یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

شناخت مفهوم قراردادهای هوشمند و ارز اتریوم و مقایسه این ارز با نخستین ارز دیجیتال (بیتکوین)

محدثه ناصحی پور

کارشناسی ارشد مدیریت مالی دانشگاه یزد، یزد m.nasehi.75@gmail.com

چکیده

از سال ۲۰۰۹ با گسترش ارزهای دیجیتال، این فناوری نوین توجه بسیاری را به خود جلب کرد. مهم ترین ویژگی این ارزهای نوین غیر متمرکز بودن آن هاست. در بین ارزهای دیجیتال متعدد پدید آمده از سال ۲۰۰۹ تا کنون اتریوم و بیت کوین دارای بالاترین جایگاه هستند به گونه ای که بسیاری از فعالان این حوزه از آن ها به عنوان پادشاه و ملکه دنیای ارز های دیجیتال نام میبرند. بیتکوین تنها یک ارز دیجیتال محسوب میشود ولی اتریوم یک قدم پا را فراتر گذاشته و امکان اجرای غیرمتمرکز کدهای کامپیوتری (قرارداد هوشمند) را هم فراهم کرده است تا بتوان علاوه بر پول، بقیه فرایندها را هم غیرمتمرکز کنیم. میتوان متصور شد که در آینده نه چندان دور اتریوم از بیتکوین پیشی بگیرد پس شناخت هرچه بیشتر این سیستم کمک خواهد کرد از قطار پرسرعت بازارهای مالی عقب نماند.

واژه‌های کلیدی

ارز دیجیتال – بلاکچین – بیتکوین – قراردادهوشمند – اتریوم – تراکنش

۱. متن مقاله

در جوامع اولیه انسان قادر نبود به تنهایی تمامی نیازهای خود را تأمین کند و با توجه به نیازهای انسانی، دادوستد کالا شکل گرفت و اولین پول یعنی پول کالایی به وجود آمد. به تدریج مشکلات پول کالایی موجب شد که انسانها از کالاهایی برای این امر استفاده کنند که قابلیت های بهتری دارند .سپس از فلزاتی مانند مس، آهن، نیکل، برنج، نقره و طلا استفاده کردند که به دلیل امتیازات نقره و طلا سایر فلزات از رده خارج شدند و سیستم پایه پولی دوفلزی به وجود آمد. سیستم دوفلزی نیز بعدها دچار اشکالاتی شد و کشورها به سمت پایه پولی تک فلزی طلا یا نقره روی آوردند. مشکالت این نوع پول نیز باعث شد که پول کاغذی (اسکناس) و پول اعتباری، جایگزین پول فلزی شده و درحال حاضر نیز شاهد هستیم که پول الکترونیکی جای خود را در جامعه باز کرده و در آینده شاهد حذف اسکناس خواهیم بود. (نوری و نواب پور به نقل از تفقدی، ۱۳۹۶)

ویژگی مشترک تمام انواع پول بیان شده این است که دارای تمرکز جغرافیایی بودند. بدین معنا که در ابتدای پیدایش پول هرمنطقه کالایی برای مبادله داشت،سپس فلزی را برای انجام مبادلات پذیرفت و اکنون نیز هر کشور یا منطقه ارز مختص به خود دارد که عرضه آن تحت کنترل بانک های همان کشور یا منطقه است. حتی ارزهایی که برای مبادلات بین المللی نیز استفاده میشوند تحت کنترل کشورهای خاصی قرار دارند.

با گسترش فناوری اطلاعات، پول الکترونیکی پا به عرصه اقتصاد گشود که ماهیت آن همان اسکناس های کاغذی است، اما از حالت فیزیکی و ملموس به یکسری اعداد و ارقام داخل کامپیوتر و شبکه تبدیل شده است. به عبارتی پول های الکترونیک یا دیجیتال، مکانیسمی جدید در پرداخت اسکناس های متداول بانکی هستند؛ اما در سالهای اخیر، پولی پدید آمد که به طور ذاتی با اسکناس های بانکی تفاوت می کند و یک واحد سنجش جدید را با سازوکاری کاملاً متفاوت و منحصربه فرد به نام (ارز دیجیتال) با خود به همراه آورده است. (نوری و نواب پور به نقل از chuen ، ۱۳۹۶)

اولین تلاش ها برای ایجاد پول ها و قراردادهای غیر متمرکز در قرن ۲۰ میلادی صورت گرفتند ولی تا سال ۲۰۰۸ در حد تئوری باقی ماندند. از زمان معرفی نخستین ارز دیجیتال تا امروز هزاران ارز دیجیتال دیگر معرفی شده اند که بسیاری از آنان هنوز در دنیای بازارهای مالی ناشناس هستند. در این میان ارزهای بیت کوین و اتریوم تا حدودی جایگاه خود را در این بازار بدست آورده و دارای بیشترین سهم بازار هستند. ارز بیت کوین در حال حاضر شناخته شده ترین ارز دیجیتال است ولی ارز اتریوم با وجود سهم بازار و همچنین مزایایی که نسبت به ارزهای دیگر دارد هنوز چندان شناخته شده نیست.

در این پژوهش تلاش شده است با جمع آوری مطالب مرتبط با ارز دیجیتال اتریوم و بیان آن به زبان ساده به شناخت بیشتر این ارز نوین کمک کرده باشیم.

هدف اصلی ما آشنایی بیشتر با ارزهای دیجیتال به خصوص ارز اتریوم به عنوان برای شناخت گوشه ای از دنیای بازارهای مالی میباشد.

فرض اصلی ما این است که ارزهای دیجیتال نسل جدید پول هستند که برای کمک به بشریت و اقتصاد پدید آمده اند پس شناخت کامل آن ها از ملزومات افراد جامعه است.

۱. بلاک چین

در دهه های گذشته با ظهور ابزارهای دیجیتال،بازار های مالی نیز به سمت دیجیتالی شدن حرکت کردند. گسترش ابزارهای نوین معاملاتی و ایجاد سیستم های معاملاتی در کشور های پیشرفته، موجب رونق بازارهای مالی این کشورها گردید و تأثیرات قابل توجهی بر اقتصاد این کشور ها گذاشت.

