مدیران مبتکر،دوره ۲، شماره ۲،تابستان ۱۴۰۱،از صفحه ۴۴-۱۳

مروری بر ارزهای دیجیتال

محمد جویا زندی[۱]

۱.دانشجوی رشته مدیریت بورس دانشگاه علمی کاربردی تحقیقات صنعتی ایران

Jooya.zandi98@gmail.com

چکیده

بیت کوین و سایر ارزهای دیجیتال مانند اتریوم به عنوان جایگزین های دیجیتالی برای پولهای منتشر شده از سوی دولت ها رشد کرده اند. از معروف ترین ارزهای دیجتال میتوان بیت کوین، اتریوم، لایت کوین،آیاس،پولکادات و غیره نام برد. برخی از ارزهای دیجیتال از جهاتی شبیه بیت کوین هستند و برخی دیگر مبتنی بر فناوری های مختلف بوده یا دارای ویژگی های جدیدی هستند که به آنها اجازه می دهد تا کاربردی بیش از انتقال ارزش داشته باشند.ارزهای دیجیتال انتقال ارزش را بدون نیاز به واسطه مانند بانک یا پردازشگر پرداخت به صورت آنلاین امکان پذیر می کنند و این امکان را فراهم می کنند که ارزش به صورت سراسری و با سرعتی بالا و در هر ساعت شبانه روز، با هزینه کم انتقال یابد. در این مقاله مروری بر موضوعات مهم رمز ارزها خواهیم داشت.

واژگان کلیدی: ارز دیجیتال، بلاک چین، رمز ارز، توکن

مقدمه

ارز دیجیتال و یا به اصطلاح برخی دیگر، ارز رمز نگاری شده یا رمز ارز در اصل یک پول دیجیتال غیر متمرکز است که برای استفاده در اینترنت طراحی شده است که در سال ۲۰۰۸ راه اندازی شد، بیت کوین اولین ارز دیجیتال بود و هنوز هم بزرگترین، تأثیرگذارترین و شناخته شده ترین آن است. در یک دهه پس از آن، بیت کوین و سایر ارزهای دیجیتال مانند اتریوم که در سال ۲۰۰۸ راه اندازی شد، اولین ارز دیجیتال بود و هنوز هم بزرگترین، تأثیرگذارترین و شناخته شده ترین آن است. در یک دهه پس از آن، بیت کوین و سایر ارزهای دیجیتال مانند اتریوم به عنوان جایگزین های دیجیتالی برای پولهای منتشر شده از سوی دولت ها رشد کرده اند. از معروف ترین ارزهای دیجتال میتوان بیت کوین، اتریوم، لایت کوین،آیاس،پولکادات و غیره نام برد. برخی از ارزهای دیجیتال از جهاتی شبیه بیت کوین هستند و برخی دیگر مبتنی بر فناوری های مختلف بوده یا دارای ویژگی های جدیدی هستند که به آنها اجازه می دهد تا کاربردی بیش از انتقال ارزش داشته باشند.ارزهای دیجیتال انتقال ارزش را بدون نیاز به واسطه مانند بانک یا پردازشگر پرداخت به صورت آنلاین امکان پذیر می کنند و به شما امکان می دهند ارزش را به صورت سراسری و با سرعتی بالا و در هر ساعت شبانه روز، با هزینه کم انتقال دهید.ارزهای دیجیتال معمولا توسط هیچ دولت یا مرجع مرکزی دیگری صادر یا کنترل نمی شوند. آنها توسط شبکه های همتا به همتا کامپیوترهایی که از یک نرم افزار رایگان و منبع باز استفاده می کنند، مدیریت می شوند. به طور کلی، هر کسی که بخواهد، میتواند در شبکه حضور داشته باشد. سوالی که ممکن است برای برخی پیش بیاید اینست که اگر بانک یا دولتی در این امر دخیل نیست، چگونه استفاده از رمز ارزها

ایمن است؟ در پاسخ باید گفت استفاده از رمز ارزها به این دلیل ایمن است که همه تراکنش ها توسط فناوری به نام بلاک چین بررسی می شوند.

حمله ۵۱ درصدی

در اولین بخش از واژه نامه بلاک چین به سراغ اصطلاحی می‌رویم که از نوعی حمله سایبری خبر می‌دهد. هکرها در حمله ۵۱٪ «۵۱٪ «Attack به بلاکچین بیت کوین حمله می‌کنند و با ایجاد نودهایی ساختگی، تقریبا نیمی از قدرت محاسباتی شبکه را می‌ربایند. این حمله می‌تواند با دستکاری تراکنش‌ها، باعث دو بار خرج کردن یک کوین شود و به این ترتیب، اعتبار بلاکچینی که مورد حمله قرار گرفته است زیر سوال می‌رود.

رمزنگاری نامتقارن

هر کسی که به سراغ فضای بلاکچین می‌رود صاحب دو کلید می‌شود. یکی از آنها «کلید عمومی (Public-key) «و دیگری «کلید خصوصی (Private Key) «هستند .کلید عمومی، چیزی است که می‌توانید آن را در اختیار تمام مردم جهان قرار دهید بدون اینکه از بابت سرقت بیت کوین‌هایتان نگران شوید؛ اما کلید خصوصی، چیزی است که اگر به دست کسی جز خودتان بیفتد، باید فاتحه بیت کوین‌هایتان یا هر ارز دیجیتالی دیگری که دارید را بخوانید! این کلیدها می‌توانند پیام‌های مختلف را رمزنگاری کنند و آن را از دسترس هکرها یا کسانی که به دنبال مشاهده اطلاعات دیگران هستند، دور نگه دارند.

بلاک چین

بلاک چین، یک دفتر کل جهانی است که داده‌های تراکنش‌ها درون آن ثبت می‌شود. تراکنش‌ها در این دفتر به صورت چندین و چند زنجیره به هم متصل می‌شوند. هر زنجیره که «بلاک» نامیده می‌شود، علاوه بر داده‌های تراکنش خودش، داده‌های تراکنش قبلی را هم دارد. این کار جلوی دستکاری و حمله هکرها را می‌گیرد. زیرا با حمله به یک بلاک، آنها باید تک‌تک بلاک‌های قبلی را هم دستکاری کنند! هر داده‌ای که در دفتر کل بلاکچین ثبت می‌شود، تا ابد، غیرقابل تغییر است و نمی‌توان به هیچ طریقی آن را حذف کرد.

تحمل خطای بیزانس

در واژه نامه بلاک چین، چیزهای جالب زیادی یافت می‌شوند که گاهی با ماجراهای تاریخی در هم آمیخته‌اند. یکی از این اصطلاح‌های جالب و کمی تاریخی «تحمل خطای بیزانس (Byzantine fault) «نامیده می‌شود. داستان این عبارت به مشکلی که ژنرال‌های دوره بیزانس با آن روبه‌رو بودند برمی‌گردد .در یکی از نبردهای آن دوره، چند ژنرال با ارتش‌های خود می‌خواستند به یک شهر حمله کنند. رمز موفقیت در اشغال آن شهر به توافق رسیدن تمام ژنرال‌ها با هم بود، اما آنها نمی‌توانستند این کار را انجام دهند چون تنها راه برای برقراری ارتباط، پیام‌هایی بود که شاید در طول مسیر دستکاری می‌شدند! گاهی در بلاکچین هم این اتفاق می‌افتد. به این ترتیب که کاربران نمی‌توانند به گره‌ها اعتماد کنند و بر سر آنها به توافق برسند. به این ماجرا، خطای بیزانس و به آستانه تحمل آن «تحمل خطای بیزانس» می‌گویند.

الگوریتم اجماع

بلاک چین، روشی جدید برای ثبت اطلاعات است. اگر قرار باشد داده جدیدی در زنجیره به ثبت برسد، باید چند کامپیوتر متصل به شبکه، آن را تایید کنند .این اجماع بر سر تاریخ یک واحد به شبکه اعتبار می‌دهد و مشخص می‌کند که هر کسی مالک چه چیزی است.

دارایی رمزنگاری شده

یکی دیگر از اصطلاح‌هایی که در واژه نامه بلاک چین به کارمان می‌آید »دارایی رمزنگاری شده» است. این دارایی‌ها، همان ارزهای دیجیتالی هستند که با اسم و رسم‌های مختلف در بلاکچین قرار دارند؛ مثلا «بیت کوین«، »اتریوم«، »لایت کوین«، »ریپل «و ... نمونه‌هایی از دارایی‌های رمزنگاری شده به شمار می‌روند.

رمزنگاری

«Cryptography»یا همان رمزنگاری، دانشی است که با استفاده از روش‌های پیچیده ریاضی راهی برای حفاظت از اطلاعات کاربران پیدا می‌کند. در این دانش که قدمتش به صدها سال قبل برمی‌گردد، اطلاعات مختلف به صورت عدد و الفبا به نمایش در می‌آید. تنها کسی که کلید این رمزها را داشته باشد می‌تواند از پیام پنهان در آنها با خبر شود.

سایفرپانک

یک مکتب فکری است که قدمت آن به زمان گسترش کامپیوترها در میان مردم باز می‌گردد. اعضای این مکتب فکری از نظارت اطلاعات توسط دولت‌ها بیزار هستند .آنها به آزادی، انتشار اطلاعات بدون محدودیت و احترام به حریم خصوصی تک‌تک کاربران اهمیت فراوانی می‌دهند. بلاک چین به دلیل غیر متمرکز و همتا به همتا بودن با استقبال زیادی از سوی سایفرپانک‌ها روبه‌رو شد.

غیرمتمرکز

غیرمتمرکز بودن ارزهای دیجیتال به این معنا است که بانک‌ها یا هر مجموعه و موسسه دیگری نمی‌توانند در ساختار بلاک چین و معامله ارزهای دیجیتال، هیچ دخالتی داشته باشند. این سازوکار به گونه‌ای طراحی شده است که بدون حضور آنها خیلی خوب کارش را انجام می‌دهد.

برنامه غیر متمرکز

در ادامه گشت و گذارمان درون واژه نامه بلاکچین به عبارت «برنامه غیر متمرکز» یا (Decentralized Application) می‌رسیم. هر «dApp» برنامه‌ای است که به وسیله چندین قرارداد هوشمند بر بستر بلاکچین پیاده‌سازی و اجرا می‌شود. این برنامه‌ها به صورت متن باز قرار می‌گیرند و هر کسی می‌تواند برای بهتر شدن آنها وارد عمل شود.

سازمان غیرمتمرکز خودگردان

این سازمان‌ها، مجموعه‌هایی مستقل و غیرمتمرکز هستند که سازوکار عمل آنها در چندین قرارداد هوشمند در بلاکچین تعریف شده است.

امضای دیجیتالی

هر فردی می‌تواند و گاهی باید یک امضای دیجیتالی داشته باشد. امضاهای دیجیتالی که به صورت کدهای هَش هستند و با استفاده از کلید خصوصی هر فرد ساخته می‌شوند این اطمینان را به وجود می‌آورند که اطلاعات بدون دستکاری به مقصد مورد نظر برسند. وقتی چنین پیامی به شما می‌رسد می‌توانید آن را با استفاده از کلید عمومی رمزگشایی کرده و از درستی اطلاعاتی که به دستتان رسیده است مطمئن شوید.

حذف واسطه

در فناوری بلاک چین، واسطه‌ها به آن معنا که در دنیای فیزیکی وجود دارند معنا ندارند .واسطه‌های بلاکچین به صورت خودکار کار خودشان را انجام می‌دهند. از میان رفتن واسطه‌ها در بلاکچین به معنی کاهش ریسک و به دنبال آن کاهش هزینه است . از طرفی، هویت کاربران مخفی می‌ماند و کسی قادر به پیگیری تراکنش‌ها نخواهد بود.

مسئله دو بار خرج کردن

"دو بار خرج کردن" که در واژه نامه بلاک چین (Double Spending) هم خوانده می‌شود، نوعی سوءاستفاده از دارایی دیجیتالی به شمار می‌رود. در این وضعیت، فرد می‌تواند یک سکه را دو بار خرج کند؛ مثلا شما می‌توانید یک عدد بیت کوین خود را به دو نفر بفروشید. با وجود آنکه بلاکچین با روند اثبات کار در مقابل این نوع کلاهبرداری ایستاده اما با این وجود بارها چنین اتفاقی افتاده است.

