

سرمایه‌گذاری غیرمستقیم شفاف در عصر دیجیتال براساس فناوری بلاک‌چین

محمد امین فضلی^{۱*} مهدی نقوی^۱ فرزانه مردوخ روحانی^۲

*نویسنده مسئول، دریافت: ۱۴۰۰/۰۶/۱۴، بازنگری: - ، پذیرش: ۱۴۰۰/۰۸/۱۲

^۱دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

^۲دانشکده مدیریت و اقتصاد، دانشگاه صنعتی شریف، تهران، ایران

چکیده

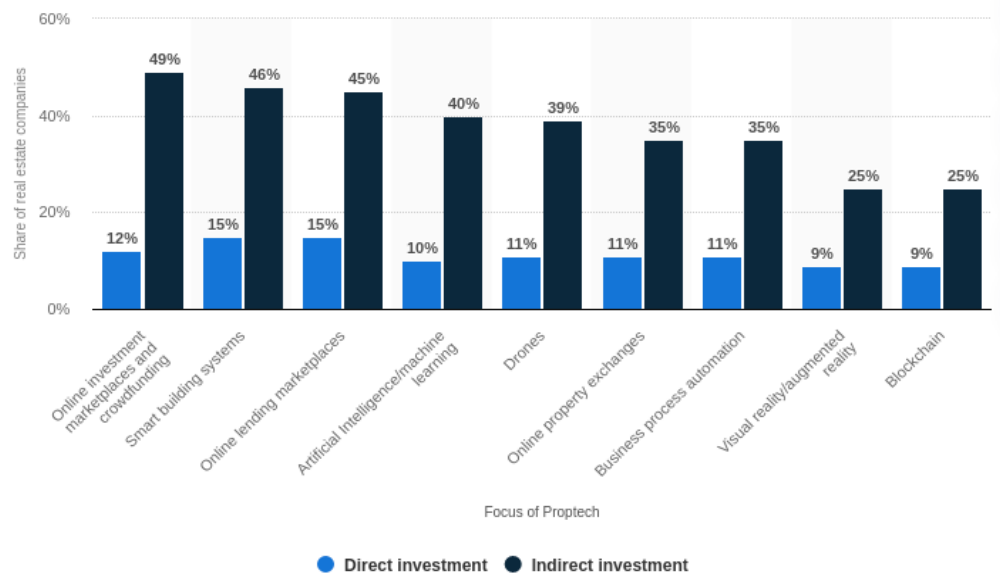
در سرمایه‌گذاری غیرمستقیم بصورت سنتی، در تمامی روش‌ها ما شاهد مشکلی بزرگ بنام عدم شفافیت و فقدان اعتماد هستیم. سرمایه‌گذاران نمی‌توانند داده‌هایی کاملاً شفاف برای مقایسه صندوق‌ها و سبدگردانی‌ها پیدا کنند و اعتماد به آن‌ها به سختی امکان‌پذیر است. فناوری بلاک‌چین و قراردادهای هوشمند، می‌توانند این چالش‌ها را برای ما برطرف سازند. آن‌ها می‌توانند با ایجاد صندوق‌های بدون نیاز به اعتماد^۱ فضای اطمینان‌بخشی برای سرمایه‌گذاران ایجاد کنند و فناوری بلاک‌چین شفافیت و صداقت داده‌های معامله‌گران را تضمین می‌کند. در این مقاله، سعی شده با بررسی فناوری بلاک‌چین و قراردادهای هوشمند Betoken، Cook و dhedge و مقایسه عملکرد آن‌ها، قدمی رو به آینده سرمایه‌گذاری برداریم.

کلمات کلیدی: بلاک‌چین، قراردادهای هوشمند، سرمایه‌گذاری غیرمستقیم، اتریوم، امور مالی غیرمتمرکز (DeFi).

۱- مقدمه

انجام می‌دهد. بدین معنی که فرد یا شرکت واسطه با تحلیل و بررسی و بطور کلی خرد خود، تصمیم به خرید و فروش دارایی‌ها می‌گیرد. از مزایای این روش می‌توان به صرفه‌جویی در وقت، استفاده از دانش و تخصص افراد حرفه‌ای در این زمینه و بررسی طیف بیشتری از بازارها اشاره کرد. این سرمایه‌گذاران به همان اندازه در معرض فراز و نشیب‌های تک تک سهام در صندوق‌های خود قرار دارند که گویی هر کدام را به صورت جداگانه خریداری کرده‌اند. در حالی که در بسیاری از مواقع فرد کارمزد بیشتری نسبت به سرمایه‌گذار مستقیم پرداخت کرده است. همچنین این سرمایه‌گذاران از مزایای مالکیت مستقیم سهام بهره‌مند نیستند.

واژه سرمایه‌گذاری با بازارهای مالی آمیخته شده است. هرگونه فعالیت در این بازارها از جمله خرید و فروش سهام، ابزارهای مشتقات و اوراق بدهی و یا قرض دادن و وام گرفتن یا ابزارهای نوین دیگر همچون سرمایه‌گذاری جمعی^۲ به نوعی با واژه سرمایه‌گذاری درهم تنیده شده است. تلاش فعالان در بازارهای مالی، کسب سود با کیفیت - بیشینه سود با تحمل ریسک منطقی - است. در این بین سرمایه‌گذاران به دو گروه سرمایه‌گذاران مستقیم و غیرمستقیم^۳ تقسیم می‌شوند. سرمایه‌گذاری غیرمستقیم به نوعی از سرمایه‌گذاری اطلاق می‌شود که فرد بصورت مستقیم به خرید و فروش دارایی‌ها مبادرت نمی‌ورزد بلکه با یک واسطه این کار را



شکل ۱- مقایسه سرمایه‌گذاری مستقیم و غیرمستقیم در زمینه‌های مختلف فناوری مالی [۲]

در هر نوع از روش‌های بالا مشکلاتی وجود دارد. اعم از:

۱. سبدگردان‌های سنتی به دلیل ناکارآمدی ذاتی ساختاری و ساختارهای سنگین هزینه، معمولاً به مشتریان خصوصی و موسسه‌های ثروتمند محدود می‌شوند.
۲. هیچ نهاد غیروابسته و بی‌طرفی برای مقایسه عملکرد معاملگران براساس معیارهای مختلف وجود ندارد.
۳. به دلیل نبود شفافیت و سیستم شایسته سالاری، ممکن است معامله‌گری برای سود شخصی خود، به تعداد زیادی از سرمایه‌گذاران غیرمستقیم ضرر برساند. شایسته سالاری‌های تشویقی نیز قبلاً هرگز با موفقیت اجرا نشده‌اند، زیرا داشتن یک بازیگر متمرکز که بتواند بی‌طرفانه درباره همه قضاوت کند تقریباً غیرممکن است.

همه این دلایل ما را به سمت استفاده از تکنولوژی بلاک‌چین سوق می‌دهند. در واقع تحقیقات نشان داده‌اند که یکی از مدل‌های کسب و کاری اصلی در دوران تحول دیجیتال و حول فناوری بلاک‌چین شکل گرفته است همین سرمایه‌گذاری با شیوه‌های جدید است که در ادامه این مطلب به تفصیل توضیح داده شده است [۱].

۱-۱- مروری بر فناوری بلاک‌چین

بلاک‌چین در پایین‌ترین سطح خود، به معنای واقعی کلمه یک زنجیره از بلوک‌های دیجیتالی است. وقتی ما از کلمات "بلوک" و "زنجیره" در این زمینه صحبت می‌کنیم، در واقع درباره اطلاعات دیجیتال - بلوک - ذخیره شده در پایگاه داده عمومی - زنجیره - صحبت می‌کنیم.

