

مفاهیم تکنولوژی بلاکچین و رمزارزها

مولف:

رضا نورمحمدی

فهرست مطالب

[**پیشگفتار** 1](#_Toc97286013)

[**مقدمه** 2](#_Toc97286014)

[**بخش اول** 3](#_Toc97286015)

[**روند تغییرات پول الکترونیکی از گذشته تاکنون** 4](#_Toc97286016)

[**مشکلات پول فیات، و رفع مشکلات با استفاده از مدل‌های DLT و فناوری بلاکچین** 4](#_Toc97286017)

[**تعریف دفتر کل توزیع شده (DLT)** 5](#_Toc97286018)

[**تعریف فناوری بلاکچین** 7](#_Toc97286019)

[**نمود بلاکچین با بیت‌کوین** 8](#_Toc97286020)

[**معرفی انواع بلاکچین** 9](#_Toc97286021)

[**بخش دوم** 10](#_Toc97286022)

[**تعریف مکانیزم اجماع و انواع مکانیزم‌های اجماع پرکاربرد** 12](#_Toc97286023)

[**مکانیزم اجماع اثبات کار (POW)** 12](#_Toc97286024)

[**مکانیزم اجماع اثبات سهام (POS)** 13](#_Toc97286025)

[**تحمل خطای بیزانس عملی** 14](#_Toc97286026)

[**بخش سوم** 15](#_Toc97286027)

[**ویژگی‌های تکنولوژی بلاکچین** 17](#_Toc97286028)

[**کاربردهای بلاکچین فراتر از ابزارهای تبادلی** 18](#_Toc97286029)

[**دسته‌بندی کاربردهای بلاکچین** 19](#_Toc97286030)

[**پرکاربردترین ابزار تبادل در بلاکچین** 22](#_Toc97286031)

[**انواع صرافی‌های رمزارزها** 24](#_Toc97286032)

[**انواع کیف پول در رمزارزها** 26](#_Toc97286033)

[**بخش چهارم** 28](#_Toc97286034)

[**دسته‌بندی حوزه‌ی فعالیت پروژه‌ها** 29](#_Toc97286035)

[**بررسی عمیق‌تر کاربردهای بلاکچین در تلاقی با فناوری‌ها و حوزه‌های دیگر** 36](#_Toc97286036)

[**هوش مصنوعی** 36](#_Toc97286037)

[**اینترنت اشیا** 37](#_Toc97286038)

[**اقتصاد غیرمتمرکز (DeFi)** 38](#_Toc97286039)

[**سازمان خود مختار غیرمتمرکز** 40](#_Toc97286040)

[**توکن‌های غیرقابل تعویض (NFT)** 40](#_Toc97286041)

[**اوراکل** 42](#_Toc97286042)

[**بخش پنجم** 44](#_Toc97286043)

[**روش‌های کسب درآمد و جذب سرمایه از طریق رمزارزها** 45](#_Toc97286044)

[**لانچ‌پد** 45](#_Toc97286045)

[**‏ ‏ایردراپ** 45](#_Toc97286046)

[**عرضه عمومی اولیه** 46](#_Toc97286047)

[**عرضه اولیه توکن** 46](#_Toc97286048)

[**عرضه اولیه توکن از طریق صرافی** 46](#_Toc97286049)

[**عرضه اولیه توکن از طریق صرافی غیرمتمرکز** 47](#_Toc97286050)

[**عرضه اولیه فارم** 47](#_Toc97286051)

[**عرضه اولیه توکن‌هایی که در حوزه بازی هستند از طریق صرافی** 47](#_Toc97286052)

[**عرضه اولیه دارایی‌هایی که در حوزه بازی ایجاد می‌شوند از طریق صرافی** 47](#_Toc97286053)

[**کسب درآمد از طریق بازی کردن** 48](#_Toc97286054)

[**کسب درآمد از طریق استیک کردنرمزارزها** 48](#_Toc97286055)

[**تأمین نقدینگی** 49](#_Toc97286056)

[**شاخص نقدینگی‌های قفل شده** 49](#_Toc97286057)

[**ییلد فارمینگ** 49](#_Toc97286058)

[**دارایی‌های مصنوعی، پل و کراس‌چینسه راه‌حل برای نقدینگی‌های قفل شده** 50](#_Toc97286059)

[**وام‌های سریع فلش لون** 51](#_Toc97286060)

[**کلام آخر** 52](#_Toc97286061)

## **پیشگفتار**

بلاکچین را فراتر از یک تکنولوژی دوست دارم. زیرا در دنیای بلاکچین زندگی جاریست. ذات وجودی بازار رمزارزها به مانند زندگی بالا و پایین دارد و برنده آن کسی است که در بالاها مغرور نشود و در پایین‌ها ناامید نباشد. در بلاکچین به مانند زندگی؛ گذشته، حال و آینده وجود دارد و آنچه در گذشته رخ می‌دهد غیر قابل تغییر است، در بلاکچین پای سخنی که بیان می‌شود باید ایستاد ولی با این حال در گذشته نمی‌توان ماند و باید از آن عبور کرد. زنجیره اصلی بلاکچین ادامه دهنده بلاکی است که در آن اطلاعات صحیح و درست قرار داشته باشد. صحت اطلاعات در آن به اثبات رسیده پس در نتیجه دیگر هیچ دیواری کج بالا نمی‌رود، چرا که در سرتاسر سیستم دموکراسی برقرار است. مکانیزم اجماع عدالت را بین اعضا ایجاد‌ می‌کند و در یک مکانیزم انگیزشی هر کس تنها به اندازه‌ای که تلاش می‌کند، پاداش می‌گیرد. در بلاکچین اعتبار افراد به دارایی‌شان نیست، بلکه به صداقت و صحت اطلاعات بستگی دارد. اگر داده‌ای اشتباه باشد، فرد جریمه خواهد شد و دیگر به او پاداشی تعلق نمی‌گیرد. برای موفقیت در این سیستم باید همه افراد عملکردی درست، شفاف و صادقانه داشته باشند و اگر گروهی باهم تبانی کنند کل سیستم شکست می‌خورد. قرارداد هوشمند امکان اشتراک‌گذاری کلیه منابع را فراهم می‌آورد و این یعنی با همکاری می‌توان هر کار بزرگی را انجام داد. با همکاری و همرسانی می‌توان از هر مانعی عبور کرد، من از خانم معصومه قربانپور، مدیار ن و خانم مریم معتقدی که با همیاری و همکاری خود، تدوین این کتاب را برایم میسر کردند، سپاسگزارم.

در تئوری آشوب عنوان می‌شود که در دل بی‌نظمی، یک نظم واحد وجود دارد، پس وقتی می‌بینیم که تمام ابعاد بلاکچین هدف مشترک تمرکززدایی را دنبال می‌کنند، می‌فهمیم که در انتها و در دل این تمرکززدایی باز تمرکزی واحد وجود دارد. در اینجا می‌خواهم به نقل قولی از ویتالیک بوترین اشاره کنم، او در مقاله‌ای می‌گوید: "ته این بازی قرار است همه به یک نقطه برسند." شاید او نیز زندگی را درک کرده است. شاید در انتها همه به یگانگی برسیم. در انتها خدا منتظر ما ایستاده است.

بلاکچین را دوست دارم، در آن زندگی جاریست.

## **مقدمه**

تکنولوژی بلاکچین و رمزارزها بیش از یک دهه است که پا به عرصه ظهور گذاشته و در این مدت با پیشرفتی که داشته به جایگاهی قابل توجهی دست یافته است. با وجود کاربردها و جذابیت‌های این تکنولوژی، اگر دانش و شناخت کافی نباشد، نمی‌توان از آن بهره برد. در ادامه مطالبی گردآوری شده تا مفاهیم و کاربردهای این حوزه معرفی گردد. با درک این تکنولوژی می‌توان سرمایه‌گذاری‌ها و معاملات هوشمندانه‌تری را به انجام رساند. همچنین، دانستن این تکنولوژی کمک می‌کند تا بتوان بهترین پروژه‌ها را بر اساس مفاهیم آن‌ها انتخاب کرده و با فناوری روز دنیا همراه و همگام شد.

## **بخش اول**

## **روند تغییرات پول الکترونیکی از گذشته تاکنون**

ریشه‌های پول الکترونیکی به ایجاد شرکت دیجی‌کش[[1]](#footnote-1) در اواخر دهه ۹۰ توسط دیوید چاوم[[2]](#footnote-2) بر می‌گردد. دیجی‌کش که در آن از علم رمزنگاری[[3]](#footnote-3) استفاده شده بود، بستری برای بانک‌ها فراهم می‌کرد تا به وسیله آن قابلیت انتقال ارزش به صورت الکترونیکی فراهم شود. پس از آن در سال 1997   نیک زابو[[4]](#footnote-4)  مفهوم هش کش[[5]](#footnote-5) را مطرح کرد و در واقع همان مکانیزم اجماع[[6]](#footnote-6) گواه اثبات کار[[7]](#footnote-7) می‌باشد که در بیت‌کوین پیاده‌سازی شده است. سال 1998 رمزارز دیگری با نام B-Money  و در سال 2005 بیت‌گلد[[8]](#footnote-8) با پشتوانه طلا آمد.

علت ناکارآمدی و شکست نسل‌های رمزارز قبل از بیت‌کوین، عدم توانایی پیاده‌سازی معماری غیرمتمرکز بود تا اینکه در سال 2008 مقاله‌ای با عنوان بیت‌کوین توسط هویت ساتوشی ناکاماتو[[9]](#footnote-9) چاپ شد. هویتی که تاکنون ناشناس است تا دسترسی‌‌ای به وی وجود نداشته باشد. بلاکچینی که امکان خلق پول را به صورت غیرمتمرکز ایجاد کرد.

## **مشکلات پول فیات، و رفع مشکلات با استفاده از مدل‌های DLT و فناوری بلاکچین**

پول فیات به بانک‌های مرکزی کنترل جامع‌تری روی اقتصاد می‌دهد، زیرا مقدار چاپ پول و اسکناس در کشورها در اختیار و کنترل بانک مرکزی است. در تمام کشورهای دنیا زمان بدهکاری دولت‌ها یا اپیدمی کرونا یا جنگ و ... دولت‌ها تصمیم به چاپ اسکناس می‌گیرند. ارزش اسکناس چاپ شده هر کشور به پشتوانه طلای ذخیره شده در خزانه بانک مرکزی آن کشور است، حال اگر چاپ اسکناس بدون پشتوانه باشد، باعث ایجاد تورم و کاهش ارزش پول ملی می‌گردد.

همچنین زمانی که قدرت، ثروت و یا حتی اطلاعات به صورت متمرکز تنها در اختیار یک مرکز قرار گیرد، وجود فساد در آن دور از ذهن نیست و این مشکلی بود که از نگاه همگان غیر قابل حل تلقی می‌شد. معماری غیرمتمرکز، در یک جامعه یا سازمان، نوعی حاکمیت را در یک سیستم به‌ وجود آورد که همه بتوانند نسبت به سهم خود و اختیاراتی که دارند، در مدیریت آن سیستم سهیم باشند و این راه‌حلی برای جلوگیری از فساد موجود در فضای متمرکز بود.

از طرفی در معماری متمرکز[[10]](#footnote-10) کنترل کلیه عملکردهای کلیدی سیستم، از طریق یک نهاد مرکزی مدیریت می‌شود. مشکل اصلی این نوع معماری، تک نقطه محو شده[[11]](#footnote-11) است، به این معنی که تنها یک نقطه وجود دارد که اگر امنیت آن مورد حمله‌ قرار بگیرد و یا دیتابیس آن از دسترس خارج گردد، کلیه اطلاعات از بین می‌روند.

بلاکچین یک فضای غیرمتمرکزی برای ذخیره اطلاعات است. به طور مثال دارایی افراد در سیستم بانکداری تنها یکسری عدد است که در دیتابیسی ذخیره شده است. حال اگر این اطلاعات فقط در اختیار بانک به صورت متمرکز نباشد و تمام کاربران یک کپی از کل اطلاعات دیتابیس را در اختیار داشته باشند، مفهوم بلاکچین ایجاد می‌گردد. بلاکچین در اصل یک دفتر کل توزیع شده است که می‌توان از آن جهت ثبت تراکنش‌های دیجیتالی استفاده کرد. در واقع کلیه اطلاعات در تمام سیستم‌های کامپیوتری روی شبکه کپی و توزیع می‌شود. این کار هزینه زیادی دارد اما دیگر امکان تغییر اطلاعات توسط هیچ‌کس وجود نخواهد داشت. چرا که یک نسخه از کل اطلاعات در اختیار سایر کاربران است. این امر باعث می‌گردد تغییر، هک یا تقلب در سیستم دشوار یا غیرممکن گردد و امنیت بالاتری در شبکه ایجاد شود. همچنین اختیار و کنترل سیستم دیگر تحت نظارت ارگان و نهاد خاصی نیست. از طرفی هویت‌ها هم نامشخص است، پس احتمال تبانی کاربران برای تغییر در اطلاعات نیز وجود ندارد.

## **تعریف دفتر کل توزیع شده (DLT)**

تکنولوژی دفتر کل توزیع شده یک سیستم دیجیتال برای ثبت معاملات دارایی‌ها است که در آن معاملات و جزئیات آن‌ها به طور هم‌زمان در چندین مکان ثبت می‌شود. بلاکچین، تنگل[[12]](#footnote-12) و هش‌گراف[[13]](#footnote-13) سه مدل پیاده‌سازی DLT هستند.

از لحاظ سرعت و مقیاس‌پذیری : بلاکچین > تنگل > هش‌گراف

در بلاک‌چین هر بلاک که شامل مجموعه‌ای از تراکنش‌های معتبر است، به یک بلاک دیگر متصل می‌باشد. در عمل آنچه بلاک‌ها را به یکدیگر متصل نگه می‌دارد، هشینگ[[14]](#footnote-14) است به طوری که در هر بلاک هش بلاک قبلی قرار دارد. فرآیند هشینگ شامل دریافت داده بدون توجه به اندازه آن و وارد کردنش در یک تابع ریاضی به منظور تولید خروجی است. خروجی حاصل یک هش نام داشته و اندازه‌اش همیشه ثابت است.

تنگل یا آیوتا تنگل یک نوع ابتکاری از فناوری دفتر توزیع شده می‌باشد که به طور اختصاصی برای محیط اینترنت اشیاء معماری شده است. در ساختار تنگل هر بلاک به دو بلاک دیگر متصل است که همین امر باعث می‌شود سرعت شبکه بالاتر برود.

هش‌گراف یک فناوری دفتر کل توزیع شده است که به عنوان ادامه یا جانشین بلاکچین توصیف شده است. در هش‌گراف ممکن است هر بلاک به یک بلاک یا دو بلاک یا حتی سه بلاک دیگر متصل شود، به عبارت دیگر ساختار ثابتی ندارد و همین امر باعث ایجاد سرعت بالاتری می‌گردد.

## **تعریف فناوری بلاکچین**

بلاکچین یک ساختار داده است، که در آن داده‌ها به صورت زمانی در بلوک‌هایی که به طور مداوم در حال اضافه شدن هستند و به صورت زنجیره‌ای به هم‌ متصل‌ می‌باشند، قرار می‌گیرند. به عبارت دیگر به عنوان یک دفتر کل توزیع شده[[15]](#footnote-15) عمل می‌کند که در آن شرکت‌کنندگان برای ثبت هر ورودی جدید باید به توافق برسند.