اتریوم

نوعی ارز دیجیتالی است که کاربردهای آن بسیار فراتر از بیت کوین است. در واقع، اتریوم یک پلتفرم آزاد بر پایه بلاکچین است که به توسعه دهندگان اجازه می‌دهد تا برنامه‌های غیرمتمرکز خودشان را در بستر آن پیاده‌سازی کنند. بلاکچین اتریوم در سال ۲۰۱۳ به وجود آمد.

فورک

آزاد بودن بلاکچین و حذف واسطه‌ها به معنی بی‌قانونی آن نیست. برعکس، در بلاکچین، قوانین حرف اول را می‌زنند. با این تفاوت که تمام قانون‌ها و تغییراتی که در بستر بلاکچین صورت می‌گیرند به رای گذاشته می‌شوند و بر اساس توافق جمعی به تصویب می‌رسند. ایجاد فورک باعث بهبود ساختار بلاکچین، از بین بردن مشکلات احتمالی و به کار بستن قوانین کاربردی‌تر می‌شود.

هَش

در واژه نامه بلاک چین، «هَش» یک تابع است. این تابع، مثل یک دستگاه تبدیل کننده رفتار می‌کند. به این ترتیب که اگر به آن داده‌ای تشکیل شده از عددها و الفبا بدهید آن را به نوعی رمز غیرقابل تشخیص تبدیل می‌کند .استفاده کردن از توابع هش، باعث افزایش امنیت داده‌ها، پسوردها و اطلاعات می‌شود. هش و هشینگ، پایه‌های فناوری بلاکچین را تشکیل می‌دهند.

هایپر لجر

(Hyper Ledger)پروژه‌ای متن باز است که توسط بنیاد «لینوکس» با هدف توسعه، استانداردسازی و پاسخ دادن به نیازهای پیش‌بینی نشده در بلاکچین آغاز شد. در هایپر لجر خبری از ارز دیجیتال نیست اما وجود بلاکچین با این پروژه گره خورده است و نمی‌توان آنها را از هم تفکیک کرد. اعضای هایپر لجر را جمعی از نخبگان مالی، برنامه نویسی، بانکداری، اینترنت اشیا و ... تشکیل داده‌اند که تعدادشان تنها کمی بیش از ۱۰۰ نفر است.

غیر قابل ویرایش

یکی از چیزهایی که به بلاکچین اعتبار می‌دهد، غیر قابل ویرایش بودن اطلاعات آن است. اگر این قابلیت وجود نداشت، هر کسی می‌توانست تمام اطلاعات تراکنش‌ها را به دلخواه خود تغییر دهد. البته بلاکچین فقط به غیر قابل ویرایش بودن اطلاعات ثبت شده بسنده نکرده است. چون حتی آن اطلاعات هم باید از طریق کامپیوترها تایید شوند. اگر قرار باشد چیزی در دفتر کل، تغییر کند باید دفتر کل هر نود از ابتدا عوض شود.

عرضه اولیه رمز ارز

به آن "عرضه اولیه سکه" یا «ICO» هم می‌گویند. این اصطلاح به اولین زمانی اشاره دارد که یک ارز دیجیتال برای اولین بار در دسترس عموم قرار می‌گیرد تا همه بتوانند آن را معامله کنند. با وجود جذابیت‌های بالایی که عرضه‌های اولیه دارند، اما به دلیل بالا بودن ریسک و احتمال بسیار زیاد کلاهبرداری، باید محتاطانه برای خرید سکه‌های جدید اقدام کرد.

اینترنت مقدار

"Internet of value" یا اینترنت ارزش که با علامت اختصاری (IoV) نمایش داده می‌شود، مفهومی است که به درجه‌ای از اینترنت اشاره دارد که در آن ارزش‌ها به آسانی، ارزان و به شکلی قابل اطمینان به همان صورت که اکنون داده‌ها منتقل می‌شوند، انتقال پیدا کنند. فناوری بلاکچین با آسان‌تر کردن دسترسی به زیرساخت‌های انتقال ارزش از این چشم‌انداز پشتیبانی می‌کند.

تعامل پذیری

در واژه نامه بلاک چین به عبارت «Blockchain Interoperability» می‌رسیم که به آن «تعامل پذیری» هم می‌گویند. ویژگی تعامل پذیری به بلاکچین‌های گوناگون این امکان را می‌دهد که بتوانند با هم ارتباط برقرار کنند. به این ترتیب، بلاکچین‌های مختلف می‌توانند منابع و حتی قدرت پردازش خود را با هم به اشتراک بگذارند و در زمان و سرعت، صرفه‌جویی کنند.

کلید

اصطلاحی است که در دنیای رمزنگاری به فراوانی از آن استفاده می‌شود .کلیدها به دو دسته «عمومی» و «خصوصی» تقسیم می‌شوند که پیام‌های مهمی را در خود نگه می‌دارند. به اشتراک گذاشتن کلید عمومی هیچ اشکالی ندارد اما اگر کلید خصوصی یک کاربر به دست دیگران بیفتد، تمام دارایی دیجیتالی او به یغما می‌رود. بدتر آنکه به دلیل ناشناس بودن هویت افراد در دنیای ارزهای دیجیتال، هیچ راهی برای پیگیری و به دام انداختن کلاهبرداران وجود ندارد.

ماینینگ

به فرایند استفاده از قدرت محاسباتی یک کامپیوتر برای معتبر سازی تراکنش دیگران و سپس افزودن آن به لیستی بلند و عمومی به نام بلاکچین «Mining» می‌گویند. در کنار مفهوم ماینینگ، »ماینر «هم قرار دارد. ماینرها اشخاص حقیقی یا حقوقی هستند که کامپیوترهای خود را برای حل مسئله‌های پیچیده به شبکه متصل می‌کنند.

نود(Node)

در واژه نامه بلاکچین به هر کامپیوتری که به شبکه بلاکچین متصل است، نود یا گره گفته می‌شود.

توکن غیر قابل تعویض

«Non Fungible Token» یا توکن غیر قابل تعویض» که به اختصار آن را «NFT» صدا می‌زنند نوعی ارز دیجیتال است. ارزهای غیر قابل تعویض، دارایی‌هایی هستند که به طور مشخص یک مالک قابل شناسایی دارند. به همین دلیل هیچ فرد دیگری نمی‌تواند صاحب ارزش مادی و معنوی این توکن‌ها شود؛ مثلا یک قطعه موسیقی، یک کتاب، یک محصول تولید شده منحصر به فرد یا حتی یک اختراع در شمار توکن‌های غیر قابل تعویض قرار می‌گیرند.

متن باز

یکی از اصطلاح‌های آشنا در واژه نامه بلاک چین، عبارت «Open source» یا متن باز است. متن بازها، کدهایی هستند که با هدف بهینه شدن، ارتقا و برطرف شدن اشکال‌های پنهان آنها در دسترس همه افراد قرار می‌گیرند.

اوراکل

«Oracle» یک پایگاه داده است که اطلاعات در آن ذخیره و نگهداری می‌شوند .اوراکل‌ها ساختاری بسیار قدرتمند و کاربردی دارند. در بلاکچین از آنها به عنوان نوعی واسطه استفاده می‌شود. اوراکل‌ها وظیفه دارند تا اطلاعات درست و ایمن را از فضای واقعی برای قراردادهای هوشمند بلاکچین به دست بیاورند .گفته می‌شود که هر چه تعداد بلاکچین‌ها و نیاز به آنها بیشتر شود، اوراکل‌ها هم قدرتمندتر می‌شوند.

شبکه همتا به همتا

«Peer-to-Peer Network» اصطلاحی است که واژه نامه بلاکچین آن را این‌گونه تعریف می‌کند: "تعدادی از کامپیوترهای هم قدرت که اطلاعات را با هم ذخیره کرده و به اشتراک می‌گذارند".

بلاکچین خصوصی

بلاکچین‌های خصوصی، یک بلاکچین مجوزدار است. این بدان معنا است که فقط افراد خاصی آن هم با یک دعوتنامه از سوی اعضای تصمیم گیرنده آن بلاکچین می‌توانند وارد شبکه شوند. در بلاکچین‌های خصوصی، تمام افراد شناسایی می‌شوند و مسئله احراز هویت بسیار جدی می‌گردد.

اثبات اعتبار

عبارت «Proof of Authority» که به اختصار آن را (PoA) صدا می‌زنند یک الگوریتم اجماع است که بر مبنای اعتبار کار می‌کند و به دنبال راه‌حل‌هایی منطقی برای حل کردن مشکلات بلاکچین‌ها می‌گردد. البته تمرکز بیشتر این الگوریتم روی بلاکچین‌های خصوصی است. چون شرکت‌ها را قادر می‌سازد تا از حریم خصوصی خودشان محافظت کنند.

اثبات سهام

عبارت بعدی که در واژه نامه بلاک چین با آن برخورد می‌کنیم، «Proof Of Stake»یا اثبات سهام است .اثبات سهام هم نوعی متفاوت از الگوریتم اجماع به حساب می‌آید که در آن ماینرها به جای استفاده از انرژی – یعنی همان برق – از سپرده اعتبارسنج‌ها برای تایید بلاک یا سهام موجود استفاده می‌کنند.

اثبات کار

«Proof of work»یا اثبات کار»سیستمی برای اندازه‌گیری و تایید تراکنش‌های انجام شده در بلاکچین است. نام دیگر فرایند اثبات کار، استخراج یا همان «ماینینگ» است.

نام مستعار

در بلاکچین‌ها هویت افراد به صورت محرمانه باقی می‌ماند به همین دلیل به جای استفاده از نام و اطلاعات هویتی از یک نام غیرواقعی یا مستعار استفاده می‌کنند. البته همیشه نمی‌توان این محرمانگی را حفظ کرد چون گاهی به هنگام معامله باید هویت فرد خریدار و فروشنده برای دو طرف روشن باشد.

بلاکچین عمومی

بلاکچین عمومی، نوعی بلاکچین است که مجوزی ندارد. همه مردم می‌توانند در این بلاکچین بدون نیاز به احراز هویت یا درگیر شدن با مسائلی که هویت آنها را نشانه می‌روند، به نوشتن و خواندن اطلاعات مختلف در بستر بلاکچین بپردازند؛ مثلا بیت کوین یک بلاکچین عمومی است که هر کسی می‌تواند در آن شرکت کند. بلاکچین‌های عمومی، بسیار ایمن هستند چون اطلاعات پس از تایید شدن از سوی دیگران به شکلی غیر قابل تغییر در می‌آیند.

مقیاس پذیری

در واژه نامه بلاک چین، مقیاس پذیری این‌گونه معنی می‌شود: «نهایت قدرت عملیاتی یک شبکه با بیشترین تعداد کاربران.» اکنون نهایت قدرت عملیاتی بلاک چین بیت کوین هفت تراکنش در ثانیه است.

زنجیره جانبی

«Side chain»، بخشی جدا از بلاک چین است که می‌تواند با یک ارتباط دو طرفه، حجم قابل توجهی از دارایی‌ها را میان خودش و بلاکچین جابه‌جا کند.

قرارداد هوشمند

پروتکل‌هایی هستند که می‌توانند تراکنش‌های معتبر را بدون نیاز به واسطه‌ها انجام دهند. این قراردادها قابلیت پیگیری دارند اما غیرقابل برگشت هستند. گذشته از این برای اجرای آنها به حضور هیچ کس نیازی نیست و می‌توانند به صورت خودکار اجرا شوند. به همین دلیل، امنیت بیشتری دارند، هزینه عملیات در آنها پایین است و خبری از خطاهای انسانی در آنها وجود ندارد. مهم‌ترین اشکال قراردادهای هوشمند، هزینه بالای نوشتن آنها توسط برنامه نویسان است.

توکن

توکن، نوعی ارز دیجیتال است که بلاکچین مستقلی ندارد و از بلاکچین ارزهای دیجیتال دیگر استفاده می‌کند. در نقطه مقابل توکن، «کوین» قرار دارد؛ یعنی همان ارزهای دیجیتالی که بلاکچین مستقل خودشان را دارند.

توکنی

فرایندی است که در آن، دارایی‌های فیزیکی شما به دارایی‌های دیجیتالی تبدیل می‌شوند. شما برای این کار به یک پلتفرم – مثلا اتریوم – یک قالب قرارداد هوشمند، یک ویرایشگر متن و یک آدرس کیف پول – در اینجا همان کیف پول اتریوم – نیاز دارید.

تراکنش

در ساده‌ترین حالت، واژه نامه بلاکچین، تراکنش‌ها را این‌گونه تعریف می‌کند: «تبادل دارایی‌های دیجیتالی از یک کامپیوتر – نود – به کامپیوتر دیگر یا یک قرارداد هوشمند، تراکنش نامیده می‌شود«.