بلوک‌ها در زنجیره بلوکی از قطعات دیجیتالی اطلاعات تشکیل شده‌اند. بلوک‌ها اطلاعات مربوط به تراکنش‌ها مانند زمان و مقدار تراکنش و آدرس فرستنده و گیرنده و همچنین شناسه بلوک قبلی را ذخیره می‌کنند. همچنین هر بلوک یک شناسه منحصر به فرد دارد. یک بلوک واحد در بلاک‌چین بسته به اندازه تراکنش‌ها می‌تواند تا یک یا چند مگابایت داده ذخیره کند. به این معنی که یک بلوک واحد می‌تواند چند هزار تراکنش را زیر یک سقف جمع کند.

بصورت کلی با تمام چالش‌های موجود در سرمایه‌گذاری غیرمستقیم، استقبال از این نوع سرمایه‌گذاری بیشتر است. در شکل ۱ که نمایانگر توزیع سرمایه‌گذاری مستقیم و غیرمستقیم در زمینه‌های مختلف فناوری مالی است به صورت کلی این تفاوت در تمامی جنبه‌های فناوری مالی مشاهده می‌شود که سرمایه‌گذاری غیرمستقیم تقاضای بیشتری داشته و حجم پول جابجا شده در آن بیشتر است. بدیهتاً می‌توان تصور نمود افراد متقاضی این صنعت نیز بسیار بیشتر از معامله‌گران مستقیم هستند.

در سرمایه‌گذاری غیرمستقیم چهار روش مرسوم وجود دارد.

۱. سرمایه‌گذاری در صندوق سرمایه‌گذاری قابل معامله^۴ و غیرقابل معامله^۵: صندوق‌های سرمایه‌گذاری که با مدیریت مرکزی و تیم سرمایه‌گذاری، به مردم سهام فروخته و ثروت جمع شده را در سبد دارایی‌های مختلف همچون بازار سهام، اوراق یا بانک و ... سرمایه‌گذاری می‌کنند. این صندوق‌ها می‌توانند براساس محل سرمایه‌گذاری یا ریسک سرمایه‌گذاری بخش‌بندی شوند [۳].

۲. سبدگردان‌ها: در سبدگردان‌ها بر خلاف صندوق‌ها، تمام دارایی در یک حساب جمع نمی‌شود بلکه سبدگردان براساس مشخصات ریسک^۶ فرد سرمایه‌گذار، در حساب شخصی آن معاملات را انجام می‌دهد. در این روش فرد سرمایه‌گذار کارمزد بیشتری پرداخت می‌کند اما سبد دارایی‌اش متناسب با ذهنیت سرمایه‌گذاری‌اش چیده می‌شود و انعطاف بیشتری در نحوه سرمایه‌گذاری‌اش دارد. در مقابل سبدگردان نیز نسبت به یک مدیر صندوق، قادر به مدیریت تعداد مشتری کمتری می‌باشد اما بخاطر طرز معامله‌گری چابک تر، می‌تواند سود بیشتری به ارمغان بیاورد.

۳. رونویسی از معامله‌گری^۷: از ترکیب فناوری‌های جدید مالی با روش‌های سنتی سبدگردانی و مدیریت صندوق پدید آمده است، بدین گونه که افراد متخصص و معامله‌گر می‌توانند در هر لحظه سبد دارایی‌های ایده‌آل خود را در آن قرار دهند و سرمایه‌گذاران بر اساس سابقه و عملکرد معامله‌گران، بخشی از سرمایه خود را از معامله‌گر مورد نظرشان، رونویسی کنند. بقیه کار را پلتفرم انجام می‌دهد، یعنی به محض تغییر سبد توسط معامله‌گر - افزودن یک سهم جدید، حذف دارایی از سبد یا تغییر نسبت دارایی‌ها - پلتفرم برای سرمایه‌گذاران مقلد^۸ تغییر سبد را اعمال کرده و سفارشات خرید و فروش را انجام می‌دهد.

رایانه‌هایی که بلوک‌ها را با موفقیت تأیید و به بلاک‌چین اضافه می‌کنند، برای کار خود، رمزارز پاداش می‌گیرند.

اگرچه تراکنش‌ها بصورت عمومی در یک بلوک ثبت می‌شوند، اما اطلاعات کاربر یا ثبت نمی‌شود یا حداقل کامل ثبت نمی‌شود. برای انجام معاملات در شبکه بیت‌کوین، شرکت‌کنندگان باید یک برنامه را به نام کیف پول^{۱۱} اجرا کنند. هر کیف پول شامل دو کلید رمزنگاری منحصر به فرد و متمایز است: یک کلید عمومی و یک کلید خصوصی. تراکنش‌ها با کلید عمومی کاربران ثبت می‌شوند. همچنین کلید عمومی به عنوان امضای دیجیتال کاربر بر روی دفتر توزیع بلاک‌چین ظاهر می‌شود [۴].

کلید عمومی کاربر یک متمم از کلید خصوصی وی است که از طریق یک الگوریتم پیچیده ریاضی ایجاد شده است. با این حال، با توجه به پیچیدگی این معادله، تقریباً غیرممکن است که روند را معکوس کرده و یک کلید خصوصی را از یک کلید عمومی تولید کرد. به همین دلیل، فناوری بلاک‌چین محرمانه محسوب می‌شود.

در نهایت فناوری بلاک‌چین به دلیل ایمنی فوق‌العاده و غیرقابل هک بودن می‌تواند در موارد قابل توجه بسیاری به کار گرفته شود و اول از همه بانکداری را متحول کند [۵].

۱-۳- قراردادهای هوشمند

قرارداد هوشمند یک قرارداد خود اجرایی است که شرایط توافق‌نامه بین خریدار و فروشنده مستقیماً بصورت خط کد کامپیوتر نوشته شده است. کد و توافق‌نامه‌های موجود در آن در شبکه توزیع شده و بصورت غیرمتمرکز در بلاک‌چین وجود دارد. کد اجرا را کنترل می‌کند و معاملات قابل پیگیری و برگشت‌ناپذیر هستند. قراردادهای هوشمند اجازه می‌دهد معاملات و توافق‌نامه‌های مطمئن بدون نیاز به مرجع مرکزی، سیستم حقوقی یا ساز و کار اجرایی خارجی در بین اشخاص ناشناس انجام شود [۶].

نخستین بار، در سال ۱۹۹۶، قرارداد هوشمند توسط نیک سابو^{۱۲} که یک متخصص کامپیوتر و رمزنگار بود، مطرح شد. پس از چندین سال، او روی این مفهوم مجدداً کار کرد و مقالات زیادی منتشر کرد. او در این مقالات، مفهوم ایجاد قراردادهای قانونی فعالیت‌های تجاری از طریق طراحی پروتکل‌های الکترونیکی بین افراد غریبه در اینترنت را شرح داد. ایده اصلی او این بود که قراردادهای را به ماشین تبدیل کند. اینگونه به هیچ واسطه‌ای همچون بانک نیازی نیست و در نتیجه هزینه کارمزدها بسیار کم خواهد شد. این امر به کمک فناوری بلاک‌چین محقق شد. به کمک این فناوری ما قادر هستیم که قراردادهای هوشمند را غیرمتمرکز کنیم تا عادلانه و بی‌اعتماد باشند. یعنی توسط یک سرور مرکزی کنترل نشوند [۷].

هنگامی که یک بلوک داده‌های جدید را ذخیره می‌کند، در انتها به زنجیره بلوکی اضافه می‌شود. زنجیره بلوکی همانطور که از نامش پیداست، متشکل از چند بلوک متصل شده است و برای اینکه یک بلوک به بلاک‌چین اضافه شود، باید چهار چیز اتفاق بیفتد: معامله باید رخ دهد، باید تأیید شود، باید در یک بلوک ذخیره شود و در نهایت باید یک “هش” به آن بلوک اختصاص داده شود. هنگامی که یک بلوک جدید به بلاک‌چین اضافه می‌شود، در معرض دید همگان قرار می‌گیرد و به صورت عمومی در دسترس است. اگر نگاهی به بلاک‌چین بیت‌کوین بیاندازید، خواهید دید که شما به داده‌های تراکنش، همراه با اطلاعات در مورد زمان، مکان و کسی که بلوک را به بلاک‌چین اضافه کرده، دسترسی دارید.

