

همه چیز درباره دنیای مالی توزیع شده

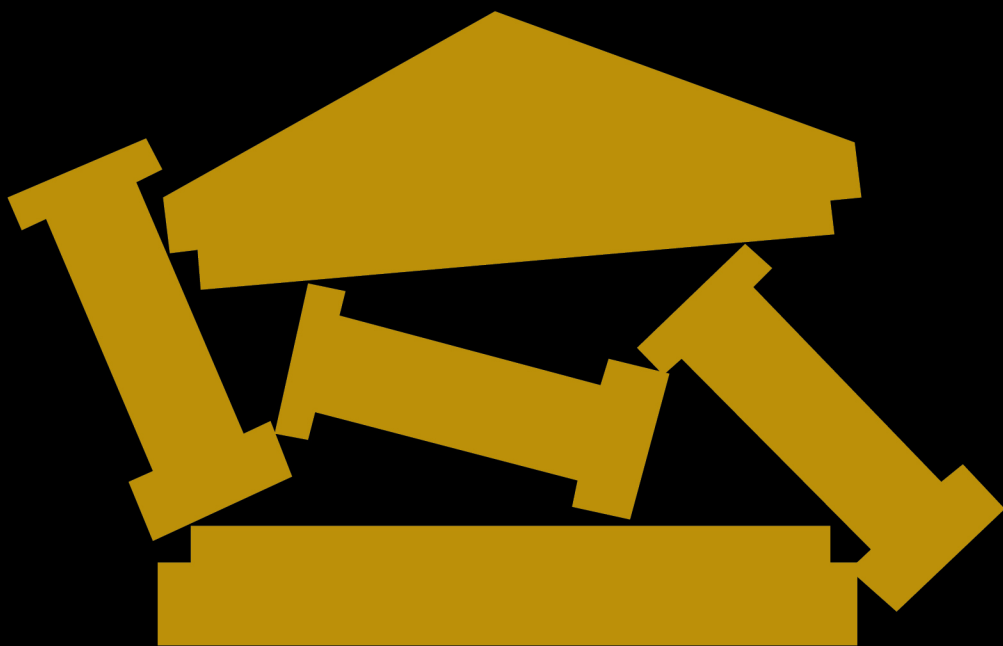
دنیای و آینده فایننس

احمد رفیعی

کمپبل هاروی، آسوین رامانچاندرا، جوئی سانتورو



با مقدمه ویتالیک بوترین خالق اتریوم



فایل نمونه

بِسْمِ اللَّهِ
الرَّحْمَنِ
الرَّحِيمِ



The mark of
responsible forestry
FSC® C009732

سرشناسه: هاروی، کمبل آر. Harvey, Campbell R.
عنوان: دیفای و آینده فایننس، همه چیز درباره دنیای مالی توزیع شده
نویسندگان: کمپبل هاروی، آشوین رامچاندرا، جوئی سانتورو
مترجم: احد درفشی
مشخصات نشر: راه پرداخت
مشخصات ظاهری: ۱۴۴ص
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۸-۷
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: DeFi and the future of finance.
یادداشت: همه چیز درباره دنیای مالی توزیع شده.
عنوان دیگر: همه چیز درباره دنیای مالی توزیع شده.
موضوع: امور مالی
موضوع: Finance
موضوع: بانک و بانکداری مرکزی
موضوع: Banks and banking, Central
شناسه افزوده: رامچاندرا، آشوین
شناسه افزوده: Ramachandran, Ashwin
شناسه افزوده: سانتورو، جوئی
شناسه افزوده: Santoro, Joey
رده بندی کنگره: HG۱۷۳
رده بندی دیویی: ۳۳۲
شماره کتابشناسی ملی: ۸۸۹۴۰۸۶

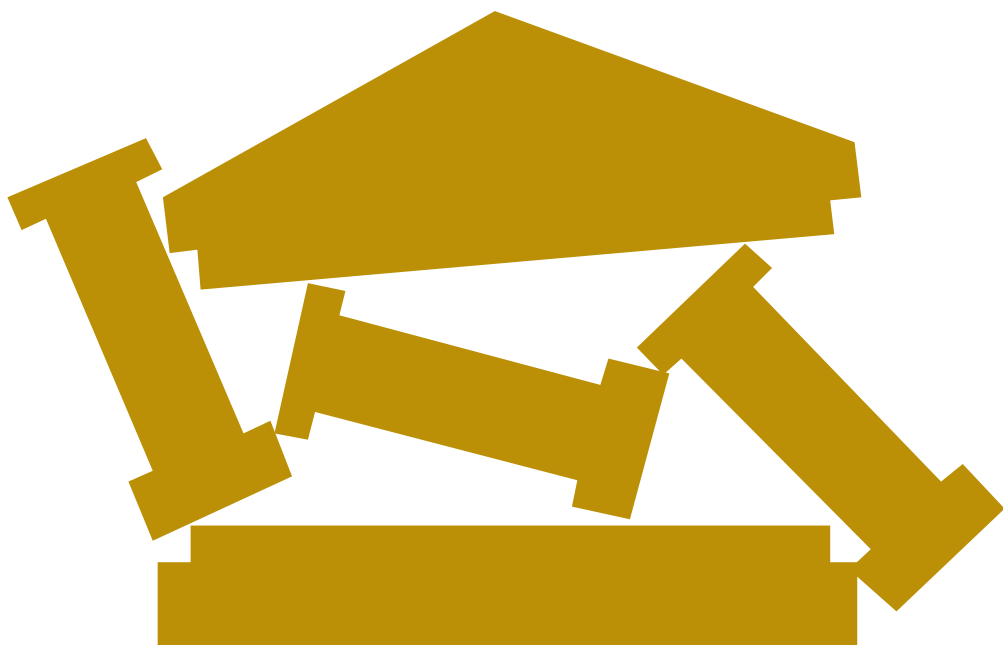
همه چیز درباره دنیای مالی توزیع شده

دنیای و آینده فایننس

احد در فستی

کمپبل هاروی، آشورین راماچاندران، جوئی سانتورو

بامقدمه ویتالیک بوتیرین خالق اتریوم





عنوان: دیفای و آینده فایننس، همه چیز درباره دنیای مالی توزیع شده

ناشر: راه پرداخت

نویسندگان: کمپبل هاروی، آشوین راماجاندران، جوئی سانتورو

مترجم: احد درفشی

ویراستار ارشد: مینا والی

ویراستار محتوایی: قاسم سرافرازی

ویراستار فنی: محدثه گودرزنی

بازبینی نهایی متن: رضا قربانی

صفحه آرا: علیرضا کیوان

ناظر چاپ: قادر شهبازی

نوبت چاپ: اول ۱۴۰۱

شمارگان: ۱۰۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۸-۷

تلفن: ۰۲۱-۴۴۴۳۹۶۶

دورنگار: ۸۹۷۸۴۹۰۲

ایمیل: publisher@way2pay.press

وبسایت: way2pay.press

لایتوگرافی: هنر اشکان

چاپ و صحافی: واژه

همه حقوق چاپ و نشر این اثر برای «انتشارات راه پرداخت» محفوظ است. هرگونه تکثیر، انتشار و بازنویسی این اثر یا قسمتی از آن به هر شکل و شیوه (چاپی، صوتی، ویدئویی، دیجیتال و ...) بدون اجازه کتبی ناشر ممنوع است.

فروشگاه انتشارات راه پرداخت نشانی: تهران، جنت آباد جنوبی، خیابان لاله غربی، روبه روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

۱۷	فصل اول: مقدمه
۱۹	پنج مشکل کلیدی سیستم‌های مالی متمرکز
۲۱	پیامدها
۲۳	فصل دوم: خاستگاه‌های مدرن امور مالی غیرمتمرکز
۲۳	تاریخچه مختصری از امور مالی
۲۴	فین تک
۲۶	بیت کوین و ارز دیجیتال
۲۹	اتریوم و دیفای
۳۱	فصل سوم: زیرساخت دیفای
۳۲	بلاکچین
۳۳	ارز دیجیتال
۳۴	پلتفرم قراردادهای هوشمند
۳۶	اوراکل‌ها
۳۷	استیبل کوین‌ها
۳۹	برنامه‌های غیرمتمرکز
۴۰	فصل چهارم: اصول اولیه دیفای
۴۱	تراکنش‌ها
۴۳	توکن‌های مثلی
۴۷	توکن‌های غیرقابل معاوضه یا غیرمثلی
۴۹	حضانت
۴۹	تنظیم عرضه
۵۴	مشوق‌ها
۵۷	سواپ
۶۰	وام‌های وثیقه‌محور
۶۱	وام‌های فلش یا فوری (بدون وثیقه)

۶۳ فصل پنجم: مسائلی که دیفای قادر است آن‌ها را حل کند

- ۶۴ ناکارآمدی
- ۶۵ دسترسی محدود
- ۶۷ عدم شفافیت
- ۶۸ کنترل متمرکز
- ۶۹ عدم تعامل پذیری

۷۲ فصل ششم: کاوش عمیق در دیفای

- ۷۳ اعتباری/وام‌دهی
- ۹۳ صرافی غیرمتمرکز
- ۱۰۲ مشتقات
- ۱۰۶ dYdX
- ۱۱۶ توکنیزاسیون

۱۲۱ فصل هفتم: ریسک‌ها

- ۱۲۲ ریسک قرارداد هوشمند
- ۱۲۵ ریسک حاکمیتی
- ۱۲۷ ریسک اوراق
- ۱۲۸ ریسک مقیاس‌پذیری
- ۱۳۰ ریسک دکس یا صرافی غیرمتمرکز
- ۱۳۳ ریسک حضانتی
- ۱۳۴ ریسک زیست‌محیطی
- ۱۳۵ ریسک رگولاتوری

۱۳۸ فصل هشتم: نتیجه‌گیری

- ۱۳۸ بازنده‌ها و برنده‌ها

[یادداشت ناشر]

رضا قربانی - انتشارات راه پرداخت

تمرکززدایی در سال‌های اخیر به روندی مهم در دنیای کسب‌وکارها تبدیل شده است. حتی به نظر می‌رسد موضوع این روزها فراتر از کسب‌وکارها است و دامنه تأثیرگذاری آن به اقتصاد، سیاست، اجتماع و فرهنگ هم رسیده است. موضوع تمرکززدایی موضوع جدیدی نیست؛ منتها ابزارهای موردنیاز برای پیاده‌سازی آن در دسترس نبوده است. بلاکچین این فرصت را در اختیار بسیاری از نهادها قرار داد که تمرکززدایی را در عمل به واقعیت تبدیل کنند. یکی از نقاطی که تمرکززدایی مورد توجه جدی قرار گرفت دنیای مالی بود. ترکیب تمرکززدایی، بلاکچین و دنیای مالی، دیفای را خلق کرد. اکنون دیفای به روندی قابل تأمل در دنیای کسب‌وکارهای مالی تبدیل شده است.