معماری بلاکچین در مجموع شامل عناصر زیر است:

1. **گره[[16]](#footnote-16):** کاربر یا رایانه است که دارای یک نسخه کامل از دفتر کل بلاکچین است.
2. **بلاک:** یک ساختار داده‌ای که برای نگهداری مجموعه‌ای از تراکنش‌ها استفاده می‌شود.
3. **تراکنش:** در هر بلاک مجموعه‌ای از تراکنش‌ها قرار دارد.

در واقع در بلاکچین کدخدایی برای تصمیم‌گیری وجود ندارد پس مسئله‌ای در اینجا مطرح می‌شود که چه کسانی اجازه نوشتن و خواندن این دیتابیس را دارند. قدرت اصلی بلاکچین در مکانیزم اجماع است، یعنی ساختار به توافق‌ رساندن عده‌ کثیری از کاربران به طوری که عدالت بین آن‌ها برقرار باشد. کسی که حق نوشتن دارد، با رأی همه کاربران، بر اساس الگوریتم مکانیزم اجماع انتخاب می‌شود.

حال مسئله دیگری مطرح می‌شود. آیا کسی که برای نوشتن انتخاب می‌شود، اطلاعات درستی در بلاکچین ثبت می‌کند یا خیر؟ ساختار بلاکچین جهت حل این مسئله یک مکانیزم انگیزشی برای کسی که برای نوشتن انتخاب شده است را مطرح می‌کند، بدین صورت که به ازای هر یک بلاکی که اطلاعات صحیحی در آن ثبت شود، به وی پاداش تعلق می‌گیرد. به عبارت دیگر گره‌ای که برای نوشتن در بلاک انتخاب شده است (ماینر[[17]](#footnote-17) یا ولیدیتور[[18]](#footnote-18)) با اثبات رفتار صادقانه خود پاداش دریافت می‌کند. در هر بلاک چند تراکنش ثبت می‌شود. هر تراکنش شامل اطلاعات مربوط به انتقال مبلغی از فرستنده به گیرنده است.

## **نمود بلاکچین با بیت‌کوین**

بلاکچین در واقع مجموعه‌ای از مفاهیم اقتصاد (مالی)، رمزنگاری، دیتا و هم بحث علم داده[[19]](#footnote-19) را در خود دارد. با اینکه رمز ارز و ارز دیجیتال برای بیان یک مفهوم بکار می‌روند، اما باهم متفاوت هستند.

* Digital Currency : ارز دیجیتال
* Crypto: رمز
* Cryptography : رمزنگاری
* Crypto Currency: رمز ارز، ارز دیجیتالی که مبتنی بر رمزنگاری است.

پول سه کاربرد اساسی در سراسر دنیا دارد. ابزاری برای تبادلات، حفظ ذخیره ارزش و ابزاری برای اندازه‌گیری است. بلاکچین بستری برای انتقال ارزش‌ها را نیز ایجاد کرده است.

 در اینجا دو تعریف اینترنت دیتا[[20]](#footnote-20) و اینترنت ارزش‌ها[[21]](#footnote-21) مطرح می‌شود:

* **اینترنت دیتا:** اینترنت شبکه‌ای از میلیون‌ها کامپیوتر متصل به هم از سرتاسر دنیا است که امکان تبادل اطلاعات یا دیتا بین کامپیوترها را ایجاد می‌کند.
* **اینترنت ارزش‌ها:** حال اگر امکان تبادل ارزش‌هایی مثل پول، تجربه، وفاداری، مالکیت، رتبه اعتباری و هر چیز با ارزش دیگری را در یک شبکه‌ای از میلیون‌ها کامپیوتر متصل به هم از سرتاسر دنیا را داشته باشیم، مفهم اینترنت ارزش‌ها ایجاد می‌شود. اینجا مفهوم پول خصوصی نیز ایجاد می‌شود چرا که هر چیز با ارزشی می‌تواند به مانند پول، وسیله‌ای برای تبادل باشد.

بیت‌کوین اولین رمز ارزی بود که توانست به عنوان ابزاری برای تبادل ارزش مطرح شود و پس از آن با رشد و مقبولیت خود توانست ابزاری برای حفظ ذخیره ارزش نیز باشد. در حال حاضر تتر[[22]](#footnote-22) نقش پول را در جابه‌جایی نقدینگی بر عهده دارد. نقطه اوج بیت‌کوین در اکتبر سال ۲۰۱۳ با انتشار خبر ضبط وب‌سایت سیلک رود[[23]](#footnote-23) توسط [اف‌بی‌آی](https://fa.wikipedia.org/wiki/%D8%A7%D9%81%E2%80%8C%D8%A8%DB%8C%E2%80%8C%D8%A2%DB%8C)[[24]](#footnote-24) بود. این سایت متعلق به [راس ویلیام اولبریکت](https://fa.wikipedia.org/wiki/%D8%B1%D8%A7%D8%B3_%D8%A7%D9%88%D9%84%D8%A8%D8%B1%DB%8C%DA%86)[[25]](#footnote-25) بوده و بیشترین کالاهایی که در سیلک‌رود برای فروش عرضه شد، در [حوزه‌ی قضایی](https://fa.wikipedia.org/wiki/%D8%AD%D9%88%D8%B2%D9%87%D9%94_%D9%82%D8%B6%D8%A7%DB%8C%DB%8C) اکثر کشورها کالای قاچاق محسوب می‌شد که نحوه پرداخت برای خرید آن‌ها از طریق بیت‌کوین صورت می‌گرفت. با انتشار این خبر بیت‌کوین بر سر زبان‌ها افتاد و شناخت عمومی این رمز ارز آغاز شد.

## **معرفی انواع بلاکچین**

بلاکچین انواع مختلفی دارد هرکدام از آن‌ها یک تکنولوژی و هدف خاصی را ارائه می‌دهد. در ادامه بررسی 4 نوع از بلاکچین‌ها آمده است.

* **بلاکچین عمومی[[26]](#footnote-26)**

شبکه بلاکچین عمومی نوعی از شبکه بلاکچین است که هرکسی می‌تواند در هر زمانی به آن بپیوندد. به طور کلی در ارتباط با مشارکت در این شبکه هیچ محدودیتی وجود نداشته و همه می‌توانند دفتر کل را مشاهده و در فرایند اجماع آن شرکت کنند. تقریباً تمام نام‌های بزرگ در دنیای رمزارزها بر اساس این نوع از بلاکچین پیاده‌سازی شده‌اند. شبکه‌هایی چون بیت‌کوین، اتریوم و لایت‌کوین از این نوع هستند که امروزه اتریوم محبوب‌ترین آن‌ها محسوب می‌گردد.

* **بلاکچین خصوصی[[27]](#footnote-27)**

عضویت در شبکه بلاکچین خصوصی فقط به ‌وسیله دعوت‌نامه امکان‌پذیر است. سطوح مختلف دسترسی به شبکه خصوصی بلاکچینی توسط یک نهاد مرجع تعیین می‌شود و کاربران برای استفاده از این شبکه باید از آن نهاد مجوز دریافت کنند. رایج‌ترین نمونه‌های بلاکچین خصوصی ریپل[[28]](#footnote-28) و هایپرلجر[[29]](#footnote-29) هستند. برخی از بلاکچین‌های عمومی نیز ناشناس بودن را مجاز می‌دانند، در حالی که بلاکچین‌های خصوصی اساساً به این امر معتقد نیستند.

* **بلاکچین کنسرسیوم[[30]](#footnote-30)**

شبکه بلاکچین فدرال یا بلاکچین کنسرسیوم یک پلتفرم غیرعمومی اما مجاز است که در آن چندین سازمان به جای یک سازمان واحد، بر آن حکومت می‌کنند.

از نمونه بلاکچین‌های کنسرسیوم می‌توان بهQuorum ، Hyperledger و Corda اشاره کرد. Quorum یک پلتفرم دفتر کل توزیع شده مبتنی بر اتریوم است که برای ارائه مشارکت در صنعت مالی با مجوز اتریوم که از حریم خصوصی تراکنش‌ها و قراردادهای هوشمند پشتیبانی می‌کند، توسعه یافته است.

* **بلاکچین هیبرید[[31]](#footnote-31)**

شبکه بلاکچین هیبریدی، ترکیبی از شبکه‌های عمومی و خصوصی می‌باشد. بهترین راه برای توصیف آن، در نظر گرفتن یک شبکه عمومی است که یک شبکه خصوصی در آن میزبانی می‌شود، و این بدان معناست که مشارکت محدودی وجود دارد که از طریق خود بلاکچین خصوصی کنترل می‌شود. یک مثال خوب از این نوع بلاکچین، در زنجیره تأمین استفاده می‌شود. Food Trust IBM با هدف بهبود کارایی در سراسر زنجیره تأمین مواد غذایی می‌تواند بهترین مثال از این نوع بلاکچین باشد.

در یک دید کلی شباهت و تفاوت این ساختارها به صورت زیر است:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | عمومی | خصوصی | کنسرسیوم | هیبرید |
| بی‌نیاز بودن به درخواست اجازه  | بله | خیر | خیر | قسمتی از آن |
| چه کسی قادر به مشاهده آن است؟ | هر شخصی | تنها افراد دعوت‌شده | بستگی دارد | کنترل‌شده |
| چه کسی قادر به استفاده از آن است؟ | هر شخصی | مشترکین تأیید شده | مشترکین تأیید شده | در صورت دلخواه |
| چه کسی مالک آن است؟ | هیچ شخصی | یک نهاد (ارگان) | چندین نهاد | یک نهاد |
| شناخته شده بودن مشترکین | خیر | بله | بله | بر اساس انتخاب |
| سرعت تراکنش‌ها | کند | سریع | سریع | سریع |

## **بخش دوم**

## **تعریف مکانیزم اجماع و انواع مکانیزم‌های اجماع پرکاربرد**

الگوریتم اجماع روشی است که از طریق آن همه کاربران شبکه بلاکچین در مورد وضعیت فعلی دفتر کل توزیع شده به توافق مشترک می‌رسند. بنابراین، یک الگوریتم اجماع در جستجوی یک توافق مشترک است که برای کل شبکه اعمال شود و وضعیت شبکه را بهبود بخشد.

سه نوع اصلی از الگوریتم‌های اجماع:

* اثبات کار[[32]](#footnote-32)
* اثبات سهام[[33]](#footnote-33)
* تحمل خطای بیزانس عملی[[34]](#footnote-34)

## **مکانیزم اجماع اثبات کار (POW)**

گره‌های یک شبکه، باید یک محاسباتی خاصی را انجام دهند و آن را اثبات کنند، تا بتوانند در یک فضای غیرمتمرکز به اجماع برسند و از سوءاستفاده یا حملات مهاجمان جلوگیری کنند. الگوریتم اجماع اثبات کار در رمزنگاری نوعی اثبات دانش صفر [[35]](#footnote-35)محسوب می‌شود که در آن یک طرف به دیگران ثابت می‌کند که مقدار مشخصی از تلاش محاسباتی خاص را انجام داده است. پس از آن تأیید کنندگان می‌توانند این ادعا را با حداقل تلاش از طرف خود تأیید کنند. هدف از الگوریتم‌های اثبات کار انجام یک کار خاص یا یک معمای محاسباتی که دردی را درمان کند، نیست. بلکه هدف آن جلوگیری از دست‌کاری داده‌ها از طریق راه‌حلی خاص برای ایجاد نیازهای کنترل انرژی و بهبود کار سخت‌افزارها است.

زمانی که ماینرها بلاک تراکنش‌های خود را تشکیل دادند، باید به دنبال یافتن امضای معتبر برای بلاک خود باشند یا به عبارتی، گواه اثبات کار را انجام دهند. هر گره باید فرایند محاسبات ریاضیاتی را طی کند. راه‌حلی که ماینرها به دنبال آن هستند، با نام هش شناخته می‌شود و یافتن آن بسیار دشوار است. اما زمانی که هش صحیح پیدا شد، تأیید آن توسط بقیه گره‌ها بسیار آسان است. یافتن هش صحیح توسط عدد نانس انجام می‌گیرد؛ ماینرها مدام نانس‌های مختلف را امتحان می‌کنند تا به هش صحیح برسند. در مورد شبکه بیت‌کوین، هش صحیح به معنای تعداد معینی عدد صفر در ابتدای هش است و گره‌ها باید این اعداد صفر را با امتحان کردن نانس‌های مختلف به دست بیاورند. زمانی که یک ماینر توانست هش خروجی صحیح برای بلاک جدید را پیدا کند، آن را به همراه امضای خود در شبکه منتشر می‌کند، تا مابقی گره‌ها نیز آن را تأیید کنند. زمانی که تعداد قابل قبولی از گره‌ها با یکدیگر به اجماع رسیدند که این هش صحیح است، بلاک جدید به بلاکچین اضافه می‌شود. گره‌ای که در این رقابت برنده می‌شود، تراکنش‌ها را از فضایی در بلاکچین به نام ممپول[[36]](#footnote-36) جمع‌آوری می‌کند و درون بلاک جدید قرار می‌دهد و پاداش بلاک به همراه کارمزد تمام تراکنش‌های داخل بلاک را دریافت می‌کند.

## **مکانیزم اجماع اثبات سهام (POS)**

پروتکل‌های اثبات سهام نوعی مکانیسم اجماع برای بلاکچین هستند که با انتخاب اعتبارسنج‌ها بر اساس تناسب با میزان دارایی، کار می‌کنند. اعتبارسنج‌هایی که می‌خواهند در کار تولید بلاک شرکت کنند و پاداش بگیرند، باید توکن‌های بومی شبکه را بخرند و به شبکه اختصاص دهند یا به عبارت دقیق‌تر سهام‌گذاری[[37]](#footnote-37) ‌کنند. سهام‌گذاری از طریق قفل‌کردن توکن‌ها در بلاکچین و به ‌منظور ایجاد و تأیید بلاک‌ها انجام می‌شود. اعتبارسنج‌ها به ‌طور مستقیم و به ‌تناسب میزان سهام‌گذاری‌ خود، پاداش دریافت می‌کنند. بر خلاف پروتکل‌های اثبات کار، این پروتکل‌ها انرژی زیادی را مصرف نمی‌کنند. اولین بار از این نوع مکانیزم در سال 2۰12 برای پیرکوین[[38]](#footnote-38) استفاده شد و امروز کاردانو[[39]](#footnote-39) بزرگ‌ترین شبکه اثبات سهام را به خود اختصاص داده است.

## **تحمل خطای بیزانس عملی**

این الگوریتم در اواخر دهه ۹۰ توسط باربارا لیسکوف[[40]](#footnote-40) و میگوئل کاسترو[[41]](#footnote-41) معرفی شد. این الگوریتم در واقع برای کارکرد مؤثر سیستم‌های ناهماهنگ و به منظور بهبود زمان معماری شده است.