نیک سابو در سال ۱۹۹۷ ، قرارداد های هوشمند را به عنوان آخرین نسل از قراردادهای الکترونیک معرفی کرد. تفاوت این قراردادها با قراردادهای سنتی، انعقاد آن ها در بستر الکترونیکی بود. ماهیت آن ها پروتکل های قراردادی در سخت افزارها و نرم افزارها بود و بالطبع

نقض آن ها هزینه زیادی در پی داشت. نیک سابو برای طرح خود از ماشین های دریافت، پردازش وپرداخت رونمایی کرد و ازقراردادهای دیجیتال به عنوان دریچه ای برای عبور از دنیای قراردادهای کاغذی به دنیای دیجیتال نام برد.اما طرح وی به دلیل عدم وجود فناوری و ابزار کافی مسکوت ماند(ناصر و رضوی ، ۱۳۹۷)

درواقع این ایده به دنبال فعال کردن پولی خصوصی بود که در میان کاربران خود با گستره ای جهان شمول و مجازی کاربرد داشته باشد و از سوی دیگر، نهادهای حاکمیتی و ازجمله بانک مرکزی در کنترل آن دخالتی نداشته باشند. در طول سالهای مختلف این ایده در قالبهای مختلف، عموماً از سوی متخصصان حوزه فناوری مانند هال فینی ، پیگیری شد. در اکتبر سال ۲۰۰۸ ،فردی به نام ساتوشی ناکاماتو را به در مقاله خود طرح سیستم پرداخت نظیر به نظیر طور عملیاتی مطرح کرد. در سال ۲۰۰۹ ،بیتکوین به عنوان اولین واحد پول مجازی و نمونه موفق عملیاتی طرحهای سابق معرفی شد(نوری و نواب پور به نقل از سلیمانی پور، ۱۳۹۶)

از دید فنی این ارزها در بستر دیجیتال قرار میگیرند و به هیچ پشتوانه ای متصل نیستند و حتی از ارزهای بدون پشتوانه رایج کنونی سرتاسر جهان نیز بی پشتوانه ترند.

در سیستم های پیش از بلاکچین تمام اطلاعات تحت کنترل یک سرور مرکزی هستند، یعنی سرور مرکزی باید اطلاعات را وارد یا تایید کند و فردی که به سرور مرکزی دسترسی داشته باشد میتواند در اطلاعات پیشین تغییر ایجاد کند یا آن ها را از بین ببرد. در سیستم بلاک چین هرکدام از کامپیوترهایی که به سیستم متصل هستند، میتوانند اطلاعات جدید وارد سیستم کنند و همچنین اطلاعات وارد شده را بررسی کنند.اطلاعات ثبت شده در بلاکچین همیشگی هستند،یعنی قابل تغییر نیستند و دسترسی همگانی به اطلاعات سیستم به معنای امکان ایجاد تغییر در آن ها نیست.

بلاکچین پیوند و ارتباطی بین چندین بلوک (بلاک) است. هر بلوک بسته به محتوایی که دارد، کدی تولید میکند که دربلوک بعدی با اطلاعات جدید دیگری ذخیره میشود. بلوک ها اسناد کامپیوتری هستند که داده های متعلق به شبکه را به صورت دائمی در خود ثبت میکنند. یک بلوک، تعدادی یا کل سوابق تراکنش های شبکه در یک بازه زمانی که در بلوک های قبلی وارد شده است را ثبت میکند، بنابراین یک بلوک مانند صفحه ای از یک دفتر کل یا دفتر ثبت اسناد است. هر بار که یک بلوک کامل میشود، ساخت بلوک بعدی در زنجیره بلوکی آغاز میشود. هر بلوک ذره ای از بلوک های قبلی و آدرس بلوک بعدی را در خود قرار میدهد تا امکان دستکاری بلوک ها یا حذف یک بلوک وجود نداشته باشد. بنابراین یک بلوک، مخزن دائمی اسنادی است که یکبار ثبت شده اند و دیگر قابل تغییر یا حذف شدن نیست. شبکه ارزهای دیجیتال شاهد حجم زیادی از تراکنش هاست. نگهداری سابقه این تراکنش ها به کاربران کمک میکند تا مقدار ارز دیجیتال موجود در هر آدرس را مورد محاسبه قرار داده و جابجایی ارزها بین آدرس های مختلف را مشاهده کنند.(سید حسینی و دعایی ، ۱۳۹۳)

این شبکه، شبکه غیرمترکزی است که بسیاری از ارزهای دیجیتال براساس این تکنولوژی هستند.منظور از شبکه غیر متمرکز این است که داده ها و اطلاعات روی یک سیستم یا کامپیوتر ذخیره نمیشوند بلکه به صورت همزمان روی ملیون ها کامپیوتر ذخیره میشود.به همین دلیل بلاکچین تغییرناپذیر است و اگر اطلاعاتی در بلاکچین تأیید شود تغییر آن غیرممکن است مگر اینکه کسی بتواند اطلاعات تمام کامپیوترهایی که بلاکچین روی آن ذخیره شده تغییر بدهد. به بیان دیگر، بلاک چین یک دفتر کل است، مشابه یک صفحه اکسل که ورودیهایش از تعداد زیادی از افراد مختلف دریافت میشوند. این دفتر کل تنها در صورتی تغییر میکند که کل گروه در خصوص تغییر اجماع نظر داشته باشند. این پایگاه داده نگهدارنده رکوردهای اطلاعات تراکنشهاست و بهطور مستمر در حال رشد است. سرورها یا نودها، نگهدارنده کل دادهها (بلاکها) هستند و هر نود داده های تراکنشهای ذخیره شده در بلاک ها را میبینند. (بهاری و احمدی جشفقانی به نقل از صالحی ، ۱۳۹۷)

ویژگی دیگر بلاکچین شفافیت است. بدین معنا که تمام تراکنش ها در بلاکچین قابل ردیابی هستند.البته این به معنی دسترسی کامل افرار به اطلاعات یکدیگر نیست،بلکه میتوانند اطلاعات قابل دسترس و عمومی را مشاهده کنند و حریم خصوصی افراد در پشت نام های مستعار پنهان خواهد ماند.

در نهایت مهمترین ویژگی و تهدید سیستم بلاکچین برای سیستم های بانکی رایج، سرعت انجام و هزینه تراکنش ها است. در حالی که انجام هر تراکنش (برحسب مقدار آن) نیازمند صرف یک یا چندروز زمان و پزداخت مبلغ کارمزد تراکنش است، مبادلات با سیستم بلاکچین میتواند در عرض چندثانیه و حتی به صورت آنی و بدون پرداخت کارمزد صورت بگیرد. همچنین تراکنش های بلاکچین نیاز به هیچ واسطه ای نیز ندارند.

بلاکچین دارای انواع مختلف است:

۱.بلاکچین عمومی: پر کاربردترین نوع بلاکچین است که همه میتوانند به اطلاعات آن دسترسی داشته باشند.

۲. بلاکچین کنسرسیومی(ائتلافی): این نوع بلاکچین توسط چند شرکت یا سازمان تشکیل میشود، در نتیجه تنها اعضای ائتلاف به اطلاعات آن دسترسی دارند و از سرعت پردازش بالاتری نسبت به نوع عمومی برخوردارند.

۳. بلاکچین خصوصی: این نوع بلاکچین توسط فرد یا افرادی ایجاد میشوند و آن ها تصمیم میگیرند که چه کسانی به اطلاعات دسترسی داشته باشند و از بالاترین سرعت در پردازش اطلاعات نسبت به دو نوع دیگر بلاکچین برخوردارند.(نیوفیند و کاسپرچیک، ۱۳۹۸)

۱,۱.اصطلاحات کلیدی :

هش(Hash): یک رشته متنی که با استفاده از یک تابع خاص تولید شده و برای جلوگیری از تقلب در سیستم بلاکچین کاربرد دارد.در اصل توابع هش نوعی تبدیل هستند که رشتهای طولانی را به عنوان ورودی دریافت میکنند و رشتهای با طول ثابت را به عنوان خروجی نمایش میدهند. مقدار هش حاصل، نمایشی از کل محتوای متن یا رشته ورودی است و میتوان آن را به نوعی (اثر انگشت دیجیتالی) برای آن متن به حساب آورد که همیشه ثابت است و از تغییر اطلاعات ثبت شده و تقلب در بلاکچین جلوگیری میکند.

