**رشد باشکوه (Royal Growth)**

**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. همچنین حل مساله هک شدن (یا exit scam) در انواع محصولات مالی‌ای که به صورت حضانتی (custodial) هستند. 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 (و دیگران) را بر روی بلاکچین بررسی کنند و صاحبان دارایی 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 اتکای نیمه حضانتی را برای نگهداری و انتقال سکه‌ها بر بستر بلاکچین اتریوم (و بلاکچینهایی که EVM مشابه دارند) 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. یکی دیگر از کاربردهای این تکنولوژی استفاده از آن در IoT است. جایی که میلیونها چیز احتیاج دارند که بین خود میلیاردها تبادل و پرداخت خُرد در ثانیه انجام دهند.

**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 و عملیات مالی نامتمرکز 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 نگهداری و انتقال سکه‌ها، 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:**

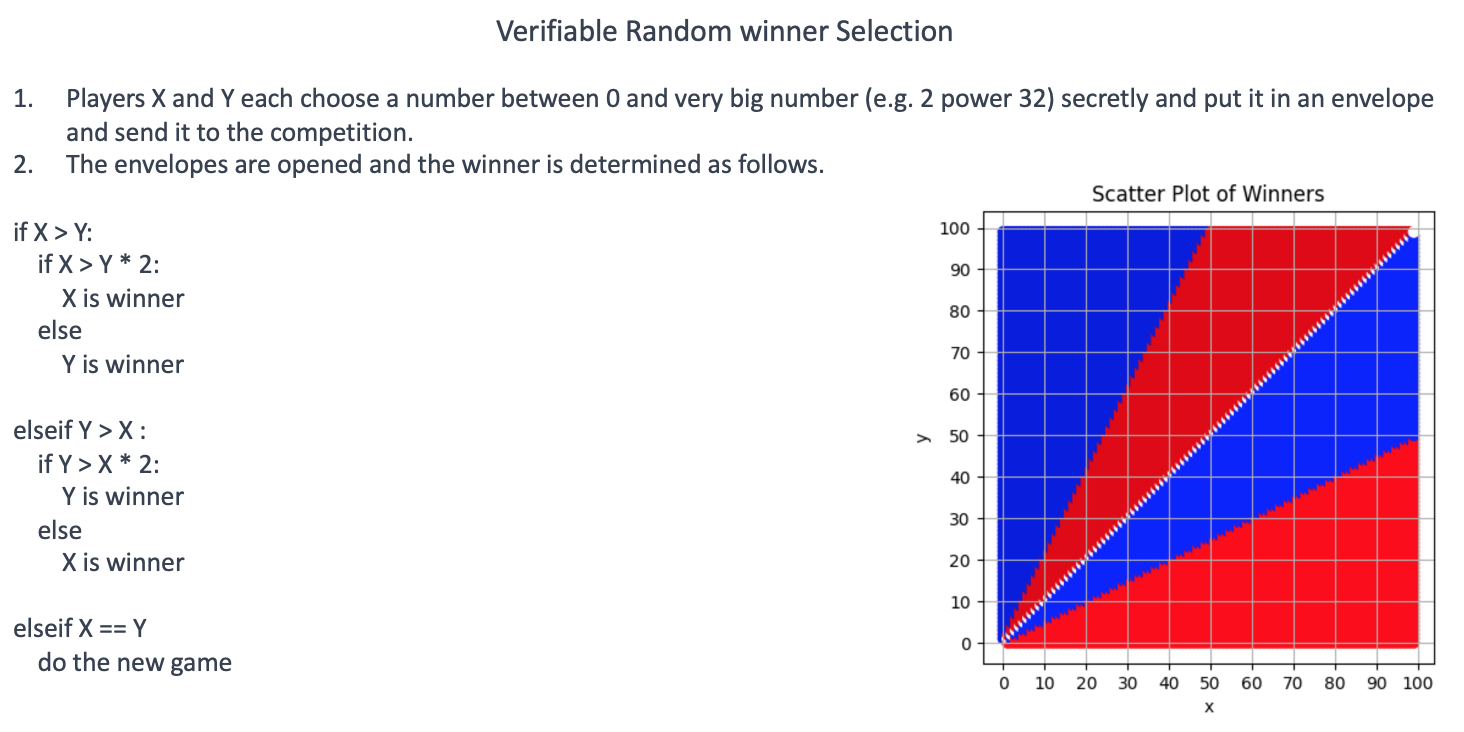
مهمتر از تامین مالی پروژه، تشکیل شبکه‌ای از افراد حاضر در اکوسیستم رمزارز و تبلیغات برای محصول نهایی است. از این رو صرف نظر از هزینه‌های ایجاد و توسعه محصول (نوشتن قرارداد هوشمند و Audit و بازرسی‌های امنیتی آن، طراحی فرانت و بک و تستهای مربوطه) مهمترین هزینه مربوط خواهد شد به برندسازی و توضیح و تشریح 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. در هر صورت چون ارائه دهنده اولیه و اصلی ما بودیم، و همچنین road map کاملی برای توسعه آن داریم، کپی‌ها شانس زیادی برای موفقیت ندارند.

**روشهای کسب درآمد:**

اصلی ترین منبع درآمد سیستم دریافت کارمزد انتقال وجه است. به اینصورت که مثلا مشتریِ شماره 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 بدون قید و شرط، از قرارداد پول برداشت کند و به حساب آنچین خود منتقل کند و یا به فرد دیگری در همین اکوسیستم انتقال بدهد.) 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 فرستنده‌ی وجه 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)



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.