اهمیت دیفای از چالش‌هایی می‌آید که دنیای سیستم‌های مالی متمرکز ایجاد می‌کند. همان‌گونه که در این کتاب مهم توضیح داده شده است سیستم‌های متمرکز مسائل زیادی دارد. این مسائل منجر به توسعه سیستم‌های توزیع شده در جهان شده است. زمانی که ریشه‌های سیستم‌های توزیع شده را بررسی می‌کنیم متوجه می‌شویم که دنیای مالی مسیر تکاملی را برای رسیدن به این نقطه طی کرده است. تاریخچه مختصر دنیای مالی، فین‌تک، بیت‌کوین و رمزارزها در نهایت به اتریوم و دیفای رسیده است.

دیفای زیرساخت‌هایی دارد که باید آنها را شناخت؛ بلاکچین، رمزارزها، پلتفرم‌های قرارداد هوشمند، اوراکل‌ها، استیبل‌کوین‌ها و اپلیکیشن‌های توزیع شده زیرساخت‌هایی هستند که دنیای دیفای را می‌سازند. دنیای دیفای ابعاد گوناگونی دارد که شناخت آنها به ما کمک می‌کند بتوانیم از این ساختارها به بهترین شکل استفاده کنیم. نکته مهمی که باید به آن توجه داشته باشیم این است که دیفای قرار است مسائل واقعی را حل کند. در نهایت به دستاوردهایی می‌رسیم که برخی از آنها مواردی مانند تأمین مالی، صرافی‌های رمزارز توزیع شده، مشتقات و توکنیزاسیون بخشی از این دستاوردها هستند.

این دنیا همه‌اش زیبایی و دستاوردهای جذاب نیست. این دنیا ریسک‌های خودش را دارد؛

در این کتاب ۸ ریسک مهم بررسی شده است و از نظر من شاید این بخش مهم‌ترین بخش کتاب است؛ در نهایت این ریسک‌ها مهم‌ترین مواردی هستند که کسب‌وکارهای حوزه دیفای برای آنها باید برنامه روشن داشته باشند.

آن چه که در بحث‌های گوناگون ممکن است مورد غفلت بگیرد همین ریسک‌ها است. هشت ریسکی که در کتاب به آنها اشاره شده مقدمه‌ای است که برای رگولاتوری مطلوب باید به آنها توجه کرد. این ریسک‌ها اگر مورد توجه جدی قرار نگیرد و برای آنها راه کار مناسب نداشته باشیم این به بحران تبدیل می‌شوند.

کتاب «دیفای و آینده فایننس» از انتشارات معتبر وایلی کتابی قابل تأمل برای مسائل امروز ماست. این کتاب از نظر علمی محتوای قابل توجهی دارد و در شرایط امروز به کار می‌آید. در سال‌های گذشته شاهد این بودیم که کسب‌وکارهای حوزه رمزارزها و بلاکچین در کشور پیشرفت‌های قابل قبولی داشته‌اند؛ همین موضوع باعث شده ریسک‌های کسب‌وکارهای این حوزه بیشتر از گذشته مورد توجه قرار گیرد. تصور می‌کنم موج بعدی، رشد کسب‌وکارهای حوزه دیفای است. اهمیت این کتاب این است که بازبانی دقیق و فنی مسائل مهم حوزه دیفای را توضیح داده است.

لازم است از مجموعه صرافای رمزارز رمزینکس که حامی انتشار کتاب شده نیز تشکر کنم. همچنین از آقایان محمدرضا ابراهیمی، مدیر ارشد مالی رمزینکس، افشین حیدرپور و محمدرضا سادات اخوی که زحمت ویراستاری محتوایی بخش‌هایی از کتاب را بر عهده داشتند، کمال تشکر دارم. امیدوارم مطالعه این کتاب به فعالان اقتصادی و کارآفرینان حوزه بلاکچین و رمزارز و به تنظیم‌گران و رگولاتورهای این حوزه کمک کند که تصمیم‌های بهتری بگیرند.

پیش گفتار

DeFi مخفف مناسبی برای عبارت انگلیسی «decentralized finance» است، اما ظرفیت بالقوه آن را آشکار نمی‌کند: سیستم مالی جدیدی که از پایه ساخته شده است. اگرچه امروزه دیفای کوچک است، به سرعت در حال رشد است (البته در زمان نگارش این متن ارزش مالی آن حدود ۱۰ میلیارد دلار است که در مقایسه با سیستم مالی سنتی که ارزشی معادل صدها تریلیون دلار دارد، رقمی کوچک به نظر می‌رسد). احتمالاً توسعه کامل دیفای چندین دهه طول خواهد کشید، با این حال معتقدم دیفای به سیستم مالی اصلی در جهان تبدیل خواهد شد. چرا؟ به این دلیل که دیفای در واقع «اینترنت پول» است. اینترنت بیانگر قدرت شبکه جهانی است و شبکه‌ای باز برای اطلاعات به شمار می‌رود. به نظر می‌رسد در ۴۰ سال آینده ایده چنین شبکه جهانی بازی و شبکه‌هایی مشابه آن برای انتقال ارزش، کاملاً بدیهی به نظر برسد اما امروزه این حقیقت از منظر عموم پنهان مانده است.

مانند هر فناوری جدیدی، رمزارز و سیستم امور مالی غیرمتمرکز جدید (که بر فراز آن ساخته شده)، با دنیای قدیم خود متفاوت خواهد بود. دیفای در مقایسه با سیستم مالی سنتی، بی‌نظیر است، چراکه بدون مجوز، دارای دسترسی باز، جهانی، قابل ترکیب و شفاف است و دیگر نیازی به نهادهای متمرکز جهت فعالیت‌های مالی ابتدایی نیست. در دیفای می‌توانید بانک خود باشید و از طریق کدهای موجود در بلاکچین، اعتبار

دریافت کنید (بدون نیاز به مؤسسه!). با این حال، تعداد کمی از زیرساخت‌های این اکوسیستم ساخته شده‌اند. شاید کمتر از یک درصد (شاید هم کمتر) از مردم جهان به دیفای به عنوان اثری خارق‌العاده نگاه می‌کنند. در حال حاضر اکوسیستم رو به رشد توسعه‌دهندگان در سراسر جهان در حال ساخت شالوده امور مالی آینده است. در شرکت سرمایه‌گذاری رمزارز پارادایم، اغلب از خود می‌پرسیم: «اگر یک جدول تناوبی از عوامل اصلی مالی وجود داشت، تا به امروز کدام یک از آن‌ها ساخته شده و چه چیزهایی برای پر کردن این جدول باقی مانده بود؟» جاهای خالی، فرصتی است برای کارآفرینان.

دیفای هم مانند اینترنت، احتمالاً خدمات مالی را ارزان‌تر، سریع‌تر، ایمن‌تر و شخصی‌سازی‌تر خواهد کرد. اگر یوتیوب به عنوان بستری با مقیاس بزرگ برای انتشار ویدئو رشد کرد به این دلیل بود که هر فردی می‌توانست به صورت رایگان و آسان از آن استفاده و فایل‌های ویدئویی خود را در آن ایجاد کند. به طور مشابه، دیفای برای محصولات مالی چه کاری انجام خواهد داد تا هر فردی بتواند چیزهایی را با هزینه تقریباً صفر ایجاد و از آن‌ها استفاده کند؟

این آینده هنوز رقم نخورده است. این کتاب نگاهی به آینده دارد و شما، به عنوان یک خواننده، قدرت خلق آن را دارید.

فرد ارسام / هم‌بنیان‌گذار کوین بیس

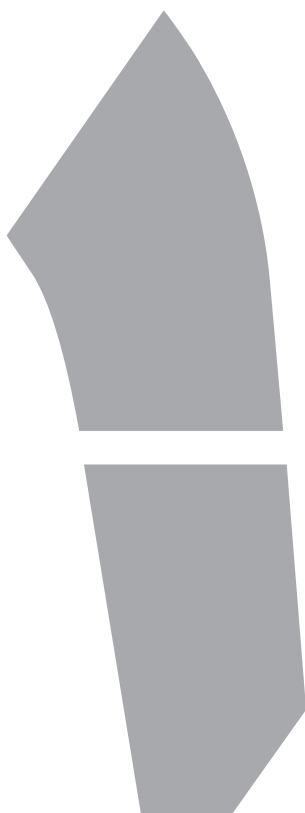
امور مالی غیرمتمرکز (یا دیفای) بخش بزرگی از آن چیزی است که امیدوار بودم افراد بر پایه اتریوم بسازند.

من و بسیاری از افراد دیگر ایده‌هایی درباره مشکلات مربوط به دارایی‌های کاربران، استیبل کوین‌ها، بازارهای پیش‌بینی، صرافی‌های غیرمتمرکز و خیلی موارد دیگر در ذهن داشتیم و سعی کردیم گام بعدی فناوری بلاکچین را برداریم؛ اما برخلاف ایجاد پلتفرمی محدود که مجموعه‌ای از موارد استفاده شناخته‌شده را هدف قرار می‌داد، اتریوم قابلیت برنامه‌ریزی با اهدافی عمومی را معرفی کرد که به قراردادهای مبتنی بر بلاکچین این اجازه را می‌داد تا دارایی‌های دیجیتال را نگه دارند و آن‌ها را طبق قوانینی از پیش تعریف‌شده منتقل و حتی از برنامه‌هایی که مؤلفه‌های مالی ندارند نیز پشتیبانی کنند.