* مسئله ژنرال‌های بیزانسی

داستان این است که چندین ژنرال شهر بیزانتیوم را محاصره کرده‌اند. با اینکه آن‌ها دورتادور شهر را در اختیار خود دارند اما برای سقوط شهر و تصرف آن، ژنرال‌ها بایستی با هماهنگی همدیگر و به‌صورت دسته‌جمعی به شهر حمله کنند. اگر همه ژنرال‌ها در یک ‌زمان حمله کنند، پیروز خواهند شد، اما اگر هر ژنرال در زمان مدنظر خود حمله کند، جنگ را خواهند باخت. این ژنرال‌ها برای هماهنگی زمان حمله، کانال‌های ارتباطی امنی بین یکدیگر ندارند؛ چرا که پیام‌های ارسالی و دریافتی توسط ژنرال‌ها ممکن است توسط مدافعین بیزانتیوم دست‌کاری یا جعل شود. حتی امکان دارد بعضی از ژنرال‌ها هم خائن باشند. در این شرایط ژنرال‎ها چگونه می‌توانند در یک‌زمان مشخص همگی به بیزانتیوم حمله کنند؟

کلاً در مفاهیم توزیع شده این مسئله مطرح است. بیت‌کوین اولین راهکار واقعی از دید پولی برای حل مسئله ژنرال‌های بیزانس بود. پیش از بیت‌کوین پیشنهادها و پروژه‌های زیادی تلاش کردند پولی مستقل از دولت‌ها ایجاد کنند، اما همگی شکست خوردند. در مسئله ژنرال‌های بیزانس، حقیقتی که تمامی افراد بایستی بر سر آن تفاهم کنند، همان بلاکچین است. اگر تمامی اعضای شبکه بیت‌کوین که به آن‌ها گره نیز گفته می‌شود موافقت کنند که کدام تراکنش‌ها و به چه ترتیبی رخ داده‌اند و مورد تأیید هستند، آن‌ها می‌توانند مالکیت بیت‌کوین‌ها را تأیید کنند و بدین ترتیب یک پول کارآمد و بدون نیاز به اعتماد بدون وجود یک نهاد متمرکز را ایجاد کنند.

این مدل از یک ساختار فرمانده و ستوان پیروی می‌کند. ابتدا یک کلاینت، درخواستی را به گره رهبر می‌فرستد و عملکرد یک سرویس را درخواست می‌کند. سپس گره رهبر درخواست را به گره‌های پشتیبان ارسال می‌کند. آن‌ها تقاضا را اجرا می‌کنند و سپس به کلاینت جواب می‌دهند. در آخر این کلاینت به اندازه X+1 جواب از گره‌های مختلف با همان نتیجه منتظر می‌شود. (X نماد ماکسیمم نودهایی است که ممکن است معیوب باشند.) در انتها همه گره‌های صادق در مورد ترتیب ثبت به توافق می‌رسند.

یکی از مزیت‌های این مدل، توانایی فراهم آوردن تراکنش بدون نیاز به تأیید است. اگر در سیستم تحمل خطای بیزانس عملی گره‌ها بر روی یک بلاک خاص توافق کنند، سپس آن بلاک نهایی خواهد شد. همچنین این مدل مصرف انرژی پایین‌تری نسبت اثبات کار دارد در نتیجه در مصرف برق صرفه‌جویی می‌شود.

## **بخش سوم**

## **ویژگی‌های تکنولوژی بلاکچین**

ویژگی‌های تکنولوژی بلاکچین را در 5 دسته می‌توان نام برد:

* **تغییرناپذیری[[42]](#footnote-42)**

تمام گره‌های شبکه یک نسخه از کل دیتای بستر بلاکچین را دارند. هر دیتایی که در شبکه ثبت شود، کاملا قطعی است و تغییری نمی‌کند. همچنین با استفاده از رمزنگاری و توزیع داده‌ها، امکان هک، حذف و تغییر اطلاعات ثبت‌ شده، تقریباً از بین می‌رود.

* **غیرمتمرکز[[43]](#footnote-43)**

در ساختار بلاکچین واحد مرکزی جهت کنترل و تصمیم‌گیری وجود ندارد و تمام فرایند به طور غیرمتمرکز انجام می‌شود. در یک مثال ساده از سیستم کلاینت-سرور[[44]](#footnote-44) هنگامی که مطلبی در گوگل جستجو می‌شود، یک درخواست برای سرور ارسال شده و نتیجه به عنوان پاسخ دریافت می‌گردد. اما در سیستم غیرمتمرکز دیگر سرور مرکزی برای ارائه سرویس وجود ندارد.

* **ظرفیت[[45]](#footnote-45)**

با ایجاد بستری غیرمتمرکز می‌توان از قدرت پردازشی و فضای ذخیره‌سازی بسیار بالایی بهره برد. تقریبا اکثر افراد تصور می‌کنند در بلاکچین تنها تراکنش‌های مالی انجام می‌گیرد، اما این تکنولوژی امکان پیاده‌سازی پروژه‌هایی را فراهم کرده تاکنون به علت وجود محدودیت‌هایی امکان اجرایی شدن نداشتند.

* **ناشناس بودن[[46]](#footnote-46)**

شیوه طراحی بیت‌کوین به گونه‌ای است که حریم خصوصی کاربرانش را به میزانی پذیرفتنی حفظ کند. بیت‌کوین تا زمانی ناشناس است که تمام اجزای آن، از آدرس گرفته تا کلید‌های خصوصی و عمومی، هیچ پیوند مستقیمی با هویت شخص نداشته باشند. اما اگر یک آدرس از دستورالعمل‌های احراز هویت مشتری[[47]](#footnote-47) استفاده کند، ‌می‌تواند آدرس تراکنش را به آسانی به هویت واقعی شخص در دنیای واقعی متصل کند.

* **امنیت**

اگر گره‌ای از شبکه خارج شود، به خاطر ساختار غیرمتمرکز به سیستم لطمه‌ای وارد نمی‌شود و امنیت برای دیتاهای داخل شبکه وجود دارد. همچنین زمانی که اعتماد کامل بین افراد وجود ندارد، بلاکچین برای حل این مسئله هم کارایی دارد. از طرفی در بلاکچین، اطلاعات با کمک الگوریتم‌های مختلفی رمزنگاری می‌شوند. بنابراین نمی‌توان اطلاعات را دستکاری کرد یا تغییر داد. این الگوریتم‌ها برای هر رمزارز متفاوت است.

## **کاربردهای بلاکچین فراتر از ابزارهای تبادلی**

نسل‌ بعد از بیت‌کوین، اتریوم[[48]](#footnote-48) بود که ویتالیک بوترین[[49]](#footnote-49) آن را ارائه داد. اتریوم از قابلیت سیستم غیرمتمرکز برای توزیع دیتا در شبکه که بیت‌کوین ارائه داده بود، در جهت انجام پردازش‌های کامپیوتری و کاربردی استفاده کرد. اتریوم با تعریف قراردادهای هوشمند (اسمارت کانترکت[[50]](#footnote-50)) قابلیت‌های جدیدی به شبکه بلاکچین اضافه کرد. قراردادی که بین گره‌ها تعریف می‌شود تا کار مشخص شده در قرارداد را انجام دهند. به عبارت دیگر یک وظیفه‌ی[[51]](#footnote-51) تعریف شده در قرارداد هوشمند، بین گره‌ها در بستر بلاکچین توزیع می‌شود، هر گره بخشی از وظیفه را انجام داده و نتیجه را بر می‌گرداند. بعد از تعریف قراردادهای هوشمند انقلابی شکل گرفت، چرا که هر پروژه‌ای که به صورت متمرکز روی یک سرور پیاده‌سازی می‌شد، اکنون می‌توانست کد خود را روی بستر اتریوم به صورت غیرمتمرکز اجرا کرده و از قدرت شبکه استفاده کند که باعث کاهش هزینه و زمان در پروژه می‌شود. توافق‌های پلتفرم وام‌دهی، استیبل کوین‌ها[[52]](#footnote-52)، برگزاری ICO ها[[53]](#footnote-53)، اوراکل‌ها[[54]](#footnote-54) و ... همگی در قراردادهای هوشمند تعریف می‌شود.

قبل از این در سیستم‌های ابری به طور مثال سرویس کلود آمازون[[55]](#footnote-55) ، این مفهوم وجود داشت. اما برای مواردی که به هر دلیلی نیاز بود، مشخص نباشد که قدرت پردازشی برای چه کاری مورد نیاز است، این سرویس کارایی نداشت. در سیستم‌های ابری اعتماد به سرور مرکزی اجباری ‌است در حالی که قرارداد هوشمند این مسئله را حل کرده است. چرا که در بلاکچین ساختار به توافق‌ رساندن تمام گره‌های شبکه با عنوان مکانیزم اجماع وجود دارد و نیازی به وجود یک سرور مرکزی برای تصمیم‌گیری نیست. از طرفی هر چیزی که در بلاکچین ثبت شود تغییرناپذیر است.

## **دسته‌بندی کاربردهای بلاکچین**

بلاکچین اولین بار در بیت‌کوین استفاده شد، اما در ادامه این تکنولوژی توسعه یافت، به طوری که اکنون کاربردهای زیادی در دنیای واقعی دارد. بلاکچین از لحاظ کاربرد در 4 دسته‌ کلی قرار می‌گیرد.

* **ارز دیجیتال[[56]](#footnote-56)**

ارز دیجیتال یا رمزارز توانست در جایگاه پول به عنوان حفظ ارزش دارایی و ابزار تبادلات قرار بگیرد. در این جایگاه به خاطر سیستم توزیع شده در بلاکچین ارگان مرکزی و خاصی وجود ندارد پس خلق پول نیز در یک نظام دموکراسی انجام می‌شود. با توسعه پروژه‌ها در این حوزه، پرداخت‌های بین‌بانکی تا پرداخت‌های خورد می‌تواند از طریق رمزارز صورت گیرد.

به طور مثال ریپل یک سیستم تسویه‌حساب آنی، شبکه مبادله ارز و حواله است که توسط Ripple Labs Inc، یک شرکت فناوری مستقر در ایالات متحده ایجاد شده است. ریپل که در سال 2012 منتشر شد، بر اساس یک پروتکل منبع باز توزیع شده ایجاد شد و از نشانه‌هایی که نمایانگر ارز فیات، رمزارز، کالاها یا سایر واحدهای دارای ارزش پشتیبانی می‌کند. ریپل قصد دارد معاملات مالی جهانی ایمن، فوری و تقریباً آزاد از هر اندازه و بدون بازگشت هزینه را امکان‌پذیر سازد. به همین منظور از رمزارز بومیXRP کمک می‌گیرد.

* **ثبت سوابق[[57]](#footnote-57)**

اطلاعات بر روی بلاکچین به صورت توزیع‌شده ثبت می‌شوند که هر کاربری با اتصال به شبکه می‌تواند یک نسخه از این اطلاعات را دریافت می‌کند. با استفاده از هش و رمزنگاری و توزیع داده‌ها، هیچ‌کس قادر نخواهد بود که اطلاعات ثبت شده روی بلاکچین را حذف کند یا تغییر دهد.

به طور مثال از این تکنولوژی می‌توان جهت رهگیری و بررسی در زنجیره تأمین بهره برد. استفاده از بلاکچین در زنجیره تأمین می‌تواند به شرکت‌کنندگان کمک کند تا قیمت، تاریخ، مکان، کیفیت، گواهینامه و سایر اطلاعات مربوط را برای مدیریت مؤثرتر زنجیره تأمین ثبت کنند. مراحل تولید محصول و برداشت از ابتدا تا لحظه رسیدن به دست مشتری روی بلاکچین ثبت شده و مشتری می‌تواند با اسکن کردن یک کد QR از اصالت و کیفیت محصول خود مطمئن شود.

همچنین در حوزه سلامت، داده‌های مرتبط با تحقیقات پزشکی یا پرونده و سوابق پزشکی بیماران اگر به صورت غیرمتمرکز و بر بستر بلاکچین ذخیره شوند، به پیشرفت بشر در این حوزه کمک بسیاری می‌شود. چرا دیتا در دنیای امروز با ارزش‌ترین دارایی است. آنالیز، تحلیل و بررسی این اطلاعات می‌تواند تا حد زیادی از شیوع بیماری‌های ژنتیکی جلوگیری کند. همچنین در تولید دارو و واکسن نیز اطلاعات بسیار مورد نیاز است. از طرف دیگر با استفاده از بلاکچین به خاطر اشتراک‌گذاری اطلاعات به طور غیرمتمرکز می‌توان در هزینه و زمان‌بر روی طرح‌ها و تحقیقات علمی و پزشکی نیز صرفه‌جویی کرد. در همین راستا سازمان بهداشت جهانی در ۲۸ مارس ۲۰۲۰ پلتفرم MiPasa را راه‌اندازی کرد. این پلتفرم با همکاری شرکت‌های بزرگ فعال در حوزه بلاکچین و تعدادی از نهادهای ملی سلامت، با هدف تشخیص زود هنگام مبتلایان به ویروس کرونا، ناقلان و کانون‌های عفونی و آلوده به این ویروس، ایجاد شد.

کمک گرفتن از بلاکچین در خصوص برگزاری انتخابات هم یکی دیگر از کاربردهای بلاکچین است. در سال ۲۰۱۹ ایتالیا از این تکنولوژی استفاده کرد که البته همچنان در حال توسعه است.

* **قراردادهای هوشمند[[58]](#footnote-58)**

قرارداد هوشمند کدی است که روی بلاکچین اجرا می‌شود تا بدون نیاز به واسطه‌ها، شرایط یک توافقنامه را بررسی و انجام دهد. از طریق قراردادهای هوشمند می‌توان برنامه‌ها و پروژه‌هایی را ساخت که بدون هیچ‌گونه واسطه‌ و توقفی به کار خود ادامه دهند. برنامه‌های غیرمتمرکز بدین صورت امکان پیاده‌سازی دارند.

* **امنیت[[59]](#footnote-59)**

اطلاعات ثبت شده در دفتر کل توزیع شده می‌تواند از نوع اطلاعات هویتی باشند. با این کار خطر هک و از بین رفتن این اطلاعات تا حد زیادی کاهش می‌یابد. همچنین در حوزه‌ی مالکیت معنوی بلاکچین برای خالق اثر مخصوصا از نوع فایل (موسیقی، عکس، فیلم و... ) امنیت در شبکه را ایجاد می‌کند تا پس از انتشار در فضای اینترنت در خطر نقض کپی‌رایت قرار نگیرد. در واقع از طریق بلاکچین می‌توان به صورت بین‌المللی حق مالکیت یک اثر را به ثبت رساند یا با استفاده از قراردادهای هوشمند برای استفاده از آن یک سری شرایط خاص مثل پرداخت بها با یک توکن خاص را تعیین کرد.

## **پرکاربردترین ابزار تبادل در بلاکچین**

رمزارزها انواع مختلفی در ساختار خود دارند که در ادامه به بررسی هر یک پرداخته شده است.

* **آلتکوین‌ها[[60]](#footnote-60)**

در اصل تمام رمزارزها را شامل می‌شوند. پس از موفقیت بیت‌کوین به عنوان اولین رمزارز بلاکچینی پذیرفته شده در میان عموم مردم، از رمزارزهای بسیاری به منظور رقابت با بیت‌کوین رونمایی شد. به تمام این رمزارزها با هر ویژگی که داشته باشند، آلتکوین گفته می‌شود که در واقع به معنی جایگزین بیت‌کوین است.

