت که راه حل پیشنهادی برای مشکلات ذکر شده قابل اجرا است. راه حل پیشنهادی شامل مشارکت میکرو اینفلوئنسرها در فرآیند کمپین نیز می باشد. میکرواینفلوئنسرها با مشارکت در روند کمپین، پستی را در رسانه های اجتماعی به اشتراک می گذارند که می تواند به حل مشکل افزایش بازده در فروشگاه های آنلاین به دلیل مشکل مناسب کمک کند. بنابراین محصول تبلیغ شده نه تنها در ماکرو اینفلوئنسرها بلکه در میکرو اینفلوئنسرها نیز تبلیغ می شود. کل فرآیند با ارتباط با شبیه سازی رسانه های اجتماعی با درخواست های HTTP خودکار می شود. هزینه های تراکنش اقدامات قراردادهای هوشمند اعداد بالایی نیستند، که به راه حل پیشنهادی اجازه می دهد برای سناریوهای دنیای واقعی قابل اجرا باشد.

## 6.2 محدودیت

محدودیت این پروژه این است که راه حل پیشنهادی در شبکه اصلی اتریوم به دلیل هزینه های مالی مربوط به اقدامات در قرارداد مستقر شده آزمایش و ارزیابی نشده است. به همین دلیل است که ارزیابی های متریک در شبکه تست Ropsten انجام شده است.

## 6.3 فعالیت آینده

فعالیت آینده پس از این پروژه درجه می تواند تجزیه و تحلیل رفتار راه حل پیشنهادی در شبکه اصلی اتریوم برای مشاهده تفاوت هزینه تراکنش بین شبکه اصلی و شبکه تست Ropsten باشد.

# فهرست کتب

[1] A Next­Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed: 2020­04­ 25.

[2] Amaratunga, D, Sarshar, M, and Newton, R. Quantitative and qualitative research in the built environment: application of “mixed” research approach. MCB UP Ltd, 2002, pp. 17–31. DOI: https : / / doi . org / 10 . 1108 / 00438020210415488.

[3] AP NEWS. https : / / apnews . com / press - release / pr - accesswire / 9520cbbdfc20b8f6a28eaf69b10c8a4a. Accessed: 2020­11­11.

[4] APPICS Official Website. https://appics.com/. Accessed: 2020­05­16.

[5] Asad Ali Siyal Aisha Zahid Junejo . Muhammad Zawish . Kainat Ahmed . Aiman Khalil, Georgia Soursou. “Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives”. In: (Jan. 2019). DOI: https://doi.org/10.3390/cryptography3010003.

[6] Bach, L. M., Mihaljevic, B., and Zagar, M. “Comparative analysis of blockchain consensus algorithms”. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2018, pp. 1545–1550.

[7] Beigepaper: An Ethereum Technical Specification. https://cryptorating. eu/whitepapers/Ethereum/beigepaper.pdf. Accessed: 2020­04­27.

[8] Bitcoin.org. Bitcoin Developer Reference. URL: https://bitcoin.org /en / developer-reference (visited on 02/18/2020).

[9] Blockchain in Insurance. Why should you care? https://www2.deloitte.com/ ca/en/pages/financial-services/articles/blockchain-in-insurance. html. Accessed: 2020­10­17.

[10] Chen, Wubing, Xu, Zhiying, Shi, Shuyu, Zhao, Yang, and Zhao, Jun. “A Survey of Blockchain Applications in Different Domains”. In: Proceedings of the 2018 International Conference on Blockchain Technology and Application. ICBTA 2018. Xi’an, China: Association for Computing Machinery, 2018, pp. 17–21. ISBN: 9781450366465. DOI: 10.1145/3301403.3301407. URL: https://doi.

org/10.1145/3301403.3301407.

[11] Dib, Omar, Brousmiche, Kei­Leo, Durand, Antoine, Thea, Eric, and Hamida, Elyes Ben. “Consortium Blockchains: Overview, Applications and Challenges”. In: International Journal on Advances in Telecommunications 11 (2018), pp. 51–64. URL: http : / / www . iariajournals . org / telecommunications / tocv11n12.html.

[12] Digital 2019. https : / / wearesocial . com / global - digital - report - 2019. Accessed: 2020­05­15.

[13] Digital Certificates Project. http://certificates.media.mit.edu/. Accessed: 2020­10­17.

[14] ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper. pdf. Accessed: 2020­04­27.

[15] ganache. URL: https://www .trufflesuite.com /docs /ganache /overview

(visited on 10/04/2020).

[16] Gopie, Nigel. What are smart contracts on blockchain? 2018. URL: https:// www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on- blockchain/ (visited on 02/03/2020).

[17] Guegan, Dominique. Public Blockchain versus Private blockhain. Documents de travail du Centre d’Economie de la Sorbonne 2017.20 ­ ISSN : 1955­611X. Apr. 2017. URL: https://halshs.archives-ouvertes.fr/halshs-01524440.