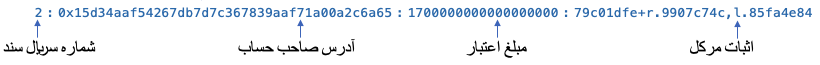
دو عملیات اصلی سیستم شارژ اولیه حساب و انتقال وجه هستند.

شارژ اولیه حساب



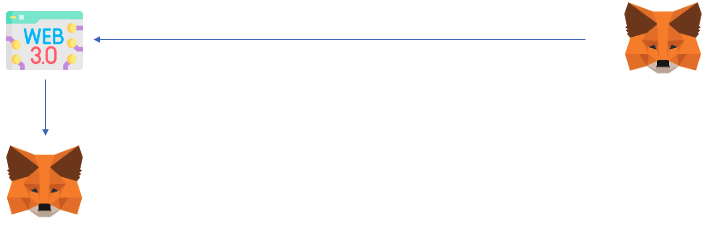
۱. کاربر کیف پول خود را به سایت ما وصل میکند و سپس مبلغی اتر را به آدرس قرارداد میفرستد.

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 Owner Contract 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 ترتیبِ 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 (و برای همه) 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.

* پیاده‌سازی کامل RG برای اتر و توکنهای ERC20
* صرافی نیمه حضانتی بر اساس order book فقط برای اتر و توکنهای erc20
* پیاده‌سازی وری‌تری و اوراکلهای قیمت و سیکلهای شرکت در لاتاری و اعلام برنده و ثبت آنچین مرکل روت اطلاعات
* استیبل کوین بر اساس over collatorizing RUSD, REURO, RIRL maker dao
* لندیگ و باروینگ
* استیکینگ
* توکن های رپ شده
* استخرهای تامین نقدینگی

به حمید

سلام، خوبی؟

آقا! اون پروژه من یادته که یکی دو ماه پیش باهم راجع بهش حرف زدیم؟ با یه سرمایه‌گذار ایرانی حرف زدم در موردش و اونم گفت که در صورتی که بتونم پرایوسی خیلی زیادی روش پیاده کنم حاضره سرمایه گذاری کنه. البته من به پرایوسی فکر کرده بودم و قصدم این بود تو آپگریدهای بعدی بهش اضافه کنم، اما با این پیشنهاد میشه road map محصول رو تغییر داد و پرایوسی رو زودتر بهش اضافه کرد. فعلا یه pitch deckبهشون دادم (اگه خواستی برای تو هم میفرستم) و منتظر جوابشون هستم. وقتی جواب دادن باهات مشورت میکنم در مورد zk-snark. فکر کنم هم کارِ مورد علاقه‌ات باشه و هم تخصصش رو داشته باشی.

اما از اونجایی که هدف من از پروژه بازارهای جهانی بوده، تصمیم گرفتم تا منتظر جواب اونا هستم یه تغییر رویکرد در پرزنتیشن پروژه هم بدم و چیزی که قبلا تو رده دوم اهمیت بوده رو بیارم و به عنوان فیچر مهم و اصلی محصول پرزنت کنم. و اون چیه؟

ایجاد زیرساخت نیمه حضانتی (semi custodial) برای نگهداری و همچنین انتقال و تبدیل اتر و تمامی توکنهای ERC20 بر روی شبکه اتریوم و تمام شبکه‌هایی که EVM رو ساپورت میکنن.

حالا این یعنی چی؟

اگه یادت باشه تو طرحم گفته بودم که تو این اکوسیستم ما دو تا عامل داریم. عامل اول agent یا بنگاهه که کارش دپلوی قرارداد و بعد از اون صادر کردن گواهی اعتباره و عامل دوم creditor یا مشتریها که با دادن پول و یا انجام کار و یا حتی انتقال اتر خودشون به قرارداد ما، در عوض یه گواهی میگیرن که با امضا کردن و فرستادن اون گواهی به بلاکچین اتریوم میتونن اتری رو که تو قرارداد وجود داره رو بردارن و به آدرس آنچین خودشون انتقال بدن. این گواهی هم چیزی نیست جز یه مرکل پروف. یه جورایی شبییه تورنادو‌کش با این تفاوت که همه چیز ترانسپرنته.

با این سیستم ما مشتریهایی داریم که هروقت بخوان میتونن پولهاشون رو (بلاشرط) از قرارداد بردارن و یا اینکه به بنگاه درخواست بدن و بگن که بخشی از پولشون رو به یه آدرس دیگه بفرسته و اینجوری به صورت آفلاین پول به همدیگه بفرستند.

بر بستر این سیستم میتونیم خیلی ابزارهای مالی جدید بسازیم که فعلا با یه صرافی central از نوع order book شروع میکنیم. فرق اصلی این صرافی با بقیه صرافی‌ها اینه که اینجا ما نمیتونیم exit scam بکنیم، و وقتیکه ما که خودمون صاحب بیزینس هستیم نتونیم سر مشتریهامون کلاه بذاریم، به صورت غیر مستقیم یعنی هک نمیشیم و کسانی از خارج از بنگاه هم نمیتونن اموال مشتریها رو بدزدند، که به نظرم فیچر خیلی خوبیه. البته اگه قصدمون از اول کلاه‌برداری نبوده باشه.