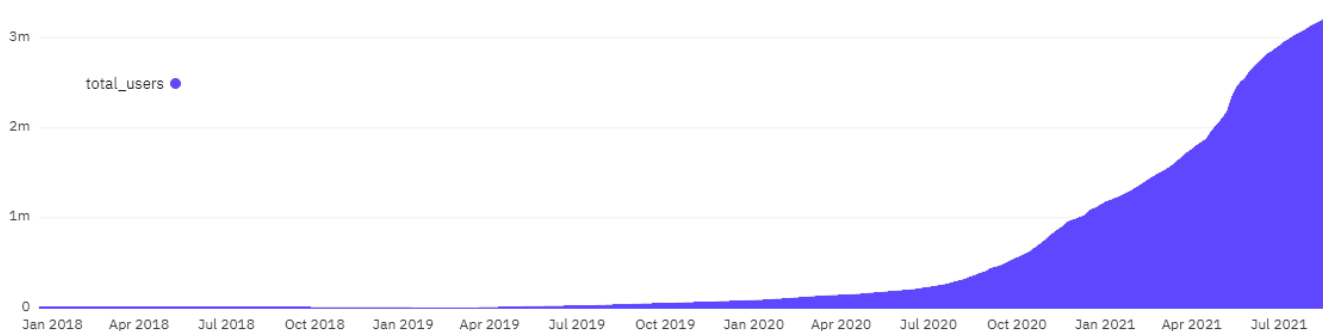
۱-۲- رمزارزها و بلاک‌چین

هدف بلاک‌چین فراهم کردن امکان ثبت و توزیع اطلاعات دیجیتال، بدون امکان ویرایش است. فهم این مفهوم می‌تواند بدون اینکه این فناوری را در عمل ببینیم، دشوار باشد. فناوری بلاک‌چین برای اولین بار در سال ۱۹۹۱ توسط دو محقق بنام‌های استوارت هابر و دیلیواسکات استورنتا معرفی شد که در پی پیاده‌سازی سیستم‌هایی بودند که زمان نشانه‌گذاری اسناد را نتوان در آنها تغییر داد. اما تقریباً تا دو دهه بعد و قبل از ظهور بیت‌کوین به عنوان جدی‌ترین رمزارز، در ژانویه ۲۰۰۹ محقق نشد. در واقع اولین ظهور بلاک‌چین و کاربرد آن در دنیای واقعی با ارزهای دیجیتال و با ارز بیت‌کوین رقم خورد.

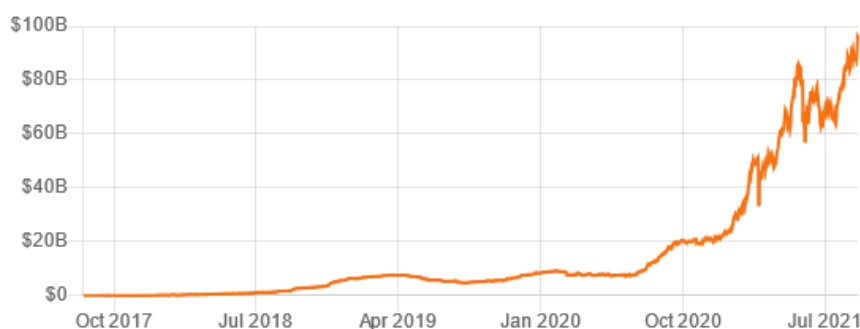
پروتکل بیت‌کوین روی بلاک‌چین ساخته شده است. در یک مقاله که در مورد ارز دیجیتال منتشر شده است، ساتوشی ناکاموتو^۹ خالق اسطوره‌ای بیت‌کوین، آن را به عنوان یک سیستم نقدی الکترونیک جدید و همتا به همتا^{۱۱} معرفی کرد که به هیچ شخص یا سیستم ثالثی اعتماد ندارد. فرض کنید یکی از میلیون‌ها نفر دارنده بیت‌کوین می‌خواهد پول خود را در بازار خرج کند. این جایی است که بلاک‌چین وارد می‌شود.

هنگامی که پای پول چاپی وسط باشد، استفاده از آن توسط یک سازمان مرکزی، معمولاً یک بانک مرکزی یا دولت تأیید می‌شود، اما بیت‌کوین توسط هیچ کسی کنترل نمی‌شود. در عوض، تراکنش‌های انجام شده در بیت‌کوین توسط شبکه‌ای از رایانه‌ها تأیید می‌شوند.

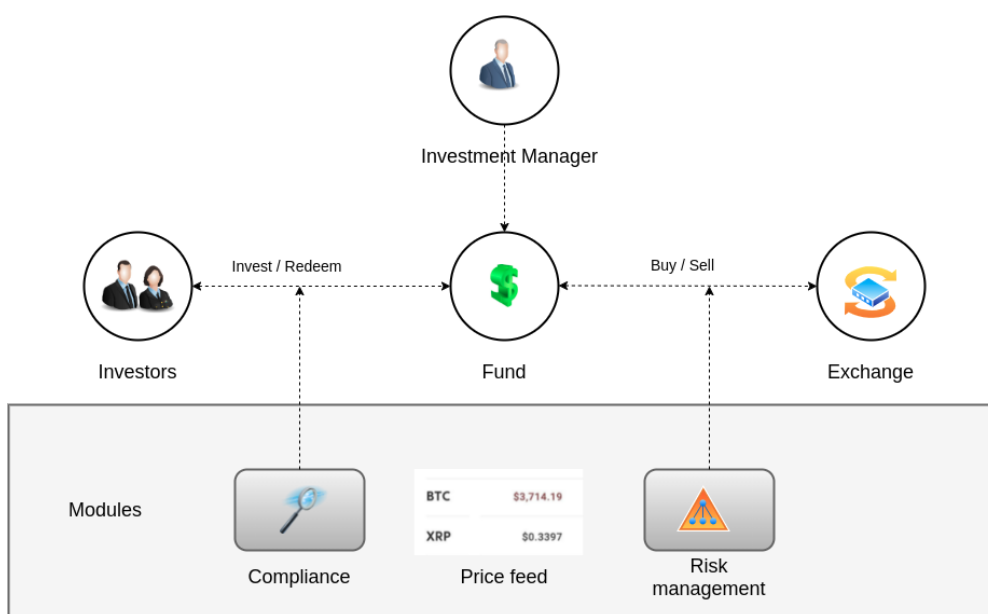
هنگامی که یک شخص برای کالاهای خریداری کرده خود از حساب بیت‌کوین خود پرداخت انجام دهد، رایانه‌ها در شبکه بیت‌کوین رقابت می‌کنند تا تراکنش را تأیید کنند. به منظور انجام این کار، کاربران بر روی رایانه خود یک برنامه اجرا می‌کنند و سعی می‌کنند یک مسئله ریاضی به نام معمای هش را حل کنند. هنگامی که یک رایانه مسئله را حل کند، بلوک را تأیید کرده است و معامله کامل به طور عمومی به عنوان یک بلوک در بلاک‌چین ضبط و ذخیره می‌شود که در این نقطه غیرقابل تغییر می‌شود. در مورد بیت‌کوین و اکثر بلاک‌چین‌های دیگر،



شکل ۲- تعداد کاربران استفاده‌کننده از قراردادهای هوشمند مالی [۱۵]



شکل ۳- حجم دارایی در گردش در DeFi [۱۴]