کیف پول

کیف پول ارزهای دیجیتال، عبارت دیگری است که در واژه نامه بلاکچین جای می‌گیرد. شما برای نگهداری از دارایی‌های دیجیتالی خودتان به یک کیف پول سخت‌افزاری یا نرم‌افزاری نیاز دارید که به آن «Cryptocurrency wallet» هم می‌گویند.

اثبات دانایی صفر

اگر یکی از طرفین اثبات کار بتواند موضوعی را بدون دادن اطلاعات اضافی به اثبات کننده دیگری ثابت کند، از روش اثبات دانش صفر یا «Zero Knowledge Proof» استفاده کرده است.

مفهوم بلاک چین

بلاک چین در ابتدا ممکن است پیچیده به نظر برسد و از جهاتی نیز واقعا این گونه است اما مفهوم اصلی آن بسیار ساده است. بلاک چین در واقع نوعی پایگاه داده است. پس برای درک بلاک چین در ابتدا باید بدانید که پایگاه داده چیست.
پایگاه داده مجموعه ای از اطلاعات است که به صورت الکترونیکی در یک سیستم کامپیوتری ذخیره می شود. اطلاعات یا داده های موجود در پایگاه های داده معمولاً در قالب جدول طراحی شده اند تا امکان جستجو و فیلتر آسان برای اطلاعات خاص را فراهم کنند. پایگاه داده به گونه ای طراحی شده است که حجم قابل توجهی از اطلاعات را در اختیار داشته باشد که به سرعت و به راحتی توسط تعداد زیادی از کاربران قابل دسترسی است. پایگاه های داده بزرگ با قرار دادن داده ها روی سرورهایی که از رایانه های قدرتمند ساخته شده اند این امر را تحقق می بخشند. این سرورها گاهی اوقات می توانند با استفاده از صدها یا هزاران رایانه ساخته شوند تا قدرت محاسباتی و ظرفیت ذخیره سازی لازم برای دسترسی همزمان بسیاری از کاربران به پایگاه داده را داشته باشند. در حالی که یک پایگاه داده ممکن است برای هر تعداد از افراد قابل دسترسی باشد، اغلب متعلق به یک کسب و کار است و توسط یک فرد خاص اداره می شود که کنترل کاملی بر نحوه کار و داده های موجود در آن دارد. بنابراین تفاوت پایگاه داده و بلاک چین در چیست؟

مزایای بلاک چین

۷ گره بزرگ که به دست بلاک چین باز می شوند عبارتند از:

۱. مدیریت هزینه‌ها

در وضعیت فعلی، هزینه‌های زیادی، بیهوده هدر می‌روند. فرقی نمی‌کند که در مورد چه سازمانی، چه سیستمی یا چه رویکردی سخن می‌گوییم. چون این هزینه‌ها با عنوان‌های مختلفی در حال هدر رفتن و آسیب رساندن به دیگر بخش‌ها هستند؛ مثلا گاهی در نقش هزینه تبلیغات ظاهر می‌شوند و گاهی دیگر خودشان را لابه‌لای کارمزدهای انتقال پول، پنهان می‌کنند.

۲. راندمان

فکرش را بکنید اگر این تکنولوژی و پتانسیل‌های آن به بهترین شکل ممکن مورد استفاده قرار بگیرند چه تحولی در بهره‌وری سازمانی، استارت‌آپ‌ها، کسب و کارها و ... به وجود می‌آید.

۳. لنگ بودن چرخ کارایی

بسیاری از فرایندهایی که با آنها درگیر هستیم، مانند سیستم‌های پرداخت، ثبت و تغییر اطلاعات یا پردازش‌های مالی می‌توانند در بستر بلاک چین سرعت و کارایی بسیار بالاتری را تجربه کنند.

۴. چالش‌های زمانی در پردازش‌های مالی

با استفاده از این فناوری، دیگر تاخیرهای پرداخت یا معطل نگه داشتن روند نقل و انتقال مالی به دلیل کاغذبازی‌های اداری، بی‌معنی خواهند شد.

۵. وضعیت نامساعد نتیجه‌ها

در کارهایی که با دخالت مستقیم انسان‌ها به سرانجام می‌رسند، امکان وجود خطا موج می‌زند. وقتی با کمک فناوری‌های پیشرفته‌تر، حجم قابل توجهی از کارها را به ماشین‌های هوشمند بسپاریم، میزان خطاهایی که به دلیل دخالت انسان به وجود می‌آیند کاهش پیدا می‌کند.

۶. مدیریت بازده

بلاک چین می‌تواند نظر ما نسبت به نتیجه کار، سود، افزایش درآمد و بازده کار نسبت به زمان و منابع مصرف شده را دگرگون کند. این تکنولوژی با ویژگی‌های منحصر به فردش نگرشی تازه در زمینه مدیریت بازده را پیش چشم ما قرار می‌دهد.

۷. مدیریت ریسک

هیچ کاری بدون ریسک نیست؛ اما می‌توان مقدار آن را کاهش داد و حتی به هنگام روبه‌رو شدن با ریسک‌های غیر قابل گریز، شدت و عمق آسیب آنها را کمتر کرد. این هم هدیه دیگری است که در قلب کسب و کار بلاک چین پنهان شده است.

شبکه لایتنینگ (Lightning)

شبکه لایتنینگ یک فناوری لایه دوم به حساب می آید که برای بیت کوین استفاده می شود و از کانال های پرداخت خرد (MicroPayment)برای مقیاس گذاری ظرفیت بلاکچین بیت کوین برای انجام معاملات با کارآیی بیشتر استفاده می کند.تراکنش های انجام شده در شبکه لایتنینگ نسبت به تراکنش هایی که مستقیماً روی بلاکچین بیت کوین انجام می شوند یعنی زنجیره ای یا on-chain سریعتر و کم هزینه تر هستند و به آسانی تأیید می شوند. این شبکه طراحی شده است تا با خارج کردن تراکنش ها از بلاکچین اصلی و تبدیل کردن آن ها به تراکنش هایی خارج از زنجیره(off-chain) ، بلاکچین بیت کوین را خلوت کند و باعث کاهش هزینه های مربوط به تراکنش ها شود. از شبکه لایتنینگ همچنین می توان برای انجام انواع دیگر تراکنش های خارج از زنجیره شامل مبادلات داخلی ارزهای دیجیتال در صرافی ها نیز استفاده کرد. شبکه لایتنینگ به عنوان مثال، برای تسهیل مبادلات اتمی (atomic swaps) که امکان مبادله یک ارز دیجیتال با ارزی دیگر را بدون دخالت واسطه ای مانند صرافی های ارز دیجیتال را فراهم می کند نیز، مفید است.

کاربردهای کلیدی شبکه لایتنینگ

شبکه لایتنینگ راه حلی فناورانه است برای حل مشکل سرعت تراکنش ها در بلاکچین بیت کوین. شبکه لایتنینگ این کار را با انتقال تراکنش ها به خارج از دفتر کل (off-ledger) بلاکچین بیت کوین، انجام می دهد.

دقیقاً مانند بلاکچین، شبکه لایتنینگ نیز موسسات مالی متمرکز را از دور خارج می کند و نیازی به آن ها وجود ندارد در حالی که این موسسات متمرکز مسئول بیشتر تراکنش های مالی فعلی در جهان هستند.
شبکه لایتنینگ برای اولین بار به طور رسمی در مقاله ای توسط جوزف پون و تادئوس درایجا در سال ۲۰۱۵ شرح و توسعه داده شد.

شبکه لایتنینگ (Lightning) چیست؟

شبکه لایتنینگ برای اولین بار توسط جوزف پون و تادئوس دریجا در سال ۲۰۱۵ توضیح داده شد و از همان زمان در دست توسعه است. مشکلی که شبکه لایتنینگ برای حل آن طراحی شد، کندی انجام تراکنش ها و توان عملیاتی بیت کوین بود.
اگر قرار است که بیت کوین به پتانسیل خود برای تبدیل شدن به ابزاری برای انجام تراکنش های روزانه برسد، باید در هر ثانیه به ده ها یا صدها هزار تراکنش برسد، شبیه کارت های اعتباری یا شبکه های پرداخت الکترونیکی.

اما با توجه به ماهیت تکنولوژی غیرمتمرکز خود که نیاز به هماهنگی همه نودهای (node) درون شبکه خود دارد، بیت کوین در وضعیت فعلی خود مملو از چنین مشکلاتی است.به عنوان مثال، اگر تعداد تراکنش ها در شبکه بیت کوین چندین برابر شود، تأیید و ذخیره آن تراکنش ها بسیار گران و وقت گیر خواهد شد. افزایش تعداد تراکنش ها، همچنین نیاز به بهبود قدرت پردازش رایانه هایی دارد که برای انجام تراکنش های بیت کوین محاسبات شبکه را انجام می دهند. علاوه بر این، انرژی لازم برای محاسبه این اطلاعات بسیار زیاد است و همیشه نگه داشتن بیت کوین در وضعیت عملیاتی برای انجام تراکنش های روزمره بسیار گران و هزینه بر خواهد بود. شبکه لایتنینگ پیشنهاد می دهد تا با ایجاد یک لایه دوم در بلاکچین اصلی بیت کوین، مشکل مقیاس پذیری آن را حل کند .این لایه دوم شامل چندین کانال پرداخت بین طرفین یا کاربران بیت کوین است .یک کانال از شبکه لایتنینگ در واقع مکانیسمی برای انجام تراکنش بین دو طرف است.با استفاده از این کانال ها، طرفین می توانند با یکدیگر مبادلات بیت کوینی انجام دهند. نحوه پردازش این تراکنش ها در مقایسه با تراکنش های استانداردی که روی بلاکچین بیت کوین انجام می شود، متفاوت است .این تراکنش ها فقط هنگامی روی بلاکچین اصلی قرار داده می شوند که یکی از طرفین کانالی را ببندد یا راه بیاندازد. بین این دو اتفاق (باز و بسته کردن کانال های مبادلاتی لایتنینگ)، طرفین می توانند بدون اطلاع بلاکچین اصلی در مورد فعالیت های شان، بی وقفه وجوه و دارایی ها را بین خود جابجا کنند. این روش سرعت تراکنش ها را به طرز چشم گیری افزایش می دهد زیرا که دیگر لازم نیست همه تراکنش ها توسط همه نودهای یک بلاکچین تأیید شوند.کانال های پرداخت بین طرفهای مختلف با هم ترکیب می شوند و شبکه ای از نود های لایتنینگ را تشکیل می دهند که می توانند معاملات را بین خود هدایت کنند. اتصالات بین کانالهای مختلف پرداختی منجر به شکل گیری شبکه لایتنینگ می شود.

شبکه لایتنینگ چگونه کار می کند؟

به عنوان مثال آلیس با کافی شاپ مورد علاقه خود یک کانال پرداختی مبتنی بر شبکه لایتنینگ باز می کند و ۱۰۰ دلار بیت کوین در آن واریز می کند. معاملات او با کافی شاپ فوری و مستقیم خواهد بود زیرا او کانالی مستقیم با کافی شاپ دارد. باب،

که کانال باز دیگری با فروشگاه مواد غذایی که بیشتر از همه به آن مراجعه می کند دارد، قهوه را از فروشگاه آلیس خریداری می کند. ارتباط بین آلیس یا کافی شاپ و باب تضمین می کند که آلیس می تواند از موجودی کانال خود با کافی شاپ برای خرید مواد غذایی از فروشگاه باب استفاده کند. به همین ترتیب، باب نیز می تواند از موجودی فروشگاه مواد غذایی خود برای انجام تراکنش با فروشگاه های موجود در شبکه آلیس استفاده کند.اگر باب کانال خود را با فروشگاه مواد غذایی ببندد (و هیچ مشتری مشترک دیگری بین کافی شاپ و فروشگاه مواد غذایی وجود نداشته باشد)، پس آلیس مجبور است کانال دیگری را با فروشگاه مواد غذایی باز کند تا بتواند از آنجا خرید کند. به این ترتیب، شبکه ای از مبادلات به صورت غیرمتمرکز بین چندین نود لایتنینگ ایجاد و هدایت می شود.به بیانی تخصصی تر، شبکه لایتنینگ از قراردادهای هوشمند (smart contract) و اسکریپت های چند امضایی (multi-signature)برای عملی کردن ایده خود استفاده می کند. یک تراکنش اولیه، به نام تراکنش تامین بودجه، زمانی ایجاد می شود که یکی از طرفین یا هر دو طرف، کانالی پرداختی را تأمین مالی کنند. در یک محیط معمولی چند امضایی (multi-signature)، در همان ابتدا دو کلید اصلی) (master key) یکی عمومی و دیگری خصوصی) رد و بدل می شوند. این مبادله کلید ها، دسترسی و خرج کردن وجوه را تسهیل می کند.

