

باسمه تعالی



گزارش پروژه زنجیره بلوکی

رمزنگاری پیشرفته

دکتر سلماسی زاده

اعضای گروه:

پوریا دادخواه

کیخسرو خسروانی

ابوالفضل یوسفی

پروژه انتخابی:

صرافی غیرمتمرکز (DEX)

UniSwap

## فهرست مطالب

معرفی تجارت غیرمتمرکز و کاربردها

صرافی های غیرمتمرکز و اهداف آن ها

معرفی پروژه uniswap و طرز کار کلی

توضیح مدل سیستمی پروژه

ساختار پیاده سازی پروژه و قراردادهای هوشمند آن

امنیت پروژه و نتایج بررسی های audit آن

جزئیات رمزگذاری های استفاده شده در پروژه

کارهای آینده و ایده های بهبود پروژه

## معرفی تجارت غیرمتمرکز و کاربردها

با ظهور بلاک چین و فناوری غیر متمرکز و ورود قراردادهای هوشمند به آن‌ها، قابلیت ایجاد برنامه‌های متنوع زیادی با اهداف مختلف بر یک بستر غیرمتمرکز به وجود آمد که باعث شد سازمان‌ها، برنامه‌ها و سرویس‌های زیادی که دارای مشکلات جدی متمرکز بودن داشتند در این چارچوب پیاده شوند. یکی از این دسته‌ها، تجارت غیرمتمرکز یا Decentralized Finance (DeFi) است که سرویس‌های تجاری مانند صرافی‌های غیرمتمرکز، بازارهای مالی و بورس، توکن‌های خرید و فروش اجناس (NFT) هستند که نسبت به مدل‌های متمرکز خود که به یک نهاد خارجی وابسته‌اند فواید زیادی دارند که مهم‌ترین‌ها را میتوان اشاره کرد:

- هزینه‌های کمتر: پلتفرم‌های DeFi معمولاً به دلیل حذف واسطه‌ها، کارمزد کمتری نسبت به موسسات مالی سنتی دارند.
- شفافیت بیشتر: تراکنش‌های روی بلاک چین عمومی و شفاف هستند که به کاربران اجازه می‌دهد یکپارچگی سیستم را تأیید کنند.
- افزایش دسترسی: DeFi برای هر کسی که به اینترنت متصل است باز است و کاربران می‌توانند از هر کجای دنیا به خدمات مالی دسترسی داشته باشند.
- کنترل بیشتر بر وجوه: کاربران بدون نیاز به واسطه، کنترل کاملی بر وجوه خود دارند.

با این حال، DeFi دارای معایبی نیز است، از جمله:

- عدم قطعیت نظارتی: فقدان وضوح نظارتی می‌تواند منجر به عدم اطمینان و ریسک برای سرمایه‌گذاران شود.
- خطرات امنیتی: پلتفرم‌های DeFi در برابر هک‌ها و سوء استفاده‌ها آسیب‌پذیر هستند و تغییرناپذیری تراکنش‌های بلاک چین می‌تواند بازبایی وجوه از دست رفته را دشوار کند.
- موانع فنی: پیمایش پلتفرم‌های DeFi برای کاربران غیر فنی ممکن است دشوار باشد، که می‌تواند دسترسی آنها را محدود کند.

برخی از پروژه‌های مهم در فضای DeFi و اهداف آنها به شرح زیر می‌باشد:

- **Uniswap**: یک صرافی غیرمتمرکز است که بر روی بلاک چین اتریوم کار می‌کند. هدف آن ارائه یک روش ساده و کارآمد برای تجارت توکن‌های ERC-20 بدون نیاز به واسطه است. Uniswap از یک سیستم بازارساز خودکار (AMM) برای تسهیل معاملات و تشویق ارائه دهندگان نقدینگی برای عرضه نقدینگی به پلتفرم استفاده می‌کند.
- **Aave**: یک پلتفرم وام‌دهی غیرمتمرکز است که به کاربران امکان می‌دهد بدون نیاز به واسطه، ارزهای دیجیتال را قرض کنند و وام دهند. هدف آن فراهم کردن دسترسی کاربران به خدمات وام‌دهی شفاف، ایمن و غیرمتمرکز است.
- **Compound: Compound**: یک پلت فرم غیرمتمرکز وام‌دهی است که به کاربران اجازه می‌دهد از دارایی‌های ارزهای دیجیتال خود سود کسب کنند. هدف آن ارائه راه کارآمدتر و شفاف‌تر به کاربران برای کسب درآمد غیرفعال از دارایی‌هایشان است.
- **MakerDAO**: یک پلتفرم غیرمتمرکز است که به کاربران اجازه می‌دهد تا استیبل‌کوین‌ها را ایجاد و مدیریت کنند، که ارزهای دیجیتالی هستند که با ارزش دارایی‌های دنیای واقعی مرتبط هستند. هدف آن ارائه راهی پایدار و مطمئن برای نگهداری و انتقال ارزش به کاربران است.

## صرافی های غیرمتمرکز و اهداف آنها

پس از معرفی کلی تجارت غیرمتمرکز اکنون به یکی از شاخه های آن که صرافی غیرمتمرکز است می پردازیم.

DEX یا صرافی غیرمتمرکز نوعی از صرافی ارزهای دیجیتال است که به صورت غیرمتمرکز و بدون نیاز به واسطه یا مقامات مرکزی برای تسهیل معاملات فعالیت می کند. برخلاف صرافی های متمرکز (CEX) که برای مدیریت دفتر سفارش و مطابقت با خریداران و فروشندگان به یک اپراتور مرکزی متکی هستند، DEX ها از مدل های سازنده بازار خودکار (AMM) یا مکانیسم های غیرمتمرکز دیگر برای فعال کردن معاملات همتا به همتا (peer to peer) استفاده می کنند.

علاوه بر این، DEX ها با هدف ارتقای شفافیت و باز بودن در اکوسیستم ارزهای دیجیتال هستند. با کار بر روی یک شبکه بلاک چین غیرمتمرکز، DEX ها یک دفتر کل عمومی ارائه می کنند که به کاربران امکان می دهد صحت و یکپارچگی معاملات و تراکنش ها را تأیید کنند.

DEX ها برای برطرف کردن چالش های پیاده سازی غیرمتمرکز و غیرمعمولتر یک صرافی و ارائه خدمات مشابه صرافی های سنتی از یکسری ابزارهای کلید استفاده می کنند که در ادامه به توضیح مختصر برخی مهم ترین ابزارها می پردازیم:

سازندگان بازار خودکار خودکار یا AMM ها (Automated market makers): نوعی مدل صرافی غیرمتمرکز هستند که از «ربات های پول» الگوریتمی استفاده می کنند تا خرید و فروش دارایی های رمزنگاری شده را برای معامله گران فردی آسان کنند و قیمت یک ارز دیجیتال را بر اساس عرضه و تقاضای آن تعیین می کنند. به جای معامله مستقیم با افراد دیگر مانند یک دفتر سفارش سنتی، کاربران مستقیماً از طریق AMM معامله می کنند.