استخراج کننده(Miner) : افرادی که از یک سخت افزار بهره میبرند تا یک تابع هش را حل کنند و در ازای آن پاداش(ارز) دریافت میکند.

نود (Node) : نود ها یا گره ها شامل تمام سیستم های کامپیوتری میشوند که به سیستم بلاکچین متصل هستند،پیرو دستورالعمل های شبکه هستند و وظایف ۳ گانه تطبیق ترانش با قوانین شبکه، اشتراک اطلاعات شبکه و ذخیره اطلاعات شبکه را بر عهده دارند.

کیف پول(Wallet): افرادی که به استخراج بیت کوین میپردازند برای نگهداری آن ها نیاز به ابزاری به نام کیف پول دارند. در اصل کیف پول در دنیای ارز های دیجیتال مشابه حساب های بانکی هستند که پول در آن حفظ میشود با این تفاوت که هیچکس جز دارنده کیف پول به اطلاعات آن دسترسی ندارد.در ادامه به شناخت انواع کیف پول خواهیم پرداخت.

۱. کیف پول دسکتاپ: این کیف پول ها برای دانلود و استفاده در لپ تاپ ها و رایانه های شخصی طراحی شده اند. آنها حتی وقتی که کامپیوتربه اینترنت متصل نیست، قابل دسترسی هستند.
۲. کیف پول های آنلاین وب: این خدمات توسط شرکت های خدمات کیف پول شخص ثالث در سرویس های ابری ارائه می شود. دسترسی به این کیف پول، تنها از طریق اتصال به اینترنت امکان پذیر است
۳. کیف پول های موبایل: کیف پول های Mycelium وBlockchain هر دوبرای پلتفرم های اندروید و IOS در دسترس هستند.
۴. کیف پول های فیزیکی: با کیف های کاغذی می توانید بیت کوین های خود را به طور مداوم به صورت سرد (آفلاین) نگهداری کنید. شما می توانید این نوع کیف پول ها را در گاو صندوق خود مانند دیگر ارزهای سنتی محافظت کنید.
۵. کلاینت های بیت کوین: این کیف پول ها در کامپیوتر هایی که نصب می شوند مستقیما به شبکه بلاک چین متصل می شوند و وظیفه ارسال و دریافت و حفاظت از ارز دیجیتال را بر عهده دارند.این نوع کیف پول از اصلی ترین انواع کیف پول هستند که پیشگامان حوزه ارزهای دیجیتال از آن بهره میبرند.
۶. کیف پول های سخت افزاری: آنها دستگاه های فوق العاده کوچکی هستند که ارز ها را به صورت آفلاین و با امنیت فوق العاده بالا ذخیره می کنند و می توانید از آن ها برای انجام تراکنش ها (ارسال و دریافت ارز) استفاده کنید. لازم به ذکر است که برای انجام

تراکنش به صورت خیلی امن به اینترنت متصل می شوند.توسعه دهندگان این دستگاه ها از رمزنگاری های سطح بالا استفاده می کنند و به طور مداوم آن ها را به روز و بررسی می کنند.(شاکری ، ۱۳۹۸)

رمز عمومی(Public key): این رمز را میتوان به شماره حساب تشبیه کرد.شما برای واریز ارز میتوانید آن را در اختیار دیگر افراد قرار دهید.

رمز خصوصی(Private key): این رمز راه دسترسی شما به ارزهای دیجیتال است.باید آن را به صورت امن نگهداری کنید زیرا اگر افراد دیگر به آن دسترسی پیدا کنند میتوانند ارز های شما را کنترل کنند.

توکن(Token): توکن ها اموالی دیجیتالی میباشند که مادی مورد معامله قـــرار میگیرند .میتوانند نماینـــده یک کالای دیجیتالی یا مادی در فضای مجازی بوده و تصاحب آن به منزله، کسب مالکیت کالای مادی یـا غیر مادی یا دارا بودن حقی بر آن باشـد. توکن ها به چهار دسته ۱. توکن های ارزی ۲. توکن های دارایی ۳. توکن های بهره وری و ۴. توکن های عدالتی.(ناصر و رضوی ، ۱۳۹۷)

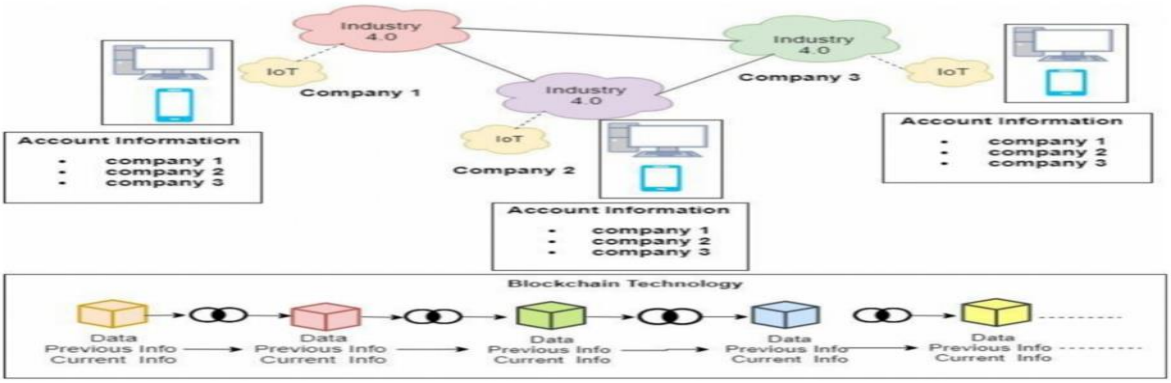
ارزهای دیجیتال دارای ۲ شکل هستند. کوین ها(Coin) که دارای شبکه و بلاکچین مجزا و مستقل هستند، مانند: بیت کوین و اتریوم. شکل دوم توکن ها هستند که سیستم بلاکچین مستقل ندارند و در بستر ارزهای دیگر گسترش میابند.

۱,۲. چگونگی استخراج(Mining) در بلاکچین:

فرایند استخراج،یک فرایند داوطلبانه است که در آن ماینرها به کمک دستگاه هایی که در اختیار دارند تایید و حفظ امنیت سیستم میکنند و در ازای آن پاداش دریافت میکند.