در مورد نود لایتنینگ اما، امضایی رد و بدل نمی شود. این کار برای جلوگیری از، شناسایی هزینه تراکنش های تامین مالی ابتدایی شبکه لایتنینگ، توسط بلاک چین اصلی انجام می شود. در عوض، دو طرف یک کلید را با یکدیگر مبادله می کنند، که برای اعتبار سنجی معاملات هزینه ای (که "مبادلات تعهدی" نیز نامیده می شود) بین خود آن ها استفاده می شود.دو طرف می توانند "مبادلات تعهدی" نا محدودی را بین خود و سایر نودهای شبکه لایتنینگ عملیاتی کنند. در آخر اینکه آنها کلیدهای اصلی خود را فقط در صورت بسته شدن و نهایی شدن کانال بین خود عوض می کنند.هزینه هایی در ارتباط با استفاده از شبکه لایتنینگ وجود دارد. این هزینه ها ترکیبی از هزینه های مسیریابی مختص مسیریابی اطلاعات پرداخت ها، بین نودهای لایتنینگ و هزینه های تراکنشی بلاکچین بیت کوین برای باز و بسته کردن کانال ها هستند.در نوامبر ۲۰۱۹، دانشمندانی از دو دانشگاه در مجارستان و موسسه علوم رایانه ای و کنترل، مقاله ای را منتشر کردند .این دانشمندان در این مقاله توانایی اپراتورهای شبکه لایتنینگ را، برای ادامه پردازش تراکنش ها، بدون افزایش چشمگیر هزینه های آن، زیر سوال بردند.نویسندگان در مقاله خود می گویند: "مشارکت در شبکه لایتنینگ برای اکثر نود های بزرگ مسیریابی، که در حال حاضر شبکه را سر پا نگه داشته اند، از نظر اقتصادی غیر منطقی است. هزینه های مربوط به ترافیک یا تراکنش ها باید به ترتیب سفارشات افزایش یابد تا مسیریابی پرداخت از نظر اقتصادی مقرون به صرفه باقی بماند".بارزترین مشکل شبکه های لایتنینگ که غایت اولیه آن ها غیرمتمرکز بودن است، این می باشد که می توانند در دام مدل قطب و اقمار (hub and spoke) گرفتار شوند، مدل و الگویی که سیستم های مالی متمرکز امروزی را تعریف می کند.در مدل فعلی جهانی، بانکها و موسسات مالی واسطه اصلی کلیه معاملات روزانه انجام شده هستند.نود های شبکه لایتنینگ، با ایجاد ارتباطات گسترده تر با دیگر طرف ها، ممکن است به هاب هایی (hub) یا نود هایی مشابه شبکه های متمرکز، تبدیل شوند. امکان دارد خرابی در یکی از این مراکز یا هاب ها به راحتی به بخش قابل توجهی از شبکه (یا کل شبکه) آسیب برساند و آن را به طور کلی از کار بیاندازد.

تفاوت بیت کوین با آلت کوین

تفاوت آلت کوین و بیت کوین بسیار است که از جمله آن می‌توان همان ویژگی‌های متفاوت آلت کوین‌ها در برابر بیت کوین را نام برد. علاوه بر آن، ارزش متفاوتی است که هریک از ارزهای دیجیتال دارند و همین امر هم سبب می‌شود تا به‌صورت متفاوت و با حجم‌های متفاوتی مورد معامله و ترید قرار بگیرند. البته علی‌رغم تمام تفاوت‌هایی که بین بیت کوین و آلت کوین وجود دارد، یک تفاوت اصلی وجود دارد و آن این است که بیت کوین به تنهایی، ارزشمندترین، قوی‌ترین، محبوب‌ترین و بهترین ارز دیجیتالی است که جهان تا به امروز به خود دیده است. بیت کوین به تنهایی در برابر تمام آلت کوین‌ها قرار دارد.

انواع آلت کوین ها

با توجه به تفاوت در ویژگی‌هایی که هر آلت کوین با آن ارائه می‌شود، انواع آن‌ها را می‌توان به گروه‌های زیر دسته‌بندی کرد:

آلت کوین‌های مبتنی بر ماینینگ Mining-Based Altcoins

این دسته از آلت کوین‌ها بیشتر از سایر انواع آن به بیت کوین شباهت دارند، زیرا آن‌ها نیز مانند بیت کوین، با استخراج بدست می‌آیند. استخراج یا ماینینگ عملی است که در طی آن با حل کردن مسائل چالش‌برانگیز ریاضیات، کوین‌ها (هر واحد از ارز دیجیتال) استخراج می‌شوند و در اختیار شبکه قرار می‌گیرند. از جمله بهترین آلت کوین‌های مبتنی بر ماینیگ می‌توان اتریوم Ethereumرا نام برد که در ماه فوریه سال ۲۰۲۰ این عنوان را به خود گرفت.

آلت کوین های با ثبات Stablecoin

ارز دیجیتال با ثبات، به دنبال کاهش نوسانات برای بهبود بیت کوین است. در واقع با اتصال ارزهای دیجیتال به ارزهای فیات (ارزهای رایج جهان مانند دلار و یورو)، ارزهای باثبات یا استبل کوین‌ها ایجاد می‌شوند که از جمله مهم‌ترین آن‌ها می‌توان « «Libra Facebookو تتر [۱]« «Tetherیا همان دلار دیجیتالی را نام برد.

توکن های امنیتی (توکن اوراق بهادار) Security tokens

این دسته از آلت‌کوین‌ها ساختاری شبیه به سهام سنتی دارند و اغلب با ارائه کوین اولیه – عرضه اولیه – ((ICOهمراه هستند و ویژگی‌هایی مانند مالکیت یا پرداخت را نوید می‌دهند و به یک معامله متصل هستند.

توکن های ابزاری (توکن کمکی) Utility tokens

توکن‌های ابزاری، همان‌طور که از نام آن‌ها هم مشخص است، به دنبال خدمت‌رسانی هستند و در برابر سایر آلت کوین‌ها، نمونه‌های ابزاری به حساب می‌آیند. معمولاً این مدل از آلت کوین نیز به‌صورت توکن اولیه ((ICOعرضه می‌شوند و یکی از نمونه‌های آن فایل‌کوین‌ها « «Filecoinاست که در فضای ذخیره‌سازی غیرمتمرکز فایل‌ها، قابلیت معاوضه دارند.

۱

آلت کوین های اولیه

پس از بیت کوین، اولین آلت کوین‌هایی که به جهان معرفی شدند، دو نمونه‌ی زیر بودند که از آن‌ها با عنوان «آلت کوین‌های اولیه» نام می‌برند:

نمکوین Namecoin

اولین نمونه آلت کوین، نمکوین بود که در ماه آوریل سال ۲۰۱۱ ارائه شد. این ارز دیجیتال نیز مانند بیت کوین از الگوریتم اثبات کار استفاده می‌کرد و محدود به ۲۱ میلیون کوین بود. نمکوین این قابلیت را به افراد می‌داد تا با استفاده از دامنه‌های «. «bitبه استخراج بپردازند و این امر با هدف ناشناس ماندن و سانسورستیزی انجام می‌شد.

لایت کوین «Litecoin

لایت کوین، دیگر آلت کوین اولیه بود که در ماه اکتبر سال ۲۰۱۱ ارائه شد. به لایت کوین «نقره‌ای در برابر طلای بیت کوین» گفته می‌شد. اگرچه لایت کوین شباهت‌های بسیاری با بیت کوین دارد، اما تفاوت‌هایی هم دارد که از جمله آن‌ها می‌توان به تعداد کوین‌های لایت کوین در برابر بیت کوین اشاره کرد. تعداد کوین‌های لایت کوین، تقریباً چهار برابر کوین‌های بیت کوین، چیزی در حدود ۸۵ میلیون لایت کوین است.

مزایای آلت کوین ها

بهبود نواقص بیت کوین

بیت کوین به عنوان اولین رمزارز جهان، قطعاً با نواقص و مشکلاتی همراه است که آلت کوین‌ها قادر به پوشش دادن این نقص‌ها هستند که از جمله آن‌ها می‌توان به بهبود سرعت، کم شدن هزینه‌ی استخراج و .... اشاره کرد.

ایجاد فضای رقابتی

همه‌ی آلت کوین‌ها به نوعی با بیت کوین رقابت دارند و می‌خواهند هربار بیشتر از پیش جایگاه خود در مارکت کریپتو را ارتقا داده و به بیت کوین نزدیک‌تر شوند. همین تمایل به رقابت با بیت کوین، اساس کار پیشرفت آلت کوین‌ها و امیدواری به آن‌ها است.

انجام تراکنش با کارمزد پایین

یکی از اصلی‌ترین مزایای آلت کوین‌ها به عنوان یک شیوه‌ی مدرن برای انجام تراکنش‌های مالی، پایین بودن کارمزد این تراکنش‌ها است که یکی دیگر از مزایای آن‌ها به حساب می‌آید.

معایب آلت کوین ها

آلت کوین‌ها علی‌رغم مزایایی که نام بردیم، معایبی نیز دارند که اگر بخواهیم بدانیم معایب آلت کوین چیست، می‌توانیم دو نمونه‌ی زیر را نام ببریم:

ارزش ناپایدار

در بین هزاران آلت کوینی که در حال حاضر وجود دارند، انتخاب مناسب‌ترین آلت کوین‌ها برای سرمایه گذاری، کار سختی است و همین امر هم سبب می‌شود تا ارزش این ارزها به‌شدت دستخوش تغییر شده و درگیر نوسانات پی‌درپی باشند.

تقلب و کلاهبرداری های بسیار

با توجه به کارایی‌های متفاوتی که هر در آلت کوین وجود دارد و اینکه همگی آن‌ها توسط یک سری برنامه‌نویسیان ایجاد شده‌اند، وجود باگ در سیستم امنیتی برخی از آن‌ها، بسیار متداول است و همین امر سبب بروز تقلب و کلاهبرداری‌های بسیاری در دنیای آلت کوین‌ها می‌شود.

بهترین آلت کوین ها

قطعاً در بین تعداد زیادی آلت کوین که در مارکت کریپتوکارنسی وجود دارند، تنها روی تعداد اندکی از آن‌ها می‌توان برای بلندمدت حساب کرد. برخی از مشهورترین آلت کوین‌ها، پس از سال‌ها امتحان خود به بازار را پس داده‌اند و لیاقت خود را ثابت کرده‌اند. پس می‌توان با اطمینان بیشتری روی آن‌ها سرمایه گذاری کرد. از جمله بهترین آلت کوین‌ها می‌توان نمونه‌های زیر را نام برد:

اتریوم ETH

اتریوم با عنوان «ملکه ارزهای دیجیتال» شناخته شده و ارائه‌ی آن به ۲۰۱۳ برمی‌گردد. اتریوم بر روی قابلیت غیرمتمرکز بودن تأکید دارد و می‌تواند کاری کند که قراردادهای هوشمند و دیگر برنامه‌های غیرمتمرکز، بدون هیچ خرابی، کلاهبرداری، تقلب یا دخالت، طراحی و اجرا شوند. اتریوم روز به روز جایگاه بالاتری را در بین تریدرهای بازار کریپتو پیدا می‌کند و یکی از بهترین آلت کوین‌ها برای سرمایه گذاری و تریدینگ به حساب می‌آید.

تِتِر USDT

تتر در سال ۲۰۱۴ پا به عرضه وجود نهاد و برعکس دیگر ارزهای دیجیتال که تمایل به افزایش قیمت دارند، این رمزارز، ارزش خود را ثابت نگه می‌دارد تا از نوسانات بازار جلوگیری کند (آلت کوین با ثبات). سرمایه گذاران هرگاه سرمایه رمزارزی خود را در خطر ببینند، می‌توانند دارایی خود با با تتر معامله کنند.

ریپل XRP

فعالیت رمزاری شرکت ریپل از سال ۲۰۱۱ آغاز و در سال ۲۰۱۳ تکمیل شد. این در حالی است که سابقه کاری اصلی شرکت ریپل به سال ۲۰۰۴ برمی‌گردد. این آلت کوین پس از فراز و نشیب‌های بسیار، امروز یکی دیگر از رمزارزهای پایه برای ترید و سرمایه گذاری به حساب می‌آید.