بازار سازان نهادهایی هستند که وظیفه دارند نقدینگی یک دارایی قابل معامله را در بورس می که ممکن است غیر نقد شونده باشد، فراهم کنند. بازارسازان این کار را با خرید و فروش دارایی ها از حساب های خود با هدف کسب سود، اغلب از اسپرد انجام می دهند - شکاف بین بالاترین پیشنهاد خرید و کمترین پیشنهاد فروش. فعالیت تجاری آنها باعث ایجاد نقدینگی می شود و تاثیر قیمت معاملات بزرگتر را کاهش می دهد.

قراردادهای هوشمند: DEX ها معمولاً در یک شبکه بلاک چین مانند اتریوم کار می کنند و از قراردادهای هوشمند برای خودکار سازی فرآیند معاملات استفاده می کنند. قراردادهای هوشمند برنامه هایی هستند که بر روی بلاک چین اجرا می شوند و با استفاده از قابلیت اجرای برنامه های سطح بالا مانند solidity که Turing complete هستند به صورت توزیع شده در نودهای مختلف شبکه اجرا شده و به طور خودکار معاملات را بر اساس قوانین و شرایط از پیش تعریف شده اجرا کنند.

اوراکل های غیرمتمرکز: DEX ها اغلب از اوراکل های غیرمتمرکز برای ارائه اطلاعات دقیق قیمت ارزهای دیجیتال استفاده می کنند. اوراکل ها خدماتی هستند که قراردادهای هوشمند مبتنی بر بلاک چین را با منابع داده خارج از زنجیره مانند فید قیمت ارزهای دیجیتال یا سایر شبکه های بلاک چین متصل می کنند.

کیف پول: DEX ها برای تسهیل معاملات به کیف پول های ارز دیجیتال کاربران متکی هستند. کاربران معمولاً کیف پول خود را به پلتفرم DEX متصل می کنند تا معاملات را فعال کنند و این پلتفرم برای انجام معاملات با کیف پول تعامل می کند.

پروتکل های تعاملی: برخی از DEX ها از پروتکل های قابلیت همکاری برای فعال کردن تجارت زنجیره ای استفاده می کنند. این پروتکل ها به کاربران اجازه می دهد تا ارزهای دیجیتال را در شبکه های مختلف بلاک چین مانند اتریوم و بیت کوین معامله کنند.

در آخر باید به چالش ها و نقاط ضعف کلی این نوع صرافی ها در مقابل صرافی های عادی اشاره کنیم که علاوه بر نقاط ضعف کلی سامانه های Defi که در بخش قبل به آن اشاره شد به صورت اختصاصی می توان به این موارد نیز اشاره کرد:

نقدینگی: DEX ها اغلب نقدینگی کمتری نسبت به CEX دارند، که می تواند خرید یا فروش ارزهای دیجیتال با قیمت مورد نظر را دشوارتر کند. این به این دلیل است که DEX ها به جای یک اپراتور متمرکز، به کاربران برای ارائه نقدینگی به پلتفرم متکی هستند.

اجرای آهسته تر: DEX ها ممکن است زمان تراکنش های کندتری نسبت به CEX داشته باشند، به خصوص در زمان های تقاضای بالا. این به این دلیل است که DEX ها برای پردازش تراکنش ها به شبکه بلاک چین متکی هستند که تایید آن ممکن است بیشتر از تراکنش های روی یک پایگاه داده متمرکز طول بکشد.

جفت های معاملاتی محدود: DEX ها ممکن است انتخاب محدودتری از جفت های معاملاتی در مقایسه با CEX داشته باشند، که می تواند معامله با ارزهای دیجیتال کمتر محبوب یا خاص را دشوارتر کند.

پیچیدگی: DEX ها ممکن است منحنی یادگیری تندتری داشته باشند و استفاده از آنها پیچیده تر از CEX ها باشد، به خصوص برای کاربران مبتدی ارزهای دیجیتال.

کارمزدهای بالاتر: DEX ها ممکن است در مقایسه با CEX ها کارمزد بالاتری داشته باشند، به خصوص برای کاربرانی که نیاز به تجارت حجم زیادی از ارزهای دیجیتال دارند. این به این دلیل است که DEX ها برای پردازش تراکنش ها به هزینه های گاز پرداختی به شبکه بلاک چین متکی هستند که در زمان تقاضای بالا می تواند گران باشد.

پس از آشنایی با ساختار کلی صرافی های غیرمتمرکز به بررسی ساختار uniswap می پردازیم.

## معرفی پروژه uniswap و طرز کار کلی

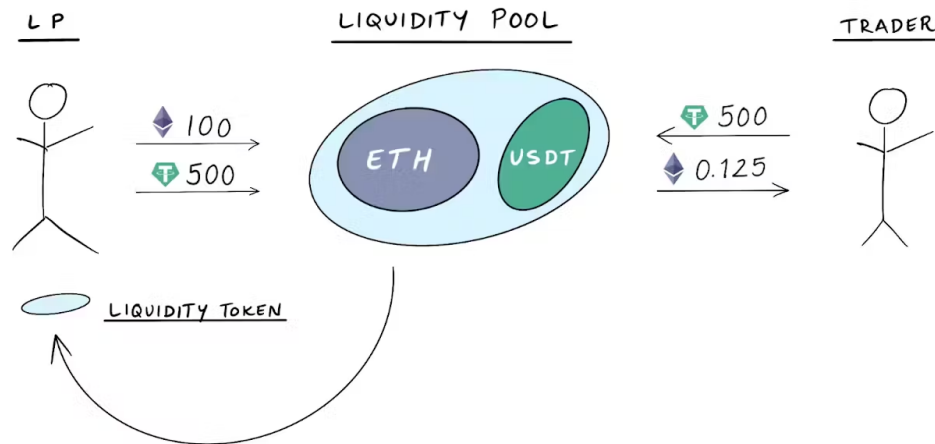
پروتکل Uniswap مجموعه ای از قراردادهای هوشمند است که با هم یک AMM ایجاد می کنند. Uniswap همچنین یک رابط وب ایجاد کرد که به پروتکل Uniswap متصل می شود و دارای یک سیستم حاکمیتی مبتنی بر توکن UNI است که دارندگان توکن UNI دارای قدرت رای برای Uniswap توزیع شده به نسبت موجودی UNI کاربر هستند.

برخلاف صرافی های متمرکز که از کتاب های سفارش برای تجارت بین خریداران و فروشندگان استفاده می کنند، Uniswap از استخرهای نقدینگی استفاده می کند. ارائه دهندگان نقدینگی (LPs) توکن ها را به یک استخر نقدینگی سپرده گذاری می کنند و با کارمزدی که هنگام انجام معاملات سایر کاربران ایجاد می شود، پاداش دریافت می کنند. معامله گران هنگام انجام معاملات، کارمزدی را به ارائه دهندگان استخر نقدینگی می پردازند. Uniswap هزینه ای برای لیست توکن ها دریافت نمی کند و نیازی به ثبت نام کاربر ندارد.