* **کوین و توکن**

توکن‌ها نشان دهنده مجموعه‌ای از قوانین رمزگذاری شده در یک قرارداد هوشمند هستند. توکن رمزنگاری در اصل یک دارایی دیجیتال است که به طور ایمن بر روی شبکه بلاکچین ذخیره شده است.

**کوین:** دارایی دیجیتالی که بر روی پلتفرم بلاکچین اختصاصی خود تعریف شده است. به عبارت دیگر بومی[[61]](#footnote-61) خود شبکه بلاکچین است. به طور مثال کوین بلاکچین اتریوم، ETH است.

**توکن:** دارایی دیجیتالی که بر روی پلتفرم بلاکچین دیگری تعریف شده است. در واقع به لطف قراردادهای هوشمند، بسیاری از توکن‌ها بر روی شبکه اتریوم و یا دیگر شبکه‌ها ساخته می‌شوند.

بسیاری از پروژه‌های رمزارز ترجیح می‌دهند ابتدا، رمزارز خود را بر بستر یک بلاکچین دیگر راه‌اندازی کنند و در صورتی که در بازار حضور موفقی داشتند، بلاکچین اختصاصی برای آن بنویسند. بایننس کوین یکی از این پروژه‌ها بود. رمزارز BNB ابتدا بر بستر اتریوم شروع به فعالیت کرد و سپس، بایننس بلاکچین اختصاصی BEP2 را برای آن نوشت.



* **توکن رپد[[62]](#footnote-62)**

یک توکن رپد رمزارزی است که پشتوانه آن یک رمزارز دیگر است. واحدهای یک رمزارز به یک آدرس مخصوص انتقال داده می‌شود و به ازای آن به ‌طور خودکار در شبکه دیگر، توکن رپد ایجاد می‌شود.

از نمونه‌های بارز توکن رپد می‌توان به رپد بیت‌کوین اشاره کرد که اولین بار روی شبکه اتریوم عرضه شد. هر توکن رپد بیت‌کوین با یک واحد بیت‌کوین پشتوانه‌سازی می‌شود و بنابراین قیمت هر واحد از آن برابر با یک واحد بیت‌کوین است. اینکه به ازای هر رپد بیت‌کوین روی شبکه اتریوم واقعاً یک بیت‌کوین به‌عنوان پشتوانه قرار دارد یا نه، را یک شرکت واسطه نظارت و ضمانت می‌کند و در واقع حضانت[[63]](#footnote-63) دارایی کاربران را دارد. پس اینکه چه شرکتی این نقش را دارد، به عنوان یک شاخص در رپد توکن‌ها باید به آن توجه کرد. به طور مثال ترون[[64]](#footnote-64) با شرکت بیتگو[[65]](#footnote-65) برای رپد توکن‌ها یک قرارداد همکاری بسته است. شرکت بیتگو دارای مجوز امنیتی به نام SoC2 است. در حوزه رمزارزها تنها سه ارگان جمینی[[66]](#footnote-66) ، کوین‌بیس[[67]](#footnote-67) و بیتگو این مجوز را دارند.

از آنجا که شبکه بیت‌کوین و اتریوم مستقل هستند و نمی‌توان به‌طور مستقیم از بیت‌کوین در تراکنش‌های اتریوم و برنامه‌های غیرمتمرکز استفاده کرد، توکن رپد بیت‌کوین به افرادی که تمایل داشته باشند با بیت‌کوین در شبکه اتریوم فعالیت کنند کمک می‌کند. از طرفی بیت‌کوین قیمت بالایی دارد و حجم معاملات آن خیلی زیاد است، پس شبکه‌هایی که در ساختارشان از بیت‌کوین رپد شده استفاده می‌کنند دارای اهمیت زیادی هستند. مثلا PolkaBTC نیز رپد بیت‌کوین روی شبکه پولکادات[[68]](#footnote-68) است. در نسخه2 Blockstack از رپد بیت‌کوین در دیفای[[69]](#footnote-69) استفاده می‌شود.

## **انواع صرافی‌های رمزارزها**

صرافی‌ها نقش حیاتی در بازار رمزارزها دارند و پلتفرم‌هایی جهت خرید و فروش رمزارزها هستند. بر اساس ساختار انواع مختلفی دارند که در ادامه معرفی شده‌اند.

* **صرافی‌های متمرکز**

صرافی‌های متمرکز توسط یک نهاد یا گروه به شکل متمرکز و با قوانینی خاص اداره می‌شوند و به همین خاطر به طور معمول در صرافی‌های متمرکز حجم نقدینگی از صرافی‌های غیرمتمرکز بیشتر است. از جمله مزایای این صرافی‌ها می‌توان به نقدینگی بالا، سرعت بالای معاملات، ابزارهای پیشرفته جهت ترید و... اشاره کرد. در این صرافی‌ها کلید خصوصی رمزارزها در اختیار صرافی است و این موضوع باعث کاهش امنیت برای کاربران است.

* **صرافی‌های غیرمتمرکز**

صرافی غیرمتمرکز، بستری برای انجام معاملات به‌صورت غیرمتمرکز است. در این صرافی‌ها از بلاکچین و قراردادهای هوشمند برای حذف واسطه‌ها استفاده می‌شود. با یک صرافی غیرمتمرکز کاربران می‌توانند بدون نیاز به واریز رمزارزها به کیف پول صرافی‌ها، از داخل کیف پول خودشان معاملات را انجام دهند. در صرافی‌های غیرمتمرکز کلید خصوصی رمزارزها در اختیار کاربران قرار دارد و به این صورت احتمال هک صرافی تقریباً به صفر می‌رسد.

|  |  |  |
| --- | --- | --- |
| **صرافی غیرمتمرکز** | **صرافی متمرکز** |  |
| کاربر بیشترین کنترل را دارد | تمام کنترل در اختیار پلتفرم قرار دارد | **کنترل** |
| امکان هک یا خطرات دیگر وجود ندارد | احتمال هک شدن وجود دارد | **امنیت** |
| خیلی محبوب نیست | بسیار محبوب | **محبوبیت** |
| کارمزد صفر یا بسیار کم | دارای کارمزد برای استفاده  | **کارمزد** |
| انواع کاملاً محدودی از سفارش‌ها را دارند | ویژگی‌های متنوعی را ارائه می‌دهد | **امکانات** |
| نیاز به مجوز ندارد | نیاز به مجوز برای کار در آن است | **مقررات** |
| بسیار کم | بسیار زیاد | **نقدینگی** |
| اجرای سفارش‌ها می‌تواند تا یک دقیقه طول بکشد | سفارش‌ها را در میلی‌ثانیه اجرا می‌کند | **سرعت** |

* **صرافی‌های هیبرید**[[70]](#footnote-70)

هیبرید ترکیبی از امنیت صرافی‌های غیرمتمرکز و قابلیت استفاده از صرافی‌های متمرکز است، ازاین‌رو، تمام مزایای هر دو را دارا است. تسویه‌پذیری بالا، معاملات سریع‌تر، امنیت عالی و حفظ حریم شخصی بهتر از ویژگی این نوع صرافی است. به عنوان مثال، یک صرافی می‌تواند سفارش‌ها کاربران خود را خارج از بلاکچین مطابقت داده و نتیجه را در بلاکچین به‌روز کند. این کار سرعت را بالا می‌برد.

* **صرافی‌های P2P**[[71]](#footnote-71)

مبادلات همتا به همتا زمانی انجام می‌شود که دو نفر برای خرید یا فروش رمزارز به طور مستقیم با یکدیگر در تعامل باشند. به زبان ساده، خریدار و فروشنده بدون نیاز به شخص ثالثی به عنوان واسطه، مستقیماً با یکدیگر معامله می‌کنند. به طور مثال بایننس که یک صرافی متمرکز است امکان مبادلات همتا به همتا را نیز فراهم کرده است.

## **انواع کیف پول[[72]](#footnote-72) در رمزارزها**

کیف پول رمزارزها مانند یک حساب بانکی امکان نگهداری، دریافت و ارسال رمزارزها را برای کاربران ایجاد می‌کنند. در واقع این کیف پول‌ها نرم‌افزارها و سخت‌افزارهایی هستند که از طریق کلید خصوصی و کلید عمومی مدیریت رمزارزها و ارتباط با شبکه بلاکچین را فراهم می‌کنند. در تکنولوژی بلاکچین کلیدهای عمومی به مانند آدرس ایمیل و کلیدهای خصوص به مانند پسورد آن است. حال اگر کلیدهای خصوصی مربوط به دارایی رمزارزها در اختیار توسعه‌دهنده آن باشد از نوع کیف پول‌های حضانتی[[73]](#footnote-73) هستند و اگر در اختیار خود کاربر باشد کیف پول غیر حضانتی[[74]](#footnote-74) است. در واقع در کیف پول‌های غیر حضانتی کنترل دارایی در دست خود کاربر است و حضانت دارایی بر عهده شخص ثالثی قرار ندارد. این یعنی هیچ نهادی قادر نخواهد بود رمزارزهای یک فرد را مسدود کند. و از طرفی باید در حفظ و نگهداری کلیدهای خصوصی دقت داشت، چرا که در صورت از دست دادن اثبات مالکیت دارایی (کلید خصوصی) هیچ راه برگشتی وجود ندارد. کیف پول‌های رمزارزها دو دسته‌بندی کلی دارند:

* **کیف پول‌های گرم**

کیف پول‌های گرم کاربرد ساده و راحتی دارند، اما این کیف پول‌ها به دلیل وصل بودن به اینترنت، در خطر تهدیدات امنیتی و سرقت سایبری هستند. این کیف پول‌ها به طور کلی 4 نوع هستند:

* کیف پول‌های دسکتاپ مانند Electrum و Atomic wallet
* کیف پول‌های موبایلی مانند Edge و Trust wallet و Coinomi
* کیف پول‌های تحت وب و Extensions مانند Freewallet و MetaMask
* کیف پول‌های ترکیبی مانند BTCpay و Blockchain.com
* **کیف پول‌های سرد**

نوعی کیف پول ارز دیجیتال که رمزارزها را بدون اتصال به اینترنت ذخیره می‌کند. این کیف پول‌ها را صرفا جهت ارسال و دریافت ارزها، باید به اینترنت متصل کرد. در این نوع کیف پول‌ها فرایند تولید تراکنش به صورت آفلاین انجام شده و پس از اتصال به اینترنت تراکنش در شبکه ارسال می‌شود. پس امضای دیجیتالی قبل از اتصال به اینترنت ایجاد شده و در حالت آنلاین به کلید خصوصی نیازی نیست. به همین خاطر امن‌ترین روش برای نگهداری ارزهای دیجیتال هستند. کیف پول‌های سخت‌افزاری مانند لجر[[75]](#footnote-75) و ترزور[[76]](#footnote-76) و کیف پول‌های کاغذی، معروف‌ترین کیف پول‌های سرد هستند.

## **بخش چهارم**

## **دسته‌بندی حوزه‌ی فعالیت پروژه‌ها**

به طور کلی پروژه‌ها بر روی بستر بلاکچین که هر یک اهداف خاصی را دنبال می‌کنند، در حوزه‌های زیر دسته‌بندی می‌شوند:

* هوش مصنوعی[[77]](#footnote-77)
* اینترنت اشیا[[78]](#footnote-78)
* زیر ساخت[[79]](#footnote-79)
* تعامل و همکاری[[80]](#footnote-80)
* اقتصاد غیرمتمرکز[[81]](#footnote-81)
* استیبل کوین[[82]](#footnote-82)
* توکن‌های غیر قابل معاوضه[[83]](#footnote-83)
* اوراکل[[84]](#footnote-84)
* صرافی متمرکز[[85]](#footnote-85)
* صرافی غیرمتمرکز[[86]](#footnote-86)
* سازمان خود مختار غیرمتمرکز (دائو)[[87]](#footnote-87)
* بازارسازان خودکار [[88]](#footnote-88)
* هویت[[89]](#footnote-89)
* محرمانگی[[90]](#footnote-90)
* واقعیت مجازی[[91]](#footnote-91)
* فضای ذخیره‌سازی غیرمتمرکز[[92]](#footnote-92)
* پرداخت‌های بین‌بانکی[[93]](#footnote-93)
* بیمه[[94]](#footnote-94)
* وام‌دهی[[95]](#footnote-95)
* متاورس[[96]](#footnote-96)

**هوش مصنوعی**

هم‌اکنون هوش مصنوعی از بزرگ‌ترین و پیچیده‌ترین پروژه‌های در حال توسعه در دنیای فناوری و بلاکچین بهترین بستری جهت گسترش ابعاد متنوع این فناوری است. به طور مثال دو ارز FET[[97]](#footnote-97) و GRT[[98]](#footnote-98) در این زمینه تعریف شده‌اند.

**اینترنت اشیا**

اینترنت اشیاء به زبان ساده ارتباط حسگرها و دستگاه‌ها از طریق شبکه اینترنت، با هدف ایجاد امکان مشاهده، کنترل و تسهیل در کاربری لوازم متصل به شبکه برای کاربران است. به طور مثال دو ارز IOTA و [[99]](#footnote-99)VET در این زمینه تعریف شده‌اند.

**زیر ساخت**

بلاکچین‌هایی که بستری برای ارائه خدمات به سایرین را فراهم می‌کنند. به عنوان مثال EOS و ETH[[100]](#footnote-100) به خاطر داشتن قابلیت قراردادهای هوشمند زیرساختی برای اجرای برنامه‌های غیرمتمرکز هستند.

**تعامل و همکاری**

به طور مشابه سوئیفت [[101]](#footnote-101)در فضای بلاکچین، اینتر بلاکچین‌ها[[102]](#footnote-102) ارتباط بین بلاکچین‌های مختلف را ایجاد می‌کنند و می‌توانند باعث افزایش مقیاس‌پذیری نیز باشند. در تعامل‌پذیری بلاکچین‌ها امکان ارتباط بین بلاکچین‌های مختلف ایجاد می‌شود. در این حالت می‌توان نقدینگی‌های موجود در شبکه، امنیت، فضای ذخیره‌سازی، قدرت پردازشی را بین بلاکچین‌ها به اشتراک گذاشت. ATOM[[103]](#footnote-103) و ICX[[104]](#footnote-104) نمونه‌هایی در این زمینه هستند.

**اقتصاد غیرمتمرکز**

در اصل، حوزه دیفای از یک بلاکچین عمومی استفاده می‌کند که در اصل به هیچ نهاد یا ارگان مرکزی وابسته نیست. اقتصاد جهان می‌تواند به صورت غیرمتمرکز در دسترس افراد از اقصی نقاط دنیا قرار بگیرد تا بتوانند به راحتی فعالیت اقتصادی و مالی خود را انجام دهند.AAVE و [[105]](#footnote-105)YFI  نمونه‌هایی از این حوزه هستند.