[18] Gupta, Suyash and Sadoghi, Mohammad. “Blockchain Transaction Processing”. In: (May 2018). DOI: 10.1007/978-3-319-63962-8\_333-1.

[19] Hennig­Thurau, Thorsten, Gwinner, Kevin P., Walsh, Gianfranco, and Gremler, Dwayne D. “Electronic word­of­mouth via consumer­opinion platforms: What motivates consumers to articulate themselves on the Internet?” In: Journal of Interactive Marketing 18.1 (2004), pp. 38–52. ISSN: 1094­9968. DOI: https: // doi. org/ 10 . 1002 / dir. 10073. URL: http://www.sciencedirect.com/ science/article/pii/S1094996804700961.

[20] How Instagram influencers turn followers into dollars. https://www.ft.com/ content/fc964254-155f-11e7-b0c1-37e417ee6c76. Accessed: 2020­12­17.

[21] IndaHash Official Website. https://indahash.com/. Accessed: 2020­05­16.

[22] IndaHash Whitepaper. https://s3.eu - central- 1 .amazonaws .com /idh- files/ico-landing/indahash\_whitepaper\_ico.pdf. Accessed: 2020­06­16.

[23] Kaulbars­Staudinger, Emilia. “Consumer online shopping behavior affected by influencer marketing ­ with a focus on sustainability”. In: (2019). URL: http:

//urn.fi/URN:NBN:fi:amk-2019052611960.

[24] Li Aiya Wei Xianhua, He Zhou. “Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems”. In: (Apr. 2020). DOI: https :

//doi.org/10.3390/su12072824.

[25] Lin, Iuon­Chang and Liao, Tzu­Chun. “A Survey of Blockchain Security Issues and Challenges”. In: I. J. Network Security 19 (2017), pp. 653–659.

[26] Luu, Loi, Chu, Duc­Hiep, Olickel, Hrishi, Saxena, Prateek, and Hobor, Aquinas. “Making Smart Contracts Smarter”. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. CCS ’16. Vienna, Austria: Association for Computing Machinery, 2016, pp. 254–269. ISBN: 9781450341394. DOI: 10.1145/2976749.2978309. URL: https://doi.org/

10.1145/2976749.2978309.

[27] McKinnon, A. “Carbon auditing the ”Last Mile”: Modelling the environmental impacts of conventional and online non­food shopping”. English. In: Proceedings of the 14th Annual Logistics Research Network Conference, Cardiff. Ed. by A Beresford. Annual Conference of the Logistics Research Network 2009 ; Conference date: 09­11­ 2009 Through 11­11­2009. 2009.

[28] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., and Qijun, C. “A review on consensus algorithm of blockchain”. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Oct. 2017, pp. 2567–2572. DOI: 10. 1109/SMC.2017.8123011.[29] Mohanty, Debajani. “Deploying Smart Contracts”. In: Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity. Berkeley, CA: Apress, 2018, pp. 105–138. ISBN: 978-1-4842-4075-5. DOI: 10.1007/978-1-

4842-4075-5\_4. URL: https://doi.org/10.1007/978-1-4842-4075-5\_4.

[30] Nakamoto, Satoshi. Bitcoin: A Peer­to­Peer Electronic Cash System. 2008. URL: https://bitcoin.org/bitcoin.pdf (visited on 02/27/2020).

[31] PATRON Whitepaper. https://patron-influencers.com/pdf/Whitepaper\_ 2019\_April\_Public\_compressed.pdf. Accessed: 2020-11-11.

[32] Ranga, Mamta and Sharma, Deepti. “INFLUENCER MARKETING- A MARKETING TOOL IN THE AGE OF SOCIAL MEDIA”. In: 2014.

[33] Raval, Siraj. Decentralized Applications. Harnessing Bitcoin’s Blockchain Technology. O’reilly Media, 2016. ISBN: 9781491924549.

[34] Remix ­ Ethereum IDE. URL: https : / / remix . ethereum . org/ (visited on 10/03/2020).

[35] Ropsten Testnet Explorer. URL: https://ropsten.etherscan.io/ (visited on 12/08/2020).

[36] Savelyev, Alexander. “Contract law 2.0: ‘Smart’ contracts as the beginning of the end of classic contract law”. In: Information & Communications Technology Law 26.2 (2017), pp. 116–134. DOI: 10.1080/13600834.2017.1301036. eprint: https://doi.org/10.1080/13600834.2017.1301036. URL: https://doi.org/ 10.1080/13600834.2017.1301036.

[37] Sharples, Mike and Domingue, John. “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward”. In: Adaptive and Adaptable Learning. Ed. by Katrien Verbert, Mike Sharples, and Tomaž Klobučar. Cham: Springer International Publishing, 2016, pp. 490–496. ISBN: 978-3-319-45153-4.