کد Uniswap منبع باز است و می توان آن را برای ایجاد صرافی های جدید فورک کرد. یک پروژه قابل توجه مبتنی بر Uniswap اما با توکن و سیستم حاکمیتی متفاوت، Sushiswap است که در آگوست 2020 راه اندازی شد.

اکوسیستم Uniswap دارای سه نوع کاربر است: ارائه دهندگان نقدینگی، معامله گران و توسعه دهندگان.

## HOW UNISWAP WORKS (BASICALLY)



ارائه دهندگان نقدینگی (LPs) تشویق می شوند که توکن های ERC-20 را به استخرهای نقدینگی مشترک با پتانسیل کسب کارمزد و سایر مشوق های نقدینگی کمک کنند. آنها در قراردادهای هوشمند Uniswap توکن هایی را برای دور زدن نقدینگی یا قفل کردن ارائه می کنند و با توکن های نقدینگی که نشان دهنده مشارکت آنها در استخر نقدینگی است، پاداش می گیرند. توسعه دهندگان می توانند از صرافی های غیرمتمرکز (DEX)، مانند Uniswap، برای راه اندازی توکن های جدید به صورت خودکار در حالی که غیرمتمرکز هستند، استفاده کنند. صدها برنامه، ابزار و کیف پول غیرمتمرکز مالی (DeFi) از Uniswap، از جمله پروژه های محبوب مانند Aave، inch1، و Compound استفاده می کنند. دارایی، مالیه، سرمایه گذاری.

رقبایی مانند Sushiswap و Coinbase پلتفرم‌های وام دهی، لانچرهای سکه و پلتفرم‌های NFT را ارائه می‌کنند که ممکن است Uniswap در آینده آنها را ادغام کند. در ژوئن 2022، یونی‌سواپ Genie، یک گردآورنده بازار NFT را خریداری کرد.

Uniswap تاکنون 3 ورژن از پروژه را منتشر کرده که به طور مختصر تحولات آن را در هر مرحله و بهبودهای صورت گرفته را بررسی می‌کنیم:

## نسخه 1

Uniswap v1 اولین بار در نوامبر 2018 در شبکه اصلی اتریوم راه اندازی شد. Uniswap v1 فقط از جفت‌های تجاری ETH-ERC20 پشتیبانی می‌کرد، بنابراین کاربران فقط می‌توانستند ETH را با یک توکن ERC-20 تعویض کنند. به عنوان مثال، اگر شخصی می‌خواست USDC را با DAI مبادله کند، باید USDC را با ETH تعویض می‌کرد و سپس به استخر ETH-DAI می‌رفت تا ETH را با DAI تعویض کند. برای انجام معاملات بین دو دارایی در Uniswap v1 معمولاً باید دو سواپ انجام شود که منجر به کارمزد و لغزش بیشتر می‌شود.

برای کاربران در مقایسه با یک تعویض. Uniswap v2 اجازه داد تا معاملات با استفاده از یک سواپ هدایت شوند و هزینه‌های بیش از حد لغزش و گاز پرداختی توسط کاربران در Uniswap نسخه 1 را حذف کرد.

Uniswap v1 همچنین مفهوم توکن‌های ارائه دهنده نقدینگی را معرفی کرد. هر ارائه‌دهنده نقدینگی مقداری توکن LP متناسب با درصد نقدینگی که به استخر نقدینگی اضافه می‌کند، دریافت می‌کند. همه توکن‌های LP نشان دهنده دارایی هستند که با تسهیل معاملات در پروتکل با ارائه نقدینگی، کارمزدی را در Uniswap ایجاد می‌کند. همه توکن‌های LP نشان‌دهنده کمک LP به استخر هستند و می‌توان آن‌ها را فروخت، معامله کرد، یا سوزاند تا توکن‌های سپرده‌شده را بازخرید کرد. علاوه بر این، هر معامله در Uniswap هزینه معاملاتی 0.3 درصدی را به همراه داشت و به‌طور خودکار به عنوان پاداشی برای LPهایی که نقدینگی ارائه می‌کردند، ارسال می‌شد.

## نسخه 2

Uniswap v2 در می 2020 راه اندازی شد. با معرفی استخرهای نقدینگی ERC20-ERC20 در Uniswap v1 بهبود یافت. پس از راه اندازی Uniswap نسخه 2، شخصی که می‌خواهد USDC را با DAI مبادله کند، می‌تواند در صورت وجود استخر USDC-DAI، USDC را مستقیماً با DAI تعویض کند، به جای اجرای دو مبادله از USDC-ETH و سپس از ETH-DAI با استفاده از Uniswap v1.

علاوه بر این، Uniswap v2 یک اوراکل قیمت یا ابزاری را که برای مشاهده اطلاعات قیمت در مورد یک دارایی استفاده می‌شود، معرفی کرد. میانگین قیمت یک دارایی را در یک دوره بلوکی قیمت میانگین وزن زمانی یا (TWAP) با تقسیم قیمت انباشته بر طول مدت زمان محاسبه می‌کند. این اوراکل‌های قیمت یک جزء حیاتی برای بسیاری از برنامه‌های مالی غیرمتمرکز، از جمله موارد مربوط به مشتقات، وام، معاملات حاشیه و بازارهای پیش‌بینی هستند.

Uniswap v3 در ماه مه 2021 راه اندازی شد و نسبت به Uniswap v2 بهبود یافته است. Uniswap v3 معرفی می کند:

نقدینگی متمرکز، به هر LP کنترل دقیقی بر محدوده قیمتی که سرمایه آنها تخصیص داده می شود، و

چندین ردیف کارمزد، به LPها اجازه می دهد تا به طور مناسب برای پذیرش درجات مختلف ریسک، جبران شوند.

Uniswap v3 همچنین روی بلاک چین های لایه 2 از جمله Polygon، Arbitrum و Optimism علاوه بر اتریوم راه اندازی شد. Uniswap V3 اوراکل قیمت خود را بهبود بخشید و ادغام آن را در برنامه ها و خدمات آسان تر و ارزان تر کرد.

نسخه 3 به LP ها سه سطح کارمزد جداگانه ارائه می دهد - 0.05٪، 0.30٪، و 1.00٪. LP هایی که از Uniswapv3 استفاده می کنند انعطاف پذیری بیشتری در حاشیه ریسک خود دارند. سطوح کارمزد کمتری برای موقعیت های با ریسک کمتر، مانند استیبل کوین ها، و سطوح کارمزد بالاتر برای موقعیت های پرخطرتر، جفت توکن های غیرهمبسته، انتظار می رود.

Uniswap v3 همچنین دارای هزینه های پروتکل مشابه Uniswap v2 است. کارمزدها به طور پیش فرض خاموش می شوند، اما می توانند توسط حاکمیت بر اساس هر استخر روشن شوند و بین 10 تا 25 درصد هزینه های LP تعیین می شوند.