بیت کوین کَش BCH

بیت کوین کَش در ماه آگوست سال ۲۰۱۷ به بازار کریپتو آمد و در پی یک هاردفورک بزرگ (بحث و جدل بین توسعه‌دهندگان رمزارزی) تکمیل و به یکی از اصلی‌ترین آلت کوین‌ها تبدیل شده است.

لایت کوین LTC

لایت کوین به عنوان یک آلت کوین اولیه، سه سال پس از بیت کوین، در ۲۰۱۱ عرضه شد. لایت کوین پایه یک پرداخت‌های جهانی است و توسط هیچ مرجعی کنترل نمی‌شود. لایت کوین بسیار سریع‌تر از بیت کوین است و برای سرمایه گذاری توصیه می‌شود.

پولکادات DOT

پولکادات در سال ۲۰۱۷ به بازار کریپتو آمد. این آلت کوین قصد دارد تا با ادغام کردن شبکه‌های بلاک چینی مختلف، یک شبکه یکپارچه بسازد. بیشتر کارشناسان، پولکادات را خطری جدی برای جایگاه اتریوم می‌دانند و رشد قوی این آلت کوین، آن را به یکی از بهترین‌های بازار کریپتو تبدیل کرده است.

کاردانو ADA

کاردانو در سال ۲۰۱۵ معرفی شد و هدف آن، ایجاد بستری مناسب و هموار برای مبادله رمزارزها است. کارانو یک رمزارز نسل سومی به حساب می‌آید. رمزارزهای نسل سوم، برخلاف سایر رمزارزهای اصلی مانند بیت کوین و اتریوم، امکان توسعه و گسترش بیشتری در سطح کلان دارند. بنابراین دیگر آلت کوین مهم و مطرح جهان، کاردانو است. به علاوه گزینه‌های فوق، آلت کوین‌هایی چون استلار لومن ««XLM، بایننس کوین « «BNBو ایاس « «EOSنیز در جایگاه خوبی برای ترید و سرمایه گذاری در بازار رمزارزها قرار دارند. البته اگر شما بدانید که آلت کوین چیست و چگونه می‌توان به ویژگی‌های هرکدام از آن‌ها پی برد، می‌توانید دیگر آلت کوین‌های ارزشمند بازار را نیز برای سرمایه گذاری خود انتخاب کرده و از مبادله‌ی آن‌ها سود کنید.

.

روش‌های مختلف برای استخراج ارز دیجیتال

اکنون که با مفهوم ماینر و ماینینگ یا استخراج ارز دیجیتال آشنا شدیم، جا دارد به بررسی روش‌های استخراج ارز دیجیتال بپردازیم. ارزهای دیجیتال زیاد و متنوعی وجود دارد مثلا ارز دیجیتال بیت کوین و اتریوم در نمونه مهم از ارزهای دیجیتال هستند. برای استخراج ارزهای دیجیتال نیز روش‌های مختلفی وجود دارد که در ادامه به بررسی آنها می‌پردازیم:

- استخراج ارز دیجیتال از طریق روش سی پی یو : (CPU) این روش یکی از روش‌های اولیه برای استخراج ارزهای دیجیتال بوده و با استفاده از سی پی یو یا همان واحد پردازش مرکزی کامپیوتر شخصی انجام می‌گیرد. این روش یکی از کندترین روش‌های استخراج ارز دیجیتال بوده و مقدار کمتری ارز استخراج می‌کند.
- استخراج ارز دیجیتال از طریق روش جی پی یو : (GPU) در این روش برای استخراج ارز دیجیتال از کارت گرافیک یا همان GPU کامپیوتر شخصی استفاده می‌شود. این روش نسبت به روش سی پی یو سریع‌تر بوده و به آن برتری دارد.
- استخراج ارز دیجیتال از طریق روش ای سیک : (ASIC) این روش یکی از بهترین و به صرفه‌ترین روش‌های استخراج ارز دیجیتال است. در این روش از از تراشه های مخصوصی به نام ای سیک استفاده می‌شود. این روش رمز های موجود در معاملات را خیلی زودتر و راحت‌تر از روش‌های CPU و GPU حدس می‌زند.

نحوه ی ذخیره ی ارزهای دیجیتال

کیف پول ارز دیجیتال

قبل از اینکه به طور تکنیکی به توضیح کیف پول ارز دیجیتال بپردازیم، بیایید کمی در مورد روش خاص شما برای ذخیره پول با هم صحبت کنیم. به این فکر کنید که چگونه پول نقد واقعی خود را ذخیره می‌کنید. قطعا آن را در دست خود نگه نمی‌دارید، بلکه آن را در کیف پول یا در یک حساب بانکی ایمن ذخیره می‌کنید. کیف پول کریپتوکارنسی نیز از همان اصول اصلی پیروی می‌کند. در نتیجه، با داشتن یک کیف پول رمزنگاری شده، توانایی ارسال و دریافت بیت کوین و سایر کریپتوکارنسی‌ها را خواهید داشت. «والت» یا همان کیف پول ارز دیجیتال یک برنامه نرم‌افزاری است که کلیدهای خصوصی و عمومی را ذخیره می‌کند و با بلاک چین‌های مختلف در تعامل است تا کاربران بتوانند ارز دیجیتال خود را بفرستند، دریافت کنند و بر تراز حساب خود نظارت داشته باشند. اگر قصد دارید از بیت‌کوین یا هر ارز دیجیتال دیگری استفاده کنید، ابتدا باید یک کیف پول دیجیتالی داشته باشید. هیچ ارز دیجیتالی به خودی خود در کیف پول قرار ندارد. بیت کوین و کریپتوکارنسی‌های مشتق شده از آن، به صورت غیرمتمرکز در یک دفترکل عمومی به نام «بلاک چین» ذخیره و نگهداری می‌شوند.

کیف پول ارز دیجیتال چگونه کار می‌کند؟

در یک حساب بانکی معمولی، پول یا بهتر است بگوییم، ارزش آن نگهداری می‌شود. اما در کیف پول ارزهای دیجیتال، کلیدهای رمزنگاری شده عمومی و خصوصی نگهداری می‌شوند. در حقیقت، کوین‌ها نمی‌توانند در یک کیف پول فیزیکی ذخیره شوند. چون کریپتوکارنسی‌ها وجود فیزیکی ندارند. آدرس کیف پول، چیزی شبیه به شماره حساب بانکی است. هیچ اشکالی ندارد اگر شما شماره حساب بانکی خودتان را به فرد دیگری بدهید، چون دیگران برای انتقال وجه به آن نیاز دارند. در دنیای ارزهای دیجیتال، اگر کسی بخواهد کوین‌هایتان را برایتان ارسال کند، شما می‌توانید به سادگی آدرس کیف پول خود را به او بدهید و کوین‌تان را دریافت کنید. درست مانند حساب‌های بانکی، هیچ یک از دو آدرس کیف پول، شبیه به هم نیستند. در نتیجه، هیچ

کس به جز شما نمی‌تواند پولتان را دریافت کند. همچنین، تعداد آدرس‌های کیف پول شما بدون محدودیت هستند. یعنی هر چند تا آدرس که دلتان بخواهد می‌توانید برای کیف پولتان بسازید. به عنوان مثال (در خصوص بیت کوین) این آدرس کیف پولی است که تصور می‌شود متعلق به خالق بیت کوین، ساتوشی ناکاموتو است:

A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa۱

همان‌طور که مشاهده می‌کنید، این آدرس یک ترکیب پیچیده از اعداد و حروف بزرگ و کوچک است. از آنجایی که اغلب بلاک چین‌ها دارای شفافیت هستند، می‌توان به آسانی پی برد که یک کیف پول خاص چه مقدار پول دارد و مالک آن چه تراکنش‌های مالی را در گذشته انجام داده است .با این حال آدرس یک کیف پول ارز دیجیتال، هویت واقعی صاحب خود را نشان نمی‌دهد.چگونه کلیدهای عمومی و خصوصی به یک آدرس کیف پول مرتبط می‌شوند؟ اکثر مردم تصور می‌کنند که کلید عمومی چیزی شبیه به آدرس یک کیف پول عمومی است. اما در حقیقت، آدرس کیف پول هر فرد، یک کلید خصوصی و عمومی منحصر به فرد دارد. کلید خصوصی این امکان را به شما می‌دهد تا به پول‌هایی که مربوط به آدرس کیف پول کریپتوی شماست، دسترسی داشته باشید. اجازه بدهید برای درک بهتر این موضوع یک مثال بزنیم .تصور کنید که می‌خواهید از حساب بانکی خود پولی را به حساب بانکی شخص دیگری انتقال دهید، در این صورت، اول باید رمز عبور شخصی خود را وارد کنید. هیچ کس دیگری به این رمز عبور دسترسی ندارد، حتی بانک. در غیر این صورت، اگر کسی آن را بفهمد، می‌تواند از حساب بانکی شما پول جابه‌جا کند! کلید خصوصی دقیقا همان کار را انجام می‌دهد و به طور خاص به آدرس کیف پول شخصی شما مرتبط است.

کلید عمومی

کلید عمومی از لحاظ ریاضی به آدرس کیف پول شما مرتبط است! با این حال، یک ‘‘ورژن هش ’’به حساب می‌آید. عملکرد هش به شما این امکان را می‌دهد تا توالی حروف/اعداد که «ورودی» خوانده می‌شوند را در مجموعه جدیدی از حروف/اعداد به عنوان «خروجی» رمزگذاری کنید. در واقع با این کار پای یک لایه امنیتی به میدان باز می‌شود و تضمین می‌کند که کیف پول شما غیرقابل هک شدن است.

- نمونه‌ای از کلید خصوصی:

bf350d2821375158a608b51e3e898e507fe47f2d2e8c774de4a9a7edecf74ed۰۳
a

- نمونه‌ای از کلید عمومی

b1ebcfc11a13df5161aba8160460fe1**601d541**۹۹

شاید در نگاه اول، این دو کلید کاملا متفاوت به نظر برسند اما فناوری نرم افزار تشخیص می‌دهد که این دو کلید به طور خاصی به یکدیگر مرتبط هستند. ارتباط بین کلیدها ثابت می‌کند که شما مالک کوین‌ها هستید و این امکان را برایتان مهیا می‌کند که هر وقت بخواهید بتوانید پول خود را انتقال دهید! در واقع ضرورتی ندارد از فن آوری و ماجراهایی که در پس زمینه رخ می‌دهند سردربیاورید. تراکنش‌های کیف پول ارز دیجیتال چیزی شبیه به استفاده از Gmail و Hotmail هستند. نرم افزار تمام کارها را برایتان انجام می‌دهد.

انواع مختلف کیف پول ارزهای دیجیتال

در حال حاضر انواع مختلفی از کیف پول‌ها در دسترس عموم هستند. کیف پول انتخابی شما به نیازهای شخصی‌تان بستگی دارد. اساسا، کیف پول‌های مختلف، امکانات متفاوتی را ارائه می‌دهند مانند امنیت، رفتار کاربر پسندانه یا حتی راحتی بیشتر. محبوب ترین انواع کیف پول ارزهای دیجیتال عبارتند از:

- **کیف پول روی دسکتاپ**

کیف پول‌های روی دسکتاپ باید در یک لپ‌تاپ یا کامپیوتر خاص دانلود شوند و تنها از آن دستگاه خاص قابل دسترسی هستند .به طور کلی، این نوع از کیف پول‌ها ترکیب خوبی از امنیت و راحتی را ارائه می‌دهند. با این حال به یاد داشته باشید که اگر یک هکر توانایی کنترل از راه دور دستگاه شما را به‌دست آورد، خیلی راحت می‌توانند به کیف پول شما دسترسی پیدا کند.

- **کیف پول روی موبایل**

کیف پول روی موبایل بسیار شبیه به کیف پول روی دسکتاپ است. چون این نوع از کیف پول نیز به طور مستقیم در دستگاه شما دانلود می‌شود. معمولا از طریق دانلود اپلیکیشنی روی موبایل خود به کیف پول کریپتوکارنسی‌تان دسترسی پیدا می‌کنید. چنین دسترسی این امکان را به شما می‌دهد تا با اسکن کردن کدQR ، کوین‌های خود را در یک فروشگاه خرج کنید.