اعضای جامعه اتریوم بلافاصله شروع کردند به کار روی برنامه‌هایی نظیر استیبل کوین‌های آن‌چین (On-chain)، بازارهای پیش‌بینی و صرافی‌ها و فقط پس از گذشت پنج سال اکوسیستم شروع به رشد کرد. به شخصه معتقدم دیفای یک سیستم مالی جدید با کاربری راحت و در دسترس برای جهان خواهد بود. به عنوان مثال، برنامه‌های کاربردی نظیر استیبل کوین‌ها برخی از نوآوری‌های باارزشی هستند که تاکنون از دیفای به دست آمده‌اند. استیبل کوین‌ها این اجازه را به همه می‌دهند تا از مزایای رفع سانسور، خودحاکمیتی و دسترسی جهانی به رمزارزها بهره‌مند شوند و در عین حال از مزیت ثبات دلار نیز بهره ببرند، یا اینکه اگر دلار ثباتش را از دست داد، به سرعت

منابع مالی‌شان را به دارایی‌های دیگر تبدیل کنند و بهترین کار را برای حفظ ثبات انجام دهند. چرا دیفای مهم است؟ سانسور مالی همچنان یکی از مشکلات گروه‌هایی است که به حاشیه رانده شده‌اند، زیرا محدودیت‌ها و سختی‌های تحمیلی اغلب بسیار فراتر از چیزی است که در واقع هر قانونی به آن نیاز دارد و وقتی حباب نسبتاً امن کشورهای توسعه‌یافته را بیشتر بررسی کنیم، این موضوع دوچندان می‌شود. دیفای هزینه آزمایش را تا حد زیادی کاهش می‌دهد و ساخت برنامه جدید را بسیار آسان‌تر می‌کند. قراردادهای هوشمند با کدهای منبع باز تا حد زیادی نیاز به تیم مؤسس را کاهش می‌دهد و باعث مدیریت بودجه می‌شود. دیفای قابلیت «ترکیب‌پذیری» دارد و این امکان را به برنامه‌های جدید می‌دهد که به راحتی و بلافاصله با هر برنامه‌ای که قبلاً وجود داشت، به تعامل برسند. این ویژگی‌ها، پیشرفت‌هایی جدی در قیاس با سیستم مالی سنتی‌اند و به اعتقاد من مواردی هستند که مورد توجه قرار نگرفته‌اند.

نویسندگان کتاب دیفای و آینده فایننس، درباره مزیت‌های بیشتر دیفای در مقایسه با سیستم مالی سنتی بحث و گفت‌وگو کرده‌اند. همچنین نویسندگان این کتاب توضیحات کاملی درباره نحوه کارکرد مهم‌ترین پروتکل‌های دیفای امروزی، نظیر استیبل کوین‌ها، بازارسازهای خودکار و غیره داده‌اند. این کتاب را به هرکسی که به یادگیری پروتکل‌های اتریوم و دیفای علاقه‌مند است توصیه می‌کنم.



فصل اول

مقدمه

به نقطه اول برگشتیم. اولین شکل مبادله در بازار، همتابه‌همتا بود که به آن مبادله یا مبادله کالا به کالا هم می‌گویند. مبادله کالایی، بسیار ناکارآمد بود، چرا که عرضه و تقاضا بین همتایان می‌بایست دقیقاً مطابقت می‌داشت. برای حل مشکل تطابق، «پول» به عنوان وسیله مبادله و حفظ ارزش معرفی شد. انواع اولیه پول، متمرکز نبود. کارگزاران در ازای دریافت کالا، هر تعداد اقلام، نظیر سنگ یا صدف، را می‌پذیرفتند. در نهایت، پول سکه‌ای پدیدار شد؛ شکلی از پول که ارزشی ملموس داشت. امروزه پول فیات را داریم که بانک‌های مرکزی کنترلش می‌کنند. شکل پول در طول زمان تغییر کرده اما زیرساخت‌های اساسی مؤسسه‌های مالی تغییر نکرده است.

با این حال، راه‌حلی برای مشکلات تاریخی‌ای که در زیرساخت فعلی مالی وجود دارند در حال ظهور است؛ دیفای یا امور مالی غیرمتمرکز به دنبال ایجاد و ترکیب بلوک‌های سازنده مالی منبع باز در محصولات پیچیده است که کمترین ناسازگاری و بیشترین ارزش را برای کاربرانی که از فناوری بلاکچین استفاده می‌کنند مهیا کند. از آنجا که ارائه خدمات به مشتری‌ای که دارایی‌اش ۱۰۰ دلار یا ۱۰۰ میلیون دلار است تفاوت هزینه چندانی ندارد، معتقدیم که دیفای جایگزینی برای تمام زیرساخت‌های مالی متمرکز هدفمند در آینده خواهد بود. این یک فناوری مشارکتی است که به موجب آن هرکسی می‌تواند با پرداخت کارمزدی ثابت از آن استفاده کند و از نوآوری‌های دیفای بهره‌مند شود.

دیفای اساساً یک بازار رقابتی از برنامه‌های مالی غیرمتمرکز است که خدمات ابتدایی مالی، نظیر مبادله، پس‌انداز، وام‌دهی و توکنیزاسیون را ارائه می‌دهد. این برنامه‌ها از اثرات شبکه‌ای حاصل از ترکیب و بازترکیب محصولات دیفای و جذب سهم بیشتر بازار از اکوسیستم مالی سنتی بهره می‌برند.

این کتاب تشریح‌کننده مسائلی است که دیفای قادر است آن‌ها را حل کند. این مشکلات عبارت‌اند از کنترل متمرکز، دسترسی محدود، ناکارآمدی، عدم کارایی و شفافیت. سپس چشم‌انداز فعلی و رو به رشد دیفای را توصیف و همچنین چشم‌اندازی از فرصت‌های پیش رو که دیفای ایجاد می‌کند ارائه خواهد کرد. ابتدا با تشریح مشکلات شروع می‌کنیم.

پنج مشکل کلیدی سیستم‌های مالی متمرکز

قرن‌هاست که در دنیای مالی متمرکز زندگی می‌کنیم؛ بانک‌های مرکزی عرضه پول را کنترل می‌کنند، تبادلات مالی عمدتاً از طریق واسطه‌ها انجام می‌شود و استقراض و وام‌دهی از طریق مؤسسه‌های بانکی سنتی صورت می‌پذیرد. با این حال، در چند سال اخیر، پیشرفتی قابل توجه در مدلی به نام امور مالی غیرمتمرکز صورت گرفته است. در این چهارچوب، هم‌تایان از طریق یک دفترکل مشترک با هم‌تایان دیگر در تعامل‌اند و این دفترکل مشترک تحت کنترل هیچ سازمان متمرکزی نیست. در ارتباط با امور مالی متمرکز، دیفای ظرفیتی قابل توجه برای حل پنج مشکل کلیدی ارائه می‌دهد: کنترل متمرکز، دسترسی محدود، ناکارآمدی، عدم کارایی و شفافیت.

۱- کنترل متمرکز. تمرکز، لایه‌های زیادی دارد. اغلب مصرف‌کنندگان و کسب‌وکارها با یک بانک واحد و محلی که نرخ‌ها و کارمزدها را کنترل می‌کند سروکار دارند. تعویض (بانک) امکان‌پذیر است، اما ممکن است پرهزینه باشد. علاوه بر این، سیستم بانکی ایالات متحده بسیار متمرکز است. چهار بانک بزرگ سهم ۴۴ درصدی از سپرده‌های بیمه‌شده را در مقایسه با سهم ۱۵ درصدی در سال ۱۹۸۴ دارند. جالب است که بدانید سیستم بانکی ایالات متحده در مقایسه با سایر کشورها، مانند بریتانیا و کانادا، تمرکز کمتری دارد. در یک سیستم بانکداری متمرکز، بانک مرکزی تلاش می‌کند نرخ بهره کوتاه‌مدت را تعیین کند و بر نرخ تورم تأثیر بگذارد.

این عارضه بیشتر از اینکه به بخش‌های مالی قدیمی برسد، به بازیگران فناوری، نظیر آمازون، فیس‌بوک و گوگل می‌رسد که بر صنایعی مانند خرده‌فروشی و تبلیغات دیجیتال تسلط دارند.

۲- دسترسی محدود. امروزه ۱/۷ میلیارد نفر به بانک دسترسی ندارند و گرفتن وام و فعالیت در دنیای تجارت اینترنتی برایشان بسیار چالش‌برانگیز است. علاوه بر این، بسیاری از مصرف‌کنندگان، برای دسترسی به وام، باید به سیستم وام‌دهی فوری متوسل شوند. با این حال، مشتری بانک بودن به معنی تضمین دسترسی نیست. به عنوان مثال، شاید بانکی نخواهد برای وام کوچکی که کسب‌وکاری جدید به آن نیاز دارد خودش

را به زحمت بیندازد. در عوض، وام کارت اعتباری را پیشنهاد می‌دهد که نرخ بهره سالیانه ۲۰ درصدی دارد (نرخ بازدهی بالا برای یافتن پروژه‌های سرمایه‌گذاری سودآور).

