

(لوگوی خواجه نصیر یا مدپا یا...)

پیشنهاد نامه سامانه مدیریت و اعتبارسنجی مالکیت فرش ها  
مبتی بر بلاکچین

(نام گروه)

دکتر سید حسین خواسته

حامد محمدی

رضا شکوری

شایان علی پور

مرداد 1397

اهداف

سامانه پیشنهادی متناسب با طرح مسئله صورت گرفته از جانب آقای سبحانی طراحی شده است. چالش مطرح شده در مورد مدیریت و تعیین مالکیت فرش ها می باشد. در این مسئله فرض شده است که فرش ها یکتا هستند و مشخص بودن مالک آن ها از اهمیت بسزایی برخوردار است. در این مسئله می بایست افراد بتوانند فرش های

جدید خود را ثبت و مالک آن را مشخص نمایند و قابلیت واگذاری آن را داشته باشند.

شرح سامانه

در ابتدا مواردی که برای ذخیره هر فرش در سیستم نیاز هست، شرح داده می شود.

برای هر فرش که قرار است در سیستم ثبت شود، فایل دیجیتالی از طرح آن فرش به همراه اطلاعات مربوط به تاریخ تولید، بارکد، مشخصات تولید کننده و.. تهیه می شود. پس از آن که مشخصات فرش ثبت شد، مالک آن می بایست رشته ای را تحت عنوان امضای خود وارد کند. داده های وارد شده طبق یکی از الگوریتم های رمزنگاری رمز می شوند و رشته ای یکتا را به وجود می آورند که منحصر به آن فرش می باشد.

عموما فرض می شود که از هر طرح، تنها یک فرش می باشد. اما ممکن است کارخانه ای صد فرش با طرح یکسان را تولید کرده باشد. مالکیت هر صد فرش تولید شده نیز اهمیت دارد چراکه توسط برترین طراح ها طراحی و با بهترین کیفیت و توسط کارخانه ای صاحب نام تولید شده است. در این صورت نیز بار کد هر یک از این فرش ها با وجود طرح و کارخانه یکسان، با یکدیگر متفاوت خواهد بود لذا عبارت رمز تولید شده همچنان یکتا خواهد بود. (جزئیات ساختار در آینده بررسی خواهد شد، در ابتدا صرفا مختصری از آن مطرح شد تا تصور ذهنی درستی شکل بگیرد)

اطلاعات مربوط به فرش هایی که برای اولین بار قرار است در سیستم ثبت شوند به صورت تراکنشی از جنس Genesis در شبکه ایجاد می شود. برای مدیریت سامانه، توکن های طراحی خواهد شد که مختص این کار می باشند. دو نوع رویکرد در مواجهه با نحوه ارزش گذاری و مدیریت توکن های تولیدی وجود دارد که عبارت است از:

1. ارزش توکن های ایجاد شده معادلی برابر پول فیات نداشته باشند.
2. توکن ها ارزشی معین در برابر پول فیات داشته باشند که توسط بازار و بر اساس عرضه و تقاضا تعیین می شود.

راهکار اول

در حالت اول می توان به سادگی به ازای هر **asset** که در اینجا می تواند فرش در نظر گرفته شود، یک توکن تخصیص داده شود. در حقیقت برخلاف **UTXO** در ساختار بلاکچین بیت کوین ما دارایی هایی معادل فرش را در نظر بگیریم. به این حالت به ازای هر نقل و انتقال فیزیکی **asset** معرفی شده مالکیت توکن معادل آن نیز به **wallet** فرد خریدار منتقل می شود. در این حالت در شبکه بلاکچینی ایجاد شده فقط سابقه نقل و انتقالات ذخیره می گردد و پرداخت بها با کمک ارز فیات و به صورت مجزا انجام می شود. در این حالت می توان سوالات و اشکالات زیر را وارد دانست که ادامه آن ها را بررسی می کنیم:

1. آیا می توان با این مکانیزم جلوی تقلب و فروش فرش غیر اصیل توسط صاحب فرش به دیگران را گرفت؟ پاسخ: در ابتدا باید در نظر بگیریم که اگر فرش مذکور یک فرش تاریخی و قیمتی است خریدار می تواند کارشناسانی را برای خود داشته باشد که به تایید اصالت مال پردازند اما با کمک مکانیزم ایجاد شده بر بستر بلاکچین نیز تا حد زیادی می توان مانع از رخدادهای این اتفاق شد. به این صورت که به محض انتقال یک فرش، مالکیت آن در شبکه بلاکچینی به طور امن به فرد دیگری منتقل شده و تمام اطلاعات در سیستم ذخیره می گردد. به این صورت حتی اگر فردی فرش تقلبی را به فرد دیگر منتقل کند، خود هرگز نمی تواند فرش اصل را به فروش برساند، چرا که مالک آن نیست و حق مالکیت برای فرد دیگری به ثبت رسیده است. بنابراین فرش اصل تا حدی ارزش نخواهد داشت و به کالایی غیر قابل انتقال تبدیل می گردد که این مانع از انجام چنین کاری می گردد.