- **کیف پول آنلاین یا روی وب**

کیف پول روی وب بهترین سطح از راحتی به هنگام ارسال کوین‌ها به دیگران را در اختیار شما قرار می‌دهد. با این حال، کم‌ترین سطح امنیت متعلق به این کیف پول است. چون معمولا تولیدکننده آن کیف پول، کنترل کاملی روی سیستم دارد. یک نمونه از چنین کیف پولی، ذخیره کردن کوین‌ها در یک صرافی کریپتوکارنسی است. این صرافی، کوین‌های شما را روی سرور مرکزی خود ذخیره می‌کند. اگر این سرور هک شود، هکر می‌تواند به تمام پول‌های شما دسترسی داشته باشد. بهتر است که تنها تعداد کمی از کوین‌های خود را روی کیف پول تحت وب نگه دارید.

- **کیف پول کاغذی**

کیف پول‌های کاغذی یکی از کم ارزش‌ترین کیف پول‌های کریپتو هستند. تنها کاری که باید انجام دهید این است که کلیدهای عمومی و خصوصی خود را روی یک تکه کاغذ پرینت بگیرید و با این کار به سادگی می‌توانید سطح امنیت پول خود را بالا نگه دارید. چون در این روش، کلیدها به هیچ سروری متصل نیستند. در نتیجه راهی به جز در اختیار داشتن آن کاغذ برای دسترسی

به کیف پول، وجود ندارد. زمانی هم که نیاز به انتقال وجه دارید، می‌توانید به سادگی کلیدها را وارد یک نرم افزار یا کیف پول تحت وب کنید، یا حتی ساده‌تر از آن، فقط کد QR چاپ شده را اسکن کنید.

- **کیف پول سخت افزاری**

به لحاظ امنیتی، هیچ کیف پولی بهتر از کیف پول سخت‌افزاری نیست. کیف پول سخت افزاری یک دستگاه فیزیکی است که تنها هدفش ذخیره‌سازی کلیدهای عمومی و خصوصی‌تان است. این دستگاه تنها در صورتی که نیاز به انتقال وجه داشته باشید به اینترنت متصل می‌شود. هنگام انتقال، شما باید پین شخصی خود را به طور مستقیم وارد دستگاه کنید. این کار دسترسی هکرها به کلیدهای‌تان را تقریبا غیرممکن می‌سازد. آیا می‌توانیم همه کریپتوکارنسی‌های خود را در یک کیف پول ذخیره کنیم؟این سوال بسیار مهمی است و جواب آن به کوین‌هایی که در دست دارید، بستگی دارد. به عنوان مثال، اگر شما فقط بیت‌کوین دارید باید یک کیف پول داشته باشید که با ارز دیجیتال بیت‌کوین سازگار باشد.اگر ارز دیجیتال بیت‌کوین و لایت‌کوین داشته باشید چطور؟اگرچه هر کدام از آن‌ها دارای بلاک‌چین مختص به خود هستند، اما می‌توان از یک کیف پول چند ارزی استفاده کرد. کیف پول‌های چند ارزی به شما این امکان را می‌دهند تا کریپتوکارنسی‌های مختلف را درون یک کیف پول ذخیره کنید. این کار بسیار ساده‌تر از به کار بردن کیف پول‌های متفاوت برای کوین‌های مختلف است. با این حال، همه چیز به این بستگی دارد که کیف پول ارزی شما از چه امکاناتی پشتیبانی می‌کند.آیا کیف پول‌های کریپتوکارنسی امن هستند؟به طور کلی، مهم نیست که از کدام کیف پول ارز دیجیتال استفاده می‌کنید، اگر کسی به کلید خصوصی شما دسترسی داشته باشد، می‌تواند به پولتان نیز دسترسی پیدا کند. پرسش کلیدی این است که چه کارهایی را برای پیش‌گیری از وقوع این اتفاقات می‌توان انجام داد؟ هر کیف پول ارز دیجیتال که با اینترنت در ارتباط باشد – به عنوان مثال روی دسکتاپ، موبایل یا وب قرار داشته باشد. همیشه امکان آسیب‌پذیری را با خود به دوش می‌کشد. هکرها همیشه راه‌های جدیدی برای دستیابی به اطلاعات دیگران پیدا می‌کنند و به همین دلیل باید هر کاری که لازم است برای محافظت از کلید خصوصی خود انجام دهید.

بهترین کیف پول ارز دیجیتال

۱ -کیف پول اکسودوس:(Exodus)

اکسودوس یک کیف چند ارزی روی دسکتاپ است که به شما این امکان را می‌دهد تا تعداد زیادی از کوین‌های مختلف مانند بیت‌کوین، لایت‌کوین، دش و نیز توکن‌های ERC-20 مختلف را روی آن ذخیره کنید. یکی از ویژگی‌های مهم و اساسی در امنیت هر کیف پول تایید دو مرحله‌ای است که اکسودوس از این ویژگی برخوردار نیست. این بدین معنی است که کیف پول شما امن‌تر از گوشی همراه یا یارانه شما نیست و در صورتیکه سرقت شوند و یا مورد حمله سایبری قرار بگیرند، دارایی‌هایتان را از دست خواهید داد. دومین ویژگی کاربردی و مهم امنیتی که اکسودوس از آن بی بهره است، قابلیت چند امضاییست. این قابلیت مانند یک لایه امنیتی عمل کردن و با فعال سازی آن، برای نهایی شدن یک تراکنش لازم است که بیش از یک دستگاه آن را تایید کند. امنیت این کیف پول از طریق یک رمز عبور و ۱۲ رشته کلمه برای بازیابی اطلاعات کیف پول گم شده صورت می‌گیرد. توجه کنید که کلیدهای خصوصی این کیف پول بجز در رایانه و تلفن همراه، در هیچ سرور دیگری ذخیره نمی‌شود و تنها راه دست یابی به کلیدهای خصوصی از طریق کاربر است و مسئولیت حفظ و امنیت آن بر عهده کاربر می‌باشد.

ویژگی های کیف پول اکسودوس

- کاربرپسندی

کاربرپسند بودن مهم‌ترین ویژگی کیف پول اکسودوس است. طراحی این کیف پول به گونه‌ای است که حتی افراد تازه کار می‌توانند به راحتی به نصب و استفاده از این کیف پول بپردازند. داشتن صرافی درون ساخت این کیف پول، این امکان را برای کاربر فراهم کرده است که علاوه بر ذخیره سازی ارزهای دیجیتال به مبادله آن‌ها درون کیف پول نیز بپردازند. این یکی از مزایای این کیف پول است که این امکان را برای کاربران تازه وارد که تجربه کافی در استفاده از صرافی‌ها ندارند، با پرداخت کارمزد بیش‌تر، به مبادله در صرافی داخلی این کیف پول بپردازند. اما متاسفانه در تمامی کیف پول‌های ارز دیجیتال، به دلیل تحریم‌ها امکان مبادله ارزها برای کاربران ایرانی غیرفعال است.

- پشتیبانی

از ویژگی‌های مثبت این صرافی در مقایسه با سایر رقبای آن، پشتیبانی تمام وقت تیم توسعه دهنده آن است. کاربران می‌توانند در هر روز و ساعتی از شبانه روز به پشتیبانی سایت و یا کیف پول پیام دهند و مشکل خود را مطرح نمایند. همچنین این کیف پول سوالات متداول زیادی را در بخش سوالات پرتکرار سایت در کنار فیلم‌های آموزشی مختلف برای کاربران خود آورده است، تا تمامی مشکلات کاربران خود را حل کنند. این کیف پول در چهار پلتفرم اندروید، iOS، ویندوز، مک و لینوکس، قابل استفاده و دانلود است. این کیف پول همچنین قابلیت ادغام با کیف پول سخت افزاری ترزور را نیز دارد و می‌توان از آن برای کنترل و یا بازیابی دارایی‌های ترزور در صورت خرابی یا مفقودی این کیف پول سخت افزاری استفاده کرد.

مزایا و معایب کیف پول اکسودوس

مزایا:

- تبدیل آسان ارز دیجیتال در لحظه
- پشتیبانی ۲۴ ساعته
- امکان دانلود رایگان بدون نیاز به ثبت نام
- پشتیبانی کردن از کیف پول سخت افزاری ترزور

معایب:

- پشتیبانی از ارزهای دیجیتال کمتری در اپلیکیشن موبایل
- نبود امکان فروش ارز در اپلیکیشن

- تحریم بودن ایران برای استفاده از امکانات مربوط به مبادله در صرافی داخلی آن

۲ -کیف پول برد ولت:(Bread Wallet)

نوعی از کیف پول ارز دیجیتال روی موبایل است که بسیار کاربر پسند و برای مبتدیان عالی است. از ویژگی جالبش این است که با آن می‌توانید کد QR آدرس کیف پولی که می‌خواهید به آن وجه ارسال کنید را اسکن کرده و در نتیجه بیت کوین خود را در یک فروشگاه واقعی نیز خرج کنید. اما متاسفانه بیت‌کوین تنها کریپتوکارنسی است که این کیف پول از آن پشتیبانی می‌کند. اما فراموش نکنید که کاملاً رایگان است. کیف پول برد ولت یک کیف پول با امنیت بسیار بالا است که امنیت کوین‌ها و اطلاعات حریم شخصی کاربرانش را حفظ می‌کند. این کیف پول به صورت مستقیم به شبکه بیت کوین متصل می‌شود و این امکان را برای کاربران خود فراهم می‌کند که خیلی سریع‌تر و امن‌تر به دارایی خود دسترسی پیدا کنند. همچنین این صرافی به منظور جلوگیری از سواستفاده و دستبرد به حساب‌های کاربران، هرمعامله‌ای که انجام می‌شود را توسط سیستم خودش تایید می‌کند. داشتن قابلیت تشخیص هویت با اثر انگشت از دیگر امکانات این کیف پول است. با فعال کردن این گزینه از قسمت تنظیمات تمامی معاملات تنها از طریق اثر انگشت امکان پذیر می‌باشد. همچنین امکان محدود کردن معاملات شما نیز از طریق این بخش وجود دارد.

ویژگی های کیف پولBread Wallet

- رابط کاربری ساده و کاربرپسند

کیف پول برد، یکی از ساده‌ترین رابط کاربری‌ها را در بین کیف پول‌های ارز دیجیتال دارد. این کیف پول دارای دکمه‌های ناوبری آسان در نمایشگرهای کوچک است. نمای پلتفرم این کیف پول ساده و شامل دو صفحه اصلی برای ارسال و دریافت پول است و تمامی کاربران آن اعم از آماتور و حرفه‌ای می‌توانند به ساده‌ترین شکل در پلتفرم این کیف پول فعالیت کنند.

- تایید پرداخت ساده

این کیف پول بدون نیاز به نرم افزار اضافی قادر به اتصال و ایجاد پول در شبکه بیت کوین است. این یکی از جذاب‌ترین قابلیت‌های این کیف پول است که آن را به یکی از امن‌ترین کیف پول‌های موبایل تبدیل کرده است.

- حریم خصوصی ایمن

برد ولت در مساله حریم خصوصی کاربران خود آنقدر سخت‌گیر و حساس است که حتی تا جای ممکن دسترسی به اطلاعات کاربران خود را برای اعضای تیمش نیز محدود کرده است.

- ثبت نام آسان

ثبت نام در این کیف پول در کسری از ثانیه و بدون نیاز به گذراندن مراحل خاصی صورت می‌گیرد.

- پشتیبانی سریع

کاربران این کیف پول می‌توانند با مطرح کردن مشکلات خود به تیم پشتیبانی برد ولت در کمترین زمان ممکن ایرادهای سیستم خود را رفع کنند.