علاوه بر این، مجوز Uniswap v3 به روزرسانی شد به طوری که ممکن است کد برای دو سال در پاسخ به فورک Sushiswap برای استفاده تجاری فورک نشود. تیم Uniswap بیانیه عمومی زیر را در مورد تصمیم به روزرسانی مجوز تجاری خود اعلام کرد.

در آخر پیش از بررسی دقیق و جزئیات پروتکل و قراردادهای شمشند آن، به بررسی بازار uniswap و حجم معاملات آن می پردازیم:

#### مشتری

مشتریان Uniswap شامل توسعه دهندگان، معامله گران و ارائه دهندگان نقدینگی هستند. توسعه دهندگان برنامه ها و ادغام های DeFi را بر اساس پروتکل Uniswap توسعه می دهند، معامله گران با استفاده از Uniswap ارزش های رمزنگاری شده مختلف را مبادله می کنند، و ارائه دهندگان نقدینگی در معاملات Uniswap کارمزد ایجاد می کنند. فراتر از توسعه دهندگان، معامله گران و ارائه دهندگان نقدینگی، Uniswap همچنین جامعه کاربران، توسعه دهندگان، طراحان و مربیان را از طریق رسانه های اجتماعی تقویت می کند. آنها از دیسکورد، توییتر، ردیت و انجمن حکومتی Uniswap برای موفقیت پروتکل Uniswap استفاده می کنند.

#### اندازه بازار

دو عامل اصلی تعیین کننده اندازه بازار برای Uniswap وجود دارد. اولین مورد TVL in DeFi و توانایی DeFi برای دور کردن سهم بازار از محصولات مالی سنتی است. این ثانیه تعداد تراکنش هایی است که در DeFi مربوط به Uniswap انجام می شود. نمودار زیر مقدار قفل شده در DEX های محبوب را از جولای 2020 تا اگوست 2022 نشان می دهد.





## Value Locked in DEXs



Source: [The Block](#)

## DeFi TVL

از سپتامبر 2022، بازار اتریوم دیفای حدود 16 میلیارد دلار TVL دارد.

آرتم تولکاف، بنیانگذار و مدیر عامل BondAppetit و سرمایه گذار DeFiHelper، معتقد است که بازار DeFi می تواند بیش از 100 برابر اندازه خود نسبت به ارزش بازار 240 میلیارد دلاری خود در نوامبر 2021 تا سال 2026 رشد کند.

DeFi به طور بالقوه می تواند سهم بازار را از امور مالی سنتی بگیرد زیرا مردم به ایمنی قراردادهای هوشمند اعتماد می کنند. در سال 2021، صنعت بانکداری مصرفی در سطح جهان 2.3 تریلیون دلار و بازار سرمایه 121 تریلیون دلار تخمین زده شد. تا ژوئن 2022، کل ارزش بازار شرکت های دولتی در سراسر جهان 105 تریلیون دلار برآورد شده است. اگر پروتکل های DeFi با برداشتن سهم بازار از محصولات مالی سنتی به رشد خود ادامه دهند، در آن صورت Uniswap احتمالاً شاهد افزایش قابل توجهی در بازار آدرس پذیر آن خواهد بود.

## تراکنش های دیفای

عامل دیگری که بر اندازه بازار Uniswap تأثیر می گذارد، علاوه بر افزایش TVL DeFiand DeFi که سهم بازار را از محصولات مالی سنتی دور می کند، تعداد فزاینده تراکنش هایی است که در Uniswap انجام می شود. هرچه تراکنش های بیشتری در DeFi و از طریق Uniswap انجام شود، اندازه بازار بالقوه Uniswap بزرگ تر می شود، زیرا تراکنش های بیشتر منجر به کسب ارزش Uniswap از طریق کارمزدهایی می شود.

دو عاملی که بر تعداد فزاینده تراکنش ها و انباشت ارزش در Uniswap تأثیر می گذارند، فعالیت ربات و سایر محصولات DeFi هستند که بر روی Uniswap ساخته شده اند.

## فعالیت ربات

هرچه افراد بیشتری در DeFi شرکت کنند، توسعه دهندگان را به سمت ایجاد ربات های بیشتری سوق می دهد که قادر به انجام خدمات از طرف کاربران هستند مانند معاملات آربیتراژ، ترکیب خودکار موقعیت نقدینگی، و بسیاری از اقدامات دیگر. در ژوئن

2022، 50.2 درصد از کل معاملات در Uniswap توسط ربات‌های حداکثر قابل استخراج (MEV) و 21.3 درصد دیگر از معاملات توسط «افراد ناشناس» که مشکوک به ربات هستند انجام شد.

پروتکل‌هایی با استفاده از Uniswap

DeFi شامل بسیاری از قراردادهای هوشمند جداگانه است که بر روی عملکردهای قراردادهای هوشمند دیگر برای ایجاد محصولات جدید و محصولات پیچیده‌تر DeFi ساخته شده است. یک تشبیه رایج برای توصیف DeFi این است که پروتکل‌ها/قراردادهای هوشمند DeFi مانند بلوک‌های لگو هستند که توسعه‌دهندگان می‌توانند آن‌ها را به هر طریقی که می‌خواهند برای ایجاد محصولات مالی پیچیده‌تر جمع‌آوری کنند. به عنوان مثال، پروتکل‌های محبوب مانند Curve Finance یک (DEX) و Compound Finance یک پلتفرم وام دهی قراردادهای هوشمندی دارند که توسط پروتکل‌های دیگر بر روی آنها ساخته شده است. Convex بر روی Curve Finance برای افزایش پاداش برای سهامداران CRV و ارائه دهندگان نقدینگی ساخته شده است، و Yearn Finance بر روی Compound Finance برای تجمع بازده و ترکیب خودکار ساخته شده است.

سه نمونه از پروژه‌هایی که در بالای Uniswap برای بهینه سازی بازده برای تامین کنندگان نقدینگی و صرفه جویی در زمان برای کاربران ساخته می‌شوند عبارتند از Popsicle Finance، Gelato Network و Mellow Protocol. پروژه‌ها همچنین بر روی Uniswap ساخته شده‌اند تا با ارائه DEXaggregators با قابلیت مسیریابی معاملات، معاملات را برای کاربران خود بهینه کنند. از طرف کاربران برای دریافت بهترین قیمت‌ها. چهار پروژه قابل توجه با استفاده از Uniswap برای بهینه سازی معاملات برای کاربران خود عبارتند از x0، Cowswap، Paraswap و 1inch. در ژوئن 2022، فعالیت Uniswap از جمع‌آوری کننده‌های DEX حدود 12 درصد از کل فعالیت تجاری در Uniswap را به خود اختصاص داد.

## توضیح مدل سیستمی پروژه

Uniswap یک pool توزیع شده برای مبادله رمز ارز هست (ERC20 token) به کاربرها اجازه می‌دهد که دو رمز ارز را با یکدیگر در اینجا تبادل کنند.

