رشد باشکوه (Royal Grow)

مسئله‌ای که قرار است حل کنیم:
مشکل مقیاس پذیری و همچنین هزینه تراکنشها در بلاکچین اتریوم و بلاکچینهای مشابه که EVM را پشتیبانی میکنند، به خصوص برای پرداختهای بسیار کوچک. در حالی که این راه حل به خودی خود مفید فایده است، همچنان میتواند به عنوان زیرساخت برای ساخت سایر ابزارهای مالی هم به کار برود.

راه حل ما:
استفاده از قرارداد هوشمند به صورتی که فقط اثبات مالکیت دارایی(ها) بر روی بلاکچین ثبت میشود. در عین حال همه میتوانند بدون هزینه کردن درستی سند مالکیت خود را بر روی بلاکچین بررسی کنند و اگر مایل بودند (با پرداخت هزینه تراکنش) سکه‌های خود را از قرارداد خارج کرده و به حساب آنچین خود انتقال بدهند.

فرصت تجاری رشد طرح:
از آنجایی که این طرح یک زیر ساخت به صرفه، امن و قابل اتکا برای انتقال مبالغ خرد را بر بستر بلاکچین اتریوم (و بلاکچینهایی که EVM مشابه دارند) را فراهم میسازد، از این زیر ساخت میتوان برای ساختن سایر ابزارهای مالی (برای تمام سکه‌های ERC20) استفاده کرد. شاید مهمترین ابزار قابل ساخت همان صرافی باشد که مردم بتوانند با خیال راحت و به صورت خُرد کریپتوکارنسی بخرند و نگران کلاه‌برداری از طرف صرافی نباشند. البته که باقی ابزارهای مالی هم بر همین بستر قابل ساخت و توسعه هستند. از جمله انواع بریج‌ها، پلتفرم‌های وام‌دهی و استخرهای تامین نقدینگی تا طرحهای جمع‌سپاری و فروش اشتراک و میکرواشتراک تا DAO های کاربردی دیگر.

محصول ما چیست:
یک قرارداد هوشمند بر روی بلاکچین اتریوم که با وبسایت web3 و backend مناسب پشتیبانی شده و تجربه لذت بخشی از خرید و انتقال کریپتو را برای مردم فراهم میکند.

تیم ما:
فعلا فقط خودم هستم و این آدرس ریپوزیتوری دموی پروژه است.
https://github.com/estainit/royal-grow

رقبا و تفاوت ما با آنها:
ایده این طرح تقریبا همان ایده کانالهای پرداخت (در بیتکوین و اتریوم) است. با این تفاوت که در طرح ما امکان انتقال پول بین چندین نفر ایجاد میشود و نه فقط یک کانال بین دو نفر یا n کانال بین n زوج که بعدا مسیریابی بین آنها انجام بشود. کاری که بسیار غیر بهینه است و در نهایت هم یک جور بازی است تا یک مسیر پرداخت واقعی.
در طرح ما علاوه بر پیاده سازی زیرساخت میکروپیمنت، مشوقهای فراوانی هم برای درگیر کردن افراد در پروتکول، تامین نقدینگی، و حتی ایفای نقش اوراکل در نظر گرفته شده است که همه اینها با هم یک اکوسیستم پویا و رو به رشد فراهم میکنند.

تامین مالی و هزینه‌های پروژه:

مهمتر از تامین مالی پروژه، تشکیل شبکه‌ای از افراد حاضر در اکوسیستم رمزارز و تبلیغات برای محصول نهایی است. از این رو صرف نظر از هزینه‌های ایجاد و توسعه محصول (نوشتن قرارداد هوشمند و Audit و بازرسی‌های امنیتی آن، طراحی فرانت و بک و تستهای مربوطه) مهمترین هزینه مربوط خواهد شد به برندسازی و توضیح و تشریح محصول و جلب اطمینان مردم و البته متخصصان این حوزه در مورد امنیت سیستم و امن بودن دارایی‌های کاربران. پیشنهاد من برای محصول یک لیسانس اوپن سورس (ترجیحا GPL 3) است که کد هر سه قسمت فرانت و بک و قرارداد هوشمند برای همه قابل بازدید و بررسی و تغییر باشد. محل درآمد ما از مشتریان خودمان خواهد بود. در حالی که هرکسی میتواند از کد ما استفاده کند و یا آنرا بهبود بدهد و برای تجارت خود به کار بگیرد و حتی کل اکوسیستم را replicate کند. اما چون ارائه دهنده اولیه و اصلی ما بودیم، کپی‌ها شانس زیادی برای موفقیت ندارند.