**استیبل کوین**

استیبل کوین‌ها درواقع رمزارزهای وابسته هستند. آن‌ها به گونه‌ای طراحی شده‌اند که ارزششان به یک رمزارز دیگر، پول فیات، الگوریتم تنظیم عرضه/تقاضا و یا یک دارایی قابل مبادله بستگی داشته باشد. استیبل کوین نوعی رمزارز است که برای کاهش نوسانات قیمت طراحی ‌شده است. همچنین به‌عنوان ذخیره کننده ارزش و وسیله‌ای برای مبادله کاربرد دارد. استیبل کوین را می‌توان قلب تپنده حوزه دیفای دانست. USDT[[106]](#footnote-106) و DAI دو استیبل کوین مطرح بازار هستند. شفافیت ویژگی مهمی است که به لطف بلاکچین در شبکه رمزارزها وجود دارد. اما در استیبل کوین‌هایی با پشتوانه فیات این ویژگی به شدت کم‌رنگ شده است. شبکه USDT، به عنوان پراستفاده‌ترین رمزارز به شدت متمرکز و در اختیار یک شرکت خاص هستند، در حالی که DAI دارای شبکه غیرمتمرکز است.

**توکن‌های غیرقابل‌معاوضه (NFT)**

NFT ها به‌عنوان یک گواهی مالکیت دیجیتالی غیرتکراری برای هر نوع دارایی دیجیتالی صادر می‌شوند. در واقع، NFT یک قرارداد هوشمند است که از طریق آن می‌توان هر آنچه که در دنیای واقعی است توکنیزه کرد تا وارد دنیای بلاکچین شود. Theta[[107]](#footnote-107) و ENJ[[108]](#footnote-108) دو مثال از این حوزه هستند.

**اوراکل**

اهمیت اوراکل‌ها آنجا نمود پیدا می‌کند که قراردادهای هوشمند بلاکچینی تنها قادر به دسترسی به اطلاعات داخل شبکه هستند. بنابراین اوراکل‌ها به عنوان یک ابزار ارتباطی ایفای نقش می‌کنند تا رویداد‌های جهان بیرون را به داده‌های دیجیتال تبدیل کنند.LINK [[109]](#footnote-109) و UMA دو مثال از اوراکل‌ها هستند.

**صرافی متمرکز**

صرافی متمرکز پلتفرمی است که می‌توان در آن دارایی‌های دیجیتال را خرید یا فروش کرد. از نمونه‌‌ توکن‌های صرافی‌ متمرکز می‌توان به [[110]](#footnote-110)KCS و BNB[[111]](#footnote-111) اشاره کرد.

**صرافی غیرمتمرکز**

صرافی غیرمتمرکز مشابه یک صرافی متمرکز است، با این تفاوت که عملکرد این صرافی به صورت غیرمتمرکز است و هیچ مرجع کنترل‌کننده‌ای وجود ندارد. تمام معاملات از طریق قراردادهای هوشمند انجام شده و در بلاکچین ذخیره می‌شود. از نمونه‌‌ توکن‌های صرافی‌ غیرمتمرکز می‌توان به 1INCH[[112]](#footnote-112) و [[113]](#footnote-113)BURGER اشاره کرد.

**سازمان خود مختار غیرمتمرکز**

ایده پشت یک دائو ایجاد شرکت یا سازمانی است که بدون مدیریت سلسله مراتبی می‌تواند کاملاً عملکرد داشته باشد. SNX[[114]](#footnote-114) و DCR[[115]](#footnote-115) دو مثال از توکن‌های این زمینه هستند.

**بازار سازان خودکار**

بازارسازهای خودکار یا AMM ها نوعی از صرافی‌های غیرمتمرکز هستند که برای تعیین قیمت یک توکن بجای سفارشات خرید و فروش به فرمول‌های ریاضی متکی هستند. UNI [[116]](#footnote-116) و CAKE [[117]](#footnote-117) نمونه‌هایی از این حوزه هستند.

**هویت**

بررسی هویت واقعی در ابعاد مختلفی می‌تواند باشد. رمز عبور چیزی که فرد می‌داند. کارت هوشمند چیزی است که فرد دارد. اثر انگشت و عنبیه چشم چیزی است که در افراد منحصر به فرد است. کاربرد احراز هویت در بلاکچین غیر از بانک‌ها یا مؤسسات مالی شامل صنایعی که به تأیید هویت کاربران احتیاج دارند نیز می‌شود. به‌ عنوان مثال، مقامات مالیاتی برای تسریع فرایندهای داخلی خود، سازمان‌های قضایی، مؤسسات رتبه‌بندی اعتبار، بازار سهام و نهادهای مشابه همگی می‌توانند از بلاکچین برای پیاده‌سازی پروژه‌های خود بهره ببرند. شرکت‌ بزرگ فناوری مانند IBM با همکاری شرکت سرمایه‌گذاری و خدمات بانکداری HSBC، دویچه بانک[[118]](#footnote-118) و خزانه‌داری کارگیل[[119]](#footnote-119) روی پروژه‌ بلاکچینی در این زمینه در حال فعالیت و توسعه هستند. همچنین ONT[[120]](#footnote-120) نیز نمونه ارزی از این حوزه است.

**محرمانگی**

پرایویسی کوین‌های حریم خصوصی همچنان بخش مهمی از اکوسیستم ارزهای دیجیتال، هستند. کوین‌های حریم خصوصی رمزارزهایی هستند که اطلاعات کاربران خود را مخفی می‌کنند. آن‌ها جایگزینی مناسب برای هر دارنده رمز ارز هستند که به هر علتی قصد دارد تا هویت خود را در فضای بلاکچین پنهان کند. این کار با تکنیک‌های رمزنگاری صورت می‌گیرد که امکان مشاهده تاریخچه تراکنش‌ها و موجودی آدرس‌ها را از بین می‌برند. هر روزه، بررسی‌های نظارتی روی بهبود حریم خصوصی در بازار دیجیتال در حال افزایش است. شاید به همین دلیل، پروژه‌های حریم خصوصی همچنان ابزارهای مهمی علیه نقض حقوق حریم شخصی باقی بمانند. XMR[[121]](#footnote-121) و ZEC[[122]](#footnote-122) از مثال‌های این حوزه هستند.

**واقعیت مجازی**

با گذشت زمان و پیدایش فناوری واقعیت مجازی این امکان فراهم شد تا افراد در خانه خود به ‌راحتی هر چه تمام‌تر در یک رویداد واقع در یک کشور یا حتی قاره دیگر حضور داشته باشند و تمام اتفاقات را لمس کنند. Unity[[123]](#footnote-123) در حوزه واقعیت مجازی قرار دارد.

**فضای ذخیره‌سازی غیرمتمرکز**

سال‌هاست که سرعت رشد و گسترش فناوری رایانش ابری توجه توسعه‌دهندگان بلاکچین را به خود جلب کرده است. AR[[124]](#footnote-124) و FIL[[125]](#footnote-125) در این فضا فعالیت دارند.

**پرداخت‌های بین‌بانکی**

شبکه‌های بلاکچین هر کدام با روش‌های متفاوت در این حوزه قصد دارند سیستم‌های پرداخت جهانی را متحول کنند. XRP[[126]](#footnote-126) و XLM[[127]](#footnote-127) دو توکن در این حوزه هستند.

**بیمه**

یکی از مهم‌ترین مشکلات صنعت بیمه پیچیده بودن فرایندها و زمان بر بودن آن‌ها است که بهره‌مندی از فناوری بلاکچین، مشکلات مذکور را تا حد زیادی می‌تواند تعدیل نماید. همچنین با ورود صنعت بیمه به این عرصه امنیت برای کاربران بالا می‌رود. [[128]](#footnote-128)TIDAL و NXM[[129]](#footnote-129) در حوزه بیمه‌ هستند.

**وام‌دهی**

یکی از مزایای سرمایه‌گذاری در رمزارزها، استفاده از دارایی رمزنگاری شده به عنوان وثیقه برای وام است. همان‌طور که در سیستم‌های سنتی بانک‌ها فرصت وام گرفتن و بهره‌مندی از مزایای بانکی وجود دارد، در دنیای رمز ارزها نیز این روش برای تمامی افراد مقدور می‌باشد. با این تفاوت که این نوع وام‌ها بسیار در دسترس‌تر هستند و برای سرمایه‌گذاران این امکان را فراهم می‌کنند تا از سرمایه خود ضمن کسب درآمد از رشد ارزها برای دریافت وام نیز استفاده کنند. COMP[[130]](#footnote-130) و MKR [[131]](#footnote-131) مثال‌هایی از حوزه وام‌دهی هستند.

**متاورس**

متاورس در حقیقت فضایی سه بعدی از دنیای دیجیتال است. این دنیای دیجیتال متشکل از فضاهای مجازی است که می‌توان در آن‌ها به واسطه آواتار (تصویر مجازی و کاراکتری که از خود می‌سازند) حضور داشت. آواتارها بیانگر شخصیت، سلیقه، تفکرات و به نوعی شناسنامه کاربر در دنیای مجازی می‌باشند. در بستر متاورس می‌توان بازی کرد، برای خرید به فروشگاه رفت، با دوستان در یک کافی‌شاپ مجازی زمان گذراند، با همکاران در یک دفتر مجازی کار کرد و خیلی کار‌های دیگر را به انجام رسانید.

پروژه‌های رمزارز مثل دیسنترالند[[132]](#footnote-132) و سندباکس[[133]](#footnote-133) هم‌اکنون دنیا‌های مجازی خود را دارند و در حال اجرا و مدیریت این فضا هستند. شرکت‌هایی مثل فیسبوک (متا‌)، مایکروسافت و Nvidia نیز در حال ساخت نسخه اختصاصی خود از دنیای دیجیتال با بهره‌گیری از به روز‌ترین تکنولوژی مورد استفاده در متاورس هستند.

از جمله برترین تکنولوژی‌های مورد استفاده در متاورس می‌توان به بلاک چین‌، واقعیت افزوده و واقعیت مجازی، بازسازی سه بعدی، هوش مصنوعی و اینترنت اشیا اشاره کرد.

تکنولوژی بلاکچین راهکاری غیرمتمرکز و شفاف برای اثبات مالکیت دیجیتال‌، ذخیره‌سازی دیجیتال‌‌، انتقال ارزش‌، حاکمیت‌، دسترسی و همکاری فراهم می‌کند. رمزارز‌ها به کاربران اجازه می‌دهند میزان ارزش مورد نظر را انتقال دهند. به عنوان مثال‌، برای خرید سرزمین‌های دیجیتال در دیسنترالند می‌توان از رمزارز استفاده کرد.

## **بررسی عمیق‌تر کاربردهای بلاکچین در تلاقی با فناوری‌ها و حوزه‌های دیگر**

## **هوش مصنوعی**

هوش مصنوعی به دستگاهی اطلاق می‌گردد که می‌تواند محیط خود را مشاهده کند و همچنین از محیط خود بازخورد دریافت کند، این سیستم داده‌های بیرون را دریافت کرده، تحلیل می‌کند و بر اساس این تحلیل می‌تواند قدم بعدی را انتخاب و تصمیم‌گیری کند. به عبارت دیگر هوش مصنوعی مبتنی بر ورودی‌ها، به عمل پردازش می‌پردازد. مشابه این کار در بدن انسان نیز رخ می‌دهد، مغز انسان هم بر اساس اتفاقات گذشته و داده‌هایی که از قبل به آن وارد شده، نتیجه‌گیری را انجام می‌دهد.

* **مثالی از کاربرد هوش مصنوعی**

یکی از اولین و عملیاتی‌ترین سیستم از مفهوم یادگیری سلسله مراتبی[[134]](#footnote-134) که به وسیله گوگل پیاده‌سازی شد، سیستم GBoard می‌باشد. یک کیبوردی که روی موبایل نصب شده و موقع تایپ کلمات را حفظ می‌کند و پیشنهاد می‌دهد. این سیستم به صورت محلی[[135]](#footnote-135) کار می‌کند. شرکت گوگل با تقسیم‌بندی واحدهای پردازشگر و قرار دادن آن‌ها در هر یک از گوشی‌های هوشمند این کار را میسر ساخته که نتیجه این اطلاعات در زمان‌بندی مشخصی (حداقل هر هفته یک‌بار) به سیستم مرکزی شرکت ارسال می‌شود. به این مفهوم ماشین یادگیری توزیع شده  [[136]](#footnote-136)گفته می‌شود.

مفهوم سیستم‌های چند عاملی[[137]](#footnote-137) در تقابل با سیستم‌های توزیع شده قرار دارد، بدین منظور که سیستم‌های توزیع شده همگی یک هدف مشخص را دنبال می‌کنند اما در سیستم‌های چندعاملی  تقسیم کار صورت گرفته و هر عامل یک هدف خاص را دنبال می‌کند.

* **تلاقی هوش مصنوعی و بلاکچین**

هوش مصنوعی یک واحد پردازشگر مرکزی است و دارای فضای متمرکز، بسته و قطعی است. از طرفی بلاکچین فضایی برای ذخیره دیتاست که حق نوشتن و خواندن را عادلانه بین کاربران توزیع می‌کند و دارای فضایی غیرمتمرکز، متن باز[[138]](#footnote-138)، شفاف و احتمالی است. در عصر حاکمیت دیتا، قدرت در اختیار شرکت‌های بزرگی مثل آمازون، فیسبوک و گوگل و ... است. با وجود تضادهایی که وجود دارد، فضایی که هوش مصنوعی و بلاکچین با هم تلاقی پیدا می‌کنند، دیتا است. بلاکچین اعتماد را حل کرده است و در این موضوع در هوش مصنوعی کاربرد دارد.

با تعریف دیگری، بلاکچین اینترنت ارزش‌هاست که مفهوم پول را در خود دارد. سیستم غیرمتمرکزی که امکان انتقال پول بین حساب کاربران را می‌تواند فراهم کند. برای توصیف این کاربرد فرض کنید، سرعت خودرویی که در اتوبان از عددی بالاتر رفت، دوربین از آن عکس بگیرد و جریمه‌ای برای راننده ثبت شود. حال چنانچه این عامل هوشمند پرداخت جریمه را از حساب راننده‌ی خودرو، به صورت اتومات نیز انجام دهد، در این حالت پرداخت مبلغ جریمه بین دو کامپیوتر انجام خواهد شد و انسانی مداخله نمی‌کند. این فضا در بلاکچین امکان پیاده‌سازی را دارد چرا که به طور غیرمتمرکز امکان انتقال دیتا و پول فراهم است.

در کاربردی دیگر وقتی نیاز باشد در مسائل هوش‌ مصنوعی یک‌بار محاسباتی سنگینی انجام شود منطقی نیست برای این کار یک سخت‌افزار عظیمی خریداری شود و این منطق سیستم‌های ابری[[139]](#footnote-139) موجود است. در بلاکچین به طور مثال گولم[[140]](#footnote-140) نام یک پلتفرم [غیرمتمرکز](https://arzmodern.net/blog/academy/item/1003-%D8%A8%D8%A7%D8%B2%D8%A7%D8%B1-%D8%BA%DB%8C%D8%B1%D9%85%D8%AA%D9%85%D8%B1%DA%A9%D8%B2-%DA%86%DB%8C%D8%B3%D8%AA%D8%9F) است که توان پردازشی را بین کاربران توزیع می‌کند. یعنی در این پلتفرم به ازای توکنی که خریداری شود، قدرت محاسباتی اجاره داده شده و این بستر بسیار مناسبی برای هوش مصنوعی است.