البته که هنوز بقیه راه‌های کلک زدن و کلاه‌برداری (مثلا Wash Trading، Pump-and-Dump و... ) بازه،

اما تمرکز ما روی جلوگیری از اگزیت اسکم در خدمات مالی نیمه حضانتیه. اینجوری هم از محاسن سیستم حضانتی استفاده میکنیم و هم اینکه معایب حضانتی رو نداریم.

خیلی طولانی شد، اما خلاصه داستان اینه که آیا تو که تو این فضا خیلی بیشتر از من هستی، آیا همچین سرویسی دیدی کسی ارائه بده؟ منظورم این مدل نیمه حضانتیه، اگر بله چه سرویسهایی؟

و اگر نه، به نظرت مارکت از همچین چیزی استقبال میکنه؟

شایدم نظرت این باشه که این فیچر نیمه‌حضانتی بودن خیلی به درد صرافی نمیخوره و بهتره مثلا تو یه استخر تامین نقدینگی استفاده بشه یا تو ...

مرسی که وقت گذاشتی و تا اینجا خوندی.

منتظر جوابت می‌مونم.

چه نوع عکس‌العملی میتونه بده؟

* اصلا جواب نده
* خیلی دیر جواب بده
* کلا قبول نکنه راه حل رو
* خیلی ایراد بگیره به این نیت که اول تسلیمم کنه، بعد اون شرایط رو خودش رو تحمیل کنه
* خوشش بیاد و با ذوق قبول بکنه

چه تاثیر بدی میتونه روی من، یا ایده و آینده پروژه بذاره؟

* تا همین الان من یه بار به اون رو انداختم و اون من رو ندید گرفته
* طرح قبلیم رویایی بوده و آنارکیک، بنابراین خیلی روی من حساب نمیکنه.
* اگه راجع به سرنوشت اون طرح پرسید چی بگم؟
* چقدر هزینه طرحه و چقدر زمان خواهد برد؟

به زنوبی

سلام آقای زنوبی، خوب هستید؟ من سعید غفاری هستم و سال ۲۰۲۱ یکبار به دفتر شما آمدم و در مورد یک پروژه کریپتویی با هم صحبت کردیم. نمیدانم یادتان هست یا نه!

در حال حاضر با چند تا از دوستان در حال طراحی یک محصول مالی/کریپتویی هستیم و خیلی ممنون میشوم اگر بتوانیم از تجربه شما استفاده بکنیم.

سعی میکنم در خلاصه‌ترین حالت ممکن پروژه را توضیح بدهم.

هدف پروژه: ایجاد امکان خرید رمزارز و کسب درآمد از آن به نیت مقابله با کم شدن ارزش پول ملی/فیات (در تمام دنیا و مخصوصا ایران) به مرور زمان و همچنین کسب درآمد از ارائه خدمات کریپتویی برای سرمایه‌گذاران بزرگ.

جمعیت هدف پروژه: افراد طبقه متوسط و یا پایینتر (از نظر درآمدی) و همچنین سرمایه‌گذاران بزرگ

ابزار انجام پروژه: ساخت محصول نرم‌افزاری مالی بر بستر بلاکچین اتریوم

مطمئن نیستم که به جزئیات فنی پروژه علاقه‌مند باشید برای همین به قسمت مالی آن میپردازم که هدف اصلی من از نوشتن این پیام برای شما بود و در انتها کمی اطلاعات فنی ضمیمه کرده‌ام که اگر علاقه داشتید بخوانید.

ایده اصلی:

یکی از کارهایی که افراد عادی برای حفظ ارزش پس‌انداز خود میکنند خرید رمزارز است. پس از آن این افراد سعی میکنند با ترید کردن سکه‌های خود را بیشتر کنند و البته معمولا هم سرمایه خود را از دست میدهند!

فکر کردم بهتر است روش دیگری را برای کمک به این افراد پیشنهاد بدهم. بنابراین سیستمی را طراحی کردم که مردم بتوانند به صورت بسیار به صرفه و اندک اندک کریپتوکارنسی (مشخصا اتریوم) بخرند و لازم نباشد پول زیادی را فقط برای انتقال سکه‌ها و به عنوان کارمزد شبکه بپردازند.

از طرفی این اترهای خریداری شده تحت کنترل خودشان بماند و در هر لحظه بتوانند (بلاشرط) آنرا به کیف‌پول خود منتقل کنند. همچنین بتوانند آن اترها را از طریق قراردادهای هوشمند وام بدهند و برای آن بهره دریافت کنند. به این صورت علاوه بر رشد ارزش اتریوم‌هایی که دارند (که معمولا در درازمدت اینگونه است) می‌توانند سرمایه خود را در داخلِ کار نگه دارند و ازین طریق هم سودی از آن ببرند.

از طرفی برای اینکه این سیستم کاربردی‌تر باشد، زیرسیستمی را هم به آن اضافه کردیم که به واسطه آن، افراد با قراردادن اترهای خود در قرارداد بتوانند استیبل کوین ریال منتشر کنند و به این وسیله افراد بیشتری بتوانند بدون نگرانی از نوسان قیمت، از رمزارز ریال و در معاملات ریز و درشت روزانه‌شان استفاده کنند. با این روش منتشر کننده ریال میتواند تا دو سوم ارزش اترِ قفل شده‌ی خود ریال دیجیتال تولید کند و آنرا به چرخه وارد کند. و این ریال دیجیتال را خرج بکند و یا وام بدهد و یا از آن برای خرید اترِ بیشتر استفاده کند.