روشهای کسب درآمد:

اصلی ترین منبع درآمد سیستم دریافت کارمزد انتقال وجه است. به اینصورت که مثلا مشتریِ یک تقاضای انتقال وجه به مشتریِ دو را دارد و از ما (به عنوان بنگاه) میخواهد که سند مالکیت وجه را برای مشتری دوم تولید کنیم (در حقیقت تعهدی بدهیم که مشتری با ارائه آن روی شبکه آنچین بتواند از قرارداد پول برداشت کند.) و همچنین مقدار طلب مشتری اول را هم کاهش بدهیم. ما برای انجام این عملیات مقداری اتر (با ارزش چند سنت) به عنوان کارمزد از فرستنده وجه طلب میکنیم.

درصدی از این درآمد به صندوق اوراکل فرستاده میشود و همزمان با انجام عملیات انتقال وجه از فرستنده میخواهیم که (در صورت تمایل) در فراهم کردن اطلاعات مهم (قیمت برابری ارزها، فلزات و همچنین سهام) ما را یاری برساند و در عوض شانس این را داشته باشد که از صندوق اوراکل مقداری اتر برنده شود.

عملیات قرعه کشی و تعیین برنده صندوق اوراکل دارای دو مرحله است. ابتدا انتخاب تعدادی از شرکت کنندگان به صورت تصادفی (الگوریتم رندوم قابل وریفای کردن که خودم نوشته ام و به آدرس https://github.com/estainit/verittery قابل دسترسی است)

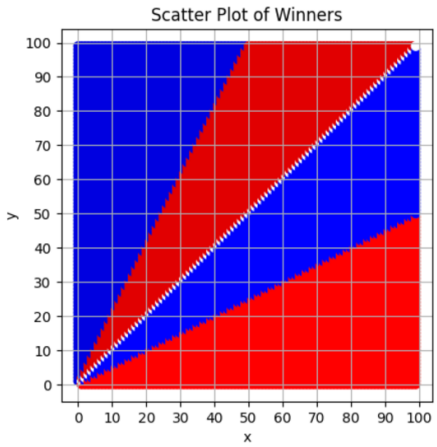
Verifiable Random winner Selection

1. Players X and Y each choose a number between 0 and very big number (e.g. 2 power 32) secretly and put it in an envelope and send it to the competition.
2. The envelopes are opened and the winner is determined as follows.

```
if X > Y:
  if X > Y * 2:
    X is winner
  else
    Y is winner

elseif Y > X :
  if Y > X * 2:
    Y is winner
  else
    X is winner

elseif X == Y
  do the new game
```



و در مرحله دوم مرتب کردن برنده‌ها بر اساس اطلاعات ارائه داده شده و در نهایت برگزیدن میانه اطلاعات و فرد ارائه دهنده آن به عنوان برنده است.

یکی دیگر از راه‌های درآمد سیستم گرفتن مالیات ثبت DCMR است. حالتی را در نظر بگیرید که ما تنها بنگاه موجود در قرارداد نیستیم و بنگاه‌های دیگر (دقیقا مانند ما) با گرفتن فیات و یا خدمات از افراد برای آنها سند مالکیت تعدادی سکه را صادر میکنند. این سندها با هم ترکیب شده و یک درخت مرکل تشکیل میدهند و ریشه درخت مرکل (DCMR) به طور مرتب (مثلا هر پنج دقیقه یکبار) بر روی بلاکچین ذخیره میشود (فقط هش ریشه درخت مرکل) و بابت این ذخیره سازی هر بنگاه موظف است مبلغی را به خزانه قرارداد واریز کند و این خزانه در دوره‌های منظم بین سهامداران پروژه تقسیم میشود.
برای اینکه سهامدار پروژه باشید باید مقداری اتر در قرارداد داشته باشید و یک هفته این مقدار دست نخورده بماند. با یک الگوریتم تنظیم سختی میتوانیم این مقدار را طوری محاسبه کنیم که در هر صورت هفته‌ای مثلا ۱۰۰ سهم جدید بیشتر تولید نشود. در ابتدای راه‌اندازی، بنگاه ما مثلا هزار سهم دارد و هر هفته ۱۰۰ سهم جدید تولید میشود و به سهم‌های موجود اضافه میشوند. حالا هر فردی که سهام سیستم را دارد متناسب با مقدار سهم خود از مالیات DCMR سهم میگیرد.
هر هویتی میتواند سهامدار باشد و لزومی ندارد که حتما یک بنگاه باشد.
این زیرسیستم و سهامداران داخل آن میتوانند برای DAO و دیگر امور حکمرانی قرارداد هم به کار گرفته شوند.