۳- ناکارآمدی. سیستم مالی متمرکز ناکارآمدی‌های زیادی دارد. شاید واضح‌ترین مثال، نرخ مبادله کارت اعتباری باشد که باعث می‌شود مصرف‌کنندگان و کسب‌وکارهای کوچک تا سه درصد از ارزش تراکنش را با هر بار کشیدن کارت به دلیل قدرت قیمت‌گذاری شبکه پرداخت از دست بدهند. کارمزدهای رمیتنس یا انتقال پول بین‌المللی پنج تا هفت درصد است. زمان نیز در دو روزی که برای «تسویه» یک معامله سهام (انتقال رسمی مالکیت) طول می‌کشد تلف می‌شود. در عصر اینترنت، این امر غیرقابل قبول به نظر می‌رسد. ناکارآمدی‌های دیگر عبارت‌اند از انتقال وجه پرهزینه (و کند)، کارمزدهای دلالتی مستقیم و غیرمستقیم، فقدان امنیت و ناتوانی در انجام تراکنش‌های خرد که بسیاری از آن‌ها برای کاربران آشکار نیستند. در سیستم بانکی فعلی، نرخ سود سپرده بسیار پایین و نرخ تسهیلات بالا باقی می‌ماند، زیرا بانک‌ها باید هزینه‌هایشان را پوشش دهند. صنعت بیمه نمونه دیگری در این زمینه است.

۴- عدم کارایی. مصرف‌کنندگان و کسب‌وکارها در محیطی با مؤسسه‌های مالی سروکار دارند که متوازن و عادلانه نیست. کاملاً مشخص است که سیستم مالی ایالات متحده به گونه‌ای طراحی شده که هزینه‌های انتقال پول در آن بالا باشد. انتقال پول از یک مؤسسه به مؤسسه‌ای دیگر می‌تواند بی‌دلیل طولانی و پیچیده باشد. به عنوان مثال، یک انتقال وجه ممکن است سه روز طول بکشد.

در تلاش برای کاهش این مشکل در دنیای مالی متمرکز، در سال ۲۰۱۹ ویزا تلاش کرد پلید (Plaid) را بخرد، محصولی که به شرکت‌ها این امکان را می‌دهد با اجازه کاربر به پشته اطلاعات یک مؤسسه متصل شوند. اگرچه این یک حرکت استراتژیک برای ویزا به جهت استفاده از زمان بود، به مشکلات اساسی زیرساخت مالی فعلی نپرداخت.

۵- شفافیت. سیستم مالی فعلی شفاف نیست. مشتریان در مورد سلامت مالی بانک خود اطلاعات بسیار کمی دارند و در عوض باید به حمایت محدود دولت از بیمه سپرده فدرال (FDIC) روی سپرده‌های خود ایمان داشته باشند. علاوه بر این، برایشان دشوار است که بدانند آیا نرخ‌های وام ارائه می‌شود رقابتی است یا خیر. اگرچه صنعت

بیمه با خدمات فین تک برای یافتن «پایین ترین» قیمت پیشرفت‌هایی کرده است، بازار وام، بسیار تکه‌تکه و متلاشی است. هنوز هم وام‌دهندگان رقیب به دلیل ناکارآمدی سیستم دچار مشکل می‌شوند. در نتیجه پایین ترین قیمت بیمه مربوط به سیستم‌های سنتی و قدیمی و هزینه‌های پشتیبانی بالاست.

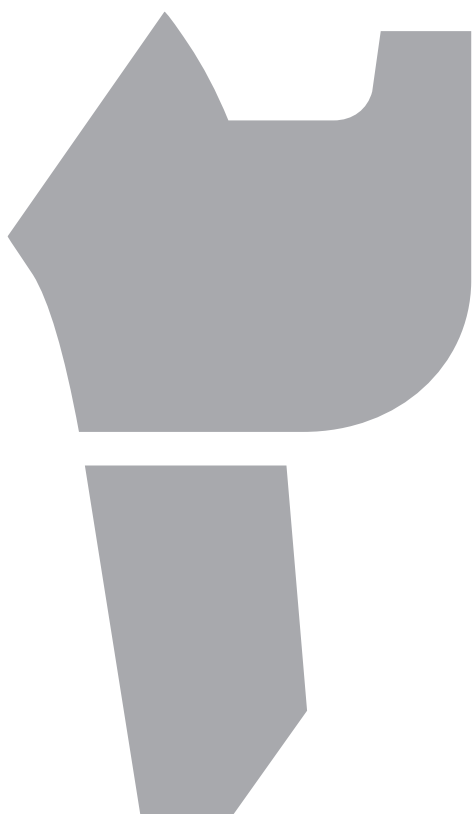
پیامدها

پیامدهای این پنج مشکل به دو قسمت تقسیم می‌شوند: اول اینکه بسیاری از این هزینه‌ها منجر به «کاهش رشد اقتصادی» می‌شوند. به عنوان مثال، اگر نرخ بهره وام به دلیل هزینه‌ها بالا باشد، ممکن است پروژه‌های سرمایه‌گذاری که کیفیت بالایی دارند (همان‌طور که قبلاً توضیح داده شد) کنار گذاشته شوند. کارآفرینی که ایده‌ای با کیفیت دارد، نرخ بازدهی ۲۰ درصدی را هدف قرار می‌دهد (دقیقاً نوعی از پروژه که باعث تسریع رشد اقتصادی است). اگر بانک به کارآفرین بگوید از کارت اعتباری با نرخ بهره سالانه ۲۴ درصدی استفاده کند، ممکن است این پروژه به‌ظاهر سودآور، هرگز دنبال نشود.

دوم، این مشکلات باعث تداوم یا تشدید نابرابری می‌شوند. از منظر سیاسی، اکثر مردم با برابری فرصت‌ها موافق‌اند: یک پروژه باید بر اساس کیفیت ایده و درستی برنامه اجرا تأمین مالی شود و نه بر اساس عوامل دیگر. مهم‌تر از همه، وقتی ایده‌های خوب تأمین مالی نشوند، نابرابری باعث محدود شدن رشد می‌شود. اگرچه ادعا می‌شود ایالات متحده سرزمین فرصت‌هاست، یکی از رکوردهای بسیار بد در انتقال از چارک پایین درآمدی به چارک بالا را دارد. نابرابری فرصت‌ها تا حدی ناشی از عدم دسترسی به سیستم بانکی فعلی، انکاب به تأمین مالی جایگزین پرهزینه، مانند وام‌دهی فوری و ناتوانی در خرید یا فروش در دنیای مدرن تجارت الکترونیکی است.

این پیامدها گسترده‌اند و هر طور که حساب کنیم این فهرست طولانی از مشکلات جدی در سیستم مالی متمرکز فعلی وجود دارد. زیرساخت‌های مالی ما نتوانسته‌اند به‌طور کامل خود را با عصر دیجیتال که در آن زندگی می‌کنیم سازگار کنند. امور مالی غیرمتمرکز فرصت‌های جدیدی را ارائه می‌دهد. این فناوری نوپاست، اما جنبه مثبت آن به‌طور بالقوه تحول‌آفرین است.

این کتاب اهداف متعددی دارد؛ ابتدا نقاط ضعف سیستم فعلی را شناسایی خواهیم کرد، از جمله بحث در مورد برخی ابتکارات اولیه که مدل‌های کسب‌وکار امور مالی متمرکز را به چالش می‌کشند. در مرحله بعد، منشأ مالی غیرمتمرکز را بررسی می‌کنیم. سپس درباره یک جزء حیاتی دیفای به نام فناوری بلاکچین بحث خواهیم کرد. در مرحله بعد، راه‌حلهایی را که دیفای ارائه می‌دهد توضیح می‌دهیم و به‌طور مفصل برخی از ایده‌های پیشرو را که در این فضای نوظهور وجود دارند بررسی می‌کنیم. سپس عوامل اصلی خطر را تجزیه و تحلیل و با نگاهی به آینده، نتیجه‌گیری و سعی خواهیم کرد برندگان و بازندگان این عرصه را شناسایی کنیم.



فصل دوم
خاستگاه‌های مدرن
امور مالی غیر متمرکز



تاریخچه مختصری از امور مالی

حتی در حال حاضر که سیستم مالی امروزی با ناکارآمدی مواجه است، بسیار بهتر از گذشته است، چراکه در آن زمان مبادلات بازار به صورت همتابه همتا صورت می گرفت و انجام مبادلات مستلزم مطابقت دقیق نیازهای دو طرف بود. در این میان، یک سیستم اعتباری غیررسمی در روستاها پدیدار شد که به موجب آن مردم سوابق ذهنی «هدایا» را نگه می داشتند. ضرب سکه مدرن خیلی بعدتر اتفاق افتاد. آنچه ما امروزه به عنوان پول از آن استفاده می کنیم اولین بار حدود ۶۰۰ سال قبل از میلاد در لیدیه ظهور کرد و بدین ترتیب پول فراهم کننده واحد محاسبه، وسیله مبادله و حفظ ارزش شد. از ویژگی های مهم پول می توان به دوام، قابلیت حمل، تقسیم پذیری، یک شکلی، عرضه محدود، مقبولیت و پایداری آن اشاره کرد. اسکناس های بانکی که منشأ آن ها چین است، در قرن سیزدهم به اروپا راه یافتند. انتقال غیرفیزیکی پول در سال ۱۸۷۱ با وسترن یونیون (Western Union) آغاز شد. شکل ۱-۲ یک کپی از انتقال اولیه به مبلغ ۳۰۰ دلار را نشان می دهد. توجه کنید که هزینه این انتقال، ۹/۳۴ دلار یا تقریباً سه درصد بوده است. قابل توجه است که در طول ۱۵۰ سال، تغییر بسیار کمی داشته است.

WESTERN UNION TEL. CO. (Form B.)

TELEGRAPH TRANSFER. No.

RECEIVED of *C.C. Antoine*

Three Hundred

to be paid to *Jas. H. Ingraham*

at *New York*

Dated at *New Orleans Aug 25 1873*

Amount of Transfer, \$ *300.00*

* Premium 1 per cent. *3.00*

Cost of Telegram, *6.34* TOTAL, \$ *309.34*

*No Premium will be less than 25 Cents.