پروژه فچ[[141]](#footnote-141) نیز سعی دارد یک راه‌حل جامع و ترکیبی از فناوری‌های هوش مصنوعی، اینترنت اشیا، یادگیری ماشین[[142]](#footnote-142)، بلاکچین و تنگل را ارائه کند و در حوزه انرژی، حمل‌ونقل و زنجیره تأمین کاربرد دارد.

## **اینترنت اشیا**

اینترنت، شبکه‌ای از میلیون‌ها کامپیوتر متصل به هم از سرتاسر دنیا است که امکان تبادل اطلاعات بین کامپیوترها را ایجاد می‌کند. اینترنت اشیاء به زبان ساده، ارتباط [حسگرها](https://fa.wikipedia.org/wiki/%D8%AD%D8%B3%DA%AF%D8%B1) و دستگاه‌ها از طریق شبکه‌‌ای است که می‌توانند با یکدیگر و با کاربران آن‌ها به یک زبان مشترک تعامل کنند. این مفهوم نخستین بار در سال ۱۹۹۹ توسط کوین اشتون مورد استفاده قرار گرفت و جهانی را توصیف کرد که در آن هر چیزی، از جمله اشیای بی‌جان، برای خود هویت [دیجیتال](https://fa.wikipedia.org/wiki/%D8%AF%DB%8C%D8%AC%DB%8C%D8%AA%D8%A7%D9%84) داشته باشند و به کامپیوترها اجازه دهند آن‌ها را سازماندهی و مدیریت کنند. این مفهوم مجموعه‌ای از فناوری‌هایی چون شبکه‌های کامپیوتری، فناوری RFID[[143]](#footnote-143)، موتورهای جستجوگر، مدیریت شبکه، سنسورها، عملگرهای مختلف و ... است.

RFID فناوری رادیو شناسه است که برای اتصال [حسگرها](https://fa.wikipedia.org/wiki/%D8%AD%D8%B3%DA%AF%D8%B1) و دستگاه‌ها محیط پیرامون به کار می‌رود. در این تکنولوژی دیتای هر دیوایس روی یک قطعه الکترونیکی[[144]](#footnote-144) ذخیره می‌شود و ارتباط از طریق امواج الکترومغناطیسی است. شبیه به کاری در سطح پایین‌تر، که در بارکد کالا اطلاعاتی مثل نام کالا و قیمت روی آن ذخیره شده است و بارکدخوان آن اطلاعات را می‌خواند.

به طور مثال لباس‌شویی در منزل از طریق یک اپلیکیشن روی موبایل امکان کنترل داشته باشد. زمان برگشتن از سرکار آن را روشن کنید و تا زمان رسیدن به منزل شست و شوی لباس‌ها تمام شده باشد.

بحثی که در اینترنت اشیا مطرح می‌شود، هک شدن دیتا یا فرایند دریافت و پرداخت دو ربات است. حال اگر اینترنت اشیا را به صورت قراردادهای هوشمند در ترکیب با هوش مصنوعی بر بستر بلاکچین تعریف شود، کاربردهای زیادی امکان پیاده‌سازی پیدا می‌کنند.

مثلاً اگر خودرو برقی داشته باشیم به ‌صورت شارژ هوشمند آیوتا[[145]](#footnote-145) خودرو برقی ما را شارژ کند. فرض کنید همسایه شما یک پنل خورشیدی دارد، ماشین شما به‌صورت هوشمند به این پنل خورشیدی متصل می‌شود و با این وصل شدن هم ماشین شما شارژ می‌شود و هم هزینه این شارژ توسط کوین آیوتا به پنل خورشیدی همسایه شما پرداخت می‌شود و بدون اینکه شما یک درصد متوجه شوید که این اتفاقات دارد اتفاق می‌افتد.

## **اقتصاد غیرمتمرکز (DeFi)**

مهم‌ترین کاربرد بلاکچین در فضای مالی است. دیفای یک مفهوم به معنای اقتصاد غیرمتمرکز است که از طریق بلاکچین ایجاد شد. هر بلاکچینی که قابلیت تعریف قرارداد هوشمند دارد می‌تواند بستری برای تعریف پروژه‌های دیفای باشد. در واقع لازم است هر کانسپت و یا سرویس موجود در بانک‌های سنتی، بر روی بستر بلاکچین نیز به طور غیرمتمرکز تعریف شود و هیچ نهاد واسطی وجود نداشته باشد. از طرفی در حال حاضر افرادی هستند که حساب بانکی ندارند[[146]](#footnote-146) و به همین خاطر از سرویس‌های ارائه شده نمی‌توانند استفاده کنند. این افراد یا موجودی ندارند که حسابی ندارند و یا سن قانونی برای افتتاح حساب ندارند، که البته تعدادشان کم نیست و در دیفای فضایی برای این دسته افراد نیز فراهم شده است. (اقتصاد باز)

نیازهای ایجاد شده منجر به پیاده‌سازی مفاهیم زیر بر روی بلاکچین شد:

* پلتفرم و پروژه‌هایی جهت تعریف سیستم وام‌دهی (قبل از این نیاز به وثیقه یا اعتبارسنجی بود، تا بر اساس آن وام تعلق گیرد. اما در دیفای نیازی به هیچ یک نیست و بلافاصله وام تعلق می‌گیرد.)
* استیبل کوین‌ها ( کوین‌هایی که پشتوانه دارند)
* صرافی‌های غیرمتمرکز
* بازارهای مشتقات (قراردادهای آتی، حق تقدم، بیمه)
* بیزینس مدل‌ها و پروژه‌های جدیدی که در فضای متمرکز امکان تعریفشان نبود.

هر بلاکچینی که قابلیت تعریف قرارداد هوشمند دارد می‌تواند بستری برای تعریف پروژه‌های دیفای باشد.

* **توکن‌های حاکمیتی**

این مفهوم از دل دیفای ایجاد شد. وقتی نهاد متمرکزی وجود ندارد، دارندگان آن توکن، می‌توانند در تصمیم‌گیری‌ها و رأی‌گیری‌ها برای آینده یک سیستم یا شبکه نقش داشته باشد. به توکن‌هایی که برای اداره و مدیریت یک پروژه یا پلتفرم تعریف می‌شوند، توکن‌های حاکمیتی یا گاورننس اطلاق می‌شوند. مثلاً در صورت ایجاد خطا، چه راه‌حلی برای آن پیاده‌سازی شود. این توکن‌ها برای افرادی که قصد دارند در آینده پلتفرم حق رأی داشته باشند کاربردی است.

به طور مثال پروتکل کامپوند[[147]](#footnote-147) یک پلتفرم وام‌دهی است. دارندگان این توکن می‌توانند در فرایندهای رأی‌گیری پروتکل کامپوند شرکت کنند. توکن SNX برای پلتفرم سینتتیکس[[148]](#footnote-148) (استیبل کوین‌ها) است. توکن MKR برای پلتفرم میکر است.

## **سازمان خود مختار غیرمتمرکز**

دائو سازمانی است که تحت حاکمیت یک شخص یا گروه خاص نیست و به ‌صورت خودگردان و غیرمتمرکز اداره می‌شود. دائو یک سازمان فیزیکی هم نیست، بلکه یک سازمان اینترنتی است که اعضای آن می‌توانند کاربرانی از نقاط مختلف جهان باشند. دائوها در حقیقت [قراردادهای هوشمندی](https://arzdigital.com/smart-contracts-explained/) هستند که تاکنون بیشتر آن‌ها روی بلاکچین [اتریوم](https://arzdigital.com/what-is-ethereum/) اجرا شده‌اند؛ اما هر بلاکچینی که از فناوری قراردادهای هوشمند پشتیبانی می‌کند، می‌تواند میزبان یک دائو هم باشد. سازوکار این نهادها کاملا خودمختار بوده و دارای قوانین شفافی هستند که از طریق قراردادهای هوشمند وضع می‌گردند. این قوانین در مرحله‌ی بعد به رأی‌گیری گذاشته شده و هنگامی که به تصمیم‌گیری واحدی برسند اجرایی خواهند شد؛ ساختار سلسله‌مراتبی استفاده‌شده در سازمان‌های خودمختار توزیع شده شباهت فراوانی به سازوکار شرکت‌های بزرگ داشته که هریک از کاربران تا حدی بر نظارت پروتکل‌های اجرایی مشارکت دارند. شاید بخش مهمی از جذابیت این نوع سازوکار هم‌راستایی پاداش‌ها و آیتم‌های انگیزه‌بخش باشد؛ به ‌بیان دیگر هر کاربر تنها لازم است به پیشنهاداتی رأی دهد که به پویایی بیشتر پروتکل منجر خواهند شد.

## **توکن‌های غیرقابل تعویض (NFT)**

مفهوم قابل تعویض[[149]](#footnote-149) : یک اسکناس یک دلاری نسبت به یک اسکناس یک دلاری دیگر از نظر ارزش کاملاً برابر است و هر دو می‌توانند با یکدیگر تعویض شوند. یعنی زمانی که یک اسکناس یک دلاری را قرض می‌دهید، انتظار ندارید که بعداً دقیقاً همان اسکناس را پس بگیرید.

مفهوم غیرقابل تعویض[[150]](#footnote-150) : اما هر قطعه الماس که یک شماره سریال منحصربه‌فرد دارد با قطعه الماس دیگری قابل تعویض نیست. یا اگر خودروی خود را قرض بدهید تا دوست شما به مسافرت برود، انتظار دارید دقیقاً همان خودرو را پس بگیرید نه یک خودروی دیگر.

NFT ها ایجاد شدند تا هر نوع دارایی‌ را بتوان به دنیای بلاکچین وارد کرد. آیتم‌‌های بازی‌های کامپیوتری، اقلام کلکسیونی، آثار هنری دیجیتال، هویت دیجیتال، بلیط رویدادهای مختلف، نام‌ دامنه‌ها، یک خانه که به‌صورت توکن درآمده و... در دسته توکن‌های غیرقابل تعویض جای می‌گیرند.

کریپتوکیتیز[[151]](#footnote-151) نوعی بازی از سبک کلکسیونی و پرورشی است که به کاربران اجازه می‌‌دهد تا در بستر بلاکچینی، گربه‌های کارتونی بامزه‌ای را جمع‌آوری کرده و آن‌ها را در پلتفرم مخصوصی خرید و فروش نمایند. کریپتوکیتی‌ها ارز نیستند بلکه یک دارایی به‌حساب می‌آیند. این بازی به‌قدری در میان جامعه کاربران بلاک چین معروف شد که در ابتدای انتشار آن، شبکه اتریوم با کندی سرعت مواجه گشت.

شرکت WISeKey یک شرکت پیشرو در امنیت سایبری[[152]](#footnote-152)، هوش مصنوعی و اینترنت اشیا، سال ۲۰۱۸ اعلام کرد که روی NFT هایی کار می‌کند که پشتوانه‌اش هویت افراد است.

شبکه بایننس اسمارت چین اولین استاندارد تولید NFT خود یعنی BEP-721 را در اواخر سال ۲۰۲۰ عرضه کرد. کمی بعد در اوایل سال ۲۰۲۱، استاندارد BEP-1155 با هدف ایجاد یک فرمت انعطاف‌پذیر و رقابت از نظر عملکرد با استانداردهای شبکه اتریوم نظیر ERC-721 و ERC-1155 ایجاد شد. در این استاندارد‌ها علاوه بر امکان خرید، فروش امکان گسترش یا تولید مثل[[153]](#footnote-153) نیز وجود دارد. اطلاعات در مورد این NFT ها را در سایت https://dappradar.com می‌توان دنبال کرد.

* **سیستم ذخیره‌سازی غیرمتمرکز محتوا**

IPFS[[154]](#footnote-154)، یک سیستم توزیع فایل همتا به همتا و غیر متمرکز است. روش ذخیره‌سازی این سیستم بر مبنای محتوا[[155]](#footnote-155) است.

در این روش هر فایل دارای یک هش است، از آنجا که تابع هش یک تابع یک طرفه است، پس اگر یک ورودی، چندین بار به این تابع داده شود خروجی یکسان خواهد بود. IPFS، به کمک این روش توانسته است از ذخیره‌سازی فایل‌های تکراری جلوگیری کند. برای دسترسی به فایل‌های ذخیره شده در این سیستم می‌توان از طریق هش منحصر به فرد آن، فایل مورد نظر را دانلود کرد. جهت اطمینان از اینکه فایل دانلود شده دقیقا همان فایل مورد نظر است، می‌توان از طریق هش این اعتبارسنجی را انجام داد.

برای ایجاد یک NFT به طور مثال یک عکس، فایل آن در یک فضای ذخیره‌سازی مانند IPFS یا آرویو[[156]](#footnote-156) یا ... ذخیره می‌شود. پس از ذخیره‌ی فایل، هش آن که یک عدد است به عنوان شناسه فایل عکس شناخته می‌گردد. در بلاکچین این شناسه به عنوان متادیتا، در یک توکن مینت شده است. حال این توکن می‌تواند‌ در مارکت پلیس‌*‌‌*ها [[157]](#footnote-157)لیست شود. خریدار این توکن، در واقع دارنده شناسه‌ای است که از طریق آن می‌تواند به عکس دسترسی داشته باشد.

## **اوراکل**

داده‌های بیرون از شبکه‌ی بلاکچین که قرارداد‌های هوشمند به آن‌ها دسترسی ندارند، توسط اوراکل به داخل شبکه بلاکچین منتقل می‌شوند. داده‌های داخل بلاکچین قطعی هستند، یعنی هر چیزی که در شبکه بلاکچین ثبت شود، دیگر امکان تغییر آن وجود ندارد. از طرفی داده‌های بیرون از بلاکچین مثل قیمت بیت‌کوین مدام در حال تغییر هستند. اوراکل پلی میان دنیای بلاکچین و دنیای بیرون از آن است.

در مبحث مربوط به NFT داینامیک[[158]](#footnote-158) نیز اوراکل‌ها اطلاعات را به فضای داخل بلاکچین انتقال می‌دهند. به طور مثال می‌تواند عملکرد یک بازیکن فوتبال باشد که در بلاکچین توکنیزه شده است. عملکرد یک بازیکن مدام در حال تغییر است و این مفهوم Event Base NFT است. اگر بازیکن گل بزند به ارزش توکن آن افزوده شده و اگر مصدوم شود، ارزش توکن آن نیز کم می‌شود. اطلاعات مربوط به عملکرد بازیکن از طریق اوراکل به داخل بلاکچین منتقل می‌گردد. پروتکل RareLink از طریق یک cross-chain که بین اتریوم و پولکادات ایجاد کرده است، زیر ساختی برای Dynamic NFT ها می‌باشد.