از آن طرف افرادی که سرمایه‌های بزرگی دارند میتوانند با استفاده از این سیستم رمزارز ریال منتشر کنند و آنرا وام بدهند. همچنین از آنجایی که لیسانس نرم‌افزار اوپن سورس خواهد بود، این سرمایه‌داران میتوانند با راه انداختن نود خود و با دادن خدمات مالی به مردم، از راه دریافت کارمزد خدمات هم درآمد جدیدی برای خود ایجاد کنند.

ممنون که تا اینجا خواندید. حالا سوالات من از شما اینها است و ممنون می‌شوم با توجه به تجربه خود در بازارهای مالی و به خصوص بازار ایران به آنها جواب بدهید یا اگر ترجیح میدهید در مورد آنها صحبت کنیم، بفرمایید تا با هم هماهنگ کنیم برای یک جلسه تماس صوتی یا تصویری.

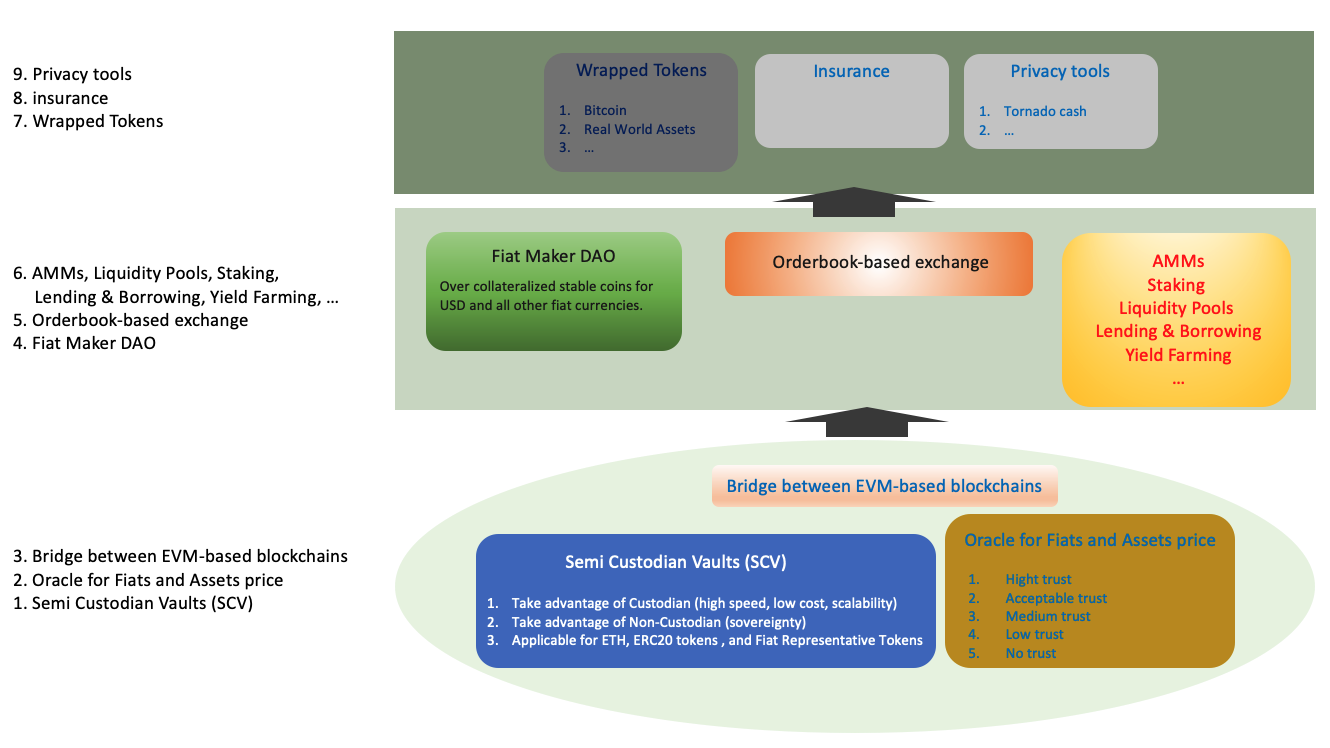
۱. آیا از نظر ذهنی و طرز فکر مردم (مخصوصا ایران و کلا کشورهایی که تورم بالا دارند) چنین طرحی مورد استقبال قرار خواهد گرفت؟

۲. اگر به نظر شما طرح خوبی است اما لازم است قسمتهایی به آن اضافه بشود یا قسمتهایی حذف بشود، آن ملاحظات چیست؟

۳. اگر به نظر شما این طرح اصلا ایده خوبی نیست اما در عوض میتوان فلان طرح اقتصادی را بر بستر این محصول تکنولوژیکی اجرا کرد، بفرمایید. زیرا من هم به تکنولوژی این محصول علاقه دارم (زیرا یک راه حل برای افزایش مقیاس و کاهش هزینه در بلاکچین اتریوم است) و هم مشتاق هستم از آن در دنیای واقعی و محصولی واقعی استفاده بکنم.

کمی اطلاعات فنی‌تر در مورد ویژگیهای این محصول مالی:

برای جلوگیری از طولانی شدن معرفی محصول از توضیح جزییات تکنیکی پرهیز میکنم.



۱. مهمترین ویژگی محصول ما استفاده از محاسن هر دو روش حضانتی و غیر حضانتی و همچنین پرهیز از معایب این دو برای نگهداری و انتقال رمزارزها است. (شکل ۱ بخش ۱)

۲. یکی دیگر از ویژگیهای این محصول پیاده سازی تابع سروش (Orcale) برای انتقال اطلاعات دنیای واقعی به دنیای بلاکچین است. با داشتن این امکان میتوانیم نرخ تبدیل به دلار به هر پول ملی را به صورت ساعتی و بر روی بلاکچین اتریوم دسترس پذیر کنیم. (شکل ۱ بخش ۲)

این اطلاعات به عنوان پایه محصولات بعدی به کار خواهد رفت.