انگونه که پیش تر بیان شد، سیستم بلاکچین از پیوند چندین بلوک(بلاک) بوجود آمده که یک مسئله ریاضی به هریک از بلوک ها پیوند زده شده است. استخراج گرانی وجود دارند که مدام در حال رقابت بر سر پردازش و ثبت تراکنش های شبکه هستند. آنها تلاش میکنند که سریعتر از بقیه، بلوک حال حاضر را تکمیل کنند تا به ازای آن، هم کارمزد معاملات را دریافت کنند و هم ارز از شبکه پاداش بگیرند. زمان ی که استخراج گر، بلوکی را تکمیل کند، برنده به حساب می آید و اقدام به حل مسائل میکند. جواب مسئل بین گره های استخراج (نودها) به اشتراک گذاشته میشود و سپس تأیید اعتبار میشود. هر بار که یک استخراج گر یک مسئله را حل کند، ارز دیجیتال جایزه دریافت می کند می تواند آن را در چرخه شبکه خرج کند. اولین مدرک ثبت شده در بلوک بعد ی تراکنش مربوط به جا یزه ای است که استخراج گر برنده بلوک قبلی دریافت کرده است. مسائل ریاضی به نحو ی است که درجه سختی آن نسبت به زمان تعیین می شود، یعنی

P. M., A. Sharma and V. V. et al. / Computers and Electrical Engineering 81 (2020) 106527



سیستم بلاکچین

درنهایت مسائل حل میشود ولی میزان محاسبات آن به صورتی تنظیم می شود که با توجه به توان محاسباتی متوسط سخت افزار کامپیوترهای مورداستفاده توسط استخراج گرها کمتر از مدت مشخصی طول نکشد. درواقع سطح دشواری مسئله ر یاضی که باید توسط استخراج گر برنده در پایان تکمیل هر بلوک حل شود، نرخ تولید ارزجدید در شبکه را تنظیم می کند.(سید حسینی و دعایی، ۱۳۹۳)

محاسباتی که برای هربلاک لازم است به مرور افزایش میابد که به آن سختی تولید(Difficulty) میگویند. هر ۴ سال یکبار سختی تولید ۲ برابر شود یا به عبارت بهتر به ازای پردازش برابر، تولید به نصف کاهش یابد. بر این اساس میتوان سه دوره برای استخراج یک ارز تعریف کرد:

۱) **دوران طلایی:** ابتدای ورود یک ارز به بازار است به دلیل میزان کم هش ریت شبکه، سختی تولیدپایین است و میزان تولید ماینرها بالاست.البته قیمت تجهیزات تولید نیز در این دوره بالاست.

۲) دوره افزایش سختی: در این دوره با هجوم ماینرها و سرمایه گذاری بر روی استخراج آن ارز میزان سختی آن با شیبی تند افزایش میابد.(شاکری، ۱۳۹۸)

۳) دوره ثبات: در این دوره با توجه به هزینه مصرف برق و نگهداری تجهیزات و استخراج یک نقطه ثبات و پایدار برای استخراج ارز به دست میاید که معمولاً پایدار میماند. استخراج بیت کوین اکنون در این مرحله قرار دارد. در این دوره تجهیزات ماینینگ ارزان شده اند و در آمد نیز نسبتاً ثابت است.

۲.بیتکوین

مزیت های فراوان رمز ارزها (مانند کاهش هزینه و زمان تراکنشهای مالی، افزایش کارایی و افزایش شفافیت) از یک سو و تهدیدات و مخاطرات آن (مانند تأثیر منفی بر شاخصهای اقتصادی همچون سرعت گردش نقدینگی و نیز ایجاد بسترهای مساعد برای جرائم مالی و پولشویی) از سوی دیگر موجب شده است که دولت ها و بانک های مرکزی جهان به فکر نظم بخشی مجدد به اکوسیستم مالی با در نظر گرفتن این بازیگران وپدیده های جدید باشند. ماهیت ویژه رمز ارزها قانونگذاران را با چالش هایی مواجه ساخته است، چرا که ضمن حفظ منافع ملی کشورها و محافظت از اقتصاد کشور در برابر تهدیدها، باید عرصه برای استفاده از فرصتهای آن تا حد امکان باز باشد. هدف از تدوین مقررات در حوزه رمز ارزها، کاهش تقلب، جلوگیری از پولشویی، حفاظت از مشتریان و کاهش ریسک بازیگران و ذینفعان آن است.(بهاری بندری و احمدی جشفقانی ، ۱۳۹۷)

بیتکوین یک شبکه غیرمتمرکز و رمز ارز است که از یک سیستم فردبه فرد و رمزگذاری شده برای تأیید و انجام تراکنشها به جای اعتماد به یک نهاد واسط استفاده میکند. با اختراع بیتکوین برای اولین بار، پرداخت ها بدون دخالت و هزینه نهاد مرکزی صورت پذیرفت.

در سال ۲۰۰۸ میلادی شخصی به نام سیتوشی ناکاموتو مقاله ای را تحت عنوان یک سیستم پول اینترنتی به نام بیت کوین روی اینترنت قرار داد که سیستمی برای معاملات الکترونیکی بود.(شاکری، ۱۳۹۸) وی قصد داشت ارز دیجیتالی تهیه کند که وابسته به تئوری ها و محاسبات ریاضی باشد، نه به اقتصادها و بازارهای پر نوسان. در۱۸ آگوست ۲۰۰۸ سایت Bitcoin.org متولد شد. این سایت امکان خرید بیتکوین را برای کاربران خود فراهم میکرد.

در سال ۲۰۰۹ اولین سکه بیت کوین با تکیه به نرم افزار آن توسط ناکاموتو استخراج شد.اولین تراکنش در بلوک ۱۷۰ بین ساتوشی و هال فاینی، فعال و توسعه‌دهنده ارزهای رمزنگاری، در ۱۲ ژانویه ۲۰۰۹ انجام شد.در ۱۵ اکتبر همان سال هر یک دلار را معادل 1.309 بیت‌کوین ارزش گذاری میشود. در همین سال شخصی به نام john papa برای خرید دو عدد پیتزا تعداد ۱۰۰۰۰ بیت کوین پرداخت کرد.(شاکری، ۱۳۹۸)

در سال ۲۰۱۰ در پروتکل بیت کوین مشکل مهمی پیدا شد و آن ورود معاملات به سیستم بلاک چین بدون اینکه به درستی تایید شود بود. در ۱۵ اگوست به دلیل این مشکل در یک معامله بیش از ۱۱۴ میلیارد بیت کوین تولید شد و به ۲ آدرس ارسال شد.(شاکری، ۱۳۹۸) این تنها ایراد و مشکل در سیستم بلاک چین بود که در عرض چند ساعت رفع و معامله انتقال آن کشف و از سیستم پاک سازی شد. همچنین در ۱۸ آگوست ۲۰۱۰ یک شرکت استارتاپی ایده ای را مطرح کرد که به چندین کاربر این امکان را می‌داد تا به‌صورت دسته‌جمعی بیت‌کوین کاوی کنند ودرسودهایشان با یکدیگر شریک بودند. (Bitcoin Pooled Mining) اولین تراکنش موبایل به موبایل بیت کوین در تاریخ ۸ دسامبر همین سال اتفاق افتاد.