شکل ۴- معماری سطح بالای صندوق‌های سرمایه‌گذاری غیرمتمرکز

۲- سرمایه‌گذاری غیرمستقیم در فناوری بلاک چین و صندوق‌های غیرمتمرکز

ایده سرمایه‌گذاری‌های غیرمتمرکز بصورت کلی - بدون جزئیات پیاده‌سازی - بدین شکل است که سرمایه‌گذار، مقداری از دارایی خود را در قرارداد واریز می‌کند. از طرفی معامله‌گران هم در قرارداد موردنظر حساب دارند و با توجه به عملکردشان رتبه‌بندی می‌شوند. سپس قرارداد براساس رتبه هر معامله‌گر مقداری از دارایی را تحت فرمان او قرار می‌دهد و در صورتی که معامله‌گر قصد خرید یا فروش هر ارزی را داشته باشد، قرارداد به کمک پروتکل‌های صرافی‌های غیرمتمرکز، آن معامله را انجام می‌دهد. سپس در هر دوره زمانی، رتبه‌بندی معامله‌گران دوباره محاسبه و بروزرسانی می‌شود و مقدار سود و ضرر سرمایه‌گذاران نیز براساس سود و ضرر کل صندوق و کارمزد معامله‌گران و موسس قرارداد محاسبه می‌شود (شکل ۴ را ببینید) [۹].

ویژگی‌های اصلی این نوع صندوق‌ها عبارت‌اند از:

۱. دسترسی برای عموم، در بخش‌های قبل اشاره شده بود که سبدگردان‌ها بخاطر ساختار خود، قادر به ارائه سرویس به تعداد زیاد مشتریان نیستند و مجبورند محدودیتی براساس ارزش دارایی برای قبول مشتری بگذارند. اما در این روش، هیچ محدودیتی برای اضافه شدن مشتری جدید وجود ندارد [۱۰].

این روزها، قرارداد هوشمند به صورت عمده توسط ارزهای دیجیتال مورد استفاده قرار می‌گیرد. پروتکل‌های غیرمتمرکز ارزهای مجازی، در اصل قراردادهای هوشمندی هستند که کدنواری و امنیت غیرمتمرکز دارند. این قراردادها به صورت گسترده در شبکه‌های رمزارز موجود به کار گرفته می‌شوند و یکی از برجسته‌ترین ویژگی‌های اتریوم^{۱۲} هستند [۸].

طبق گزارش دون آنالیتیکس^{۱۴} که در شکل نشان داده شده است، حجم دارایی‌های در گردش و کل آدرس‌های منحصر به فرد اتریوم^{۱۵} در قراردادهای هوشمند مالی^{۱۶} در اوایل سال ۲۰۲۰ رشد چشمگیری داشته و در جولای سال ۲۰۲۱ بیش از ۳ میلیون نفر است. حجم دارایی در گردش نیز از ۶۰۰ میلیون دلار در ابتدای سال ۲۰۲۰ به ۹۵۰ میلیارد دلار در سپتامبر ۲۰۲۱ رسیده است. انتظار می‌رود روند رشد ادامه یابد [۱۲، ۱۳].

برای سرمایه‌گذاری مستقیم در بازار رمزارزها ابزارهای بسیاری همچون صرافی‌های متمرکز و غیرمتمرکز و پروتکل‌هایی همچون compounds که قابلیت قرض دادن دارایی در آن‌ها فراهم شده وجود دارند اما ابزارهای قدرتمندی برای سرمایه‌گذاری غیرمستقیم در بازار رمزارزها وجود ندارد در حالی که بنظر بسیاری از سرمایه‌گذاران به آن نیاز دارند. در این مقاله قصد داریم برنامه‌های کاربردی غیرمتمرکز^{۱۷} در حوزه سرمایه‌گذاری غیرمستقیم را بررسی و تحلیل کنیم.

۴. نسبت تعداد سرمایه‌گذاران به مدیران: تعداد سرمایه‌گذاران بیشتر از مدیران است و در نتیجه مدیران یا باید اهرم‌های بسیار سنگینی قبول کنند یا بخش قابل توجهی از صندوق بدون مدیر باقی بماند.

۳- بررسی و تحلیل چند نمونه صندوق سرمایه‌گذاری غیرمتمرکز

۳-۱- صندوق Betoken

Betoken یک صندوق سرمایه‌گذاری غیرمتمرکز ساخته شده بر روی بلاک‌چین اتریوم است که در توکن‌های ERC-20 سرمایه‌گذاری می‌کند. Betoken برای تصمیم‌گیری در مورد سرمایه‌گذاری به تعداد زیادی از مدیران و معامله‌گران متکی است که هر یک از آن‌ها بخشی از صندوق را مدیریت می‌کنند. پورتهوهای معامله‌گران در سیستم تصمیم‌گیری منحصر به فردی که شایسته سالاری خطاب می‌شود، بررسی می‌شود و به طور مداوم تصمیمات سرمایه‌گذاری را به مدیرانی که سودآورترین سرمایه‌گذاری را دارند، توزیع می‌کند [۸، ۱۷].

مهم‌ترین بخش‌های این سیستم عبارتند از:

۱. ارزش‌های سیستم شایسته سالاری، بصورت توکن شده‌اند. به این توکن‌ها، توکن کنترل (Kairo) گفته می‌شود.
۲. توکن کنترل ارزشمند و غیرقابل فروش هستند.
۳. اقدامات خوب یک معامله‌گر متناسب با حجم و کیفیت آن عمل پاداش می‌گیرند.

۴. یک معامله‌گر متناسب با حجم و کیفیت سرمایه‌گذاری بدی که کرده و خساراتی که به صندوق وارد کرده است جریمه می‌شود و از تعداد توکن‌های کنترلش کم می‌شود.

همانگونه که قبلاً اشاره شده بود، سیستم‌های شایسته سالاری هیچوقت با موفقیت پیاده‌سازی نشده‌اند، زیرا داشتن یک بازیگر متمرکز که بتواند بی‌طرفانه درباره همه قضاوت کند تقریباً غیرممکن است. با این حال ما می‌توانیم به کمک بلاک‌چین‌هایی که از قراردادهای هوشمند پشتیبانی می‌کنند بازیگران غیرمتمرکزی را بسازیم که می‌توانند قوانین ناگسستگی را اجرا کنند. Betoken اولین برنامه غیرمتمرکز است که شامل پیاده‌سازی شایسته سالاری تشویقی است. صندوق Betoken در چرخه‌های سرمایه‌گذاری فعالیت می‌کند. هر چرخه به ۲ مرحله تقسیم می‌شود.

- مرحله وقفه: در این مرحله که ۳ روز طول می‌کشد، مدیران دسترسی به سید خود و ارسال سفارش جدید ندارند. در این فاز دو عمل اصلی انجام می‌شود:

- واریز و برداشت: کاربران می‌توانند وجوه خود را واریز و برداشت کنند. کاربران می‌توانند رمزارز اتر یا هر رمزارز دیگر تحت پروتکل ERC-20 را به صندوق واریز کنند و سهام صندوق دریافت کنند. سهام صندوق تحت پروتکل ERC-20 و با نام ETKS شناخته می‌شود.

- دریافت کمیسیون: مدیران صندوق می‌توانند متناسب با توکن‌های کنترل - توکن Kairo - خود از کمیسیون خود استفاده کنند.

- مرحله مدیریت: در این مرحله که ۲۷ روز طول می‌کشد، مدیران براساس میزان توکن Kairo که دارند، اختیار مدیریت صندوق را داشته و می‌تواند سفارشات خرید و فروش خود را ارسال کنند. هر مدیر می‌تواند حداکثر به میزانی که در فرمول زیر محاسبه می‌شود سرمایه‌گذاری کند. یعنی مجموعه معاملات او نمی‌تواند بیشتر از مقدار زیر شود.