۴. یکی از مهمترین اهداف این پروژه ایجاد امکان انتشار Stable-coin هایی برای پولهای ملی کشورهای مختلف (از جمله ریال) است. در حقیقت با داشتن تابع سروشِ قیمتهایِ ارزهایِ ملی، باقی کار چیز سختی نیست. زیرا همین حالا هم پروتکول Maker DAO این امکان را برای دلار آمریکا فراهم آورده است. البته ما میتوانیم این پروتکول را با توجه به زیرساخت نیمه حضانتی و امکانات ویژه‌ی آن، بهینه کنیم، به طوری که استفاده از آن سریعتر و کم خرج‌تر از معاملات آنچین در Maker DAO کلاسیک باشد.

۵. یکی از بدیهی‌ترین کسب و کارهای مربوط به کریپتو صرافی‌ها هستند که ما میتوانیم بر بستر تکنولوژی ها و ابزارهای فراهم شده آنرا بسازیم.

۶. از دیگر محصولات قابل توسعه بر این بستر نرم‌افزاری، همچنین بازار سازها، استخرهای نقدینگی، وام‌دهی و ... هستند. در این لحظه امکان وام دهی مهمترین ویژگی‌ای است که من دنبال آن هستم. تصور کنید شما اتریوم خود را (که ارزش آن تقریبا همیشه رشد میکند) در قرارداد Maker میگذارید و با آن رمزارزِ ریال منتشر میکنید. حالا میتوانید ریال خود را در استخر نقدینگی گذاشته و آنرا وام بدهید و بابت آن سود دریافت کنید.

موارد دیگر را برای جلوگیری از طولانی شدن توضیح نمیدهم. فقط این نکته را یادآوری میکنم که شکل ۱ به نوعی Road Map پروژه هم هست و به صورت تقریبی ترتیب توسعه ماژولهای مختلف را در طول سالهای آتی نشان میدهد.

با سپاس

سعید غفاری

EPF

سلام، اینجا میخوام نشون بدم که در یک سیستم DAG که تو اون CAP تئوری رو کاستومایز کردیم چه جوری مشکل دو خرجی رو حل میکنیم. اول باید یه کم در مورد کپ تئوری براتون توضیح بدم. این تئوری میگه که تو یه سیستمی که احتمال داره پارتیشن بشه (یعنی بخشی از اون ارتباطش رو با یه بخش دیگه‌ای از دست بده، مثلا شبکه قطع بشه و شبکه به دو قسمت ایزوله تقسیم بشه) ما نمیتونیم همزمان consistency و availability رو با هم داشته باشیم. یعنی چی؟ فرض کنید ما یک بانک داریم که این بانک فقط دو تا دستگاه ATM داره که از هم دور هستند و با اینترنت به هم وصل هستند. این بانک یه مشتری داره که ۱۰۰ دلار پول تو حسابش داره و میخواد که بره از دستگاه A پولش رو برداره. فرض کنید پیش از برداشت پول اینترنت قطع بشه! حالا ما باید چه کنیم؟ دستگاه آ میدونه که تا پیش از قطع شدن اتصال مشتری ۱۰۰ دلار پول تو حسابش داشته، اما الان مطمئن نیست که مشتری پولش رو از طریق دستگاه ب برنداشته باشه! و مهمتر از اون، بعد از برداشت مشتری نمیتونه بالانس مشتری رو به روز کنه!

ما دو تا انتخاب میتونیم بکنیم. یا Constantcyرو انتخاب کنیم و به مشتری بگیم تا زمان اتصال مجدد شبکه و به روزرسانی اطلاعات مشتری‌ها نمیتونیم به شما پولی بدیم، که خوب امنه، اما تجربه کاربری بدی داره و یا اینکه Availability رو انتخاب کنیم و برای جلب رضایت مشتری بهش اجازه بدیم که صد دلارش رو برداره و اینجوری از consistency صرف نظر کردیم.

بگذریم، ما تو سیستمی که طراحی کردیم کپ رو سفارشی کردیم و گفتیم که دیدن موجودی حساب همیشه avilableاست ولی برای انتقال پول باید ۱۲ ساعت از واریز اون پول زمان گذشته باشه.

حالا نمودار رو نگاه کنید!

در قسمت یک دیده میشه که شبکه ما سه نود ا ب سی داره و همه بلاک جنسیس رو دارند.

در قسمت دوم میبینید که نود الف بلاک یک را تولید کرده و اون رو به نود ب هم میفرسته.

در قسمت ۳ میبینید که نود ب بعد از اعتبارسنجی و تایید بلاک یک اونرو به نود س میفرسته.

در قسمت ۴ میبینیم که نود آ بلاک دو و نود ب بلاک ۳ رو تولید کرده

و به همین ترتیب در قسمتهای ۵ و ۶ میبینیم که نودها بلاکها رو به همدیگه میدن و در حالت ۷ هر ۳ تا نود ۳ تا بلاک ۱، ۲ و ۳ را در حافظه لوکال خودشون دارند.

توجه کنید که ما همه بلاکهای معتبر رو قبول کردیم. در اینجا حتی بلاکهای دارای دوخرجی هم فعلا معتبر حساب میشوند.