مزایا:

- رایگان بودن اپلیکیشن
- عدم نیاز به گذاراندن مراحل ثبت نام برای شروع
- اتصال مستقیم به شبکه بیت کوین
- امکان فعال سازی گزینه ورود با اثر انگشت
- امنیت بالای حفظ اطلاعات مشتریان
- پشتیبانی فعال و سریع
- امکان خرید بیت کوین به صورت مستقیم از طریق اپلیکیشن
- ایجاد کردن خودکار آدرس کیف پول برای هر تراکنش

معایب:

- عدم داشتن احراز هویت دو مرحله‌ای
- تداشتن قابلیت چند امضایی
- نیاز به استفاده از سرویس‌های متفرقه علاوه بر خود اپلیکیشن برای خرید بیت کوین
- پشتیبانی نکردن از آلت کوین‌ها

واقعیت مجازی VR

این تکنولوژی درحال حاضر متشکل از تجهیزات سخت افزاری مثل عینک، هدفون و دستکش های مخصوص می باشد. در واقع عینک مخصوص که در مقابل چشمان شما قرار دارد یک تصویر سه بعدی را در مقابل چشمان شما ایجاد می کند و هدفون نیز همزمان یک صدای نزدیک به واقعیت را در کنار عینک تداعی می کند. این دو در کنار هم باعث می شوند شما از لحاظ دیداری و شنیداری حس کنید که در یک جهان جدید قرار دارید. در واقع شما یک دنیای مصنوعی و ساختگی را از طریق کامپیوتر تجربه می کنید اما با حس های دنیای واقعی. این تکنولوژی به سرعت در حال توسعه و پیشرفت است، برای مثال با ورود به دنیای سرگرمی و گیمینگ می تواند تجربه نزدیک به واقعیت را از طریق بازی های ویدیوئی ایجاد کند. همچنین می

تواند در شبیه سازی آموزش های خلبانی و پزشکی که هزینه های بسیار زیاد داشته و خطرناک اند بکار آید. فراتر از کاربرد آن در سرگرمی و صنعت، این تکنولوژی در حوزه بلاکچین و دنیاهای متاورسی در حال ظهور است، به این صورت که شما علاوه بر دنیای واقعی خود، در یک دنیای موازی و مجازی به زندگی بپردازید. تجربه ها و حس‌هایی که امکان حس آن‌ها در این جهان نیست را تجربه کنید، هم از لحاظ فیزیکی و هم روانی.

ویژگی های مختلف تکنولوژی واقعیت مجازی VR

این تکنولوژی از دید کارشناسان باید دارای چند ویژگی بخصوص باشد تا بتواند یک تجربه بسیار نزدیک به واقعیت را در جهان های متاورسی ایجاد کند. چند مورد از مهمترین این ویژگی ها عبارتند از:

۱. باورپذیر و تعاملی: تکنولوژی ایجاد یک محیط شبیه سازی شده یک ایده جدیدی نیست، تنها بحث جدید توان انتقال تمامی حس های فیزیکی، روانی و ذهنی انسان به دنیای موردنظر است تا باورپذیری بالایی را برای کاربر ایجاد کند، برای مثال فیلم سه بعدی نیز از این تکنولوژی تاحدودی بهره می‌برد اما وقتی صحنه سقوط از یک بلندی را به کاربر نمایش می‌دهد، آیا کاربر از لحاظ فیزیکی حس سقوط و معلق بودن در هوا را تجربه میکند؟ البته که نه. بیننده فقط از لحاظ دیداری و شنیداری این حس را تجربه می کند، حال شما فرض کنید با پیشرفت این تکنولوژی تا این حد، چه تجربیات منحصر به فردی که به دلیل هزینه های بالا یا خطرناک بودن، امکان حس آنها در این دنیا وجود ندارد را می‌توانیم کسب کنیم.

۲. گستردگی و جامع بودن: منظور از جامع بودن، داشتن جزئیات فراوان همانند دنیای واقعی است. وقتی صحبت از توسعه کسب و کار، امکان برگزاری جلسات و مراسمات در دنیای متاورسی می‌شود باید این دنیا دارای جذابیت‌ها و جزئیات فراوانی باشد تا بتواند نظر اکثریت را به خود جلب کند.

انواع واقعیت مجازی

همانطور که در بالا نیز اشاره شد، واقعیت مجازی اولین بار توسط محیط های متاورسی برای استفاده مطرح نشدند، برای مثال در آموزش خلبانی از این نوع شبیه سازی چندین سال است که استفاده می‌شود. پس دلیل اینهمه سر و صدا پیرامون این جریان چیست؟ می توان گفت دلیل اصلی در انواع بکار رفته از واقعیت مجازی و دسته بندی های مختلف آن است. در زیر به دو دسته کلی تکنولوژی واقعیت مجازی اشاره می کنیم تا درک بهتری از آن را کسب کنید.

۱. شناوری یا غوطه وری: در بالا تجربه یک صحنه سقوط را مثال زدیم. برای درک بهتر فرض کنید در یک جهان متاورسی یا شبیه سازی شده ای قرار دارید که می توانید با استفاده از آواتار خود در مسابقه موتور سواری شرکت کنید هنگامی که شما سوار موتورسیکلت می شوید اگر بتوانید حس لمس قطعات آن، بادی که به صورت شما اصابت می کند و حتی جابجا شدن و تکان خوردن بدن خود روی موتورسیکلت را کاملا تجربه کنید، این یک شناوری کامل است، با این تفاوت که خطر جانی و مالی دنیای واقعی را ندارد.

۲. غیر شناوری یا غیر غوطه وری: این نوع واقعیت مجازی چندین سال است که کاربرد دارد و در صنعت آموزش و پزشکی از آن استفاده می شود. در این نوع از VR کاربر فقط از لحاظ دیداری یک تصویر سه بعدی را می تواند ببیند و حواس دیگر او درگیر نمی شوند.

البته لازم به ذکر است که در حال حاضر شناوری کامل یک تصور ایده آل می باشد و هنوز به واقعیت تبدیل نشده و راه بسیاری دارد، اما برای مثال شرکت متا (فیس بوک سابق) از یک دستکشی رونمایی کرد که توانایی انتقال حس لامسه به کاربر را داشت. در این بین پلتفرم های متاورسی مختلفی که در حال حاضر وجود دارند می توان گفت در سطحی مابین دو گزینه بالا بوده و با پیشرفت روزافزون این فناوری آنها نیز رو به جلو و بهبود حرکت می کنند.

کاربرد VR

- پزشکی : توانبخشی، آموزش جراحی به دانشجویان
- آموزش خلبانی و شبیه ساز پرواز
- درمان اضطراب و افسردگی : فرد را با استفاده از VR در معرض عامل استرس زا و ترس او قرار می دهند. درحالی که در یک محیط کاملا امن از لحاظ فیزیکی قرار دارد، در واقع در عین حس امنیت فرد را با ترس او روبرو می کنند.
- آموزش : در مبحث آموزش دانشگاهی یا هرگونه دوره آموزشی می توان بدون حضور فیزیکی به یادگیری پرداخت، بدون اینکه تعامل با دیگران را همانند آموزش اینترنتی حذف کرد.
- متاورس : دنیای متاورس و بلاکچین اوج این فناوری می تواند باشد، به این صورت که شما می توانید بسیاری از کارهای روزمره خود همانند جلسه کاری، مراسمات، بازدید از مکان های گردشگری، خرید و دیدارهای دوستانه را با VR و شناوری کامل انجام دهید.

واقعیت افزوده (Augmented Reality)

واقعیت افزوده فناوری می‌باشد که دنیای دیجیتالی و مجازی را با دنیای واقعی اطراف ما ترکیب می‌کند. این تکنولوژی نیز با یک عینک و هدفون خاص اشیا، متن، اشکال هندسی و هرچیزی را با یک همبستگی خاصی در قالب دیجیتالی وارد دنیای واقعی می‌کند و شما از لحاظ دیداری و شنیداری آن را به صورت سه بعدی دیده و صدای آن را نیز می‌شنوید. این تکنولوژی باید یک همبستگی هندسی دقیق و منطقی بین شی مجازی و واقعی ایجاد کند، تا برای مثال وقتی یک عروسک متحرک را بر روی میز خود میبینید، واقعا حس حضور آن را از لحاظ دیداری به شما القا کند. این تکنولوژی در واقع تلفیق VR با دنیای واقعی است. یکی از هدست های مخصوص واقعیت افزوده که توسط شرکت مایکروسافت تولید شده Hololens نام داردکه این هدست با بهره گیری از چند میکروفون، دوربین و سنسورهای اپتیکی پشرفته برای سنجش محیط، هولوگرام های ترکیبی با محیط را ایجاد می کند.

کاربردهای واقعیت افزوده AR

این فناوری نیز کاربردهای اساسی بسیاری همانند بازی های ویدیوئی، طراحی و مدلسازی در معماری و شهرسازی، تعمیر، نگهداری، پزشکی، گردشگری، بازدید و کسب اطلاعات از وسایل قبل از خرید و سیستم های ناوبری کاربرد بالایی دارد.

انواع واقعیت افزوده

دسته بندی های گوناگونی برای فناوری واقعیت افزوده بیان می شود، اما در کل برحسب کاربرد و سخت افزار بکار رفته به چند دسته زیر تقسیم می شوند.

- واقعیت افزوده مبتنی بر الگو (Pattern Based) : این نوع واقعیت افزوده بر روی گوشی های تلفن همراه و با استفاده از یک اپلیکیشن کاربرد دارد، به این صورت که شما دوربین گوشی همراه خود را به سمت یک ساختمان، شی یا حتی بدن می گیرید (که می شود همان الگو)، و اپلیکیشن برای شما یک سری اطلاعات راجع به همان ساختمان و شی اعم از سال ساخت، سازنده، اطلاعاتی راجع به یک اندام بدن و ... را در کنار آن روی صفحه تلفن همراه نمایش می دهد. این مورد در گردشگری و خرید، برای کسب اطلاعات از منو وظرفیت یک رستوران، یا اطلاعات یک محصول کاربرد بسیاری دارد.
- مبتنی بر مکان (Location Based) : این نوع واقعیت افزوده همانطور که از اسمش مشخص است بر اساس مکان جغرافیایی کاربر کار می کند و با استفاده از GPS واقعیت افزوده های از قبل تعریف شده برای همان مکان را بر روی صفحه گوشی نمایش می دهد.
- واقعیت افزوده بر اساس تصویر سازی و قرارگیری (Superimposition based AR) : در این نوع AR که می توان گفت تا به الان پیشرفته ترین مدل آن است با ایجاد نور های مصنوعی، هولوگرام ها یا اشیائی را بر روی سطوح فیزیکی واقعی به نمایش در می آورند، با این که طبیعی جلوه دادن آن و هماهنگی شی مجازی با سطح فیزیکی کمی چالش برانگیز است اما جذابیت بصری بسیار بالایی دارد.

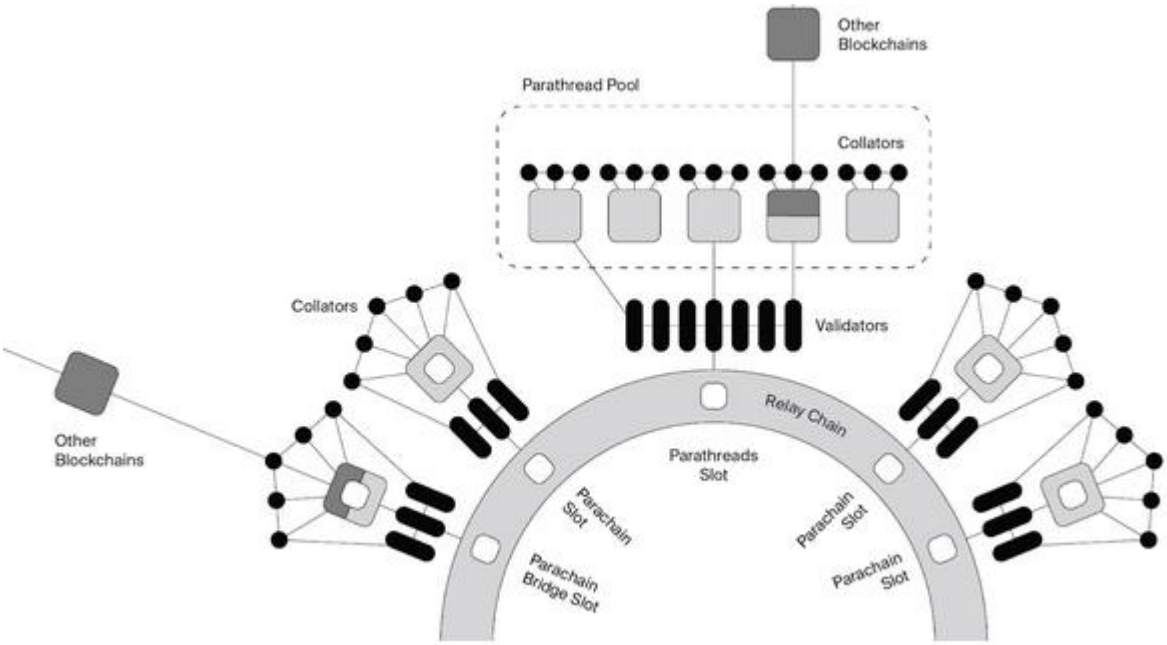
تفاوت واقعیت افزوده AR و واقعیت مجازی VR

واقعیت افزوده و مجازی یک تفاوت اساسی دارند. واقعیت مجازی شما را وارد مکان و دنیایی غیر از این دنیای واقعی می کند که همه چیزدر آن شبیه سازی شده بوده و تمام حواس فیزیکی و ذهنی شما را درگیر می کند. اما واقعیت افزوده یک سری اشیا یا موجودات مجازی را با این دنیای واقعی ترکیب می کند، و شما را کلا از این جهان جدا نمی کند.نقش اینترنت در دنیای امروز انکار ناپذیر است. تقریبا همه آدمها کم و بیش با زندگی اینترنتی درگیر هستند و هرشخص برای خود هویت مجازی دارد. مانند اکانت اینستاگرام که هویت مجازی افراد بوده و معرف آن ها در دنیای مجازی است یا فروشگاه اینترنتی که یکی از اجزای هویت مجازی افراد و شرکت ها را تشکیل می دهد.ارتباطات افراد با دوستان و همکارانشان در دنیای امروز نیز به صورت مجازی شده است، در قالب گروه های اجتماعی که در آن عضو هستند یا حتی بازی هایی که برای سرگرمی افراد در دنیای کامپیوتری ایجاد شده اند نیز بخشی از هویت مجازی افراد را تشکیل داده اند.