به این صورت که مثلاً یک فرد به نام liquidity provider از هر رمز ارز مثلاً A و B دارد و یک liquidity pool می‌سازد. حال مثلاً اگر کاربر Alice بخواهد رمزارز خود که از A هست را به B تبدیل کند در این pool این کار را انجام می‌دهد و 0.3% کارمزد برای انجام آن می‌پردازد. به این ترتیب معاملات انجام می‌شود و liquidity provider سود می‌برد.

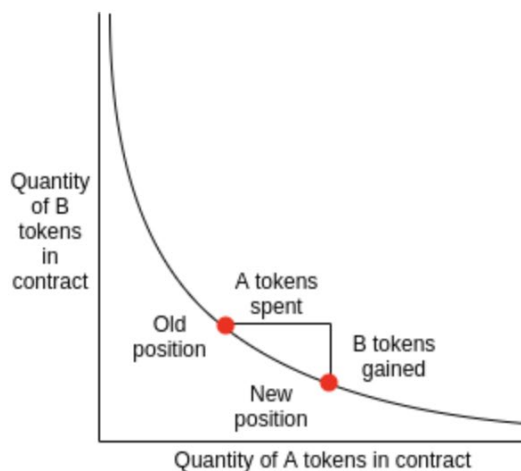
این پروتکل روی بلاک Ethereum قرار دارد و در سال 2018 به وسیله Hyden Adams ساخته شده است.

از Uniswap و AMM استفاده می‌کند که مدل قدیمی central order book را حذف می‌کند. Central order book نیاز به یک نهاد سوم شخص دارد که هر فرد به او بگوید چه مقدار از رمز ارز خود را به چه قیمت می‌خرد/می‌فروشد و آن نهاد افراد را به هم وصل می‌کند.

در این مدل قیمت گذاری از یک رابطه ساده تبعیت می‌کند

Constant product automated market maker

$$x * y = k$$



For larger horizontal movements (coins spent) there are diminishing returns to the vertical movement (coins received).

که x مقدار coin نوع اول و y مقدار coin نوع دوم است. مثلاً فرض کنید این pool برای Doge coin-Shiba باشد و LP مقدار x از Shiba و y تا از Doge coin در pool قرار می‌دهد.

حال چند سوال پیش می آید :

- (1) چگونه قرار است pool با  $xy=k$  کار می کند
- (2) اگر کل کوین های یکی از انواع تمام شود یا کم شود چه؟

برای پاسخ به سوال اول بیایید ببینیم محاسبات مقدار ارز مبادله شده و ارزش هر ارز بعد از تغییر مقدار هر ارز موجود در pool چگونه محاسبه می شود؟

یا به عبارت بهتر رابطه  $xy = k$  چگونه کار می کند.

این طرح یک constant value AMM است که مبنای کار uniswap می باشد.

فرض کنید در یک pool در ابتدا 50000 تا ارز A و 50000 تا ارز B داریم و ارزش هردو هم برابر است.

حال یک نفر درخواست مبادله 7000 تا از ارز B با ارز A را داشته باشد.

انگاه با کمک رابطه  $xy=k$  چون k ثابت است مقدار A نهایی را محاسبه می کنیم و با تفاضل از A کنونی مقدار A لازم برای برقراری این مبادله را حساب می کنیم.

$$57000 * x_A = 2500000000 = 50000 * 50000$$

$$x_A = 43859.65$$

$$50000 - 43859.65 = 6140.35 = \Delta x_A$$

پس ما 7000 تا از ارز B را با 6140.35 تا از ارز A مبادله می کنیم.

حال بررسی می کنیم که قیمت های نهایی در pool کنونی چند می شود:

قیمت اولیه هر دو در ابتدا با هم برابر و برابر 1 دلار بوده است.

قیمت ارز A حاصل :

$$\frac{\text{initial amount}}{\text{final amount}} * \text{initial price} = \text{final price}$$

$$\frac{50000}{43859.65} * 1 = 1.1399$$

پس قیمت جدید ارز A 1.1399 هست

قیمت ارز B :

$$\frac{50000}{57000} * 1 = 0.877$$

پس قیمت جدید ارز B 0.877 هست.

روند بالا نحوه محاسبه مقادیر لازم برای مبادله و قیمت های نهایی پس از مبادله در uniswap را بیان می کند.

جواب به سوال دوم راحت است پایداری این مدل بر مبنای equilibrium point هست  
یعنی مثلاً فرض کنید یک مقدار زیادی Doge coin را با shiba عوض کند در نتیجه مقدار آن کم و قیمت آن زیاد می شود و مقدار shiba زیاد و قیمت آن کم می شود. حال اگر قیمت shiba در این pool از قیمت shiba در بازار معاملات واقعی کمتر باشد افرادی برای کسب سود shiba را از این pool ارزان تر خریداری می کنند و در بازار اصلی می فروشند و این خرید و فروش را ادامه می دهند تا قیمت در این pool با قیمت در بازار اصلی یکی شود که نقطه حاصل همان نقطه equilibrium point است.

این کار سه فایده برای pool دارد :

- (1) قیمت ارز ها در pool با قیمت ارز ها در بازار اصلی برابر می شود
- (2) قیمت ارز ها در این pool به خاطر خاصیت equilibrium point دنبال کنند قیمت ها در بازار اصلی است و این oracle یک آرایه دهنده قیمت خوب برای دیگر مدل ها و smart contract ها هست.
- (3) پراکندگی دو رمز ارز متعادل می شود.

در اینجا ممکن است بگوییم liquidity provider ضرر کرده است زیرا مقداری از ارزهای خود را ارزان تر از قیمت بازار اصلی فروخته است. به این ضرر اسمی Impermanent loss گویند .

حال آیا واقعا ضرر کرده است؟

بیایید چک کنیم:

در ادامه یک مثال از نحوه کارکرد ریاضیات مدل uniswap را می بینیم.

فرض کنید یک liquidity provider به یک pool 50/50 که هنوز مقداری در آن تزریق نشده است به مقدار ارزش برابر از دو رمز ارز را تزریق کند:

قیمت DAI را 1 دلار و ETH را 500 دلار در نظر می گیریم

پس اگر او 10000 تا DAI و 20 تا ETH تزریق کند به هر دو رمز ارز مقدار ارزش برابر 10000 را داده است.  
در این صورت

$$x = 20, \quad y = 10000, \quad xy = 200000 = k$$

حال فرض کنید قیمت ETH در دنیای واقعی به 550 بالا رود.

افرادی برای سود کردن ETH با قیمت 500 را در اینجا با DAI مبادله می کنند تا قیمت ETH به 550 برسد:  
بعد از رسیدن قیمت ETH به 550 مقدار های نهایی هر کوین به صورت زیر است:

DAI تا 10988.9

ETH تا 19.07

پس مقدار 0.93 تا ETH را با 488.09 تا DAI مبادله کرده است.