Hello, here I want to show how to solve the double spending problem in an asynchronous DAG data structure, where we customized the CAP theorem.

First, I have to explain a little about cap theory.

This theory says that in a system that is likely to be partitioned (means, a part of it will lose its connection with another part, for example, the network will be disconnected and the system will be divided into two isolated parts), we cannot have **consistency** and **availability** at the same time.

What does it mean? Suppose we have a bank that has only two ATM machines that are far from each other and are connected through the Internet.

This bank has a customer who has 100 dollars in his account and wants to withdraw money from ATM A.

Suppose the internet is cut off before withdrawing the money! What should we do now?

ATM A knows that before the internet connection goes down, the client had $100 in his account, but now he is not sure that the client did not withdraw his money through ATM B!

And more importantly, after withdrawing, the ATM A cannot update the customer's balance!

What should we do?

We can make two choices. Either choose "Constancy" and tell the customer that we can't pay you until the network is reconnected and the customer information is updated, which is good and secure, but it has a bad user experience,

or we can choose "Availability" and allow withdraw to satisfy the customer. He took his dollar and thus we gave up on "Consistency"!

Anyway, in the system we designed, we customized the CAP theorem and said that it is always available to see the account balance, but to transfer coins, 12 hours must have passed since the deposit of that coins.

Now look at the chart!

In part one, it can be seen that our network has three A,B, and C nodes and they all have the Genesis block.

In the second part, you can see that node A produces block 1 and sends it to other nodes.

In part 3, you can see that node B after validating and confirming

block 1 sends it to node C as well.

In part 4, we see that node A produced block 2 and node B produced block 3

And in the same way, in parts 5 and 6, we see that nodes share blocks with each other, and in part 7, every 3 nodes have blocks 1, 2, and 3 in their local memory.

Note that we accepted all valid blocks. Here, even the blocks with double-spending are considered valid for now.

بلاک یا نه؟

چرا باید افراد متنوعی را دنبال کرد و باهاشون تعامل داشت؟

اینکه چی میگه به تنهایی مهم نیست، بلکه چه کسی میگه هم مهمه! و اینکه اینطور نیست که یه گفته همیشه و همه جا

درست باشه.

I am Toufic Abou Assali from Assali Advertising & Marketing company.  
  
We are expanding our business into the blockchain and cryptocurrency fields. There are many products that need to combine web3 and blockchain technology.(e.g. e-sports apps to turn it into p2e by adding a crypto token.)  
We are seeking a highly skilled and experienced Blockchain Developer to join our innovative team. This role is ideal for someone passionate about decentralization, blockchain technology, and the future of the internet. Our ideal candidate will have a solid foundation in solidity, rust and web 3.0 languages, a background in working with big tech companies, or an academic background from top-tier schools.  
  
Key Responsibilities  
- Design, develop, integrate and deploy decentralized applications (DApps) on various blockchain platforms.  
- Work closely with cross-functional teams to develop high-quality, secure, and scalable web 3.0 applications.  
- Stay up-to-date with the latest trends, technologies, and best practices in the blockchain and web 3.0 space.  
  
Benefits  
- Competitive salary and benefits package.  
- Dynamic and supportive work environment.  
- Opportunities for professional growth and development.  
- Engage in projects that have a real-world impact.  
  
Job Type: Full-time or part-time, remote work  
Pay: $140,000.00 - $210,000.00 per year or $70/hr ~ $120/hr for part-time position  
  
How to be hired  
- Submit your resume, cover letter, and portfolio of relevant projects.  
- Test your blockchain skills for about 10 ~ 15 minutes.  
- Pass technical interview with CTO.  
  
Please reply by uploading your resume and github and then we will immediately begin the interview process with a skill test.  
  
(It could be a part time job just in case that you have a full time job and paid hourly or project by project. Or you can introduce an experienced team or developers for this position. We would pay you for that. )

من توفیک ابو عسلی از شرکت تبلیغاتی و بازاریابی عسلی هستم.

ما در حال گسترش کسب و کار خود در زمینه های بلاک چین و ارزهای دیجیتال هستیم. محصولات زیادی وجود دارند که نیاز به ترکیب فناوری وب 3 و بلاک چین دارند. (مثلاً برنامه های ورزش الکترونیکی برای تبدیل آن به p2e با افزودن یک رمز ارز).

ما به دنبال یک توسعه دهنده بلاک چین بسیار ماهر و با تجربه هستیم تا به تیم نوآور ما بپیوندد. این نقش برای افرادی که علاقه زیادی به تمرکززدایی، فناوری بلاک چین و آینده اینترنت دارند ایده آل است. کاندیدای ایده‌آل ما پایه محکمی در زبان‌های استحکام، زنگ زدگی و وب 3.0، سابقه کار با شرکت‌های بزرگ فناوری، یا پیش‌زمینه آکادمیک از مدارس سطح بالا خواهد داشت.

مسئولیت های کلیدی

- طراحی، توسعه، ادغام و استقرار برنامه های غیرمتمرکز (DApps) در پلتفرم های مختلف بلاک چین.

- برای توسعه برنامه های کاربردی وب 3.0 با کیفیت بالا، ایمن و مقیاس پذیر با تیم های متقابل کار کنید.

- با آخرین روندها، فناوری ها و بهترین شیوه ها در بلاک چین و فضای وب 3.0 به روز باشید.

فواید

- بسته حقوق و مزایا رقابتی.

- محیط کاری پویا و حمایتی.

- فرصت های رشد و توسعه حرفه ای.