کمی جزئیات فنی:
ما دو عامل اساسی در سیستم داریم
Agent یا بنگاه: ما هستیم که زیر ساخت سیستم را فراهم کرده‌ایم.
Creditor یا مشتری: کاربران سیستم هستند که در ازای پرداخت پول فیات (یا انجام خدمات) از ما کریپتوکارنسی میخرند. مشتریها میتوانند کریپتو را بین خودشان هم انتقال بدهند.

همچنان این پیش‌فرضها و ملزومات باید در سیستم برقرار باشد.
- بنگاه نتواند به هیچ روشی سر مشتری‌ها کلاه بگذارد.
- مشتری هروقت که خواست بتواند سکه‌های خود را در سریعترین زمان ممکن از قرارداد خارج کند و به حساب خود منتقل کند.
- استفاده از سیستم برای مشتری باید آسان و سریع و به صرفه باشد.

دو عملیات اصلی سیستم شارژ اولیه حساب و انتقال وجه هستند.

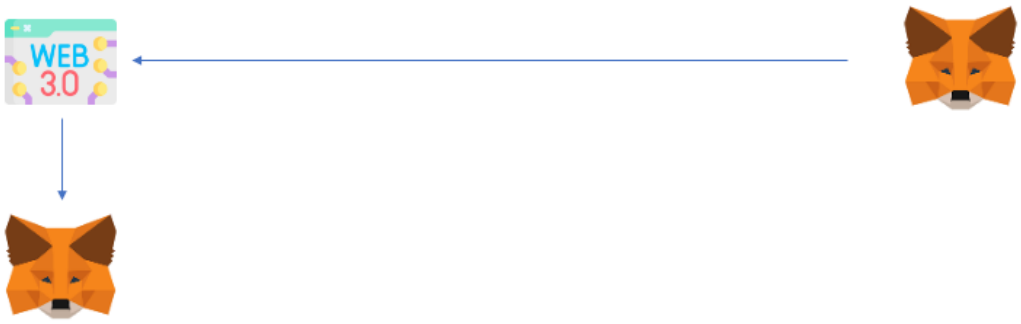
شارژ اولیه حساب

۱. کاربر کیف پول خود را به سایت ما وصل میکند و سپس مبلغی اتر را به آدرس قرارداد میفرستد.
۲. به محض پرداخت این مبلغ کاربر رسیدی را برروی وبسایت میبیند که میتواند آنرا کپی کرده و در جایی امن ذخیره کند و هر وقت که خواست پولش را از قرارداد پس بگیرد از این سند استفاده خواهد کرد. بدیهی است که در طی تراکنشهای بعدی بالانس مشتری تغییر خواهد کرد و به همین دلیل رسید

جدیدی به مشتری ارائه میشود و رسیدهای قبلی (با شماره سریال کمتر) باطل میشوند. سند ارائه شده چنین فرمتی خواهد داشت.

نکته: در حالت عادی (یعنی وقتی که بنگاه درستکار است) کاربر احتیاجی به این رسید ندارد و همیشه بر سکه‌های خود کنترل کامل دارد. این رسید فقط برای وقتی صادر میشود که بین بنگاه و مشتری اختلاف به وجود بیاید.

انتقال وجه



۱. کاربر از طریق کیف پول خود که به سایت ما وصل شده است درخواست انتقال توکن را امضا میکند و آنرا به بکند ما میفرستد.
۲. در بکند پس از انجام همه کنترلهای امنیتی ۲ رسید جدید میسازیم و در بانک اطلاعاتی ذخیره میکنیم. یک رسید آپدیت شده برای فرستنده و یک رسید جدید برای گیرنده و هر دو را به فرستنده ارائه میکنیم. حالا فرستنده با دیدن هر دو سند مطمئن میشود که انتقال به درستی انجام گرفته است. فرستنده میتواند سند دوم را مستقیما به گیرنده بدهد و یا اینکه از گیرنده بخواهد خودش (با آدرس ذکر شده در سند) به سایت ما وصل شده و سند را دانلود کند.