2. با وجود این ساختار به استخراج کننده های (Miners) شبکه چه چیزی به عنوان کارمزد و پاداش پرداخت شود؟ پاسخ: اولین پاسخ آن است که از مکانیزم POS (Proof Of Stake) استفاده گردد لذا این افراد مانند POW (Proof of Work) به انجام کار محاسباتی نمی پردازند. در حقیقت با بهبود شبکه، دارایی های خود را ارزشمندتر می کنند، لذا نیازی به پرداخت فیه اضافی و پاداش به استخراج کننده ها نیست.

## راهکار دوم

در این حالت هر توکن شبکه معادل یک فرش در نظر گرفته نمی شود و ارزش معینی در برابر ارز های فیه دارد. این ارزش توسط بازار و بر اساس میزان عرضه و تقاضا تعیین می گردد. از طرفی ارزش خود فرش ها نیز مقدار معینی بر اساس پول فیه است. سیستم تعیین ارزش فرش ها به صورت مستقل (Autonomous) و خودکار عمل خواهد کرد.

در راهکار دوم، دو حالت تراکنش ممکن است انجام شود:

1. خرید و فروش توکن ها

2. خرید و فروش فرش ها

مورد اول: برای آن که کاربری بتواند از امکانات این سامانه استفاده کند، می بایست توکن این سامانه را خریداری کند لذا امکان خرید و فروش توکن ها فارغ از موجودیت فرش ها وجود دارد. به این معنی که مانند شبکه بیت کوین تراکنش هایی رخ دهد و در سیستم ذخیره شود.

مورد دوم: این حالت زمانی رخ می دهد که کاربری بخواهد فرشیه را خریداری کند. همان طور که اشاره شد، تنها با توکن های این شبکه امکان معامله وجود دارد، لذا در هر تراکنش بخش هایی مانند:

- آیا فرش نیز معامله می شود
- کد فرش
- مالک قبلی
- مالک بعدی
- ...

وجود دارد که در هنگام خرید و فروش فرش می بایست مقدار داشته باشند. مطابق این حالت، تمام سوابق خرید و فروش یک فرش در سیستم ذخیره می شود و قابل ردگیری می باشد. از طرفی سوابق تراکنش های مالی مرتبط با فرش ها نیز ذخیره می شود لذا این امر مانع کلاه برداری خواهد شد.

راه حل دیگری که می توان متصور شد که از دو راه حل قبل بسیار سریع تر و کم هزینه تر است آن است که برای این کار از شبکه اتریوم و قرارداد های هوشمند نوشته شده با **solidity** استفاده شود، به این صورت که توسط یک قرارداد هوشمند ما به ایجاد توکن های خاصی می پردازیم که این توکن ها اطلاعات فرش های مورد نظر را به صورت دیجیتالی در خود نهفته دارند حال برای انتقال مالکیت فرش ها به انتقال این توکن ها پرداخته می شود که این توکن ها در حقیقت در والت اتریوم شخص به صورت حفاظت شده قرار خواهند گرفت که امنیت این روش معادل امنیت شبکه اتریوم خواهد بود همچنین به یک **issuer** نیاز است که برای فرش های جدید توکن های متناسب آن را وارد شبکه کند و بعد از آن انتقال مالکیت فرش ها به صورت کاملاً دیجیتالی مبتنی بر شبکه اتریوم صورت خواهد پذیرفت، در این حالت از آنجا که به ازای هر فرش یک توکن در نظر گرفته می شود این توکن ها از ارزش ثابتی به ازای هر توکن نسبت به ارزش فیات ندارند پس خود خرید و فروش باید با ارزش فیات صورت بپذیرد همچنین برای افزایش امنیت نقل و انتقالات می توان انجام معاملات و پرداخت ها را منوط به پرداخت اتر یا دیگر توکن های شبکه اتریوم کرد به این حالت می توان در توکن های مالکیت فرش یک رکورد کامل از اطلاعات پرداخت ها را نیز داشت که باعث افزایش امنیت خواهد شد.