۲. غیرقابل توقف، این صندوق‌ها به دلیل ساختار ذاتی قراردادهای هوشمند از اصل "قد قانون است" پیروی می‌کنند. در نتیجه هیچکس حتی پدید آورنده آن نمی‌تواند آن را متوقف کند یا از آن اختلاس نماید. مشتری با خواندن قرارداد - که منظور همان کد قرارداد است - و قبول آن با آرامش خاطر همیشه می‌تواند از آن استفاده کند و نگران تغییر یا سواستفاده از قرارداد نخواهد بود.

۳. کاملاً شفاف، تمامی اطلاعات در پایگاه داده بلاک‌چین ذخیره می‌شود و هیچگاه تغییر نمی‌کنند یا حذف نمی‌شوند و در نتیجه می‌توان آن را با دیگر محصولات مقایسه کرد و عملکرد مطلوب را استخراج کرد [۱۱].

۴. سرمایه‌گذاری در این صندوق‌ها شبیه معامله با اهرم است، معامله‌گر با قرار دادن پول در صندوق^{۱۹} می‌تواند تا چندین برابر دارایی خود، از صندوق دارایی بگیرد و آن‌ها را مدیریت کند.

۵. معامله‌گران در صورتی که سود یا ضرر نکنند بسته به میزان مدیریتشان کارمزد می‌گیرند.

۶. هزینه‌های نگهداری و جمع‌آوری سرمایه ندارند. سبب‌گردان‌ها و صندوق‌های سرمایه‌گذاری برای جلب نظر مشتریان و جذب آن‌ها، همواره باید هزینه‌های هنگفتی برای تبلیغات بکنند اما در این روش، پلتفرم محل مناسبی برای معرفی آن‌ها به مشتریان هدف می‌باشد.

۷. نیاز به حسابداری و معامله‌گری ندارند تمامی سفارشات خرید و فروش برای سرمایه‌گذاران توسط سیستم انجام می‌شود و مدیران تنها به بهینه‌سازی چینش سبد خود اهتمام می‌ورزند. همچنین امور حسابداری و محاسبه سود و ضرر و کارمزد ها توسط سیستم انجام می‌گردد.

۲-۱- چالش‌های سرمایه‌گذاری غیرمتمرکز

صندوق‌های سرمایه‌گذاری غیرمتمرکز علی‌رغم مزایا و ویژگی‌های متنوعی که دارند برای سرمایه‌گذاران و دولت‌ها چالش‌هایی ایجاد کرده‌اند. تحقیقات نشان داده‌اند که بیش از ۲۰ مورد انواع اشکالات پروتکلی داشته است که به از بین رفتن بیش از ۱۳۰ میلیون دلار دارایی سرمایه‌گذاران منجر شده است [۱۳، ۱۶]. در این بخش این چالش‌ها را مرور می‌کنیم:

۱. تخلفات اقتصادی همچون پول‌شویی و فرار از مالیات: پول‌شویی یکی از مشکلات ذاتی بلاک‌چین است و هر قرارداد هوشمندی که بر این بستر نوشته شود، با این مشکل سردر گریبان است. به عنوان مثال، مالیات ممکن است بسته به محل اجرای معامله با فرمول خاصی اعمال شود. قانون لازم برای شبکه‌های بلاک‌چین باید از قبل مشخص شود تا از درگیری جلوگیری شود.

۲. ریسک‌های عملیاتی: خطا و اشتباه می‌تواند در هر محصول نرم افزاری رخ دهد اما به دلایل ذاتی ساختار بلاک‌چین از جمله برگشت‌ناپذیری، ریسک‌های آن به شدت بیشتر است. البته تلاش‌های برنامه‌نویسان این حوزه در رعایت اصول نرم‌افزاری و تست زیاد و استفاده از بنیه‌های برنامه‌نویسی منبع باز^{۲۰} و وجود بسیاری از شرکت‌های معتبر که قراردادهای هوشمند را از لحاظ امنیتی و عملکردی تست و تایید می‌کنند، شدت این ریسک را کاهش داده است.

۳. معامله دارایی‌های خارج از بلاک‌چین: بعنوان مثال فرض کنید قرارداد هوشمند شما در بستر اتریوم است و معامله‌گر، می‌خواهد رمزارز بیت‌کوین بخرد. این امکان توسط بعضی از پروتکل‌ها فراهم شده و شما بعنوان مثال می‌توانید در بلاک‌چین اتریوم wrapped bitcoin بخرید که معادل بیت‌کوین است اما برای همه‌ی ارزش‌ها این امر میسر نیست.

Betoken در مقابل مدیران کم‌فعالیت واکنش‌های مختلفی نشان می‌دهد. در صورتی که یک مدیر فعالیتی نداشته باشد، متناسب با میزان توکن Kairo دارد، کارمزد دریافت می‌کند. Betoken در صورتی که یک مدیر در ۲ دوره هیچ فعالیتی نداشته باشد، یعنی هیچ معامله‌ای انجام ندهد، مدیر را بازنشسته خطاب می‌کند و توکن‌های Kairo او را باطل می‌کند. در صورتی که مدیری فعالیت کمی داشته باشد و هر ماه یک معامله ساده انجام دهد و سریع آن را ببندد، شامل بند بالا نمی‌شود و می‌تواند از کارمزد ثابت صندوق برای همیشه استفاده کند.

Betoken به هر مدیر متناسب با فرمول زیر کارمزد می‌دهد.

$$\text{kairoTokens} \times \text{riskProfileProportion}$$

نسبت مشخصات ریسک مدیر، عددی بین ۰ تا ۱ است و هر چقدر کاربر فعالیت کمتری داشته باشد، این عدد به صفر نزدیک‌تر شده و کارمزد دریافتی مدیر کمتر خواهد شد. این نسبت به کمک فرمول‌های زیر محاسبه می‌شود.

$$\text{Risk} = \sum_{i \in \text{Investments}} \text{Duration}(i) \times \text{Stake}(i)$$

$$\text{Threshold} = \text{KairoBalanceAtCycleStart} \times 3 \text{ (days)}$$

$$\text{riskProfileProportion} = \min\left(1, \frac{\text{Risk}}{\text{Threshold}}\right)$$

بعنوان مثال فردی ده توکن Kairo دارد و در طول فاز مدیریت، دو معامله انجام داده است که در معامله اول ۱ توکن را به مدت ۱۵ روز فروخته‌اشته است و در معامله دیگر ۲ توکن را به مدت ۵ روز. نسبت مشخصات ریسک این مدیر بدین ترتیب است:

$$\text{Risk} = 1 \times 15 + 2 \times 5 = 25$$

$$\text{Threshold} = 10 \times 3 = 30$$

$$\text{RiskProfileProportion} = \min\left(1, \frac{25}{30}\right) = 83\%$$

در نتیجه این کاربر ۸۳ درصد از کل کارمزد اختصاصی به خود را دریافت خواهد کرد.

Betoken برای تشویق مدیران به تبلیغ صندوق و جذب سرمایه‌های جدید نیز راه‌کار جالبی برگزیده است. به ازای هر مشتری که با کد مدیری ثبت نام کند، معادل ۵ درصد از ارزش دارایی‌های آن مشتری را به مدیر او برای مدیریت می‌دهد. همچنین Betoken از معامله‌های اهرمی پشتیبانی می‌کند. Betoken از پروتکل‌های Compound Finance و Fulcrum برای اجرای معاملات اهرمی و سفارشات فروش تعهدی استفاده می‌کند [۱۷].

$$\text{investmentAmount} = \text{totalFunds} \times \frac{\text{decisionStake}}{\text{totalKairoSupply}}$$

پس از بستن معامله، مقدار توکن Kairo بازگشتی به کاربر با فرمول زیر محاسبه می‌شود:

$$\text{stake} \times (1 + \text{ROI})$$

بعنوان مثال اگر معامله‌ای ۲۰ درصد به ارمغان بیاورد، مدیر بیست درصد توکن Kairo بیشتر دریافت می‌کند. در صورتی که مدیر در دوره ۲۷ روزه خود معامله‌ای را نبندد، میزان توکن Kairo مربوط به آن سفارش کامل از دست می‌رود. در صورتی که معامله‌ای بیشتر از ۲۵ درصد ضرر کند، میزان توکن Kairo بازگشتی صفر خواهد بود. در صورتی که میزان ضرر بین ۱۰ تا ۲۵ درصد باشد، میزان توکن Kairo بازگشتی بصورت تصاعدی، کمتر خواهد شد.