WESTERN UNION
Telegraph Office
AUG 25 1873
37 CENTS DOLLARS, 100

شکل ۱-۲ انتقال پول توسط وسترن یونیون از ۱۸۷۳

دنیاى مالی در ۷۵ سال گذشته اولین‌هاى بسیاری را به خود دیده است: کارت اعتبارى در سال ۱۹۵۰ (داینرز کلاب)، دستگاه خودپرداز در سال ۱۹۶۷ (بانک بارکلیز)، بانکدارى تلفنى در سال ۱۹۸۳ (بانک اسکاتلند)، بانکدارى اینترنتى در سال ۱۹۹۴ (اتحادیه اعتبارى فدرال استنفورد)، پرداخت از طریق شناسايى فرکانس رادىوبى (RFID) در سال ۱۹۹۷ (موبایل اسپیدپس)، کارت‌هاى اعتبارى chip-and-pin در سال ۲۰۰۵ (مسترکارت) و آپل‌پى با دستگاه تلفن همراه در سال ۲۰۱۴ (آپل).

نکته مهمى که در همه این نوآورى‌ها وجود دارد این است که ستون فقرات همه‌شان امور مالی متمرکز است. با وجود پیشرفت‌هاى تکنولوژیکى صورت گرفته، ساختار سیستم بانكى امروزی در ۱۵۰ سال گذشته تغییر چندانى نکرده است و فرایند دیجیتالی شدن در این حوزه روندی کند داشته است. هزینه‌هاى بالایى که این سیستم قدیمى تحمیل کرده است، باعث پیشرفت بیشتر در زمینه‌اى به نام فین تک شد.

فین تک

وقتی هزینه‌ها بالا باشند، نوآورى برای سرمایه‌گذارى روى ناکارآمدى‌ها ظاهر مى‌شود. با این حال گاهى اوقات لایه‌اى از افراد میانی مى‌تواند این فرایند را آهسته کند. نمونه اولیه امور مالی غیرمتمرکز، ۲۰ سال پیش در بازار ارز خارجى (فارکس) ظاهر شد. در آن زمان، شرکت‌هاى بزرگ از بانک‌هاى سرمایه‌گذارى شان برای مدیریت نیازهاى فارکسى خود استفاده کردند. مثلاً شرکتى که در ایالات متحده مستقر است مى‌خواهد در پایان سپتامبر برای کالاهای خریدارى شده در آلمان، ۵۰ میلیون یورو بپردازد. بانک این شرکت، نرخى را برای انجام این معامله اعلام مى‌کند. در همان زمان یکى از مشتریان بانک مى‌خواهد فروشى معادل ۵۰ میلیون یورو در پایان سپتامبر داشته باشد.

بانک نرخى متفاوت را اعلام مى‌کند. این تفاوت نرخ، اسپرید نامیده مى‌شود (سودى که بانک به جهت واسطه بودن کسب مى‌کند). با توجه به بازار چند تریلیون دلارى فارکس، این کار بخش مهمى از سود بانكى را شامل مى‌شد.

در اوایل سال ۲۰۰۱، یک استارت‌آپ فین تکی، ایده زیر را ارائه کرد: به جای اینکه شرکت‌ها به صورت انفرادى شروع کنند به پرس و جو و دریافت بهترین نرخ

از بانک‌های مختلف، چرا یک سیستم الکترونیکی برای خریداران و فروشندگان به صورت مستقیم با قیمت توافقی و بدون اسپرد ایجاد نکنند؟ در واقع، بانک می‌تواند این خدمات را به مشتریان خود ارائه دهد و کارمزدی معقول (در مقایسه با اسپرد) دریافت کند. علاوه بر این، با توجه به اینکه برخی از مشتریان با چندین بانک سروکار دارند، می‌توان مشتریان را در تمام بانک‌های شرکت‌کننده در یک شبکه هم‌تابه همدیگر متصل کرد. برخورد یک بانک را با این نوآوری می‌توانید تصور کنید: «امکان دارد توضیح بدهید که چگونه در یک سیستم الکترونیکی سرمایه‌گذاری کنم که قرار است یک منبع درآمد اصلی من را حذف کند؟» با این حال، حدود ۲۰ سال پیش بانک‌ها متوجه شدند که بزرگ‌ترین مشتریان‌شان از سیستم فعلی بسیار ناراضی‌اند.

مثالی دیگر افزایش معاملات سهام شبکه معاملاتی غیرشفاف (dark pool) است. در سال ۱۹۷۹، کمیسیون بورس و اوراق بهادار ایالات متحده (SEC)، با وضع قانون 19c3 این اجازه را به سهام شرکت‌های فهرست‌شده در بورس داد که همانند اوراق بهادار نیویورک (NYSE) در خارج از بورس نیز معامله شوند. بسیاری از مؤسسه‌های بزرگ، حجم‌های بزرگ معاملاتی‌شان را به این شبکه معاملاتی غیرشفاف منتقل کردند، به طوری که با هزینه‌های بسیار کمتر از معاملات سنتی، معامله هم‌تابه هم‌تابه انجام می‌دادند.

هزینه‌های گزاف تراکنش‌ها باعث ایجاد بسیاری از نوآوری‌ها در زمینه فین‌تک شده‌اند. پی‌پال بیش از ۲۰ سال پیش تأسیس شد و یک پیشرو در فضای پرداخت محسوب می‌شود. در سال ۲۰۱۷، هفت بانک از بزرگ‌ترین بانک‌های ایالات متحده، سیستم پرداخت‌شان به نام Zelle را به سرویس‌های خود اضافه کردند. مهم‌ترین وجه مشترک این پیشرفت‌های فین‌تک که باعث کاهش هزینه‌ها شده این است که همگی به ستون فقرات متمرکز زیرساخت مالی فعلی متکی‌اند.

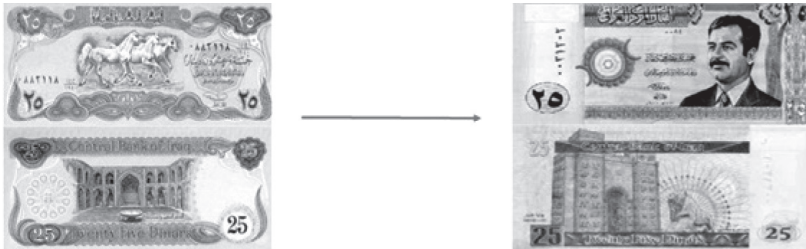
بیت‌کوین و ارز دیجیتال

دهه‌های ابتکاری که در زمینه ارز دیجیتال در اوایل دهه ۱۹۸۰ شروع شدند، همگی شکست خوردند. با این حال انتشار وایت‌پیپر معروف ساتوشی ناکاموتو در باره بیت‌کوین در سال ۲۰۰۸ که سیستمی هم‌تابه هم‌تابه می‌داد که غیر متمرکز بود و از مفهوم بلاکچین

استفاده می‌کرد این چشم‌انداز را تغییر داد. بلاکچین را اولین بار هابر و استورنتا در سال ۱۹۹۱ اختراع کردند. بلاکچین در ابتدا به صورت یک سیستم زمان‌بندی برای پیگیری نسخه‌های مختلف یک سند در نظر گرفته شد. نوآوری کلیدی بیت‌کوین، در ترکیب ایده بلاکچین با سازوکار اجماعی به نام اثبات کار (proof of work) بود (که در سال ۲۰۰۲ معرفی شد). این فناوری با ایجاد دفترکل غیرقابل تغییر، مشکلی را که در دارایی‌های دیجیتال وجود داشت از بین برد. مشکل کلیدی‌ای که دارایی‌های دیجیتال داشتند این بود که امکان دوبار خرج کردن آن‌ها وجود داشت. بلاکچین ویژگی‌های مهمی را که در حفظ ارزش وجود دارند امکان‌پذیر می‌کند، که قبلاً هرگز به طور همزمان در یک دارایی وجود نداشتند. بلاکچین کمیاب است (بیت‌کوین دارای سقف عرضه ثابت ۲۱ میلیون است)، در برابر سانسور مقاوم است، حق حاکمیت کاربر (هیچ نهادی غیر از کاربر نمی‌تواند نحوه استفاده از وجوه را تعیین کند) را به رسمیت می‌شناسد و قابلیت حمل دارد (می‌توان هر مقداری را با کارمزدی پایین به هر کجا ارسال کرد). ترکیب این ویژگی‌ها در یک فناوری واحد، ارزش دیجیتال را به یک نوآوری قدرتمند تبدیل می‌کند.

ارزش پیشنهادی بیت‌کوین مهم است و می‌توان ارزش آن را با ارزش سایر دارایی‌های مالی سنجید. به عنوان مثال، دلار آمریکا (USD) را در نظر بگیرید؛ قبل از اینکه استاندارد طلا در سال ۱۹۷۱ کنار گذاشته شود، پشتوانه آن طلا بود. اکنون تقاضا برای دلار آمریکا از طریق: الف) مالیات، ب) خرید کالاهای ایالات متحده به دلار، ج) بازپرداخت بدهی به دلار است. این سه مورد با همدیگر ارزشی ایجاد می‌کنند که ذاتی نیست، بلکه مبتنی بر شبکه‌ای است که دربرگیرنده اقتصاد ایالات متحده است. انبساط یا انقباض در این اجزا می‌تواند بر قیمت دلار تأثیر بگذارد. علاوه بر این، شوک‌های وارده به عرضه دلار، قیمت آن را در سطح معینی از تقاضا تعدیل می‌کند. فدرال رزرو می‌تواند از طریق سیاست‌های پولی برای دستیابی به اهداف مالی یا سیاسی خود، عرضه دلار را تنظیم کند. تورم، توانایی دلار را برای حفظ ارزش در طول زمان کاهش می‌دهد. شاید فردی نگران تورم سرسام‌آور باشد و این نگرانی منجر به فرار به سمت دارایی‌هایی شود که در برابر تورم مقاوم‌ترند. طلا، به دلیل عرضه محدود، سودمندی ذاتی و قابل اعتماد بودن، ثابت کرده است که پناهگاهی در برابر تورم است. با این حال، با توجه به اینکه ارزش طلا متغیر است، توانایی پوشش

ریسک مالی آن فقط در افق‌های بسیار طولانی تحقق می‌یابد. استدلال برخی بر این است که بیت‌کوین ارزشی «ملموس» ندارد، بنابراین کارآمد نیست. این در حالی است که تقریباً از دو سوم طلای موجود برای ساخت جواهرات و مازاد آن در سخت‌افزارها استفاده می‌شود. طلا ارزشی ملموس دارد. با اینکه دلار آمریکا یک ارز فیات است، به عنوان «پول رایج قانونی» دارای ارزش است. با این حال نمونه‌های تاریخی زیادی وجود دارند که ارزی بدون هیچ پشتوانه‌ای به وجود آمده است. یک نمونه نسبتاً جدید دینار سوئیس عراق است که تا جنگ اول خلیج فارس در سال ۱۹۹۰ واحد پول عراق به حساب می‌آمد. صفحات چاپی در سوئیس تولید (از این رو به آن دینار سوئیس می‌گویند) و برای چاپ به بریتانیا ارسال می‌شدند. در سال ۱۹۹۱، عراق تقسیم شد و کردها کنترل شمال عراق و صدام حسین کنترل جنوب عراق را در دست گرفتند. به دلیل تحریم‌ها، عراق نمی‌توانست دینار را از انگلیس وارد کند و مجبور به تولید داخلی شد. در ماه مه ۱۹۹۳، بانک مرکزی عراق اعلام کرد شهروندان سه هفته فرصت دارند تا ۲۵ دینار قدیمی را با دینار جدید مبادله کنند (شکل ۲-۲) و پس از آن، دینار قدیمی غیرقابل بازخريد خواهد شد.