جمع ارزش ها در ابتدا 20000 بوده و در الان با مقادیر جدید و قیمت های جدید جمع ارزش به 20976.59 رسیده است. حال دیده می شود در اینجا liquidity provider مقدار 976.59 دلار سود کرده است ولی اگر دارایی خود را pool نمی کرد مقدار  $10000 + 20 * 550 = 21000$  می داشت که با مقایسه با دارایی الان که 20976.59 بوده 23.41 دلار ضرر کرده است به این ضرر *impermanent loss* گویند.

که تازه بخشی از آن ضرر با fee دریافت کرده از مبادله پوشانده می شود

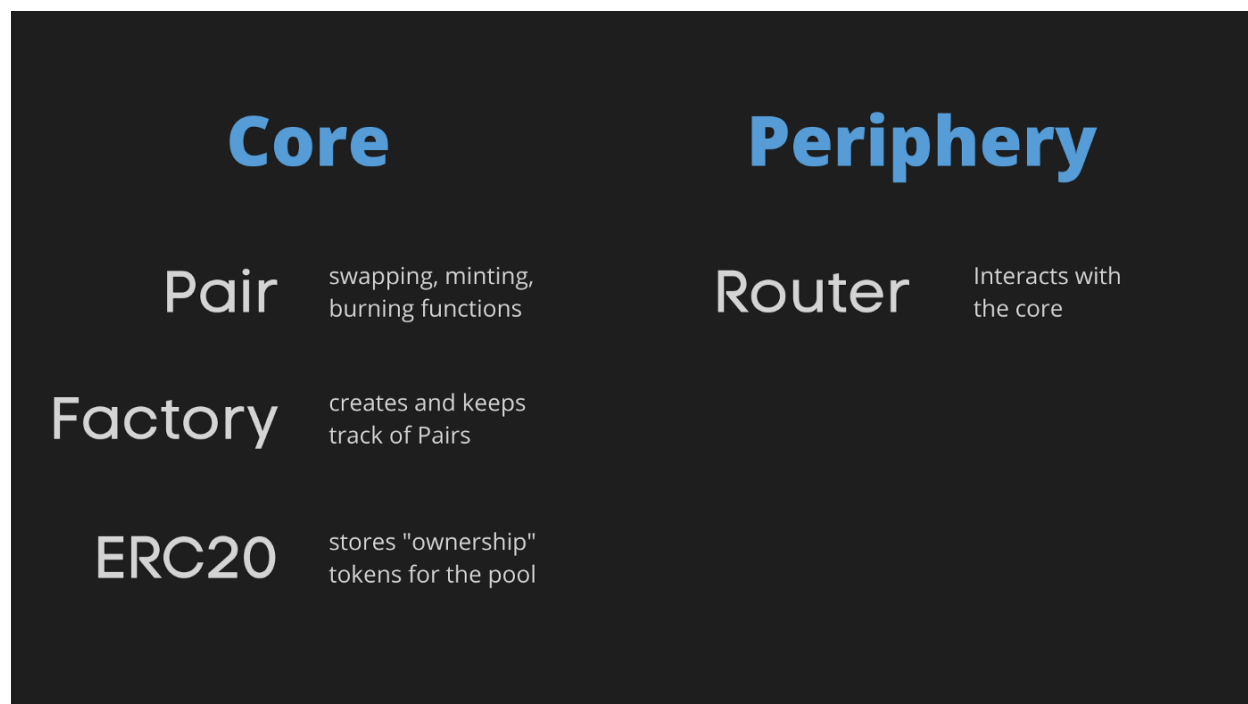
پس در واقع *impermanent loss* ضرری است که liquidity provider اگر دارایی خود را در pool نمی گذاشت و قیمت ETH ناگهانی بالا نمی رفت این ضرر را نمی کرد

بدون در نظر گرفتن این نوسانات بازار سود او از تبادل مالی حاصل می شود که به ازای هر تراکنش 0.3٪ از آن را به عنوان کار مزد دریافت می کند و در حالتی که  $collected\ fee > impermanent\ loss$  باشد سود می برد.

ساختار پیاده سازی پروژه و قراردادهای هوشمند آن

Uniswap در مجموع دارای 4 تا smart contract هست

که در دو دسته core و periphery قرار دارند. مطابق شکل زیر :



Core مسئول ذخیره سرمایه ، توکن ها ، تولید pair ، عملیات مبادله رمز ارز ، انتقال جایزه ها و ... هست و شامل سه smart contract زیر است:

- Pair (1)
- Factory (2)
- ERC20 (3)

که در ادامه به معرفی آنها می پردازیم:

: Pair

این قرارداد هوشمند وظیفه مبادلات رمزارزها و minting ( واریز سرمایه به pool توسط LP ) و burning ( برداشت سرمایه از pool توسط LP ) را بر عهده دارد.

کد تابع swap (مبادله رمز ارز) به صورت زیر است:

```
157
158 // this low-level function should be called from a contract which performs important safety checks
159 function swap(uint amount0Out, uint amount1Out, address to, bytes calldata data) external lock {
160     require(amount0Out > 0 || amount1Out > 0, 'UniswapV2: INSUFFICIENT_OUTPUT_AMOUNT');
161     (uint112 _reserve0, uint112 _reserve1,) = getReserves(); // gas savings
162     require(amount0Out < _reserve0 && amount1Out < _reserve1, 'UniswapV2: INSUFFICIENT_LIQUIDITY');
163
164     uint balance0;
165     uint balance1;
166     { // scope for _token{0,1}, avoids stack too deep errors
167         address _token0 = token0;
168         address _token1 = token1;
169         require(to != _token0 && to != _token1, 'UniswapV2: INVALID_T0');
170         if (amount0Out > 0) _safeTransfer(_token0, to, amount0Out); // optimistically transfer tokens
171         if (amount1Out > 0) _safeTransfer(_token1, to, amount1Out); // optimistically transfer tokens
172         if (data.length > 0) IUniswapV2Callee(to).uniswapV2Call(msg.sender, amount0Out, amount1Out, data);
173         balance0 = IERC20(_token0).balanceOf(address(this));
174         balance1 = IERC20(_token1).balanceOf(address(this));
175     }
176     uint amount0In = balance0 > _reserve0 - amount0Out ? balance0 - (_reserve0 - amount0Out) : 0;
177     uint amount1In = balance1 > _reserve1 - amount1Out ? balance1 - (_reserve1 - amount1Out) : 0;
178     require(amount0In > 0 || amount1In > 0, 'UniswapV2: INSUFFICIENT_INPUT_AMOUNT');
179     { // scope for reserve{0,1}Adjusted, avoids stack too deep errors
180         uint balance0Adjusted = balance0.mul(1000).sub(amount0In.mul(3));
181         uint balance1Adjusted = balance1.mul(1000).sub(amount1In.mul(3));
182         require(balance0Adjusted.mul(balance1Adjusted) >= uint(_reserve0).mul(_reserve1).mul(1000**2), 'UniswapV2: K');
183     }
184
185     _update(balance0, balance1, _reserve0, _reserve1);
186     emit Swap(msg.sender, amount0In, amount1In, amount0Out, amount1Out, to);
187 }
188
```