- در پروژه هایی شرکت کنید که تأثیری در دنیای واقعی دارند.

نوع شغل: تمام وقت یا پاره وقت، کار از راه دور

پرداخت: 140,000 دلار - 210,000 دلار در سال یا 70 دلار در ساعت تا 120 دلار در ساعت برای موقعیت پاره وقت

نحوه استخدام

- رزومه، نامه پوششی و نمونه کارهای پروژه های مربوطه خود را ارسال کنید.

- مهارت های بلاک چین خود را برای حدود 10 تا 15 دقیقه آزمایش کنید.

- قبولی در مصاحبه فنی با CTO.

لطفا با آپلود رزومه و github پاسخ دهید و سپس ما بلافاصله فرآیند مصاحبه را با یک آزمون مهارت آغاز خواهیم کرد.

(این می تواند یک شغل پاره وقت باشد فقط در صورتی که شما یک کار تمام وقت دارید و به صورت ساعتی یا پروژه ای با حقوق پرداخت می کنید. یا می توانید یک تیم یا توسعه دهندگان با تجربه را برای این موقعیت معرفی کنید. ما برای آن به شما پول می دهیم.)

سلام حمید، خوبی؟

آقا اون پروژه من (مقیاس‌پذیری پرداختهای خُرد در اتریوم) داره به جاهای خوبی میرسه و به احتمال زیاد بتونم تو این مرحله یه سرمایه‌گذار از داخل ایران بگیرم.

به کمکت برای مشاوره (و اگر بتونی کد بزنی برای کد زدن هم) حرفه‌ای احتیاج دارم. فعلا راجع به مشاوره صحبت کنیم چون خودت قبلا اعلام آمادگی کرده بودی. لطفا بگو به عنوان مشاور چند ساعت در هفته میتونی به این پروژه اختصاص بدی؟ شما ماکسیمم دسترس پذیری هفتگیت رو اعلام کن، احتمالا همیشه به صورت ماکسیمم نباید باشی. و اینکه بابت هر ساعت مشاوره چقدر دستمزد خوبه؟ شاید هم در کل مدل دیگه‌ای برای همکاری رو ترجیح میدی که خوشحال میشم بشنوم. منتظر جوابت می‌مونم.

سلام مجدد

در مورد شرایط کار کردن فرموده بودین نظرم رو بگم.

اول اینکه همونطور که گفتم من رو از خودتون و متعلق به اونور میز بدونید.

به نظر من دو تا از مهمترین مواردی که میتونیم برای شروع بهش فکر کنیم نسبت تقسیم سهام (توکنهای حکمرانی) پروژه و حقوق دریافتی است. با توجه به اینکه من یکی از هم‌بنیان‌گذاران پروژه و همچنین یکی از اصلی‌ترین توسعه‌دهنده‌های اون هستم (و خواهم بود) شاید دریافت ۴۰ درصد از سهام به علاوه حقوق متعارف برای یک مدیر پروژه در ایران(که مدیرفنی و دولوپر هم هست) اعداد مناسبی برای شروع مذاکره باشند.

از طرفی چون هنوز راجع به جزييات اجرای پروژه (اینکه کدوم قسمتها از کل پروژه تو این مرحله انجام بشه) هیچ تصمیمی نگرفتیم نمیتونیم برآوردی حدودی از میزان سرمایه مورد نیاز و همچنین زمان مورد نیاز برای انجام این مرحله از توسعه انجام بدیم.

این رودمپی است که فعلا وجود داره.

اگر ما تمرکزمون روی دو مورد

**2.** Oracle for Fiats and Assets price

**1.** Semi Custodian Vaults (SCV)

باشه من میتونم به طور تقریبی عدد ۵ توسعه دهنده (به جز خودم) در زمان سه ماه رو به عنوان نیاز حداقلی پروژه اعلام کنم. البته که من فقط قسمت فنی اون رو گفتم و مواردی از قبیل نیروی انسانی در بخش مارکتینگ و تولید محتوا و ... و یا هزینه‌های عمومی مثل اجاره محل شرکت وهزینه‌ها سرور و زیرساخت و یا هزینه‌های جانبی رو نیاوردم. همچنین ممکنه که درصدی از سهام رو به توسعه‌دهندگان اولیه بدیم که باید در مورد اون هم توافق کنیم.

البته که باید در باره این موارد گفته شده و موارد دیگری همچون تصمیم گیری در مورد road map پروژه و تعریف پیروزی و یا شکست در هر مرحله از پروژه و اینکه در صورت بروز هرکدام (پیروزی یا شکست) چه کاری باید انجام بدیم و... صحبت کنیم.

از طرفی هم این تحقیقات بازار که فرمودین در حال اجراست هم کمک زیادی خواهد کرد برای تصمیم‌گیری در مورد مسیر توسعه پروژه و من منتظر اون جلسه مشترک با این دوستان هم هستم.

اینها مختصری از چیزهایی بود که باید در موردش به توافق برسیم.

منتظر جواب شما می‌مونم..

سلام آقای نقی‌پورفر،

مدت زیادیه که از هم بیخبر بودیم. امیدوارم حالتون خوب بوده باشه.