## **بخش پنجم**

## **روش‌های کسب درآمد و جذب سرمایه از طریق رمزارزها**

## **لانچ‌پد**[[159]](#footnote-159)

لانچ‌پد یک پلتفرم برای عرضه توکن‌ها است. لانچ‌پد به پروژه‌ها کمک می‌کند که برای توسعه بیشتر خود در فضای رمز ارزها، به جذب سرمایه بپردازند. در عرضه اولیه بخشی از توکن‌ها به بخشی از کاربران اختصاص می‌یابد. مکانیزم اجرایی اختصاص توکن‌ها به کاربران دو گونه است. یک روش تصادفی است. یعنی افرادی که به آن‌ها توکن‌های عرضه شده اختصاص داده می‌شود، تصادفی انتخاب می‌شوند. در روش دیگر یک استخر وجود دارد که کاربران می‌توانند با خریداری توکن‌های معرفی شده و قفل کردن آن‌‌ها در این استخرها شانس خود را افزایش دهند. به طور مثال فردی که 100 تا توکن دارد نسبت به فردی که 10 تا توکن دارد از شانس بیشتری جهت انتخاب شدن برخوردار است. در این حالت ممکن است، لانچ‌پدی با پروژه‌های مختلف دیفای قرارداد همکاری داشته باشد. به طور مثال یک لانچ‌پد اعلام می‌کند چنانچه کاربر در پلتفرم بلنسر[[160]](#footnote-160) توکن تتر را به عنوان نقدینگی قرار دهد و توکن BAL دریافتی را در استخر لانچ‌پد قفل کند از شانس بالاتر برخوردار می‌شود.

## **‏ ‏ایردراپ**[[161]](#footnote-161)

در ایردراپ مقدار مشخصی توکن به طور رایگان بین کاربران توزیع می‌شود. ایردراپ معمولا توسط تیم یک رمزارز انجام می‌شود تا کاربران را به استفاده و افزایش محبوبیت کوین یا توکن تشویق کند. اکثر کمپین‌های ایردراپ با سازوکاری نظیر دریافت کوین یا توکن در ازای انجام کارهای ساده مانند به اشتراک‌گذاری اخبار، مطلع کردن دوستان یا دانلود برنامه اجرا می‌شوند.

مثلاً در ایردراپ شبکه فلیر[[162]](#footnote-162) در یک لحظه زمانی از شبکه ریپل عکس فوری[[163]](#footnote-163) گرفتند و به تمام دارندگان ریپل با نرخ یک به یک، توکن اسپارک[[164]](#footnote-164) توزیع شد. جهت دریافت توکن‌های ایردراپ، اینکه ارز اولیه در کجا نگهداری می‌شود، اهمیت دارد. به طور مثال دارندگان ریپل اگر ارز خود را در کیف پول خود ریپل نگه داشته بودند ارز اسپارک به آن‌ها تعلق گرفت، اما اگر در صرافی‌هایی که از ایردراپ ارز اسپارک پشتیبانی نمی‌کردند، مانند صرافی‌های ایرانی یا حتی کوین‌بیس[[165]](#footnote-165) ارز ریپل[[166]](#footnote-166) خود را نگه داشته بودند، ارز اسپارک به آن‌ها تعلق نگرفت. چرا که زمانی شما صاحب یک توکن هستید که کنترل آن دست خودتان باشد. وقتی توکن را در صرافی‌های متمرکز نگهداری می‌کنید، این ارز در کیف پول صرافی قرار دارد و کلید خصوصی کیف پول نیز در اختیار صرافی است. یعنی صرفا یک اعتبار عددی در اکانت شما نمایش داده می‌شود. حال اگر صرافی با ایردراپ موافق باشد به کاربران توکن اختصاص می‌دهد، در غیر این صورت کاربران در ایردراپ شرکت داده نمی‌شوند.

## **عرضه عمومی اولیه**

IPO[[167]](#footnote-167) یک عرضه عمومی اولیه است. زمانی که یک شرکت برای اولین بار سهام خود را به بازار سهام عرضه می‌کند، افراد و سایر شرکت‌هایی که به آن علاقه‌مند هستند، می‌توانند سهام شرکت را با قیمت مشخص خریداری کنند. از این سهام می‌توان برای رأی‌گیری درباره اقدامات خاصی که شرکت انجام می‌دهد استفاده کرد، زیرا خریدار واقعاً صاحب جزئی از شرکت شده‌ است.

## **عرضه اولیه توکن**

ICO[[168]](#footnote-168) همان مفهوم عرضه اولیه توکن را دارد. توسعه‌دهندگان پروژه از این طریق سرمایه جذب می‌کنند. برای انتخاب یک ICO‌ جهت سرمایه‌گذاری به ایده پروژه و نقشه راه آن، پشتوانه‌ و تیم‌ توسعه‌دهنده‌اش و همچنین میزان مشارکت افراد باید توجه کرد.

## **عرضه اولیه توکن از طریق صرافی**

از سال ۲۰۱۹ مفهوم IEO[[169]](#footnote-169) شکل گرفت و در صرافی‌ها یک پلتفرم جهت برگزاری عرضه اولیه توکن‌ها ایجاد شد تا کاربران صرافی در آن شرکت کنند. توجه شود به صرف اینکه به طور مثال بایننس برگزار کننده عرضه اولیه است، به پروژه برای سرمایه‌گذاری نمی‌توان اعتماد کرد.

## **عرضه اولیه توکن از طریق صرافی غیرمتمرکز**

این روش، از نظر ساختاری بسیار مشابه IEO است اما عرضه توکن در یک صرافی غیرمتمرکز صورت می‌گیرد. به طور مثال دائومیکر[[170]](#footnote-170) و پولکاستارتر[[171]](#footnote-171) دو پلتفرم‌های ارائه دهنده IDO[[172]](#footnote-172) هستند.

## **عرضه اولیه فارم**

IFO[[173]](#footnote-173) اولین‌بار توسط صرافی غیرمتمرکز پنکیک سواپ[[174]](#footnote-174) مطرح شد، یکی از مدل‌های تأمین سرمایه در بازار رمزارزها است. در این رویداد رمزارزها قبل از لیست شدن در صرافی‌ها پیش‌فروش[[175]](#footnote-175) می‌شوند. پس کاربران می‌توانند رمزارز را با قیمتی کمتر از عرضه عمومی خریداری کنند.

## **عرضه اولیه توکن‌هایی که در حوزه بازی هستند از طریق صرافی**

در IGO[[176]](#footnote-176) صرفا توکن‌هایی که در حوزه بازی هستند عرضه می‌گردد. پروژه‌هایی که در صنعت بازی فعالیت دارند، جهت جذب سرمایه و توسعه نرم‌افزار بخشی از توکن‌های خود را از طریق لانچ‌پد‌ها عرضه می‌کنند.

## **عرضه اولیه دارایی‌هایی که در حوزه بازی ایجاد می‌شوند از طریق صرافی**

در بازی‌ها مفهومی با عنوان دارایی[[177]](#footnote-177) وجود دارد. به طور مثال در یک بازی با عبور از مرحله‌ای امتیاز به کاربر تعلق می‌گیرد. کاربر با این امتیازها می‌تواند ماشین، قایق، لباس و یا ... برای کاراکتر بازی تهیه کند. حال این ماشین در حکم یک دارایی برای کاربر است. در مفهوم IAO[[178]](#footnote-178) این دارایی می‌تواند در لانچ‌پدها عرضه شده و برای کاربر کسب درآمد داشته باشد.

## **کسب درآمد از طریق بازی کردن**

از زمانی که بازی کریپتوکیتیز[[179]](#footnote-179) طرفداران بسیاری را به سمت خود جلب کرد، صنعت بازی نیز رشد کرد و بازی‌های دیگر هم توسعه یافتند. این بازی‌ها از مدل Play to Earn یا Gamefi استفاده می‌کنند و در واقع ترکیبی از گیمینگ[[180]](#footnote-180)، امور مالی و روشی برای کسب درآمد هستند. بر خلاف بازی‌های آنلاین سنتی که برای برنده شدن باید پول پرداخت کرد، سیستم‌های Play to Earn یا Game Mining مدل "بازی کنید تا به دست بیاورید" را معرفی می‌کنند. به طور مثال اکسیدمی[[181]](#footnote-181) یک بازی روی شبکه پولکادات است. در این پروژه تورنمنت[[182]](#footnote-182) یا مسابقه‌هایی برگزار می‌شود و به برنده بازی از توکن XED جایزه تعلق می‌گیرد. افرادی هم می‌تواند روی برنده بازی شرط‌بندی کنند و درآمد داشته باشند.

## **کسب درآمد از طریق استیک کردن**[[183]](#footnote-183) **رمزارزها**

در فرآیند استیک کردن رمزارز دارایی‌ها به عنوان یک وثیقه، در جهت افزایش اعتبار و منابع آن شبکه قفل می‌شود تا به اضافه شدن بلوک جدید به زنجیره شبکه کمک کند. در واقع وقتی اقدام به استیک کردن یک رمز ارز می‌کنید، تبدیل به یک گره در شبکه آن می‌شوید و به بررسی تراکنش‌ها و اضافه کردن بلاک‌های جدید به بلاک چین می‌پردازید و به ازای انجام این کار پاداش دریافت می‌کنید. همان‌ کاری که دستگاه‌های ماینر انجام می‌دهند. البته در استیکینگ گره‌ها به جای ماینر (استخراج‌کننده)، اعتبارسنج[[184]](#footnote-184) نام دارند. پس گره‌هایی که میزان بیشتری از رمزارز شبکه را استیک کرده‌اند، شانس بیشتری برای کسب فرصت ساخت بلاک بعدی و اضافه شدن به بلاکچین خواهند داشت و پاداش بیشتری دریافت می‌کنند. امکان استیک کردن در رمزارزهایی وجود دارد که مکانیزم اجماع آن‌ها POS است.

## **تأمین نقدینگی**[[185]](#footnote-185)

بر خلاف صنایع مرسوم، حوزه دیفای یک استخر سرمایه خود ساخته ندارد که وجود نقدینگی را تضمین کند. پس تأمین نقدینگی این استخرها از طریق سپرده‌گذاری در پلتفرم‌های دیفای (از جمله صرافی‌ها یا پلتفرم‌های وام‌دهی) با هدف کسب درآمد برای سرمایه‌گذار، به صورت یک بازی برد-برد انجام می‌گردد.

از طرفی کشف قیمت در واقع درک معامله‌گر از وضعیت عرضه و تقاضای آن بازار و انتظار او از فرصت‌های آینده در بازار است. این نوع سپرده‌گذاری ظرفیت این را دارد که تخصیص منابع را بالا ببرد و حتی به سرمایه‌گذاران و نهادهای مالی مختلف این امکان را بدهد که بر اساس قیمت، تصمیمات منطقی‌تری بگیرند.

## **شاخص نقدینگی‌های قفل شده**

کل نقدینگی‌های قفل شده در استخرهای نقدینگی است. TVL[[186]](#footnote-186) شاخصی جهت ارزیابی بازار دیفای و یک معیار مؤثر برای مقایسه سهم بازار از پروتکل‌های مختلف دیفای است.

## **ییلد فارمینگ**[[187]](#footnote-187)

ییلد فارمینگ به معنای قرض دادن رمز ارز به دیگران، از طریق قراردادهای هوشمند و دریافت سود است. در واقع عرضه‌کنندگان نقدینگی به استخرهای نقدینگی این سود را دریافت می‌کنند. این کاربران معمولا سرمایه خود را بین پروتکل‌های مختلف به گردش در می‌آورند تا محصول (ییلد) بیشتری به دست آورند و بهترین روش‌های ییلد فارمینگ را مخفی نگه می‌دارند چرا که هر قدر افراد بیشتری از یک روش اطلاعات داشته باشند، اثربخشی آن کاهش می‌یابد. محاسبه سود به خاطر سرعت بالای دیفای، بطور هفتگی یا حتی روزانه انجام می‌شود.

 شیوه مناسب اندازه‌گیری میزان اعتبار محیط ییلد فارمینگ دیفای ارزش کل نقدینگی بلوکه شده (TVL) است. هر قدر که ارزش بیشتری بلوکه شود، ییلد فارمینگ بیشتری نیز اتفاق می‌افتد.

افرادی که این دارایی‌ها را قرض می‌گیرند، باید وثیقه‌ای معادل با قرض به امانت بگذارند. اگر ارزش وثیقه، پایین‌تر از حداقل مورد نیاز برای پروتکل باشد، وثیقه لیکوئید خواهد شد. برای جلوگیری از لیکوئید شدن باید وثیقه بیشتری اضافه کنند. از این ‌رو بسیاری از سیستم‌ها از نسبت وثیقه بسیار بالا مثلا 750% استفاده می‌کنند تا کل بستر را از خطر لیکوئید شدن در ایمنی نسبی قرار دهند.

## **دارایی‌های مصنوعی**[[188]](#footnote-188)**، پل**[[189]](#footnote-189) **و کراس‌چین**[[190]](#footnote-190) **سه راه‌حل برای نقدینگی‌های قفل شده**

در پروژه‌های دیفای نهاد یا ارگانی جهت تأمین نقدینگی مورد نیاز وجود ندارد، پس کاربران از طریق سپرده‌گذاری این نقدینگی را تأمین می‌کنند. رشد دیفای وابسته به میزان نقدینگی‌های قفل ‌شده در استخرها است. همچنین با استقبال از حوزه‌ی دیفای نیاز به افزایش حجم نقدینگی نیز بالا می‌رود. چرا که در پلتفرم‌هایی کاربران جهت انجام تراکنش درخواست ثبت کردند، اما به علت نبود نقدینگی تراکنش آن‌ها انجام نشده و در صف انتظار قرار می‌گیرد. مفهوم ییلد فارمینگ جهت افزایش انگیزه کاربران برای نگهداری نقدینگی‌ها در پلتفرم‌های دیفای ایجاد شد. از طرفی کاربران با قفل کردن دارایی خود در پلتفرم‌*‌*ها فرصت‌های دیگر سرمایه‌گذاری و یا ترید را از دست می‌دهند.

برای حل این مشکلات پروژه‌*‌*ها سه راه‌حل ارائه دادند. یکی ایجاد دارایی‌های مصنوعی و دیگری ارتباط بین بلاکچین‌*‌*ها از طریق پل یا کراس‌چین است.

به طور مثال در پروژه فانتوم[[191]](#footnote-191) مفهوم Liquid Staking مطرح شد. با این قابلیت کاربران ضمن اینکه نقدینگی خود را در پلتفرم قفل کرده‌اند، می‌توانند در بازار ثانویه[[192]](#footnote-192)، بخشی از این دارایی را به کار ببرند. در واقع این پلتفرم به ازای درصدی از نقدینگی قفل شده، برای کاربران مقداری دارایی مصنوعی ایجاد می‌کند که کاربران از این دارایی می‌توانند در پلتفرم‌های دیفای مثلاً به عنوان وثیقه برای دریافت وام یا به عنوان تأمین نقدینگی صرافی‌های غیرمتمرکز استفاده کنند.

در راه‌حل دوم ارائه شده، بین بلاکچین‌های مختلف یک واسطی مانند پل ایجاد می‌شود. با این کار شبکه‌ها به هم متصل شده و نقدینگی می‌تواند بین ‌آن‌ها جا به جا شود.

از طرفی بعضی پروژه‌ها در ساختار خود ارتباط چند بلاکچین را دارند. این پروژه‌ها کراس‌چین هستند.