شکل ۲-۲ دینار سوئیس عراق و دینار جدید

اما همچنان در شمال این کشور از دینار قدیمی سوئیس عراق استفاده می‌شد. در جنوب، دینار جدید دچار تورمی شدید شد. در نهایت، نرخ مبادله یک دینار سوئیس عراق برابر با ۳۰۰ دینار جدید شد. دیدگاه کلیدی در اینجا این است که دینار سوئیس

عراق پشتوانه رسمی نداشت، اما به عنوان پول پذیرفته شد. بدون هیچ ارزش ملموسی ارزشمند بود. نکته مهم این است که ارزش را می‌توان هم از منابع ملموس و هم از منابع ناملموس استخراج کرد.

ویژگی‌هایی از بیت‌کوین که به آن‌ها اشاره کردیم (به‌ویژه کمیابی)، آن را به یک پناهگاه در برابر ناآرامی‌های سیاسی و اقتصادی تبدیل می‌کند. بارشد شبکه، ارزش پیشنهادی فقط به دلیل افزایش اعتماد و نقدینگی افزایش می‌یابد. اگرچه در ابتدا بیت‌کوین به عنوان یک ارز همتا به همتا در نظر گرفته شده بود، ویژگی‌های ضد تورمی و کارمزدهای ثابت آن مانع استفاده از آن در معاملات کوچک شدند. استدلال ما بر این است که بیت‌کوین گل سرسید دارایی‌های جدید (یعنی ارزهای دیجیتال) است که می‌توانند موارد استفاده متفاوتی را بر اساس ساختار شبکه‌ای خود داشته باشند. معتقدیم که بیت‌کوین می‌تواند به عنوان ابزاری برای ذخیره ارزش و یک محافظ در برابر تورم، به رشد خود ادامه دهد.

ارزهای دیجیتال اولیه جایگزینی برای سیستم‌های مالی ای بودند که تحت تسلط دولت‌ها و نهادهای متمرکز، مانند بانک‌های مرکزی، قرار داشتند و قصد داشتند سیستم‌های مالی ناکارآمد را با الگوریتم‌های منبع باز تغییر ناپذیر (بدون محدودیت) جایگزین کنند. این ارزهای جدید می‌توانند پارامترهای خود (مانند تورم و مکانیسم اجماع) را از طریق بلاکچین زیربنایی‌شان جهت ایجاد گزاهای ارزشی متفاوت، مطابقت دهند. بعداً در مورد بلاکچین و ارز دیجیتال مفصل بحث خواهیم کرد، اما در حال حاضر روی یک ارز دیجیتال خاص که ارتباطی ویژه با دیفای دارد تمرکز می‌کنیم.

اتریوم و دیفای

در حال حاضر اتریوم (ETH) دومین ارز دیجیتال بزرگ از نظر ارزش بازار است. ویتالیک بوتیرین این ایده را در سال ۲۰۱۴ معرفی و اتریوم اولین بلوک خود را در سال ۲۰۱۵ استخراج کرد. اتریوم به نوعی توسعه منطقی کاربردهای بیت‌کوین است زیرا امکان ایجاد قراردادهای هوشمند را فراهم می‌کند (قراردادهای هوشمند کدهایی هستند که روی بلاکچین قرار می‌گیرند و قابلیت کنترل داده‌ها و دارایی‌ها را دارند و همچنین تعاملات بین دارایی‌ها، داده‌ها و مشارکت کنندگان شبکه را تعریف می‌کنند). قابلیت قراردادهای

هوشمند، اتریوم را به یک پلتفرم قرارداد هوشمند بدل کرده است. اتریوم و دیگر پلتفرم‌های قرارداد هوشمند، به‌طور خاص باعث ایجاد برنامه‌های کاربردی غیرمتمرکز (decentralized application) یا دی‌آپ شدند. اجزای پشتیبان این برنامه‌ها، با قراردادهای هوشمند و به‌صورت شفاف ساخته شده‌اند و تا زمانی که بلاکچینی وجود داشته باشد، این برنامه‌ها هم‌روی همان بلاکچین وجود خواهند داشت. دی‌آپ‌ها این امکان را به هم‌تایان خود می‌دهند که به‌طور مستقیم با همدیگر تعامل کنند و لزوم وجود یک شرکت به‌عنوان مرکز تسویه حساب مرکزی برای تعاملات برنامه را از میان برمی‌دارند. در این میان دی‌آپ‌های مالی اهمیت فوق‌العاده‌ای پیدا کردند.

حرکت به سمت دی‌آپ‌های مالی به جنبش دیفای تبدیل شد، که به دنبال ساخت و ترکیب زیرساخت‌های مالی منبع باز با محصولات پیچیده است که حداقل ناسازگاری و حداکثر ارزش را برای کاربران داشته باشد. از آنجا که ارائه خدمات مالی به مشتری‌ای که دارایی‌اش ۱۰۰ دلار یا ۱۰۰ میلیون دلار است تفاوت هزینه چندانی ندارد، طرفداران دیفای معتقدند تمام زیرساخت‌های مالی با قراردادهای هوشمند جایگزین خواهند شد و می‌توانند ارزش بیشتری را به گروهی بزرگ‌تر از کاربران ارائه کنند. هرکسی با پرداخت هزینه‌ای ثابت می‌تواند از قرارداد استفاده کند و از نوآوری‌های دیفای بهره‌مند شود. در فصل سوم درمورد پلتفرم‌های قرارداد هوشمند و دی‌آپ‌ها به‌طور مفصل صحبت خواهیم کرد.

دیفای اساساً یک بازار رقابتی از دی‌آپ‌های مالی است که خدمات مالی اولیه، نظیر مبادله، وام‌دهی و توکنیزاسیون را ارائه می‌دهند. این برنامه‌ها از اثرات شبکه‌ای حاصل از ترکیب و بازترکیب محصولات دیفای و جذب سهم بیشتری از بازار در قیاس با اکوسیستم مالی سنتی بهره می‌برند. هدف ما در این کتاب ارائه نمایی کلی از مسائلی است که از طریق دیفای قابل حل هستند و نیز توصیف چشم‌انداز فعلی و در حال رشد دیفای و ارائه چشم‌اندازی از فرصت‌هایی است که دیفای در آینده ایجاد خواهد کرد.



فصل سوم زیرساخت دیفای



در این فصل درباره نوآوری‌هایی که به دیفای منتهی می‌شوند بحث و اصطلاحات رایج در مورد آن‌ها را بیان خواهیم کرد.

بلاکچین

کلید همه برنامه‌های حوزه دیفای این است که شالوده آن‌ها غیرمتمرکز باشد و این کار با بلاکچین امکان‌پذیر است. اساساً بلاکچین‌ها پروتکل‌های نرم‌افزاری هستند و این امکان را برای طرفین فراهم می‌کنند که بدون نیاز به اعتماد، تحت فرضیات و داده‌های مشترک فعالیت کنند. این داده‌ها هر چیزی می‌توانند باشند، نظیر اطلاعات مکانی و مقصد اقلام در زنجیره تأمین یا مانده حساب یک توکن. داده‌ها به صورت «بلوک‌ها» بسته‌بندی و به صورت «زنجیره‌ای» رمزنگاری می‌شوند تا امکان پیگیری سوابق فعالیت‌ها فراهم شود (به همین دلیل است که به آن زنجیره بلوکی یا بلاکچین می‌گویند).

بلاکچین به دلیل پروتکل‌های اجماع، امکان‌پذیر می‌شود (اجماع به مجموعه قواعدی گفته می‌شود که تعیین می‌کند چه بلوک‌هایی به زنجیره اضافه و به واقعیت تبدیل شوند). پروتکل‌های اجماع برای محافظت در برابر دست‌کاری‌های مخرب طراحی شده‌اند و مشخص‌کننده مرزهای امنیتی هستند. اغلب بلاکچین‌های فعلی از پروتکل اجماع اثبات کار استفاده می‌کنند که مبتنی بر میزان محاسبات و انرژی مصرفی است و بر این اساس تعیین می‌کنند که کدام بلوک باید به زنجیره اضافه شود. اگر مهاجمان بخواهند زنجیره‌ای طولانی‌تر بسازند که حاوی تراکنش‌های مخرب باشد، باید از میزان محاسباتی شبکه پیشی بگیرند. برای انجام چنین کاری باید بیشترین توان شبکه (نرخ هش) را در اختیار داشته باشند. از این رو حمله معروف ۵۱ درصدی، مرز امنیتی اثبات کار به حساب می‌آید. خوشبختانه برای هر بازیگری (حتی یک کشور) فوق‌العاده دشوار است که بتواند چنین قدرت شبکه‌ای را برای پرکاربردترین بلاکچین‌ها (نظیر بیت‌کوین یا اتریوم) فراهم کند. حتی اگر بتوان اکثریت توان شبکه را به طور موقت به دست آورد، میزان تاریخچه بلوکی که می‌توان بازنویسی کرد به مدت زمانی که می‌توان این اکثریت را حفظ کرد، محدود می‌شود.