A bunch of assertions

کد زیر تابع mint را نشان می دهد

```
109 // this low-level function should be called from a contract which performs important safety checks
110 function mint(address to) external lock returns (uint liquidity) {
111     (uint112 _reserve0, uint112 _reserve1,) = getReserves(); // gas savings
112     uint balance0 = IERC20(token0).balanceOf(address(this));
113     uint balance1 = IERC20(token1).balanceOf(address(this));
114     uint amount0 = balance0.sub(_reserve0);
115     uint amount1 = balance1.sub(_reserve1);
116
117     bool feeOn = _mintFee(_reserve0, _reserve1);
118     uint _totalSupply = totalSupply; // gas savings, must be defined here since totalSupply can update in _mintFee
119     if (_totalSupply == 0) {
120         liquidity = Math.sqrt(amount0.mul(amount1)).sub(MINIMUM_LIQUIDITY);
121         _mint(address(0), MINIMUM_LIQUIDITY); // permanently lock the first MINIMUM_LIQUIDITY tokens
122     } else {
123         liquidity = Math.min(amount0.mul(_totalSupply) / _reserve0, amount1.mul(_totalSupply) / _reserve1);
124     }
125     require(liquidity > 0, 'UniswapV2: INSUFFICIENT_LIQUIDITY_MINTED');
126     _mint(to, liquidity);
127
128     _update(balance0, balance1, _reserve0, _reserve1);
129     if (feeOn) kLast = uint(reserve0).mul(reserve1); // reserve0 and reserve1 are up-to-date
130     emit Mint(msg.sender, amount0, amount1);
131 }
132
```

liquidity providers

protocol fee



کد زیر تابع burn را نشان می دهد

```
132
133 // this low-level function should be called from a contract which performs important safety checks
134 function burn(address to) external lock returns (uint amount0, uint amount1) {
135     (uint112 _reserve0, uint112 _reserve1,) = getReserves(); // gas savings
136     address _token0 = token0; // gas savings
137     address _token1 = token1; // gas savings
138     uint balance0 = IERC20(_token0).balanceOf(address(this));
139     uint balance1 = IERC20(_token1).balanceOf(address(this));
140     uint liquidity = balanceOf(address(this));
141
142     bool feeOn = _mintFee(_reserve0, _reserve1);
143     uint _totalSupply = totalSupply; // gas savings, must be defined here since totalSupply can update in _mintFee
144     amount0 = liquidity.mul(balance0) / _totalSupply; // using balances ensures pro-rata distribution
145     amount1 = liquidity.mul(balance1) / _totalSupply; // using balances ensures pro-rata distribution
146     require(amount0 > 0 && amount1 > 0, 'UniswapV2: INSUFFICIENT_LIQUIDITY_BURNED');
147     _burn(address(this), liquidity);
148     _safeTransfer(_token0, to, amount0);
149     _safeTransfer(_token1, to, amount1);
150     balance0 = IERC20(_token0).balanceOf(address(this));
151     balance1 = IERC20(_token1).balanceOf(address(this));
152
153     _update(balance0, balance1, _reserve0, _reserve1);
154     if (feeOn) klast = uint(reserve0).mul(reserve1); // reserve0 and reserve1 are up-to-date
155     emit Burn(msg.sender, amount0, amount1, to);
156 }
```

liquidity providers  
protocol fee

Factory : برای تولید pair (زوج ارز) و نظارت بر آن استفاده می شود.

کد قسمت تولید pair آن به صورت زیر است

```
function createPair(address tokenA, address tokenB) external returns (address pair) {
    require(tokenA != tokenB, 'UniswapV2: IDENTICAL_ADDRESSES');
    (address token0, address token1) = tokenA < tokenB ? (tokenA, tokenB) : (tokenB, tokenA);
    require(token0 != address(0), 'UniswapV2: ZERO_ADDRESS');
    require(getPair[token0][token1] == address(0), 'UniswapV2: PAIR_EXISTS');
    bytes memory bytecode = type(UniswapV2Pair).creationCode;
    bytes32 salt = keccak256(abi.encodePacked(token0, token1));
    assembly {
        pair := create2(0, add(bytecode, 32), mload(bytecode), salt)
    }
    IUniswapV2Pair(pair).initialize(token0, token1);
    getPair[token0][token1] = pair;
    getPair[token1][token0] = pair; // populate mapping in the reverse direction
    allPairs.push(pair);
    emit PairCreated(token0, token1, pair, allPairs.length);
}
```

: ERC20

زمانی که LP به pool بودجه می‌دهد به جای آن pool ownership token می‌گیرد که به واسطه آن‌ها پاداش کارمزد حاصل از مبادله را دریافت می‌کند.

و وقتی پول خود را باز بخواهد با تحویل دادن این token سرمایه خود را به همراه کارمزدهایی که از تراکنش‌ها گرفته به دست می‌آورد

کار ERC رسیدگی به این توکن‌ها، تولید و سوزاندن آنها است. در حالی که ویژگی switchable protocol فعال باشد که الان نیست، 1/6 کارمزد به uniswap team و 5/6 به LP‌ها ولی الان کل آن به LP‌ها می‌رود.

: Periphery

کار این بخش فراهم کردن یک api برای کار با uniswap هست.

تنها از یک smart contract تشکیل شده است که آن Router است.

Router : در واقع API برای استفاده از توابع core است و نقش آن یک ارتباط دهنده بین کاربر و smart contract‌های core است.

Uniswap دارای یک interface در مدل خود است که آن در قرارداد هوشمند Router قرار دارد.

علاوه بر این مدل‌های مختلف دیگری خارج از uniswap هم interface مناسبی برای کار با uniswap ارائه می‌دهند از قبیل : zapper – 1inch - matcha

کاربرد دیگر uniswap، price oracle

به خاطر Arbitrage که در قسمت equilibrium loss بررسی کردیم، قیمت‌ها در uniswap خیلی نزدیک به قیمت‌های بازار واقعی است. پس uniswap price oracle یک تخمین خیلی خوب از قیمت‌های واقعی بازار است.

امنیت پروژه و نتایج بررسی های audit آن

## جزئیات رمزگذاری های استفاده شده در پروژه

پروتکل Uniswap از انواع اولیه رمزنگاری برای ایمن سازی عملیات خود استفاده می کند، از جمله توابع هش، امضای دیجیتال و رمزگذاری متقارن و نامتقارن:

1. توابع هش: برای تولید خروجی های با اندازه ثابت از ورودی های با اندازه متغیر استفاده می شود؛ در Uniswap از تابع هش Keccak-256 برای اطمینان از یکپارچگی داده ها و تراکنش ها در بلاک چین برای تولید آدرس های قطعی، برای توکن ها و استخرها و همچنین برای تولید درختان Merkle برای ذخیره سازی کارآمد و اثبات گنجاندن یا عدم وجود داده ها استفاده می شود.