در سال ۲۰۱۱، سایت آنلاینی به نامSilk Road ، بازار سیاه و غیرقانونی تبادل بیت‌کوین برای دارو راه‌اندازی کرد و نام آن را eBay for Drugsگذاشت . در ۲۷ مارس ۲۰۱۱ اولین صرافی بیت‌کوین در انگلستان به نام Bitcoin راه‌اندازی شد و همچنین در ۵ آوریل همان سال، BitMarket.eu که نخستین بازار برای تبادل بیت‌کوین با واحدهای پولی زلوتی لهستان، یورو و برخی دیگر از ارزها بود افتتاح شد.

در سال ۲۰۱۲ طبق گزارش بیت پی (bit pay) نزدیک به ۱۰۰۰ بازرگان پرداخت توسط بیت کوین را پذیرفتند. در همان سال، سازمان FBI گزارشی با عنوان ارز مجازی بیت‌کوین منتشر شد و در آن گزارش عنوان کرد که چالش‌های بسیاری برای جلوگیری از فعالیت‌های غیرقانونی وجود دارد و همین موضوع باعث این نگرانی شد که روش‌های پرداخت با بیت‌کوین می‌تواند به‌راحتی در خریدوفروش‌های غیرقانونی مورد استفاده قرار گیرد.

در اکتبر سال۲۰۱۳ ، FBI چیزی حدود 80000 بیت کوین را از سایتroad silk کشف و ضبط کرد و صاحب این سایت را بازداشت کرد. شرکت هایrobocoin وbitcoiniacs دراین سال دستگاه های خودپرداز بیت کوین را در کانادا راه اندازی کردند .در نوامبر این سال دانشگاه نیکوزیا برای پرداخت شهریه دانشجو ها از بیت کوین استفاده نمود. همچنین در ابتدای سال ۲۰۱۳ سرمایه بازار به یک ملیون دلار رسید و در اواخر این سال، بیت‌کوین رکورد جدیدی زد و به قیمت 1242 دلار رسید. هم‌چنین در این زمان، میزان تراکنش‌های انجام‌شده توسط بیت‌کوین از میزان تراکنش‌های انجام‌شده توسط وسترن یونیون بیشتر شده بود.

در سال۲۰۱۵ میزان سرمایه گذاری بیت کوین به بالاترین رقم رسید ودر میان دیگر ارز های دیجیتال رتبه اول را کسب کرد (۱۱۶ میلیون دلار آمریکا). همچنین در این سال حدود ۱۶۰۰۰۰ تاجر پرداخت با بیت کوین را پذیرفتند(شاکری، ۱۳۹۸) . استارت‌آپ 21 Inc اعلام کرد توانسته 116 میلیون دلار جذب سرمایه داشته باشد که این مبلغ، بیشترین مقداری است که یک شرکت مرتبط با ارزهای دیجیتالی توانسته به دست آورد.

در سال۲۰۱۶ ژاپن ارز های مجازی مشابه بیت کوین را به رسمیت شناخت. همچنین افریقای جنوبی بازار انلاین پرداخت بیت کوین را برای خریداران و فروشندگان راه اندازی نمود. در این سال دستگاه های خود پرداز بیت کوین دو برابر شد و به تعداد 770 دستگاه در سراسر جهان رسید.

بیتکوین موضوع پیچیدهای است که رمزنگاری و مهندسی نرم افزار و اقتصاد را درهم می آمیزد و پوشش میدهد. بیتکوین ارزی دیجیتالی و غیرمتمرکز است. مخترع بیتکوین حتی در زمان انتشارش مجهول بوده و فقط نام مستعار او دردسترس است. با این وجود، ممکن است ارزهای دیجیتال موضوعی ضدشهودی و غیرعقلانی به نظر برسند. مخترع این ارز سرسخت نیز قادر به کنترل آن نبوده و ازآنجا که کد آن از انواع کد باز است، مالکیت این ارز را مالکیت عمومی تلقی میکنند.(رحیمی و شریفیان به نقل از اخوان، ۱۳۹۸)

هر بیت کوین تا هشت رقم قابلیت ریز شدن دارد که به ریزترین واحد، ساتوشی اطالق میشود. البته بر اساس نیاز و توافق استخراج گران این واحد میتوان ریزتر بشود. از چهار طریق میتوان بیت کوین بدست آورد:

۱. فروش کالا و خدمات بر اساس بیت کوین

۲. خرید بیت کوین از صرافیهای بیت کوین

۳. خرید بیت کوین از افرادی که بیت کوین دارند

۴ .جایزه گرفتن بیت کوین از طریق فرآیند رقابتی استخراج تولید بیت کوین(میرحسینی و دعایی، ۱۳۹۳)

بیتکوین هایی که به عنوان پاداش به ماینر برنده داده میشود حدوداً هر چهار سال نصف میشود تا اینکه این تعداد به صفر میرسد. یکی از تفاوت های اصلی بیتکوین (پول های دیجیتال) با پول بانکی بدون پشتوانه خاصیت ضد تورمی آن است. راه تولید بیتکوین های جدید توسط کد منبع بیتکوین برنامه نویسی شده است. حداکثر تعداد بیتکوین های صادرشده حدود ۲۱ میلیون خواهد بود. این عرضه پولی ثابت، خاصیت ضد تورمی خواهد داشت. مدل ضد تورمی برای اینکه بتواند ویژگی نایاب بودن را به بیتکوین اعطا کند تا آن ارزشمند شود، به عنوان یک ضرورت انتخاب شده است تا اینکه یک ویژگی از آن باشد.

بیتکوین های جدید در یک برنامه زمانبندی ضرب میشوند و به کاربرانی که به امنیت شبکه کمک میکنند پرداخت میشود. این شیوه از طراحی در باطن دو سیاست بسیار ارزشمند دارد؛ اول، برای بیتکوین ها در عین نبود ارزش ارزشی پدید می آید. دوم، ایجاد انگیزه برای کاربران متصل به شبکه تا دراختیارگذاشتن قدرت محاسباتی رایانه خود به امنیت شبکه کمک شایانی کنند. (Nakamoto ,2008)

اتریوم:

در اصل اتریوم یک پلتفرم محسوب میشود که در آن امکان فعالیت های مالی آزاد و غیر متمرکز وجود دارد. بطور کلی متوان اینگونه بیان کرد که اتریوم یک زیر ساخت بر اساس سیستم بلاکچین می باشد که امکان اجرای برنامه های کامپیوتری غیر متمرکز را دارد و برخی اتریوم را با نام " قرارداد هوشمند " نیز می شناسند.