در ادامه لازم است کمی در مورد DCMR و شیوه نگهداری آن بر روی بلاکچین توضیح بدهم. همانطور که میدانیم یک بنگاه ممکن است میلیونها تراکنش آفچین انجام دهد و در نهایت وضعیت بالانس‌های تمام حسابها را به صورت یک درخت مرکل محاسبه کند و ریشه مرکل آن درخت را محاسبه کرده و آنچین ذخیره کند. این ریشه به انتهای یک آرایه دائمی که بر روی بلاکچین ذخیره میشود، push میشود و به این ترتیب ما همیشه سابقه‌ای از DCMR را بر روی بلاکچین داریم و این سابقه حذف نمیشود. از طرف دیگر مقادیر برگهای این درخت مرکل و اثباتهای آن هم به صورت شفاف و برای همه بر روی سایت قابل دسترسی است. بدین ترتیب هر کسی (هر مشتری‌ای) با دیدن رکورد مربوط به طلب خود و اثبات مربوطه میتواند از ذکر شدن طلب خود در سند DC مطمئن شود و از طرفی با جمع زدن جمع کل طلبها میتوانند مطمئن شوند که بنگاه خالی فروشی نکرده است. در حقیقت هر بنگاه میتواند تا ۹۵ درصد موجودی در قرارداد سند بدهی صادر کند و پنج درصد باقی

مانده همیشه به عنوان رزروی هست که اگر بنگاه سند جعلی درست کرد، اولین نفری که این تقلب را گزارش داد این ۵ درصد را به عنوان جایزه دریافت کند.
به طور کلی در چنین سیستمی مهمترین مساله این است که بنگاه نتواند تقلب کند. وگرنه مشتری (که برای هر نوع انتقالی وابسته به بنگاه است) کار زیادی نمیتواند انجام دهد. اگر بتوانیم جلوی تقلب بنگاه را بگیریم به صورت غیر مستقیم جلوی هک سیستم (هک‌های متداول صرافی‌ها که معمولا با لو رفتن کلیدهای خصوصی و یا کشف حفره‌هایی در عملیات پرداخت انجام میشوند) را هم گرفته‌ایم.
به این منظور امکان برداشت پول از قرارداد را به وجود «سند اثبات اعتبار» منحصر کرده‌ایم و فقط از این راه میتوان فاندهای داخل قرارداد را خارج کرد. حتی مدیریت بنگاه و Contract Owner هم نمیتواند هیچ پولی از قرارداد خارج کند!
ممکن است این سناریو به ذهن برسد که آیا صاحب بنگاه نمیتواند یک سند DCMR مخدوش را برروی بلاکچین ثبت کند که به موجب آن خودش بتواند همه منابع را بردارد؟ پاسخ این فرض بله است، اما شرایط تکمیلی‌ای وجود دارد که انجام این عمل را غیر ممکن میکند. به اینصورت که بعد از آپدیت کردن DCMR (که مثلا هر پنج دقیقه یکبار اتفاق می‌افتد) به مدت دو دقیقه برداشت از قرارداد قفل میشود و درخواستهای برداشت به یک صف انتظار فرستاده میشوند که بعد از رفع قفل به ترتیب رسید قابل برداشت شوند. اما در همین دو دقیقه اگر کسی ادعایی نسبت به DCMR جدید داشت و اینکه در این سند و اثباتهای همراهش طلب او ذکر نشده است، میتواند جلوی برداشت را به طور کلی سد کند تا وضعیت ادعای او بررسی شود. و در صورت درست بودن ادعای مشتری، آخرین DCMR از درجه اعتبار ساقط شده و یکی مانده به آخری (و قبلی تر ها) معتبر هستند.
اولین کسی که گزارش مخدوش بودن را ثبت کند همچنین جایزه‌ای بابت این اعلام دریافت میکند که این باعث میشود نه تنها مواظب فاندهای خود باشد بلکه یک تست سریع بر روی تمام فاندهای موجود بکند و یا حتی سرویسهایی را راه‌اندازی کند که با گرفتن وجهی از مشتریها، کار حفاظت از پولهای آنها را هم به عهده بگیرد.

نقاط ضعف:

بلی، وبسایت ما باید مانند یک وبسایت کلاسیک صد در صد مواقع عملیاتی و بالا باشد و خدمات ارائه بدهد و در این زمینه ادعایی مانند بیتکوین ندارد. ضمن اینکه تمام رمزارزها (به غیر از بیتکوین) به سایت طرف سومی وابسته هستند که خدمات اتصال به بلاکچین را فراهم میکنند و ادعای نامتمرکز بودن از طرف آنها فقط یک کلاه تبلیغاتی است.
بلی، سایت ما میتواند تراکنشها را سانسور کند و بعضی آدرسها را از خدمات دهی محروم کند، همچنان که در حال حاضر همه رمزارزها این محدودیت را دارند و فقط بیتکوین تا حدی از این قاعده مستثنی است.
بلی، این اپ کار زیادی در مورد افزایش حریم خصوصی کاربران انجام نمیدهد، اگرچه احتمال دارد در توسعه‌های آینده آن تکنولوژی‌های جدیدتری همچون اثبات دانش صفر آنرا بهبود بدهد.