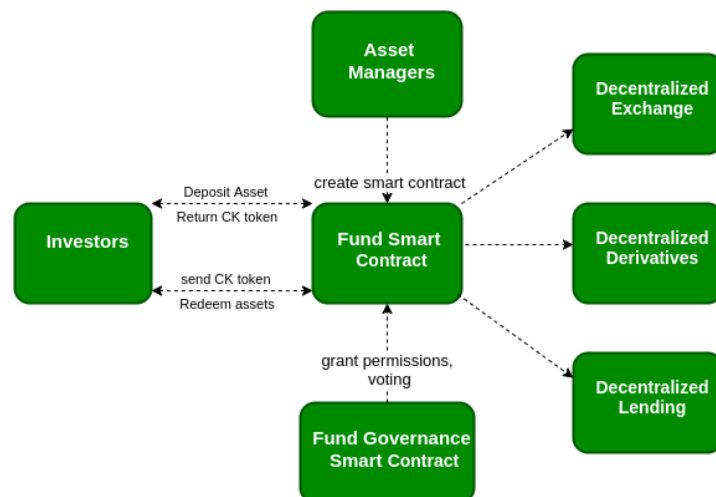
۳-۱-۱- توکن Kairo

این توکن نشان شهرت و عملکرد خوب یک مدیر است، بدین معنی که یک مدیر هر چقدر بیشتر از این توکن داشته باشد، در سرمایه‌گذاری بهتر عمل کرده است. مدیران سرمایه پس از ثبت نام می‌توانند به میزان حداکثر یک درصد از کل Kairoهای صادر شده تا آن لحظه، توکن Kairo را به کمک رمزارزهای دیگر بخرند. اینگونه وال‌ها انگیزه‌ای برای دستکاری در صندوق با خرید مقدار زیادی از توکن Kairo ندارند. همچنین این توکن قابل فروش و جابجایی نیست.

۳-۱-۲- ساختار کارمزدها

پس از پایان دوره مدیریت، کارمزدها بدین صورت محاسبه می‌شوند:

- ۰.۱ درصد از کل صندوق Betoken، بین مدیرانی که توکن Kairo دارند، تقسیم می‌شود.
- ۰.۱ درصد از کل صندوق برای نگهداری و توسعه‌ی صندوق به حساب تیم توسعه‌دهنده ارسال می‌شود.
- ۲۰ درصد از کل سود ماهیانه صندوق به مدیران نگهدارنده توکن Kairo که در چرخه مدیریتشان سود کرده‌اند داده می‌شود. رقم کارمزد متناسب با دارایی تحت مدیریت و مشخصات ریسک مدیر است.



شکل ۵- معماری صندوق‌های سرمایه‌گذاری در پروتکل Cook

۳-۲-۲- صندوق Cook

۳-۲-۲- نحوه تامین اهداف صندوق Cook

در این بخش به طور خلاصه مشخص می‌کنیم که اهداف مختلفی که برای پروتکل Cook در نظر گرفته شده بود، چگونه محقق می‌شوند:

- ترکیب‌پذیری: هر صندوق در پلتفرم پروتکل Cook دارای یک قرارداد هوشمند مربوطه و یک ckToken مخصوص است. از آنجا که هر نوع ckToken با استاندارد ERC-20 مطابقت دارد، ckToken می‌تواند از ckTokenهای دیگر تشکیل شوند. این امر امکان ایجاد یک توکن برای نشان دادن تعداد نامحدود توکن‌های دیگر را فراهم می‌کند. از آنجا که بودجه در پروتکل Cook قابل انعطاف است، می‌توان چندین لایه انتزاع ایجاد کرد. این باعث می‌شود بودجه مانند بلوک‌های لگو ساخته شود که می‌تواند برای تولید محصولات مالی با سطح بالاتر و برنامه‌های غیرمتمرکز مورد استفاده قرار گیرد.

- نقدشوندگی بالا: وجوه توسط دارایی‌های اساسی خود وثیقه گرفته می‌شوند، که این بدان معناست که وجوه بصورت قابل اعتمادی از دارایی‌های اساسی برخوردار هستند و تنها از طریق روش‌های آشکار آن می‌توان به آن‌ها دسترسی داشت. ckToken نشان دهنده مالکیت وجوه مربوطه است. نقدشوندگی بالای توکن‌های ERC-20 به سرمایه‌گذاران این امکان را می‌دهد تا ckToken را برای دارایی‌های اساسی بازخرید کنند یا در هر زمان آن‌ها را در بازار آزاد معامله کنند و مانند Betoken نیاز به گذران دوره ۲۷ روزه و رسیدن دوره وقفه ندارد.

- صرفه‌جویی در مصرف gas: خرید و انتقال چندین نشانه ERC-20 مستلزم پرداخت هزینه تراکنش در نقل و انتقالات هر رمزارز است. با استفاده از پروتکل Cook، کاربران فقط باید هزینه معاملات را در یک معامله واحد برای دارایی‌های اساسی که نمایندگی می‌کنند بپردازند و اینگونه در هزینه gas صرفه‌جویی زیادی می‌کنند. علاوه بر این، جمع کردن دارایی‌ها در یک صندوق به سرمایه‌گذاران صندوق این امکان را می‌دهد تا هزینه gas مصرفی حاصل از فعالیت‌های سرمایه‌گذاری را با یکدیگر تقسیم کنند.
- امنیت بیشتر و صندوق‌های trustless: برخلاف Betoken که برای حفظ اعتماد بین سرمایه‌گذاران و مدیران از روش‌های مختلفی همچون محدود سازی صدور Kairo و تنبیه مدیران ضررده استفاده می‌کرد، در اینجا از آنجا که مدیران تحت یک قرارداد هوشمند، صندوق خود را ارائه می‌کنند، براساس اصل "کد قانون است" سرمایه‌گذاران می‌توانند با امنیت بیشتری اقدام به سرمایه‌گذاری کنند.

۳-۳- صندوق dHEDGE

این پلتفرم که بر بستر بلاک‌چین اتریوم ساخته شده است، یک ابزار رونیسی از معاملات است که مدیران و معامله‌گران در آن قادرند استخر^{۲۲} مخصوص خود را تشکیل داده و سپس سرمایه‌گذاران در آن استخرها سرمایه‌گذاری کنند. مدیران همیشه تلاش می‌کنند که با بهترین عملکرد به صدر جدول مدیران^{۲۳} بیایند و اینگونه سرمایه بیشتری جذب کنند. همچنین اگر تصمیمات مدیر سودآور باشد، مدیر کارمزد عملکرد خود را به عنوان درصدی از بازده کل حاصل از استخر دریافت می‌کند. کارمزدها در استخر توکن‌ها جمع می‌شوند، به این معنی که اگر مدیر عملکرد موفق آمیزی داشته باشد، مالکیت کلی وی بر روی استخر با گذشت زمان افزایش می‌یابد. مدیران می‌توانند استخرهای عمومی یا خصوصی داشته باشند. همچنین می‌توانند از طریق سایت یا الگوریتم و به کمک api استخر خود را مدیریت کنند. ضمناً این پلتفرم از پروتکل Synthetix قدرت گرفته است.