[38] Solidity. URL: https://solidity.readthedocs.io/en/v0.7.3/ (visited on 10/03/2020).

[39] Swan, Melanie. Blockchain: Blueprint For A New Economy. O’reilly Media, 2015. ISBN: 9781491920497.

[40] Szabo, Nick. “Smart Contracts”. In: Virtual School (1994).

[41] The Auth0 Authentication API. URL: https ://www .auth0 .com/ (visited on 12/07/2020).

[42] Vujičić, D., Jagodić, D., and Ranđić, S. “Blockchain technology, bitcoin, and Ethereum: A brief overview”. In: 2018 17th International Symposium INFOTEH­JAHORINA (INFOTEH). 2018, pp. 1–6.

[43] web3.js ­ Ethereum JavaScript API. URL: https://web3js.readthedocs.io/ en/v1.2.6/ (visited on 10/03/2020).

[44] WOMEN ARE THE NEW MEDIA. How influencers became publishers. https:

/ / labs . indahash . com / wp - content / uploads / 2017 / 06 / indaHash \_ LABS \_ report\_2017.pdf. Accessed: 2020-05-16.

[45] Yaga, Dylan, Mell, Peter, Roby, Nik, and Scarfone, Karen. “Blockchain technology overview”. In: (Oct. 2018). DOI: 10 . 6028 / nist . ir . 8202. URL: http://dx.doi.org/10.6028/NIST.IR.8202.

[46] Yang, R., Murray, T., Rimba, P., and Parampalli, U. “Empirically Analyzing Ethereum’s Gas Mechanism”. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW). 2019, pp. 310–319.

[47] ZHANG, YAKUN. “Product Returns in a Digital Era: The Role of Multidimensional Cognitive Dissonance, Regret, and Buying Context in the Post-purchase Appraisal Process”. In: (2018).

[48] Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”. In: 2017 IEEE International Congress on Big Data (BigData Congress). 2017, pp. 557–564. DOI: 10.1109/BigDataCongress.2017.85.

[49] Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, Chen, Weili, Chen, Xiangping, Weng, Jian, and Imran, Muhammad. “An overview on smart contracts: Challenges, advances and platforms”. In: Future Generation Computer Systems 105 (2020), pp. 475–491. ISSN: 0167-739X. DOI: https://doi.org/10.1016/

j. future. 2019 . 12 . 019. URL: http://www.sciencedirect.com/science/

article/pii/S0167739X19316280.

[50] Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, Chen, Xiangping, and Wang, Huaimin. “Blockchain challenges and opportunities: A survey”. In: International Journal of Web and Grid Services 14 (Oct. 2018), p. 352. DOI: 10.1504/IJWGS.2018.095647.

**Abstract**

Blockchain, a solution for different parties to reach consensus in a peer­to­peer (P2P) networks, allows us to distribute data across different entities. Many areas, including financial, health care, eCommerce, marketing, can benefit from blockchain technology. Influencer marketing also takes benefit from the properties of blockchain technology. Most of the time, social media influencers have an” ideal” body, affecting how the product they are advertising looks on them, which results in increased returns in online shopping. Moreover, existing applications are not involving micro­influencers (10,000 ­ 100,000 followers) in the campaigns that brands have created. In order to tackle the mentioned problems, a blockchain distributed size and fit application framework is proposed in this thesis. The framework offers a possibility for micro­ influencers to participate in the brands’ campaigns. However, micro­influencers are not directly involved in communication with brands. Instead, macro­influencers (over 100,000 followers) play a role as a bridge between micro­influencers and brands by creating sub­campaigns of the brands’ campaigns. With the involvement of micro­ influencers in the proposed framework, they also share their pictures with the same outfit (different body sizes and shapes), which gives potential buyers a better idea of how the same outfit would look on them before they decide to buy. The proposed solution is implemented with smart contracts using Solidity and tested in the Ropsten test network. Testing the smart contract in the Ropsten test network shows that the proposed solution is feasible in terms of financial costs. The proposed framework is not limited to giving the possibility to only brands to advertise products, but it also offers macro­influencers and potential micro­influencers an opportunity to earn a reward in exchange for promoting the products of brands. The whole process starting from applying for a campaign to claiming reward is handled without manual intervention.

Keywords

Blockchain, Smart Contract, Distributed application, Fashion

****

**Payam Noor University**

**Department of Computer Engineering and Information Technology**

**Seminar Report (M.Sc)**

Title:

**BlockChain Technologies in the World of Fashion**

**Supervisor:**

**Dr. Ali Razavi**

**By:**

**Mostafa zare**

**990133173**

Junary 2022

1. Block chain [↑](#footnote-ref-1)
2. Smart Contract [↑](#footnote-ref-2)
3. Distributed application [↑](#footnote-ref-3)
4. Fashion [↑](#footnote-ref-4)