متاورس

برخی از افراد نیز دارایی های اینترنتی بر بستر اینترنت دارند که به آن ها ارزهای دیجیتال گفته می شود یا بازی هایی که برای برخی از آیتم های آن ها پول پرداخت شده است. مثلا شخصی ماشینی را برای بازی اینترنتی خریداری کرده است اما مشکل اینجاست که نمی تواند این ماشین را برای بازی دیگری استفاده کند یا در بستر دیگری از فضای اینترنت آن را به کار ببرد. اینجاست که پای متاورس به میان می آید. دنیای مجازی بر بستر اینترنت که تمام دارایی های دیجیتال شخص در این دنیا به یکدیگر مرتبط می شوند. یک زندگی کاملا مجازی با میلیون ها کاربر که در آن افراد با تمام هویت و متعلقات دیجیتالی خود با یکدیگر در ارتباط باشند و در کنار هم یک زندگی مجازی داشته باشند.از نظر لغوی متاورس ترکیبی از کلمات meta و universe است. متا به معنای فراتر از... و یونیورس به معنای جهان. ترکیب این دوکلمه معنای متاورس را تشکیل می دهد که به معنای فراتر از دنیاست. جهانی دیجیتال متشکل از واقعیت مجازی، اینترنت و واقعیت افزوده است.این اصطلاح در رمان علمی تخیلی نیل استفنسون در سال ۱۹۹۲ به نام سقوط برف برای اولین بار مطرح شد. جایی که انسان ها به عنوان آواتار با یکدیگر و از طریق عوامل نرم افزاری در فضای مجازی سه بعدی که از استعاره دنیای واقعی استفاده می کند، تعامل دارند.چشم انداز metaverse این است که یک جهان مجازی اجتماعی، سه بعدی و متشکل از بسیاری از فضاهای مجازی سه بعدی به هم پیوسته را تشکیل دهد. چیزی که ما در حال حاضر با بازی هایی مانند Fortnite و Roblox تجربه می کنیم. از نظر بسیاری از افراد و کارشناسان، بازی‌های ویدئویی مانند روبلاکس و فورتنایت پیشگامان شکل گیری متاورس هستند. قرار است متاورس جانشینی برای اینترنت امروزی باشد، نسل بعدی اینترنت. متاورس چیست؟ در واقع متاورس ارتباط بین جهان فیزیکی و جهان مجازی را آنگونه که افراد دوست دارند فراهم خواهد کرد، طوری که بتوانند در دنیایی که مورد دلخواهشان است گشت و گذار کنند. به عبارت دیگر، جهانی دیجیتال با ویژگی های منحصر به فرد است که در آن هرچه بخواهید وجود دارد و شما عناصر دنیای فیزیکی واقعی را با عناصر جهان مجازی ترکیب خواهید کرد.

بلاکچین و پاراچین در کریپتوکارنسی



شکل ۱- بلاکچین و پاراچین

یکی از اولین مباحثی که هر شخص وارد این بازار می شود شناخت بستر و امنیت این مارکت است، تمامی ارزهای دیجیتال این بازار بر بستری امن به نام بلاکچین فعالیت می کنند. هدف همه بلاکچین های ساخته شده، دست یابی به ۳ فاکتور بسیار مهم تمرکز زدایی، امنیت و مقیاس پذیر است با این حال دستیابی به بلاکچین ها به ۳ هدف یک چالش بسیار بزرگ است، علاوه بر این ۳ هدف مهم، بلاکچین های دیگر به دنبال ویژگی های ترکیب پذیری و ارتباط بین زنجیره ای هستند.

جدول ۱- ویژگی های مهم برای یک بلاکچین

بالا بودن امنیت
مقیاس پذیری
تمرکز زدایی
ترکیب پذیری
ارتباط بین زنجیره ای

پاراچین را می توان گونه ای از شبکه بلاکچین در نظر گرفت، این ساختار، ساختاری خاص برای مدیریت داده و اطلاعات است که به صورت موازی در اکوسیستم ارز دیجیتال پولکادات) - (DOT در هر دو شبکه پولکادات و کوساما (اجرا می شود، مهم ترین تفاوت آن این است که با اتصال به شبکه مرکزی، نیازی به تعریف نودهای مجزا ندارد.

آشنایی با پروژه پولکادات

پولکادات به صورت یک شبکه چند زنجیره ای ۳ لایه ای عمل می کند، لایه اول آن، لایه ۰ نامیده می شود، که قابلیت اتصال به ۱۰۰ شبکه بلاکچین را دارد، به عبارتی دیگر، ساختار شبکه پولکادات به صورت یک شبکه چند زنجیره‌ای طراحی شده که در لایه یک آن امکان راه اندازی تقریبا ۱۰۰ شبکه بلاکچین تحت عنوان **پاراچین** وجود دارد. تمامی این شبکه‌ها به شبکه اصلی پولکادات و نودهای این شبکه متصل هستند.

خصوصیات پاراچین

جدول ۲- خصوصیات شبکه قدرتمند پولکادات

انعطاف پذیری
مقیاس پذیری
قابلیت همکاری
حاکمیت

انعطاف پذیری

مدل ساخت پاراچین پولکادات به این صورت است که در اینترنت آینده بلاکچین ها بتوانند با یکدیگر همکاری داشته باشند، همانطور که نسخه فعلی اینترنت نیازهای مختلف جامعه را برآورده می‌کند، بلاکچین ها نیز باید بتوانند خدمات متنوع تری را برای تسریع خدمات ارائه دهند. یک زنجیره ممکن است برای بازی طراحی شود و یا یک شبکه برای مدیریت هویت طراحی شده باشد، دیگری برای امور مالی و ... در عین حال این شبکه ها باید بتوانند با هم تعامل داشته باشند و دیتا و اطلاعات را میان هم به اشتراک بگذارند. لذا پاراچین، انعطاف‌پذیری بسیار بالایی برای این امر مهم دارد. نکته قابل ذکر در مورد پاراچین این است که هر پاراچین می تواند طراحی توکن و روند حاکمیتی خاص خود را داشته باشد که برای استفاده خاص خود طراحی شده است، همچنین پاراچین ها می توانند به عنوان شبکه های عمومی و خصوصی نیز مورد استفاده قرار گیرد.

مقیاس پذیری

با استفاده از مدل پیشرفته پاراچین پا، پولکادات به زنجیره های بلوکی اجازه می‌دهد تا مقیاس پذیری را در لایه ۱ بدست آورند. این یک روش غیرمتمرکز و کارآمدتر برای دستیابی به مقیاس پذیری بلاکچین است .پاراچین اجازه می‌دهد تا تراکنش ها به صورت موازی در یک اکوسیستم از بلاکچین های لایه ۱ پخش و پردازش شوند؛ که به طور قابل توجهی باعث بهبود توان و مقیاس پذیری می‌شود.

حاکمیت

پاراچین ها در پولکادات در انتخاب مدل حاکمیتی که مناسب خود می دانند آزادانه عمل می کنند و می توانند به تعدادی ماژول از پیش ساخته شده برای پیاده سازی سیستم های مختلف حاکمیتی دسترسی پیدا کنند. هر پروژه می‌تواند مدل مدیریتی خود را پیاده سازی و اجرا کند.

الگوریتم اجماع پاراچین

هر شبکه پاراچینی که بر روی شبکه پولکادات راه اندازی شده است ملزم به پیروی از الگوریتم اجماع شبکه پولکادات است، این الگوریتم، الگوریتم اجماع شبکه مرکزی پولکادات نام دارد، این به معنی این است که شبکه ها در انتخاب الگوریتم اجماع خود حق انتخابی نداشته و نمی توانند از الگوریتم دیگری پیروی کنند.هر تراکنش در شبکه پولکادات به صورت موازی در پاراچین اجرا می شود و به زمان ثبت این تراکنش بر روی رله چین اسلات گفته می شود، قابل ذکر است که برای اینکه یک پاراچین به پولکادات اضافه شود باید در یکی از اسلات‌های موجود قرار گیرد. بسیاری از کسب و کارها با مطرح شدن فناوری بلاکچین به دنبال استفاده از این فناوری هستند اما ایجاد یک شبکه بلاکچین مستقل، به زمان، تخصص و هزینه بالایی نیاز دارد. راه‌اندازی پاراچین یکی از راه حل های جایگزین است. هزینه راه اندازی و اجرای شبکه های همچون کازماس، تزوس (XTZ)و ایاس (EOS) چیزی در حدود ۱۰ میلیون دلار در سال است. شبکه های بزرگ و مطرحی همچون اتریوم و بیت کوین، هزینه سالانه بالغ بر یک میلیارد دلار در سال دارند. شبکه پولکادات در گزارشی اعلام کرده است که هزینه سالانه راه اندازی Parachain در این شبکه، چیزی در حدود ۱۰۰ تا ۲۰۰ هزار دلار است. این عدد در مقایسه با راه‌اندازی یک شبکه بلاکچین مجزا، بسیار کمتر است.

کاربردهای پاراچین

هدف اصلی از طراحی رمز ارز محبوب پولکادات، ایجاد یک طیف وسیعی از امکانات برای تیم های پاراچین برای طراحی بلاکچین های لایه ۱ است، در جدول زیر می توانید کاربردهای مهم آن را بررسی کنید:

کاربردهای پاراچین

جدول ۳-کاربرد های پاراچین

بازی
امور مالی غیر متمرکز (DeFi)
گواهینامه ها
اوراکل ها
کیف پول های دیجیتال
تائید هویت
اینترنت اشیا
قراردادهای هوشمند

تفاوت قرارداد هوشمند وParachain

قراردادهای هوشمند بر روی بلاک چین های اختصاصی مانند اتریوم، الگورند، سولانا(SOL)، تزوس، کاردانو و... کار می کنند. اما از آنجایی که این قراردادها بر روی بلاکچین اجرا می شوند و رقبای زیادی نیز دارند، ممکن است هزینه تراکنش ها، سرعت کمی را به دلیل تراکم زیاد به دنبال داشته باشد. در واقع، این یکی از چالش های بزرگ برای پذیرش گسترده زیرساخت های بلاکچین است؛ چرا که آن‌ها به اندازه کافی قابل استفاده نیستند.از طرف دیگر، پاراچین ها بلاکچین های مستقلی هستند که برای هدف خاصی ایجاد می شوند و طیف وسیعی از خدمات و کاربردها را به مشتریان خود ارائه می دهند.

نتیجه گیری

پاراچین را می توان گونه ای از شبکه بلاکچین در نظر گرفت، این ساختار، ساختاری خاص برای مدیریت داده و اطلاعات است که به صورت موازی در اکوسیستم ارز دیجیتال پولکادات (DOT) در هر دو شبکه پولکادات و کوساما اجرا می شود،

همچنین Parachain کاربردها و ویژگی های زیر را نیز داراست: انعطاف پذیری، مقیاس پذیری، قابلیت همکاری و حاکمیت از مهم ترین خصوصیات شبکه Parachain است.

Refrences:

1. Mougayar, W(2016), The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology , Wiley,208 p , ISBN:1119300312, 9781119300311
2. Quiniou M (2019), Blockchain: The Advent of Disintermediation, Wiley-ISTE,164 p , ISBN: 978-1-786-30403-2
3. Tapscott D (2018), Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World,432 p , ISBN-13 : 978-1101980149
4. coinmarketcap.com
5. polkadot.com
6. mehdirajabi.com