یک قرارداد عادی، توافقی بین دو یا چند شخص است که آنها را به چیزی در آینده متعهد می‌کند و آنچه که باعث تفاوت قرارداد معمولی و قرارداد هوشمند می‌شود این است که درقراردادهای هوشمند کدهای کامپیوتری مشکل نیاز به اعتماد را برطرف می‌کنند. زمانی‌که یک قرارداد هوشمند بر روی یک بلاک چین آزاد مثل اتریوم اجرا شود، دیگرقابل‌توقف نیست وهیچ‌کس نمی‌تواند جلوی اجرای آن را بگیرد. با قراردادهای هوشمند می‌توان برنامه‌ها و پروژه‌هایی را ساخت که بدون هیچ‌گونه واسطه و از کارافتادگی به کار خود ادامه دهند، به‌طوری که حتی برنامه‌نویس قرارداد هوشمند هم نمی‌تواند کد قرارداد هوشمند ثبت‌شده در بلاک چین را تغییر دهد. (Buterin, 2014)

ایده شبکه اتریوم در اواخر سال ۲۰۱۳ توسط "ویتالیک بوترین" مطرح شد. این طرح بواسطه استارتاپ نرم افزاری که پدر وی در سال ۲۰۱۳ برگزار کرد، به ذهن ویتالیک خطور کرد و در اواخر ۲۰۱۳ ایده هایش را در غالب وایت پیپر به دوستانش معرفی کرد.

طبق گفته ویتالیک بوترین، قراردادهای هوشمند میتوانند برای کدگذاری، غیرمتمرکز و امن سازی و معاملات تقریبا هرچیزی به کار برده شوند: رأی گیری، دامنه های اینترنتی، مبادلات مالی، تامین مالی جمعی، اداره شرکت، تنظیم و پیشبرد انواع قراردادها و توافق ها، دارایی های مالکیت معنوی و ... . بنابراین میتوان هزاران کاربرد برای اتریوم و تکنولوژی قراردادهای هوشمند آن متصور شد. (Buterin, 2014)

سال ۲۰۱۴ شبکه اتریوم به صورت عمومی اعلام شد، عرضه اولیه اتریوم پایان یافت و سرمایه ای معادل ۱۸,۴ میلیون دلار برای آن به ارمغان آورد. در همین سال توسعه دهنده این شبکه به همراه باقی همکاران خود در دفتر اصلی که در کشور سوئیس بنا شده است کار خود را آغاز کردند. این شبکه دارای چندین فرد اصلی بود که به عنوان توسعه دهنده فعالیت می کردند. این افراد عبارت اند از:

ویتالیک بوترین(Vitalik Buterin)

میهای آلیسی(Mihai Alisie)

آنتونی دی‌لوریو(Anthony Di Iorio)

گاوین وود(Gavin Wood)

جوزف لوبین(Joe Lubin) (arzdigital.com)

در سال ۲۰۱۵ بنیاد اتریوم چندین نمونه آزمایشی از پلتفرم اتریوم را آزمایش کرد و در انتها نسخه آزمایشی اتریوم، " Olympic " نیز منتشر شد .در این سال اولین مرحله از توسعه شبکه اتریوم که " Frontier " نام داشت نیز منتشر شد. به طور کلی روند توسعه اتریوم به چهار مرحله تقسیم شد. این کار باعث شد تا توسعه دهندگان بتوانند شرایط خود را با آن وفق دهند. در این نسخه اتریوم امکان خرید و فروش برای کابران فراهم شد و همچنین کاربران می توانستند آن را استخراج کنند و یا اینکه قرار دادهای هوشمند و همچنین برنامه های غیر متمرکز بسازند.

اوایل سال ۲۰۱۶، اولین نسخه پایدار اتریوم با نام هوم اِستید (Homestead) با ۱۱۵۰۰۰۰ بلوک عرضه شد، ولی چند ماه بعد هک "DAO" اتفاق افتاد. این حمله و عواقبش به حدی بزرگ بود که توسعه‌دهندگان آن مجبور شدند به‌منظور دفع و پیشگیری از حملات مشابه، این ارز دیجیتالی را دوباره بسازند، پس در اواخر سال اتریوم فورک منتشر شد . ارز اتری که در حال حاضر در رتبه دوم مارکت است، روی همین زنجیره است و اتریوم پیشین با نام اتریوم کلاسیک شناخته میشود.

اپلیکیشن DAO ابتدا یک توکن یا صندوق سرمایه گذاری برای جذب سرمایه برای برنامه های غیرمتمرکز بود که اتریوم دریافت و در ازای این اتریوم ها توکن DAO به سرمایه گذاران میپرداخت. (peyrott , 2017) DAO ظرف کمتر از یک ماه چیزی حدود ۱۵۰ میلیون دلار اتریوم جذب کرد و در ۱۷ ژوئن ۲۰۱۶، یک هکر از شکافی که در این سیستم برای خروج وجود داشت استفاده کرد و حدود یک سوم سرمایه DAO (مبلغی بالغ بر ۵۰ ملیون دلار) از دست رفت. بسیاری این هک را بخاطر مشکلات اتریوم دانسته و این اتفاق باعث خدشه دار شدن اعتبار پلتفرم اتریوم شد به حدی که قیمت اتریوم از ۲۰ دلار به ۱۲ دلار رسید ولی توسعه دهندگان این شبکه چنین فکر نمیکردند و «گاوین وود»، از بنیان‌گذاران اتریوم در اظهارنظری اعلام کرد: «مثل این است که بگوییم هرگاه وب‌سایتی از دسترس خارج می‌شود، باید بگوییم تمام اینترنت خراب‌شده است!».

تیم اتریوم برای این که اعتبار شبکه را برگردانند، تصمیم به اجرای یک هاردفورک گرفتند. هاردفورک، روی یک بلاک قبل از هک انجام شد تا اتریوم های سرقت شده برگردد که باعث به وجود آمدن زنجیره جدید اتریوم شد.

فورک ها در اصل به معنی ایجاد انشعاب و شبکه جدید از دل یک شبکه هستند وبا تغییراتی در شبکه بلاکچین ارز دیجیتال، ایجاد می شوند. در هارد فورک که در شبکه اتریوم اتفاق افتاد، بلاک های شبکه شکسته شده به دو بلاک جداگانه تبدیل می شوند که در نهایت سبب ایجاد یک ارز جدید در دنیای ارزهای رمز پایه می شوند. به عبارت دیگر، طی فرایند هارد فورک، تغییرات اساسی در شبکه بلاک چین ارز ایجاد می شود که این تغییرات را شبکه قبلی نمی تواند پشتیبانی کند. در نتیجه برای حمایت از این تغییرات، نیاز است که یک ارز جدید در همان شبکه ایجاد شود که تغییرات جدید را بتواند پشتیبانی کند. (peyrott , 2017)

اتریوم یک دفتر توزیع شده متن باز با بستر تورینگ کامل بوده و میتواند برای ایجاد و توزیع کاربردهای غیرمتمرکز مورد استفاده قرار گیرد. طبیعت تورینگ کامل بودن اتریوم روند تولید برنامه های کاربردی زنجیره بلوکی را بسیار راحتتر و کارآمدتر از قبل کرده است. به جای آنکه لازم باشد تا برای هر برنامه یا هر کاربرد جدید یک زنجیره بلوک کاملاً جدید ساخته شود، اتریوم این امکان را فراهم کرده تا بتوان تنها روی یک بستر، هزاران برنامه مختلف را توسعه داد. به عبارتی قراردادها در اتریوم شبیه عوامل خودمختاری هستند که در زنجیره بلوکی اجرا میشوند .حامیان اتریوم بر این باورند که یک زبان تورینگ کامل به توسعه بسیاری از برنامه های ابتکاری مالی و غیرمالی، در همان راهی منجر خواهد شد که معرفی جاوا اسکریپت به توسعه برنامه های کاربردی نوآورانه تحت وب منجر شده است.(, Buterin ۲۰۱۴)