تا زمانی که هیچ گروهی نتواند کنترل اکثریت قدرت محاسباتی شبکه را به دست آورد،

تراکنش‌ها توسط بازیگران خوش نیت پردازش می‌شوند و وقتی بلوکی به‌عنوان بلوک «برنده» انتخاب شد، به دفتر کل (ledger) الحاق می‌شود.

تمرکز ما در اینجا روی اثبات کار است، اما سازوکارهای اجماع دیگری هم به‌عنوان جایگزین وجود دارند که مهم‌ترین آن‌ها اثبات سهام (proof of stake/PoS) است. در سازوکار اثبات سهام، اعتبارسنج‌ها برای تأیید معتبر بودن یک بلوک، مقداری سرمایه (سهام) متعهد می‌شوند و با سهام‌گذاری (staking) ارزش دیجیتال خود، آن را در دسترس قرار می‌دهند، سپس می‌توانند بلوکی را پیشنهاد دهند که باید توسط اعتبارسنج‌های دیگر تأیید شود. اعتبارسنج‌ها، هم با پیشنهاد یک بلوک و هم با تأیید اعتبار بلوک‌های پیشنهادی توسط دیگران، سود می‌برند. میزان محاسبات انجام‌شده توسط اثبات سهام بسیار کمتر است و به انرژی کمتری برای انجام محاسبات نیاز دارد.

ارز دیجیتال

محبوب‌ترین کاربرد فناوری بلاکچین، ارز دیجیتال است. ارز دیجیتال، توکنی است (معمولاً کمیاب) که به‌صورت رمزنگاری محافظت و منتقل می‌شود. کمیاب بودن باعث ارزشمند شدن آن می‌شود و یک نوآوری در زمینه بلاکچین است. به‌طور معمول، اشیای دیجیتالی به‌راحتی کپی می‌شوند. همان‌طور که «اریک اشمیت»، مدیرعامل سابق گوگل، گفت: «بیت‌کوین یک دستاورد رمزنگاری قابل توجه است و توانایی ساخت فناوری‌ای که نتوان یک کپی از آن را در دنیای دیجیتال ایجاد کرد، ارزش بسیار زیادی به آن می‌دهد.» چون از کلید رمزنگاری نامتقارن برای محافظت از حساب‌ها استفاده می‌شود کسی نمی‌تواند بدون داشتن مالکیت حساب مربوطه، تراکنشی ساختگی ارسال کند. یک کلید عمومی دارید که آدرس دریافت توکن‌ها را نشان می‌دهد و یک کلید خصوصی که برای باز کردن قفل حساب و استفاده از توکن‌هایی که تحت مالکیت شما هستند به کار می‌رود. از نمونه مشابه همین نوع رمزنگاری، برای محافظت از اطلاعات و داده‌های کارت بانکی شما هنگام استفاده از اینترنت استفاده می‌شود. یک حساب نمی‌تواند توکن‌های خودش را «دو بار خرج کند» (double spend)، چراکه دفتر کل، موجودی را دائماً حسابرسی می‌کند و تراکنش معیوب مشخص و شفاف نخواهد بود. توانایی جلوگیری از دو بار خرج

کردن بدون وجود یک مرجع مرکزی، مزیت اصلی استفاده از بلاکچین برای حفظ دفترکل را نشان می‌دهد.

مدل اولیه که برای ارزهای دیجیتال مطرح شده، بلاکچین بیت‌کوین است و تقریباً به‌طور انحصاری به‌صورت یک شبکه پرداخت عمل می‌کند که قابلیت ذخیره و معامله بیت‌کوین به‌صورت آنی و بدون سانسور و واسطه در سراسر جهان را دارد. این قابلیت، بسیار ارزشمند است و باعث می‌شود بیت‌کوین ارزش زیادی پیدا کند. اگرچه اثرات شبکه‌ای آن بسیار قوی است، با این حال رقاباتی در حوزه ارزهای دیجیتال وجود دارد که عملکردی پیشرفته‌تر را ارائه می‌دهند.

پلتفرم قرار دادهای هوشمند

یکی از اجزای مهم دیفای، پلتفرم قرارداد هوشمند است که فراتر از شبکه ساده پرداخت (مانند بیت‌کوین) است و باعث افزایش قابلیت‌های این زنجیره می‌شود. اولین نمونه آن، اتریوم است. قرارداد هوشمند قطعه کدی است که می‌تواند داده‌ها و توکن‌های دل‌خواه را در بلاکچینی که به آن تعلق دارد ایجاد و تبدیل کند. همچنین این اجازه را به کاربر می‌دهد که بدون نیاز به اعتماد، قوانین را برای هر نوع تراکنشی اعمال و حتی دارایی‌های کمیاب با عملکردهای خاص ایجاد کند. بسیاری از بندهای قرارداد کسب و کارهای سنتی را می‌توان به یک قرارداد هوشمند منتقل کرد، که نه تنها تک بندهای قرارداد را بررسی می‌کند، بلکه به‌صورت الگوریتمی نیز اجرا می‌شود. قراردادهای هوشمند فراتر از مسائل امور مالی اند و در بازی‌های رایانه‌ای، مدیریت داده و زنجیره تأمین نیز می‌توان از آن‌ها استفاده کرد.

اتریوم برای هر تراکنشی کارمزدی به نام گس (Gas) دریافت می‌کند، مانند این می‌ماند که برای رانندگی باید بنزین بزنید و هزینه‌ای بابت بنزین پرداخت کنید. اتریوم را همانند رایانه‌ای غول‌پیکر با تعداد زیادی اپلیکیشن (یعنی قراردادهای هوشمند) تصور کنید. برای استفاده از این رایانه، باید برای هر واحد محاسبه‌ای که انجام می‌شود مبلغی پرداخت کنید. برای انجام یک محاسبه ساده مانند ارسال اتر دست‌کم چند کار کوچک باید انجام دهید تا موجودی حساب‌ها به‌روز شود، بنابراین کارمزد گس آن نسبتاً کم

است. محاسبات پیچیده‌تر، مانند ضرب (تکثیر) سکه و بررسی شرایط مختلفی که در بسیاری از قراردادها وجود دارند، به گس بیشتری نیاز دارد و در نتیجه کارمزد بیشتری هم خواهد داشت. با این حال کارمزدهای بالای گس ممکن است به تجربه کاربری ناامیدکننده‌ای منجر شوند، چراکه این عمل کارگزاران را مجبور می‌کند برای پرداخت هزینه گس، موجودی اتر را نگه دارند که این امر به نگرانی‌هایی در زمینه پرداخت بیش از حد مقدار گس، یا پرداخت مبلغ کمتری از هزینه گس یا عدم انجام تراکنش منجر می‌شود؛ بنابراین راهکارهایی برای حذف کارمزد گس از تراکنش‌های مصرف‌کنندگان نهایی در حال ظهورند؛ برخی از زنجیره‌های رقیب مفهوم گس را به‌طور کامل حذف کرده‌اند.

با این حال، گس یک سازوکار اولیه برای جلوگیری از حملات سیستمی است که حلقه نامحدودی از کد تولید می‌کند. شناسایی کدهای مخرب از این نوع قبل از اجرای آن‌ها امکان‌پذیر نیست، در علم کامپیوتر به چنین مسائلی «مسئله توقف» (the halting problem) می‌گویند. فرض کنید خودرویی در حالت اتوپیلوت است و کنترل‌کننده بنزین آن گیر کرده و راننده‌ای ندارد. بنزین به‌عنوان عاملی محدودکننده عمل می‌کند: خودرو در نهایت با خالی شدن باک بنزین متوقف می‌شود. به همین روش، کارمزد گس، باعث هزینه‌بر بودن حملات می‌شود و امنیت بلاکچین اتریوم را تضمین می‌کند. همچنین قراردادهای هوشمندی که بسیار کارآمد باشند را تشویق می‌کند، زیرا قراردادهایی که از منابع کمتری استفاده می‌کنند و احتمال عدم موفقیت کاربر را کاهش می‌دهند، شانس بسیار بیشتری برای استفاده و موفقیت در بازار دارند.

این امکانات باعث گسترش سریع یک پلتفرم قرارداد هوشمند می‌شوند و آن را فراتر از آنچه توسعه‌دهندگانی که مایل به ادغام برنامه‌های مختلف هستند، قرار می‌دهد. این کار به پذیرش رابط‌های استاندارد برای عملکردهای مختلف منجر می‌شود. در اتریوم، این استانداردها «درخواست اتریوم برای نظرات» (Ethereum Request for Comments /ERC) نامیده می‌شوند. شناخته‌شده‌ترین آن‌ها معرف انواع مختلفی از توکن‌هاست که رفتاری مشابه دارند. ERC-20 استاندارد برای «توکن‌های قابل تعویض» یا «توکن‌های مثلی» و رابطی برای توکن‌هایی است که

واحدهای آن‌ها از نظر کاربردی و عملکردی یکسان‌اند. همچنین شامل خصوصیات نظیر انتقال واحدها و تأیید اپراتورها برای استفاده از بخش خاصی از موجودی کاربر است. استاندارد دیگر، ERC-721 معروف به توکن «غیرقابل تعویض» یا «غیرمثلی» (NFT) است. این توکن‌ها منحصر به فرد است و اغلب برای کلکسیون یا دارایی‌هایی نظیر وام‌های همتا به همتا مورد استفاده قرار می‌گیرد. مزیتی که این استانداردها دارند در این است که توسعه‌دهندگان برنامه می‌توانند کدی را برای یک رابط بنویسند و از هر توکنی که آن رابط را پیاده‌سازی کرد، پشتیبانی به عمل بیاورند. بعداً در مورد این رابط‌ها به‌طور مفصل بحث خواهیم کرد.