2. امضای دیجیتال: برای احراز هویت مبدا پیام و اطمینان از یکپارچگی آن استفاده می شود. Uniswap از طرح امضای ECDSA (الگوریتم امضای دیجیتال منحنی بیضی) برای اعتبار سنجی تراکنش ها و اطمینان از اینکه تنها طرف های مورد نظر می توانند آنها را اجرا کنند، استفاده می کند.

3. تسهیم راز: از Shamir's Secret Sharing برای توزیع کلیدهای خصوصی قراردادهای هوشمند Uniswap بین توسعه دهندگان آن استفاده می شود تا از هر نقطه شکستی جلوگیری شود.

4. رمزگذاری متقارن: Uniswap از الگوریتم رمزگذاری AES برای اطمینان از محرمانه بودن و یکپارچگی داده های ارسال شده از طریق شبکه استفاده می کند. در API پروتکل Uniswap پیاده سازی شده است که از رمزگذاری HTTPS برای محافظت از داده ها در حین انتقال استفاده می کند.

هنگامی که کاربر از طریق مرورگر وب یا برنامه تلفن همراه خود با Uniswap تعامل می کند، تمام داده های منتقل شده بین دستگاه کاربر و سرورهای Uniswap با استفاده از HTTPS با رمزگذاری AES رمزگذاری می شود. این شامل اعتبار ورود کاربر، داده های تراکنش و سایر اطلاعات حساس است.

علاوه بر این، Uniswap از رمزگذاری برای ایمن سازی کلیدهای خصوصی کیف پول کاربران خود استفاده می کند. هنگامی که کاربران کیف پول خود را در Uniswap ایجاد می کنند یا به آن دسترسی پیدا می کنند، کلیدهای خصوصی آنها با استفاده از الگوریتم رمزگذاری AES-256-CBC قبل از ذخیره در دستگاه یا مرورگر کاربر رمزگذاری می شود.

5. رمزگذاری نامتقارن: Uniswap از پروتکل تبادل کلید ECDH (Elliptic Curve Diffie-Hellman) برای ایجاد یک کلید مخفی مشترک بین طرفین استفاده می کند بدون اینکه آن را در معرض استراق سمع قرار دهد.

در پروتکل ECDH, Uniswap به عنوان بخشی از فرآیند امضای تراکنش ها استفاده می شود. هنگامی که یک کاربر یک تراکنش را برای اجرای یک معامله در Uniswap امضا می کند، کلید خصوصی او با یک عدد تصادفی ترکیب می شود تا یک امضای منحصر به فرد ایجاد شود. سپس این امضا برای اجرای معامله به قرارداد هوشمند Uniswap ارسال می شود.

برای اطمینان از امنیت این فرآیند، از ECDH برای ایجاد یک کلید مخفی مشترک بین کاربر و قرارداد هوشمند استفاده می شود. این کلید مشترک برای رمزگذاری شماره تصادفی مورد استفاده در تولید امضا استفاده می شود و اطمینان حاصل می کند که نمی تواند توسط شخص ثالث رهگیری یا دستکاری شود.

به طور کلی، Uniswap از طیفی از رمزنگاری های اولیه برای اطمینان از امنیت، یکپارچگی، حریم خصوصی و کارایی پروتکل خود و تراکنش های انجام شده بر روی پلت فرم خود استفاده می کند.

## کارهای آینده و ایده های بهبود پروژه

در اینجا چند ایده بالقوه برای بهبود پروژه Uniswap وجود دارد که چند مورد را صرفا اشاره می کنیم و یک مورد را با جزئیات بیشتری شرح می دهیم:

کاهش هزینه ها: Uniswap می تواند راه هایی را برای کاهش هزینه هایی که کاربران برای تجارت روی پلتفرم می پردازند، بررسی کند. این می تواند شامل بهینه سازی مصرف گاز یا کاهش در ساختارهای جدید هزینه ای باشد که برای کاربران مقرون به صرفه تر است.

بهبود رابط کاربری: رابط کاربری Uniswap را می توان بهبود بخشید تا کاربر پسندتر و در دسترس طیف وسیع تری از کاربران باشد. این می تواند شامل ساده کردن فرآیند تجارت، ارائه منابع آموزشی بیشتر یا بهبود دسترسی به تلفن همراه باشد.

کاهش راه حل های لایه ۲: Uniswap می تواند راه حل های لایه ۲، مانند زنجیره های جانبی یا کانال های حالت، را برای بهبود مقیاس پذیری و سرعت پلتفرم بررسی کند. این می تواند به کاهش زمان تراکنش و هزینه های گاز کمک کند و در عین حال امنیت و عدم اعتماد پلت فرم را حفظ کند.

ضرر LP ها در مواقع معادل سازی قیمت:

بر اساس پروتکل uniswap و اعمال قیمت گذاری بر اساس عرضه و تقاضا، عده ای میتوانند با عرضه مقدار زیادی از یک ارز باعث ایجاد یک حباب از ارز دیگر شده و قیمت غیر واقعی نسبت به دنیای بیرون ایجاد کرده و سود کنند که در اینجا ضرر اصلی به LP های میرسد. ایده حل این مشکل را به این صورت بیان می کنیم:

اضافه شدن یک تابع به قرارداد هوشمند router که از یکی از بازارهای اصلی قیمت دو ارزی که در حال استفاده است را با قیمت مدل خود چک کند و اگر اختلاف این دو خیلی زیاد است کار زیر را انجام دهد: علاوه بر استخر اصلی، خود provider یک pool دیگر مجازی ایجاد کند که هر موقع قیمت از یک ترشهولدی بیشتر شد، خودش از خودش آن ارزی که قیمتش بیشتر است را خرید کند که ضرر نکند.

## جمع بندی:

در این گزارش پس از آشنایی با مفهوم تجارت غیرمتمرکز و امکانات و فوایدی که فراهم می‌آورد به دسته خاصی از آن یعنی صرافی‌های غیرمتمرکز پرداختیم و ساختار کلی و چالش‌های آن‌ها را بیان کردیم. سپس یکی از محبوب‌ترین صرافی‌های فوق که uniswap بوده را معرفی کرده و ضمن آشنایی با پروژه و هدف آن و ابزارها و مشتریانی که دارد حجم بازار فعلی و مسیر پیش رو را نشان دادیم. در ادامه نیز به توضیح دقیق پروتکل و مدل سیستمی آن و پیاده‌سازی عملی این پروتکل با قراردادهای هوشمند پرداخته و امنیت آن را نیز با نتایج audit های انجام شده روی آن بررسی کردیم. در آخر به مقایسه این پروژه با پروژه‌های رقیب پرداخته و ایده‌هایی برای بهبود این پروتکل ارائه کردیم.