Cook با هدف کاهش gas مصرفی و نقدشوندگی بیشتر و طراحی یک اپ بی اعتماد^{۲۱} آمده است. Cook یک صندوق سرمایه‌گذاری نیست، بلکه پروتکلی برای ساخت صندوق سرمایه‌گذاری است و در آن می‌توان صندوق‌های زیادی تاسیس کرد و سرمایه‌گذاران می‌توانند براساس استراتژی خود، به مقدار دلخواه در هر کدام از صندوق‌ها سرمایه‌گذاری کنند. پروتکل Cook قصد دارد تا به سکویی تبدیل شود که با طیف گسترده‌ای از نیازهای سرمایه‌گذاران و مدیران صندوق مطابقت داشته باشد و در عین حال بی‌اعتماد و شفاف باشد. در ابتدا نحوه کارکرد این آپ و پروتکل آن را توضیح می‌دهیم، سپس بررسی می‌کنیم که Cook چگونه به این اهداف رسیده است (را ببینید).

پروتکل Cook بر روی بلاک‌چین Ethereum ساخته شده است و مجموعه‌ای از صندوق‌های سرمایه‌گذاری را به سرمایه‌گذاران ارائه می‌دهد. هر صندوق یک توکن منحصر به فرد ERC-20 دارد و سرمایه‌گذاران پس از واریز وجه به حساب صندوق، توکن مخصوص آن صندوق را متناسب با سهم آن‌ها در صندوق، دریافت می‌کنند. این توکن - که در ادبیات Cook، ckToken خوانده می‌شود - مختص هر صندوق است و می‌تواند در میان سرمایه‌گذاران مبادله شود یا با دارایی‌های اساسی آن در داخل صندوق بازخرید شود. مفهوم ckToken مشابه سهم در بازار سهام است و شبیه محصولات مالی مانند ETF کار می‌کند [۱۸].

۳-۲-۱- فرآید تاسیس صندوق Cook

مدیر صندوق سرمایه‌گذاری، اهداف صندوق خود را در قالب کدهای یک قرارداد هوشمند بیان می‌کند و سپس پروتکل Cook را پیاده‌سازی می‌کند. بعنوان مثال مدیری قصد تاسیس صندوقی دارد که همیشه ۵ رمزارز بزرگ بازار را به نسبت ارزش بازارشان در سبد صندوق به روز کند. ابتدا مدیر قرارداد هوشمندی می‌نویسد که:

- اگر نسبت ارزش بازار دارایی‌ها عوض شد، نسبت رمزارزهای تحت مدیریت را عوض کند.
- در صورتی که ۵ رمزارز بزرگ بازار تغییر کردند، مثلاً یکی از لیست خارج شد و یک رمزارز به لیست پنج رمزارز برتر وارد شد، کل دارایی رمزارز فعلی را فروخته و با رمزارز جدید جایگزین کند.
- در صورتی که به صندوق لیستی از ارزهای پشتیبانی شده واریز شد، به نسبت دارایی‌های تحت مدیریت و بصورت بهینه‌ای swap شود.
- در صورتی که کاربری قصد برداشت دارایی‌اش را داشت، بصورت بهینه‌ای رمزارز تقاضا شده توسط کاربر را به او بدهد.

سپس پروتکل Cook را پیاده می‌کند. در این پروتکل، مدیر صندوق می‌تواند کارمزد دریافتی، لیست رمزارزهایی که برای واریز و برداشت پشتیبانی می‌کند و وقایعی که صندوق باید به آن‌ها واکنش نشان دهد را تعریف کند. سپس پروتکل برای او یک ckToken می‌سازد و صندوق راه‌اندازی می‌شود. هم‌اکنون در نرم‌افزار Cook، دو صندوق وجود دارند که این پروتکل را پیاده‌سازی کرده اند.

۱. صندوق دو رمزارز بزرگ بازار که دارایی‌شان شامل بیت‌کوین و اتریوم است.

۲. صندوق ۵ توکن بزرگ بازار اتریوم که دارایی‌شان شامل اتریوم، توکن صرافی uniswap، maker، aave، chainlink و compounds است.

حال کاربران می‌توانند با واریز رمزارزی که صندوق پشتیبانی می‌کند، سهام این صندوق را بخرند. به محض واریز تعداد سهام معادل صندوق به کیف پولشان واریز می‌شود.

جدول ۱- مقایسه ویژگی‌های پلتفرم‌های معرفی شده

نام پلتفرم	نقدشوندگی	تقسیم بودجه	مصرف gas مدیران	رمزارهای پشتیبانی شده برای واریز و برداشت
Betoken	فقط در سه روز از ماه	فقط یک صندوق وجود دارد	زیاد	بیش از ۷۰ رمزارز
Cook	بالا	دارد	متوسط	برای صندوق‌های فعلی ۵ رمزارز
dHEDGE	متوسط	دارد	زیاد	بیش از ۴۰ رمزارز

فراهم‌کننده نقدینگی برخوردار نیستند. در نتیجه استقبال از این محصولات به ویژگی‌های بلاک‌چین اتریوم بسیار گره خورده است.

مراجع

[1] Chen, Yan, and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *Journal of Business Venturing Insights* 13 (2020): e00151.

[2] School SB, Group A (2019) Direct and indirect investments in Proptech firms by real estate companies worldwide in 2019, by type of technology. Statista.com. <https://www.statista.com/statistics/1128676/cre-real-estate-investment-direct-indirect-proptech-firm-global/>. Accessed 12 October 2020.

[3] Manda, V. Kittu, and Prasada Rao SS, "Blockchain technology for the mutual fund industry," In *National Seminar on Paradigm Shifts in Commerce and Management*, pp. 12-17, 2018.

[4] Nakamoto, Satoshi, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review* (2008): 21260.

[5] Vujičić, Dejan, D. Jagodić, and S. Randić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," In *2018 17th international symposium infoteh-jahorina (infoteh)*, pp. 1-6, IEEE, 2018.

[6] Zheng, Zibin, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems* 105 (2020): 475-491.

[7] Sheikh, Husnara, R. Meer Azmathullah, and F. Rizwan, "Smart contract development, adoption and challenges: the powered blockchain," *International Research Journal of Advanced Engineering and Science* 4, no. 2 (2019): 321-324.

[8] Schär, Fabian., "Decentralized finance: On blockchain- and smart contract-based financial markets." *FRB of St. Louis Review* (2021).

[9] Van Binsbergen, Jules H., Michael W. Brandt, and Ralph SJ Koijen. "Optimal decentralized investment management." *The Journal of Finance* 63, no. 4 (2008): 1849-1895.

[10] Fiergbor, David Doe. "Blockchain technology in fund management." In *International Conference on Application of Computing and Communication Technologies*, pp. 310-319. Springer, Singapore, 2018.

این بدان معنا است که معامله‌گران قادرند بدون نگرانی از لغزش سفارش خود، معامله انجام دهند و مطمئن باشند قیمت معامله شده برای کل استخر، به اندازه قیمت سفارش است.

جدول رتبه‌بندی مدیران، استخرها را بر حسب فرمول زیر رتبه‌بندی می‌کنند.

$$\text{Score} = \text{Sortino Ratio} * \text{SQRT}(7 \text{ Day Average Pool Value})$$

نسبت Sortino بازدهی متناسب با ریسک را اندازه‌گیری می‌کند و از زمان تأسیس استخر محاسبه می‌شود و سالانه تنظیم می‌گردد. بازده هدف در فرمول Sortino روی ۲۰٪ تعیین شده است.

معیار ریسک برای یک استخر تابعی از نوسانات نزولی است که در محاسبه نسبت Sortino نیز مورد استفاده قرار می‌گیرد. معیار ریسک برای استخرهایی که دارای نوسانات نزولی بسیار اندک هستند یک و برای استخرهایی که دارای نوسانات نزولی زیاد هستند ۵ است.