هدف اتریوم ادغام و بهبود مفاهیم کد نویسی، آلتکوین ها و پروتکل های زنجیره ای است و به توسعه دهندگان اجازه میدهد برنامه های مبتنی بر اجماع دلخواه را ایجاد کنند که دارای مقیاس پذیری، استاندارد سازی، کامل بودن، سهولت توسعه و قابلیت همکاری به صورت همزمان هستند و زبان برنامه نویسی تورینگ کامل در اتریوم، به همه این امکان را میدهد که قراردادهای هوشمند و برنامه های غیرمتمرکز بنویسند. (Buterin , ۲۰۱۴)

بلاک چین اتریوم اساسا یک ماشین حالت (**state machine**) مبتنی بر تراکنش است. در ابتدا بلاکچین در حالت صفر(genesis state) مانند لوح سفیدی است هنوز هیچ تراکنشی در شبکه انجام نگرفته است. هر تراکنش‌که انجام می‌شوند، حالت جنسیس به حالت‌های بعدی انتقال می‌یابد. در هر نقطه‌ای از زمان، آخرین حالت، نشان‌دهنده حالت فعلی اتریوم است. هر حالت اتریوم میلیون‌ها تراکنش دارد. این تراکنش‌ها در «بلاک‌ها» دسته‌بندی می‌شوند. یک بلاک حاوی یک سری از تراکنش‌هاست و هر بلاک با بلاک قبلی به‌شکل زنجیره به هم متصل‌اند. (2017, Wood)

برای گذر از یک حالت به حالت بعدی، تراکنش باید معتبر باشد. برای اینکه اعتبار یک تراکنش مشخص شود، باید فرایند استخراج (ماینینگ) صورت بگیرد. هر نود در شبکه که خودش را به‌عنوان یک ماینر اعلام می‌کند، می‌تواند یک بلاک را ایجاد و اعتبارسنجی کند. هر ماینر یک «گواه یا اثبات» ریاضی را در هنگام ارسال یک بلاک به بلاک چین ارائه می‌کند و این گواه به‌عنوان یک ضمانت عمل می‌کند: اگر گواه وجود دارد پس بلاک باید معتبر باشد. برای اضافه شدن یک بلاک به بلاک چین اصلی، یک ماینر باید سریع‌تر از همه ماینرهای رقیب آن را اثبات کند. فرایند اعتبارسنجی هر بلاک که یک ماینر برای آن گواه یا اثبات ریاضی را ارائه می‌کند به "اثبات کار" (proof of work)معروف است. (2017, Wood)

در روش "اثبات سهام"، افراد برای مشارکت در کار اعتبارسنجی تراکنش‌ها و ایجاد بلاک، باید اتر بخرند و در یک کیف پول به شبکه اختصاص دهند. به این ترتیب، می‌توانند در کار تأیید تراکنش‌ها مشارکت کنند و واحدهای جدید ارز دیجیتال (اتر) دریافت کنند. مشارکت‌کنندگان کارمزد تراکنش‌های شبکه را برای خود برمی‌دارند. طبق این رویکرد، برای مشارکت در شبکه دیگر نیاز به خرید سخت‌افزارهای گران‌قیمت نیست.

شبکه جهانی اتریوم از تعداد بسیار زیادی جزء کوچک به نام «حساب» ساخته شده است که قادرند از طریق یک چارچوب انتقال پیام با یکدیگر تعامل برقرار کنند. هر حساب دارای حالت مخصوص به خودش و یک آدرس 20 بایتی است. آدرس در اتریوم یک شناسه 160 بیتی است که برای شناسایی حساب از آن استفاده می‌شود. دو نوع حساب وجود دارد:

۱.حساب‌های با مالکیت خارجی، که با کلیدهای خصوصی مدیریت می‌شوند و هیچ کد مخصوصی ندارند. یک حساب با مالکیت خارجی می‌تواند با استفاده از کلید خصوصی‌اش یک تراکنش انجام دهد، امضا کند و از این طریق پیامی به حساب با مالکیت خارجی یا حساب مبتنی بر قرارداد دیگری ارسال کند.

۲.حساب‌های مبتنی بر قرارداد(پیمان) که با کد قراردادشان مدیریت می‌شوند و حاوی کد مرتبط با آنها هستند.هر بار که پیامی برای یک حساب مبتنی بر پیمان ارسال میشود،کد آن فعال میشود و به وی این امکان را میدهد تا انتقال توکن‌ها، نوشتن چیزی روی فضای ذخیره‌سازی داخلی، ایجاد توکن‌های جدید، انجام یک سری محاسبات و ایجاد قراردادهای جدید را انجام دهد.(Buterin, 2014)

حساب‌های مبتنی برپیمان نمی‌توانند خودشان تراکنش‌های جدید را وارد کنند و به اصطلاح آغازکننده باشند. این حساب‌ها فقط می‌توانند تراکنش‌ها را در پاسخ به تراکنش‌های دیگری که دریافت می‌کنند (از حساب‌های با مالکیت خارجی یا حساب‌های مبتنی بر قرارداد دیگر) ارسال کنند.

یک حساب اتریوم شامل ۴ قسمت است:

۱. نانس(nonce): اگر یک حساب از نوع مالکیت خارجی باشد، این عدد نشان‌دهنده تعداد تراکنش‌های ارسال‌شده از آدرس آن حساب است. اگر این حساب مبتنی بر قرارداد باشد، نانس تعداد قراردادهای ایجاد شده توسط این حساب را نشان خواهد داد.
۲. کد قرارداد حساب (در صورت وجود): مربوط به حساب های مبتنی بر پیمان است.
۳. موجودی حساب: مقدار اتر ذخیره شده در هر حساب است.
۴. فضای ذخیره سازی حساب: محتویات ذخیره‌شده در حساب را رمزگذاری می‌کند و مقدار آن به طور پیش‌فرض خالی است. (Buterin, 2014)

در بلاک چین اتریوم دو نوع تراکنش وجود دارد: تراکنش برای فراخوانی پیام (message calls) و تراکنش برای ایجاد قرارداد (یعنی تراکنش‌هایی که قراردادهای جدید اتریوم را ایجاد می‌کنند). تراکنش‌ها (هر دو نوع آن) همیشه از سوی حساب‌های با مالکیت خارجی آغاز و به بلاک چین فرستاده می‌شوند و قراردادهای روی اتریوم می‌توانند با یکدیگر به شکل داخلی، از طریق «پیام‌ها» یا «تراکنش‌های داخلی» مذاکره کنند. پیام ها مشابه تراکنش ها در با این تفاوت که توسط قراردادها ایجاد می‌شوند و برخلاف تراکنش‌های خارجی به‌شکل سری مرتب نمی‌شوند و فقط در محیط اجرایی اتریوم وجود دارند.(wood, 2017)