تو این مدت من یه ربات تلگرامی نوشتم که بر پایه پروژه‌ای که قبلتر در موردش صحبت کرده بودیم (همون پروژه مقیاس‌پذیری در پرداختهای خرد بر بستر اتریوم RG ) کار میکنه. ایده ربات کرپتافه (کریپتو برای کافه) اینه که کاربر با انجام وظائف روزانه و یاد گرفتن و جواب دادن به سوالات مقداری توکن کریپتافه جمع میکنه و در پایان ۱۸۰ روز مشارکت و انجام چالشهای روزانه، توکنهای همه کاربرها (به علاوه ایردراپ احتمالی) به بلاکچین اتریوم منتقل میشه و اونجا میتونن توکنهاشون رو تو صرافی‌ها بفروشن و یا با استفاده از ابزارهای مالی‌ای که بر بستر زیرساخت RG ساخته شده کارهای DeFi انجام بدن. بات فعلا ۶ زبان فارسی، انگلیسی، ایتالیایی، ترکی، عربی و اسپانیایی رو ساپورت میکنه و مخاطبش تازه‌واردهای به عرصه کریپتوکارنسی‌ها هستند که دوست دارند رمزارزی داشته باشند که بعدا با ارزش بشه و در عین حال میترسن پول خرج کنن و کریپتو بخرن.

این پروژه یکی از ده‌ها کاربرد RG است و علاوه بر این میتونیم این زیرساخت رو برای هرجایی که احتیاج به پرداخت خُرد و بر پایه پول‌های فیات داره استفاده کنیم. مثلا IoT یکی از اون جاهاست که من آینده خیلی خوبی رو برای RG میبینم.

من لینک استفاده از بات رو برای شما میفرستم. بعد از عضویت شما اون رو طوری تنظیم میکنم که لازم نباشه برای انجام هرچالش ۲۴ ساعت صبرکنید و در عوض هر پنج دقیقه یکبار بتونید چالشهای روزانه را انجام بدید. اینجوری سریعتر با محصول و سیر پرسشها و آموزشهای آن آشنا میشید. لازمه که یادآوری کنم محصول کریپتافه بیانگر نظرات و ایده‌ال‌های منه و الزامی نداره که نسخه تجاری اون صد در صد همینی باشه که من دوست دارم یا دقیقا همین راه رو بره و همین هدفها رو داشته باشه. هرچند که اگر اینطور بشه من خوشحال‌تر خواهم بود.

ارادتمند

<https://t.me/cryptafeBot?start=rlqrcs7959>

اگر لینک کار نکرد کافیه که این ربات رو تو تلگرام جستجو کنید. cryptafeBot

سلام آقای زنوبی،

مدت زیادیه که از هم بیخبر بودیم. امیدوارم حالتون خوب بوده باشه.

تو این مدت من یه ربات تلگرامی نوشتم که بر پایه پروژه‌ای که قبلتر در موردش پیغام داده بود (همون پروژه مقیاس‌پذیری در پرداختهای خرد بر بستر اتریوم RG ) کار میکنه. و اینکه بر خلاف نظر شما مبنی بر نرفتن به سمت ارزهای ملی و فیات، اتفاقا روی اون تمرکز کردم. حالا توضیح میدم چرا.

ایده ربات کرپتافه (کریپتو برای کافه) اینه که کاربر با انجام وظائف روزانه و یاد گرفتن و جواب دادن به سوالات مقداری توکن کریپتافه جمع میکنه و در پایان ۱۸۰ روز مشارکت و انجام چالشهای روزانه، توکنهای همه کاربرها (به علاوه ایردراپ احتمالی) به بلاکچین اتریوم منتقل میشه و اونجا میتونن توکنهاشون رو تو صرافی‌ها بفروشن و یا با استفاده از ابزارهای مالی‌ای که بر بستر زیرساخت RG ساخته شده کارهای DeFi انجام بدن. بات فعلا ۶ زبان فارسی، انگلیسی، ایتالیایی، ترکی، عربی و اسپانیایی رو ساپورت میکنه و مخاطبش تازه‌واردهای به عرصه کریپتوکارنسی‌ها هستند که دوست دارند رمزارزی داشته باشند که بعدا با ارزش بشه و در عین حال میترسن پول خرج کنن و کریپتو بخرن.

این پروژه یکی از ده‌ها کاربرد RG است (که قبلا توضیح دادم) و علاوه بر این میتونیم این زیرساخت رو برای هرجایی که احتیاج به پرداخت خُرد و بر پایه پول‌های فیات داره استفاده کنیم. مثلا IoT یکی از اون جاهاست که من آینده خیلی خوبی رو برای RG میبینم.

من لینک استفاده از بات رو برای شما میفرستم. بعد از عضویت شما اون رو طوری تنظیم میکنم که لازم نباشه برای انجام هرچالش ۲۴ ساعت صبرکنید و در عوض هر پنج دقیقه یکبار بتونید چالشهای روزانه را انجام بدید. اینجوری سریعتر با محصول و سیر پرسشها و آموزشهای آن آشنا میشید. لازمه که یادآوری کنم محصول کریپتافه بیانگر نظرات و ایده‌ال‌های منه و الزامی نداره که نسخه تجاری اون صد در صد همینی باشه که من دوست دارم یا دقیقا همین راه رو بره و همین هدفها رو داشته باشه. هرچند که اگر اینطور بشه من خوشحال‌تر خواهم بود.

<https://t.me/cryptafeBot?start=i006456b1ae>

اگر لینک کار نکرد کافیه که این ربات رو تو تلگرام جستجو کنید. cryptafeBot

خوشحال میشم ازش استفاده کنی و بتونیم یه جوری ازش یه محصول تجاری بسازیم. مخصوصا الان که به نظر میاد در ابتدای یه بولران دیگه هستیم.

ارادتمند