اوراکل‌ها

مشکل جالبی که در پروتکل‌های بلاکچین وجود دارد این است که از دنیای خارج از دفترکل اطلاعی ندارند. به این معنا که بلاکچین اتریوم فقط از اتفاقاتی که داخل بلاکچین اتریوم رخ می‌دهد آگاه است و اطلاعاتی در مورد شاخص S&P 500 یا اینکه کدام تیم برنده مسابقه قهرمانی فوتبال آمریکایی (سوپربول) شده است ندارد. این محدودیت، برنامه‌ها را به قراردادهای توکن‌های بومی اتریوم محدود می‌کند و در نتیجه کاربرد پلتفرم قرارداد هوشمند را محدود می‌کند. همه این مسائل به نام «مسئله اوراکل» (oracle problem) شناخته می‌شوند. در زمینه پلتفرم‌های قرارداد هوشمند، اوراکل منبع داده‌ای برای گزارش اطلاعات خارج از بلاکچین به شمار می‌رود. چطور می‌توان اوراکلی ایجاد کرد که اطلاعات برون‌زنجیره را به‌طور معتبر و به روشی با حداقل اعتماد بیان کند؟ بسیاری از برنامه‌ها به یک اوراکل نیاز دارند و پیاده‌سازی‌ها درجات مختلفی از متمرکز بودن را نشان می‌دهند. در برنامه‌های مختلف دیفای، چنین پیاده‌سازی‌هایی از اوراکل وجود دارد. یک رویکرد رایج این است که برنامه کاربردی، خودش اوراکل خودش را میزبانی کند یا اینکه به یک پلتفرم قابل اعتماد به اوراکل وصل شود. پلتفرمی مبتنی بر اتریوم به نام «چین‌لینک» (Chainlink) برای حل این مشکل اوراکل طراحی شده است که از انبوهی از منابع داده استفاده می‌کند. وایت‌پیپر چین‌لینک سیستم مبتنی بر اعتبار را پیشنهاد کرده است. بعداً در مورد مسئله اوراکل به‌طور مفصل بحث خواهیم کرد. مطمئناً اوراکل‌ها یک سؤال

بازو چالشی برای دیفای به حساب می‌آیند تا بتوانند کاربرد این حوزه را فرای زنجیره خود ببرند.

استیبل کوین‌ها

یکی از کاستی‌های اساسی در بسیاری از ارزهای دیجیتال، وجود نوسانات بیش از حد در آن‌هاست. این مسئله، ناسازگاری‌هایی را برای کاربرانی به وجود می‌آورد که مایل‌اند از برنامه‌های دیفای استفاده کنند، اما تحمل ریسک برای دارایی‌های بی‌ثباتی مانند اتر را ندارند. برای حل این مشکل، استیبل کوین‌ها به وجود آمده‌اند. به عنوان مثال، استیبل کوین‌ها با هدف حفظ برابری قیمت با برخی از دارایی‌های هدف، نظیر دلار یا طلا، ثبات لازم را برای سرمایه‌گذارانی که به دنبال استفاده از برنامه‌های دیفای هستند فراهم می‌کنند و یک راه‌حل برای خروج از موقعیت‌های پرنوسان دارایی‌های دیجیتال به شمار می‌روند. سازوکاری که باعث حفظ ثبات استیبل کوین‌ها می‌شود با توجه به پیاده‌سازی‌های شان متفاوت است. سه سازوکار اصلی عبارت‌اند از: استیبل کوین‌هایی با پشتوانه فیات، استیبل کوین‌هایی با پشتوانه رمزارز و استیبل کوین‌هایی بدون پشتوانه. در حال حاضر بزرگ‌ترین دسته از استیبل کوین‌ها دارای پشتوانه فیات هستند. این دسته از استیبل کوین‌ها پشتوانه دلاری در خارج از زنجیره دارند و معمولاً توسط یک نهاد خارجی یا گروهی از نهادها نگهداری می‌شوند تا برای تأیید وجود پشتوانه، تحت حسابرسی قرار بگیرند. بزرگ‌ترین استیبل کوین با پشتوانه فیات، تتر یا یواس‌دی‌تی (USDT) با ارزش بازار ۶۲ میلیارد دلار است که در زمان نگارش این کتاب آن را به سومین ارز دیجیتال بزرگ پس از بیت‌کوین و اتریوم تبدیل کرده است. تتر همچنین بالاترین حجم معاملات را در بین ارزهای دیجیتال دارد. یواس‌دی‌سی (USDC) دیگر استیبل کوینی است که دارایی دلاری آن به‌طور منظم حسابرسی می‌شود. هر یواس‌دی‌سی معادل یک دلار است و بالعکس و در صرافی کوین‌بیس بدون کارمزد قابل تبدیل است. USDT و USDC برای ادغام در پروتکل‌های دیفای بسیار محبوب‌اند زیرا تقاضا برای فرصت‌های سرمایه‌گذاری در حوزه استیبل کوین‌ها زیاد است. با این حال تا زمانی که این استیبل کوین‌ها به صورت متمرکز کنترل می‌شوند و حق بلوکه کردن

حساب‌های کاربران را دارند، استفاده از آنها با ریسک همراه است.

دومین دسته بزرگ از استیبل کوین‌ها با پشتوانه رمزارز هستند، به این معنی که با مقدار بیشتری از حد وثیقه توسط ارز دیجیتال دیگری پشتیبانی می‌شوند. ارزش آن‌ها با توجه به سازوکارشان می‌تواند کم‌وبیش به دارایی‌های پایه وابسته باشد. در زمان نگارش این متن، دای (DAI) محبوب‌ترین استیبل کوینی است که پشتوانه رمزارزی دارد و ارزش بازار آن پنج میلیارد دلار است و توسط میکردائو (MakerDAO) ایجاد شده و پشتوانه آن اتر و دیگر دارایی‌های کریپتویی است. در فصل ششم به‌طور مفصل درمورد میکردائو و دای بحث خواهیم کرد. یکی دیگر از استیبل کوین‌هایی که پشتوانه رمزارز محبوبی دارد، اس‌یواس‌دی (sUSD) است. از مزایای استیبل کوین‌هایی که پشتوانه رمزارز دارند، عدم تمرکز و داشتن پشتوانه ایمن است. مشکلی که وجود دارد مقیاس‌پذیری محدود آن‌هاست. برای ضرب استیبل کوین بیشتر، کاربر با ایجاد پوزیشن بدهی بیشتر از وثیقه، از صدور آن حمایت می‌کند. در برخی موارد، مانند دای، سقف بدهی بیشتر باعث محدود شدن رشد عرضه می‌شود.

آخرین و شاید جالب‌ترین دسته استیبل کوین‌ها، استیبل کوین‌های بدون پشتوانه یا الگوریتمی هستند. این استیبل کوین‌ها هیچ دارایی پایه‌ای به‌عنوان پشتوانه ندارند و اغلب از یک مدل حق مالکیت با گسترش الگوریتمی و کاهش عرضه به ثبات قیمت نزدیک می‌شوند و دارندگان توکن در این نوع پلتفرم‌ها، با افزایش تقاضا، پذیرای افزایش عرضه هستند. هنگامی که تقاضا کاهش می‌یابد و قیمت پایین می‌آید، این پلتفرم‌ها اوراق قرضه را به‌شکلی منتشر می‌کنند که قبل از اینکه دارندگان توکن سهم خود را دریافت کنند، به دارنده آن حق عرضه انبساطی در آینده را بدهند. استیبل کوین بیسیس (basis) که به دلیل موانع رگولاتوری به کار خود خاتمه داد، از جمله نمونه‌های استیبل کوین‌های بدون پشتوانه به شمار می‌رود. نمونه‌های کنونی استیبل کوین‌های الگوریتمی عبارت‌اند از آمپل‌فورس (Ampleforth) و امپتی‌ست‌دالر (Empty Set Dollar). مشکلی که در استیبل کوین‌های غیروثیقه‌ای وجود دارد این است که فاقد ارزش ذاتی‌اند و پشتوانه‌ای برای مبادله توکن‌هایشان نیستند. در دوران رکود، این کار می‌تواند به هجوم برای تبدیل این استیبل کوین‌ها به دارایی با ارزش دیگری منجر

هیچ ندیده‌ای هنوز

انتشارات **راه پرداخت**

برای سفارش اینترنتی این کتاب به وبسایت انتشارات راه پرداخت مراجعه کنید

way2pay.shop

همان طور که بسیاری رمزارزها را آینده پول می دانند، می توان «دیفای» را نیز آینده امور مالی یا همان فایننس در نظر گرفت. نویسندگان کتاب «دیفای و آینده فایننس» نیز همین عقیده دارند و چشم انداز فایننس کنونی را در حال فروپاشی توصیف می کنند و خبر از انقلابی در این حوزه می دهند. انقلابی که طی آن دست بانک ها و مؤسسه های مالی غول پیکر از معاملات مالی قطع خواهد شد و پروتکل های نوآورانه و الگوریتم ها نقش های اصلی را در این حوزه ایفا خواهند کرد. صحبت از چنین انقلابی شاید اکنون اغراق آمیز باشد؛ چرا که ارزش اکوسیستم دیفای در حال حاضر به زحمت به ۱۰ میلیارد دلار می رسد و در مقایسه با سیستم مالی سنتی که صدها تریلیون دلار ارزش دارد، چندان به چشم نمی آید. اما از نظر نویسندگان این کتاب، ما در ابتدای راه این انقلاب هستیم و شاید چندین دهه باید بگذرد تا این دگرگونی عظیم به معنای واقعی کلمه رخ دهد. نویسندگان در این کتاب رویکردی واقع گرایانه را در پیش گرفته اند و علاوه بر اینکه کارکردهای دیفای در فایننس را بر شمرده اند و از مزایای آن سخن گفته اند، به مسائل و مشکلات این فناوری نیز پرداخته اند و تأکید کرده اند که اگر برای این مسائل راه حل هایی پیش بینی نشود، همه چیز به شکست خواهد انجامید.

ISBN 978-622-7702-18-7



۱۱۰ هزار تومان

انتشارات راه پرداخت

ناشر فناوری و نوآوری

way2pay.press