## **وام‌های سریع فلش لون**[[193]](#footnote-193)

وام‌های فلش امکان وام‌گیری ساده و به صورت لحظه‌ای را فراهم می‌کنند.کل فرآیند دریافت و بازگرداندن این وام در یک تراکنش انجام می‌شود؛ یعنی در طی یک تراکنش، وام دریافت می‌شود و در همان تراکنش، همراه با کارمزد، بازپرداخت خواهد شد. چنانچه تراکنش کامل و به درستی انجام نشود، کل تراکنش انجام نخواهد شد و تمام کارهای انجام شده از ابتدا را خنثی خواهد کرد. این امنیت دارایی‌ها را در استخر مربوطه تضمین می‌کند.

زمانی که حرف از تراکنش در شبکه‌ی بلاکچین می‌شود، ذهن ما به سمت انتقال رمز ارز از یک کیف پول به کیف پول فرد دیگر معطوف می‌شود. اما تراکنش در یک شبکه بلاکچین، به معنی ارسال یک پیام در شبکه به هدف ذخیره‌سازی آن در دفترکل توزیع شده‌ی آن شبکه است. این پیام در ساده‌ترین شکل خود می‌تواند درخواست انتقال یک کوین از کیف پول الف به کیف پول ب باشد و یا می‌تواند ترکیبی از چندین تراکنش (در دل یک تراکنش بزرگ باشد).

به طور مثال فرض کنید ۱ واحد اتریوم را در پلتفرم کامپوند وثیقه‌گذاری کنید و در ازای آن ۱۰۰۰ واحد دای[[194]](#footnote-194) وام بگیرید (تراکنش یک)، سپس این ۱۰۰۰ واحد دای را به پلتفرم کرو فایننس[[195]](#footnote-195) برده و در استخرهای آن، به رمز ارز تتر تبدیل کنید (تراکنش دو)، پس از آن تتر دریافتی را به پلتفرم یونی سواپ[[196]](#footnote-196) برده و در آن به کوین اتریوم تبدیل کنید (تراکنش سه). در اینجا سه تراکنش مختلف انجام گرفت. اما به مدد قراردادهای هوشمند، می‌توان این سه تراکنش را در قالب یک قرارداد هوشمند نوشته و به صورت یک تراکنش (که در دل خود سه تراکنش دارد) به شبکه اتریوم ارسال کرد. یعنی اول بلاک وام دریافت و تا آخر بلاک تسویه شود. (همه در یک تراکنش)

نکته مهم در اینجا این است که وام فلش را نمی‌توان در یک کیف پول ذخیره کرد و به طور کلی نمی‌توان از پلتفرم‌های حوزه دیفای خارج کرد. مثلا اگر این وام سریع را از یک پلتفرم ارائه فلش لون روی شبکه اتریوم دریافت کنید، تنها می‌توانید این وام را بین پروتکل‌های روی شبکه اتریوم بچرخانید و راهی برای واریز وام به کیف پول و یا سایر صرافی‌های متمرکز وجود ندارد. محبوب‌ترین روش برای سود کردن از وام لحظه‌ای، آربیتراژ است. یعنی شما از اختلاف قیمت دارایی‌ها در پلتفرم‌های معاملاتی مختلف استفاده می‌کنید.

## **کلام آخر**

دنیای بلاکچین و کاربردهای آن بسیار عمیق‌تر و وسیع‌تر از آن است که در اینجا عنوان شد. تلاش بر آن بود تا با معرفی بخشی از مفاهیم و کاربردهای اولیه آن آشنایی ضمنی در این حوزه ایجاد گردد. با کسب دانش و شناخت ابعاد مختلف این تکنولوژی ضمن کسب درآمد، می‌توان آینده‌ای روشن‌تر برای خود و جامعه جهانی ساخت.

1. DGCash [↑](#footnote-ref-1)
2. David Chaum [↑](#footnote-ref-2)
3. Cryptography [↑](#footnote-ref-3)
4. Nick Szabo [↑](#footnote-ref-4)
5. Hash Cash [↑](#footnote-ref-5)
6. Consensus Mechanism [↑](#footnote-ref-6)
7. Proof of Work [↑](#footnote-ref-7)
8. Bit Gold [↑](#footnote-ref-8)
9. Satoshi Nakamoto [↑](#footnote-ref-9)
10. Centralized [↑](#footnote-ref-10)
11. Single Point of Faded [↑](#footnote-ref-11)
12. Tangle [↑](#footnote-ref-12)
13. Hash graph [↑](#footnote-ref-13)
14. Hashing [↑](#footnote-ref-14)
15. Distributed Ledger Technology (DLT) [↑](#footnote-ref-15)
16. Node [↑](#footnote-ref-16)
17. Miner [↑](#footnote-ref-17)
18. Validator [↑](#footnote-ref-18)
19. Data Science [↑](#footnote-ref-19)
20. Internet of Data [↑](#footnote-ref-20)
21. Internet of Value [↑](#footnote-ref-21)
22. Tether [↑](#footnote-ref-22)
23. Silk Road [↑](#footnote-ref-23)
24. Federal Bureau of Investigation (FBI) [↑](#footnote-ref-24)
25. Ross William Ulbricht [↑](#footnote-ref-25)
26. Public Blockchain [↑](#footnote-ref-26)
27. Private Blockchain [↑](#footnote-ref-27)
28. XRP [↑](#footnote-ref-28)
29. Hyperledger [↑](#footnote-ref-29)
30. Consortium Blockchain [↑](#footnote-ref-30)
31. Hybrid Blockchain [↑](#footnote-ref-31)
32. Proof of Work (POW( [↑](#footnote-ref-32)
33. Proof of Stake (POS( [↑](#footnote-ref-33)
34. Practical Byzantine Fault Tolerance (PBFT) [↑](#footnote-ref-34)
35. Zero-Knowledge Proof [↑](#footnote-ref-35)
36. Mempool [↑](#footnote-ref-36)
37. Stake [↑](#footnote-ref-37)
38. Peercoin [↑](#footnote-ref-38)
39. Cardano (ADA) [↑](#footnote-ref-39)
40. Barbara Liskov [↑](#footnote-ref-40)
41. Miguel Castro [↑](#footnote-ref-41)
42. Immutable [↑](#footnote-ref-42)
43. Decentralized  [↑](#footnote-ref-43)
44. [Client-Server](https://fa.wikipedia.org/wiki/%D9%85%D8%AF%D9%84_%D8%B3%D8%B1%D9%88%DB%8C%D8%B3%E2%80%8C%DA%AF%DB%8C%D8%B1%D9%86%D8%AF%D9%87-%D8%B3%D8%B1%D9%88%DB%8C%D8%B3%E2%80%8C%D8%AF%D9%87%D9%86%D8%AF%D9%87) [↑](#footnote-ref-44)
45. Capacity [↑](#footnote-ref-45)
46. Anonymity [↑](#footnote-ref-46)
47. Know Your Customer (KYC) [↑](#footnote-ref-47)
48. Ethereum [↑](#footnote-ref-48)
49. Vitalik Buterin [↑](#footnote-ref-49)
50. Smart Contract  [↑](#footnote-ref-50)
51. Task [↑](#footnote-ref-51)
52. Stablecoins [↑](#footnote-ref-52)
53. Initial Coin Offering  [↑](#footnote-ref-53)
54. Oracles [↑](#footnote-ref-54)
55. Amazon Web Service (AWS) [↑](#footnote-ref-55)
56. Digital Currency [↑](#footnote-ref-56)
57. Record Keeping [↑](#footnote-ref-57)
58. Smart contracts [↑](#footnote-ref-58)
59. Security [↑](#footnote-ref-59)
60. Altcoin (Alternative to BITCOIN) [↑](#footnote-ref-60)
61. Native [↑](#footnote-ref-61)
62. Wrapped Token [↑](#footnote-ref-62)
63. Custodian [↑](#footnote-ref-63)
64. TRX [↑](#footnote-ref-64)
65. BitGo [↑](#footnote-ref-65)
66. Gemini [↑](#footnote-ref-66)
67. Coinbase [↑](#footnote-ref-67)
68. DOT [↑](#footnote-ref-68)
69. DeFi [↑](#footnote-ref-69)
70. Hybrid [↑](#footnote-ref-70)
71. Peer-to-Peer [↑](#footnote-ref-71)
72. Wallet [↑](#footnote-ref-72)
73. Custodial [↑](#footnote-ref-73)
74. Non-Custodial [↑](#footnote-ref-74)
75. Ledger [↑](#footnote-ref-75)
76. Trezor [↑](#footnote-ref-76)
77. Artificial Intelligence (AI) [↑](#footnote-ref-77)
78. Internet of Things (IOT) [↑](#footnote-ref-78)
79. Infrastructure [↑](#footnote-ref-79)
80. Interoperability [↑](#footnote-ref-80)
81. Decentralized Finance (DeFi) [↑](#footnote-ref-81)
82. Stable Coin [↑](#footnote-ref-82)
83. Non-fungible Token (NFT) [↑](#footnote-ref-83)
84. Oracle [↑](#footnote-ref-84)
85. Centralized Exchanges (CEX) [↑](#footnote-ref-85)
86. Decentralized Exchanges (DEX) [↑](#footnote-ref-86)
87. Decentralized Autonomous Organization (DAO) [↑](#footnote-ref-87)
88. Automated Market Makers (AMM) [↑](#footnote-ref-88)
89. Identity [↑](#footnote-ref-89)
90. Privacy [↑](#footnote-ref-90)
91. Virtual Reality (VR) [↑](#footnote-ref-91)
92. File Storage [↑](#footnote-ref-92)
93. Payment [↑](#footnote-ref-93)
94. Insurance [↑](#footnote-ref-94)
95. Lending [↑](#footnote-ref-95)
96. Metaverse [↑](#footnote-ref-96)
97. Fetch.ai [↑](#footnote-ref-97)
98. The Graph [↑](#footnote-ref-98)
99. VeChain Token [↑](#footnote-ref-99)
100. Ethereum [↑](#footnote-ref-100)
101. Society for Worldwide Interbank Financial Telecommunication (SWIFT) [↑](#footnote-ref-101)
102. Inter Blockchain [↑](#footnote-ref-102)
103. Cosmos [↑](#footnote-ref-103)
104. ICON [↑](#footnote-ref-104)
105. Yearn. finance [↑](#footnote-ref-105)
106. Tether [↑](#footnote-ref-106)
107. Theta Network [↑](#footnote-ref-107)
108. Enjin Coin [↑](#footnote-ref-108)
109. Chainlink [↑](#footnote-ref-109)
110. KuCoin Token [↑](#footnote-ref-110)
111. Binance  [↑](#footnote-ref-111)
112. 1inch Network [↑](#footnote-ref-112)
113. Burger Swap [↑](#footnote-ref-113)
114. Synthetix [↑](#footnote-ref-114)
115. Decred [↑](#footnote-ref-115)
116. Uniswap  [↑](#footnote-ref-116)
117. PancakeSwap  [↑](#footnote-ref-117)
118. Deutsche Bank [↑](#footnote-ref-118)
119. Treasuries of Cargill [↑](#footnote-ref-119)
120. Ontology Coin [↑](#footnote-ref-120)
121. Monero [↑](#footnote-ref-121)
122. Zcash [↑](#footnote-ref-122)
123. Unity Protocol [↑](#footnote-ref-123)
124. Arweave [↑](#footnote-ref-124)
125. Filecoin [↑](#footnote-ref-125)
126. Ripple [↑](#footnote-ref-126)
127. Stellar  [↑](#footnote-ref-127)
128. Tidal Finance [↑](#footnote-ref-128)
129. Nexus Mutual [↑](#footnote-ref-129)
130. Compound [↑](#footnote-ref-130)
131. Maker [↑](#footnote-ref-131)
132. Decentraland [↑](#footnote-ref-132)
133. Sandbox [↑](#footnote-ref-133)
134. Federated Learning [↑](#footnote-ref-134)
135. Local [↑](#footnote-ref-135)
136. Distributing Machine Learning [↑](#footnote-ref-136)
137. Multi Agent System [↑](#footnote-ref-137)
138. Open Source [↑](#footnote-ref-138)
139. Cloud System [↑](#footnote-ref-139)
140. GNT [↑](#footnote-ref-140)
141. Fetch [↑](#footnote-ref-141)
142. Machine Learning [↑](#footnote-ref-142)
143. Radio Frequency Identification  [↑](#footnote-ref-143)
144. Integrated Circuit (IC) [↑](#footnote-ref-144)
145. IOTA [↑](#footnote-ref-145)
146. Unbanked People [↑](#footnote-ref-146)
147. COMP [↑](#footnote-ref-147)
148. Synthetix [↑](#footnote-ref-148)
149. Fungible [↑](#footnote-ref-149)
150. Non-fungible [↑](#footnote-ref-150)
151. CryptoKitties [↑](#footnote-ref-151)
152. Cyber Security [↑](#footnote-ref-152)
153. Breed [↑](#footnote-ref-153)
154. InterPlanetary File System [↑](#footnote-ref-154)
155. Content Based Address [↑](#footnote-ref-155)
156. Arweave (AR) [↑](#footnote-ref-156)
157. Marketplaces [↑](#footnote-ref-157)
158. Dynamic [↑](#footnote-ref-158)
159. Launchpad [↑](#footnote-ref-159)
160. Balancer [↑](#footnote-ref-160)
161. Airdrop [↑](#footnote-ref-161)
162. Flare [↑](#footnote-ref-162)
163. Snapshot [↑](#footnote-ref-163)
164. Spark [↑](#footnote-ref-164)
165. Coinbase [↑](#footnote-ref-165)
166. Ripple (XRP) [↑](#footnote-ref-166)
167. Initial Public Offerings [↑](#footnote-ref-167)
168. Initial Coin Offering [↑](#footnote-ref-168)
169. Initial Exchange Offering [↑](#footnote-ref-169)
170. Dao Maker [↑](#footnote-ref-170)
171. Polkastarter [↑](#footnote-ref-171)
172. Initial DEX Offering [↑](#footnote-ref-172)
173. Initial Farm Offering [↑](#footnote-ref-173)
174. PancakeSwap [↑](#footnote-ref-174)
175. Pre-Sale [↑](#footnote-ref-175)
176. Intinal Game Offering [↑](#footnote-ref-176)
177. Asset [↑](#footnote-ref-177)
178. Intinal Asset Offering [↑](#footnote-ref-178)
179. CryptoKitties [↑](#footnote-ref-179)
180. Gaming [↑](#footnote-ref-180)
181. Exeedme [↑](#footnote-ref-181)
182. Tournament [↑](#footnote-ref-182)
183. Staking [↑](#footnote-ref-183)
184. Validator [↑](#footnote-ref-184)
185. Liquidity Providing (Mining) : LP [↑](#footnote-ref-185)
186. Total Value Locked [↑](#footnote-ref-186)
187. Yield Farming [↑](#footnote-ref-187)
188. Synthetic Asset [↑](#footnote-ref-188)
189. Bridge [↑](#footnote-ref-189)
190. Cross-Chain [↑](#footnote-ref-190)
191. FTM [↑](#footnote-ref-191)
192. Second Market [↑](#footnote-ref-192)
193. Flash Loan [↑](#footnote-ref-193)
194. Dai [↑](#footnote-ref-194)
195. Curve Finance [↑](#footnote-ref-195)
196. Uniswap [↑](#footnote-ref-196)