سرمایه‌گذاران می‌توانند با بیشتر از ۴۰ رمزارز پشتیبانی شده توسط Synthetix در استخرها سرمایه‌گذاری کنند. به محض واریز رمزارز، توکن استخر مدنظر به کیف پول آن‌ها واریز می‌شود. این توکن به معنای مقدار سهام سرمایه‌گذار در استخر است. هر زمان که سرمایه‌گذار قصد خروج از استخر و فروش سهام مربوط به آن را داشته باشد، می‌تواند از طریق سایت و ارتباط مستقیم با قرارداد هوشمند پلتفرم این کار را انجام دهد. هر چند به روش‌های دیگر همچون انتقال به کیف پول دیگر یا فروش در صرافی نیز می‌توان سهام استخر را فروخت، اما توصیه می‌شود با این کار به صورت مستقیم توسط قرارداد هوشمند پلتفرم انجام شود.

۴- نتیجه‌گیری و مقایسه

پلتفرم‌های دیگری در بستر بلاک‌چین برای پیاده‌سازی ابزارهای سرمایه‌گذاری غیرمستقیم وجود دارد اما اغلب با تغییر فرمول‌ها بوجود آمده‌اند و تفاوت ساختاری با سه پلتفرم معرفی شده ندارند. بعنوان مثال پلتفرم Peakdefi از نظر ساختاری و دوره‌های سرمایه‌گذاری کاملاً مشابه با Betoken می‌باشد و صرفاً در جزئیات کمی متفاوت است. به همین دلیل بررسی تعداد بیشتر اپلیکیشن را خارج از حوصله این مقاله دیدیم. در جدول ۱ مقایسه کاملی از ویژگی‌های هر پلتفرم ارائه شده است.

سه پلتفرم معرفی شده هر سه به دلیل استفاده از بلاک‌چین اتریوم از مشکلات یکسانی رنج می‌برند که مهم‌ترین آن قیمت بالای gas می‌باشد. قیمت بالای gas سرمایه‌گذاری را در سمت مدیران پرخطر و گران‌تر کرده است و آن‌ها توانایی معاملات با فرکانس بالا را ندارند.

پلتفرم‌های سرمایه‌گذاری غیرمستقیم نیاز بسیاری از سرمایه‌گذاران می‌باشد و بخاطر خصوصیات خاص سرمایه‌گذاری غیرمتمرکز، بسیار مورد توجه قرار گرفته‌اند. اما با توجه به افزایش هزینه‌ها و کارمزدهای بلاک‌چین اتریوم استقبال از آن‌ها رو به کاهش قرار گرفته و ممکن است بسیاری از آن‌ها در سال‌های آینده به فراموشی سپرده شوند. از طرفی بلاک‌چین‌های دیگر نظیر ترون و کاردانو، از ابزارهای مالی غنی همچون صرافی‌های با پشتیبانی از ابزارهای مشتقه و

فرزانه مردوخ روحانی فارغ التحصیل

کارشناسی ارشد سیاست گذاری علم و فناوری از دانشگاه صنعتی شریف است. به عنوان دانشجوی برگزیده ارشد در پژوهشکده سیاست گذاری علم و فناوری شریف برنده گرنت پژوهشی شده که به دلیل علاقه اش، تحقیقات در زمینه فناوری بلاکچین را انتخاب کرده و در چندین نشریه معتبر داخلی مقالاتی را به چاپ رسانده است. در حال حاضر نیز مسیر شغلی خود را در زمینه صنعت آی.تی ادامه داده و در شرکت یکتانت مدیر محصول است.

آدرس پست الکترونیکی ایشان عبارت است از:

farz.mardukh@gmail.com



[11] Blake, David, Alberto G. Rossi, Allan Timmermann, Ian Tonks, and Russ Wermers. "Decentralized investment management: Evidence from the pension fund industry." The Journal of Finance 68, no. 3 (2013): 1133-1178.

[12] Popescu, Andrei-Drăgoș. "Decentralized finance (defi)-the lego of finance," Social Sciences and Education Research Review 7, no. 1 (2020): 321-349.

[13] Werner, Sam M., Daniel Perez, Lewis Gudgeon, Arian Klages-Mundt, Dominik Harz, and William J. Knottenbelt. "Sok: Decentralized finance (defi)," arXiv preprint arXiv: 2101.08778 (2021).

[14] DeFi Pulse, "The decentralized finance leaderboard at defi pulse," 2021. [Online]. Available: <https://defipulse.com/>.

[15] Dune Analytics, "Total DeFi Users Over Time," 2021, [Online]. Available: <https://dune.xyz/>.

[16] DeFi Hacks, "Defi hacks," 2021. [Online]. Available: <https://defihacks.wiki/>.

[17] Betoken White Paper, [online]. Available: <https://github.com/Betoken/Whitepaper/blob/master/BetokenWhitepaper.md>.

[18] Cook White Paper, [online]. Available: <https://www.cook.finance/docs/Whitepaper.pdf>.

[19] dHEDGE White Paper, [online]. Available: <https://docs.dhedge.org/>.

محمد امین فضلی دکتر، کارشناسی ارشد و

کارشناسی خود را در رشته مهندسی کامپیوتر از دانشگاه صنعتی شریف اخذ کرده است. وی پس از گذراندن یک دوره پست دکترا در همین دانشگاه، به عضویت هیئت علمی دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف نائل



شده و هم‌اکنون به عنوان استادیار مشغول به کار است. علاقه مندی های پژوهشی ایشان، شبکه های اقتصادی و اجتماعی، تحلیل داده، طراحی الگوریتم و مهندسی نرم افزار است.

آدرس پست الکترونیکی ایشان عبارت است از:

fazli@sharif.edu

مهدی نقوی فارغ التحصیل رشته

مهندسی کامپیوتر از دانشگاه صنعتی شریف است و ۳ سال در صنعت تکنولوژی مالی، در زمینه معاملات الگوریتمی در بازار بورس سهام و اختیار ایران و



همچنین بازار رمزارز فعالیت دارد.

آدرس پست الکترونیکی ایشان عبارت است از:

amirmehdinaghavi@gmail.com

¹ Trustless

² Crowdfunding

³ Direct and Indirect Investors

⁴ Exchange Traded Fund (ETF)

⁵ Mutual Funds

⁶ Risk Profile

⁷ Copy Trading

⁸ Copier

⁹ Satoshi Nakamoto

¹⁰ Peer to Peer

¹¹ Wallet

¹² Nick Szabo

¹³ Ethereum

¹⁴ Dune Analytics

¹⁵ Ethereum

¹⁶ DeFi

¹⁷ Decentralized Finance Application (DeFi)

¹⁸ Code is law

¹⁹ Staking

²⁰ Open Source

²¹ trustless

²² Pool

²³ Leaderboard

Transparent Distributed Investment in Digital Era Based on Blockchain Technology

MohammadAmin Fazli¹

Mehdi Naghavi¹

Farzaneh Mardookh Rouhani²

¹Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

²Graduate School of Management and Economic, Sharif University of Technology, Tehran, Iran

ABSTRACT

In traditional indirect investment, in all methods we see a big problem called lack of transparency and lack of trust. Investors cannot find completely transparent data to compare funds and portfolios, and it is difficult to trust them. Blockchain technology and smart contracts can meet these challenges. They can create a safe environment for investors by creating trust-free funds, and blockchain technology ensures the transparency of traders' data. In this article, we try to take a step towards the future of investment by examining blockchain technology and protocols like Betoken, Cook and d HEDGE and comparing their performance.

Keywords: Blockchain, Smart Contract, Indirect Investment, Ethereum, Decentralized Finance (De Fi).