هر محاسبه‌ای که برای اجرای یک تراکنش در شبکه اتریوم انجام می‌شود هزینه‌ای دارد و این هزینه با سوخت یا گس (Gas) پرداخت می‌شود.هر هزینه شامل ۲ مفهوم است.مفهوم اول،قیمت سوخت (gas price) است که مقدار اتر پرداختی برای هر واحد سوخت است ومفهوم دوم، حد سوخت (gas limit) است که نشان‌دهنده بیشترین مقدار سوختی است که فرستنده می‌خواهد برای اجرای تراکنش خرج کند. کسی که تراکنش را ارسال می‌کند، باید حد سوخت و قیمت سوخت را برای آن تعیین کند. حاصل‌ضرب این دو مقدار، نشان‌دهنده بیشترین مقدار اتر است که فرستنده می‌خواهد برای اجرای این تراکنش بپردازد. اگر این فرستنده در حسابش به اندازه کافی اتر داشته باشد و این مقدار بیشینه را پوشش دهد، همه چیز خوب پیش خواهد رفت. در انتهای تراکنش، سوخت اضافی استفاده‌نشده به فرستنده بازگردانده می‌شود.(wood, 2017) کل مبلغی که فرستنده برای سوخت مصرف می‌کند، به آدرس «ذی‌نفع» فرستاده می‌شود که به طور معمول آدرس یک ماینر است. زیرا این ماینرها هستند که تلاش می‌کنند محاسبات را انجام دهند و تراکنش‌ها را اعتبارسنجی کنند، از این رو به‌عنوان پاداش کارمزد سوخت را برمی‌دارند.

ارز دیجیتال داخلی شبکه اتریوم اتر است که می‌توان آن را با ارزها و دارایی‌های دیگر مبادله کرد. مالکیت اتر دقیقاً مثل مالکیت بیت کوین (BTC) روی بلاک چین رهگیری می‌شود. به اتر «سوخت شبکه اتریوم» هم می‌گویند، چراکه کاربرد اصلی آن کارمزد و انگیزه مشارکت در شبکه است.

آخرین طرح ارائه شده اتریوم، ethereum 2.0 نام دارد. این شبکه برای مقیاس‌پذیری بیشتر (تراکنش‌های سریع‌تر و ارزان‌تر)، به‌جای الگوریتم اثبات کار (Proof Of Work) از الگوریتم اثبات سهام (Proof Of Stake) استفاده می کند. این هاردفورک در ابتدا هاردفورک سرنیتی (Serenity) نام داشت و در سال ۲۰۱۹ به ETH 2.0 تغییر کرد. این پروژه دارای سه فاز است؛ فاز صفر، فاز یک و فاز دو. فاز صفر در سال 2020 اجرا شده است و پیش‌بینی می‌شود اجرای فاز یک و فاز دو حداکثر پنج سال زمان ببرد. با این به‌روزرسانی، اتریوم در نهایت الگوریتم اجماع اثبات کار (ماینینگ) را ترک می‌کند و از اثبات سهام استفاده خواهد کرد. همچنین مقیاس‌پذیری این شبکه (سرعت و کارمزد تراکنش‌ها) تا حد زیادی افزایش خواهد یافت.

شباهت های اتریوم و بیت کوین:

۱.هر دو دارای بلاکچین مستقل هستند(توکن نیستند).

۲.هردو دارای شبکه عمومی هستند و همه میتوانند به آن دسترسی داشته باشند.

۳.مبتنی بر استخراج (ماینینگ) هستند و افرادی که بخواهند در فرایند ساخت بلاک شرکت کنند، باید قدرت پردازش سخت‌افزارهای کامپیوتری را برای شرکت در عملیات استخراج (ماینینگ) به شبکه اختصاص دهند و شبکه در ازای این قدرت پردازش که در نهایت باعث امنیت و تأییدشدن تراکنش‌ها خواهد شد، به استخراج‌کنندگان پاداش اهدا می‌کند.

تفاوت اتریوم و بیت کوین:

۱.تراکنش‌های اتریوم سریع‌تر هستند. در بیت کوین به‌طور میانگین بلاک‌های حاوی تراکنش هر 10 دقیقه یکبار ایجاد می‌شوند، اما در اتریوم این زمان فقط 14 ثانیه است.

۲. بیت کوین حداکثر 7 تراکنش در ثانیه انجام می‌دهد، اما اتریوم می‌تواند تا 16 تراکنش را در ثانیه پردازش کند.

۳. روی بیت کوین هم می‌توان قرارداد هوشمند ایجاد کرد، اما زبان اسکریپت این شبکه بسیار ابتدایی است و کار را برای توسعه‌دهندگان سخت می‌کند. روی اتریوم، خیلی سریع‌تر و راحت‌تر می‌توان کد برنامه‌نویسی پیاده‌سازی کرد.

۴. تفاوت اصلی بیت کوین و اتریوم، تعداد واحدها (عرضه) این دو است. بیت کوین محدودیت عرضه دارد، اما اتر نامحدود عرضه خواهد شد. طبق پروتکل بیت کوین، فقط 21 میلیون واحد از این ارز دیجیتال استخراج می‌شود ولی در مورد اتریوم، هیچ محدودیتی وجود ندارد.

ارزش ذاتی پول های دیجیتال به تعداد کاربران آنها است. بدون داشتن یک اعتماد عمومی سیستم پول های مجازی به عنوان یک روش پرداخت جایگزین پایدار نخواهند بود. در این راستا نکات مثبت و منفی وجود دارد که در این پذیرش عمومی و رشد صنعت تأثیرگذار است. علیرغم افزایش صحبت ها و تبلیغات پولهای رمزی در بازارهای عمومی، همچنان این نوع از پول برای طیف زیادی از افراد ناشناخته هستند .(بهاری بندری و احمدی جشفقانی ، ۱۳۹۷)

پیشبینی های صورت گرفته اتریوم:

۱. ولاف کارلسون وی(Olaf Carlson-Wee) ، مدیر عامل شرکت پلی چین(Polychain) ، دیدگاهی مثبت در خصوص قیمت اتریوم در میان مدت و بلند مدت دارد. وی پیشبینی کرده است اتریوم در سال‌های پیش رو تا 7000 دلار اوج می‌گیرد. به عقیده کارلسون وی، بستر فناوری اتریوم از تمام رقبای بازار جلوتر است و هر چه زمان می‌گذرد مردم بیشتر به قابلیت‌های بالقوه اتریوم در حوزه‌های فناوری و اقتصادی پی خواهند برد.

۲. وایبهاو کادیکا(Vaibhav Kadikar) ، بنیان‌گذار و مدیرعامل کلوزکراس(CloseCross) معتقد است اتریوم بزرگترین بلاک چین با لایه‌ای از قراردادهای هوشمند است، با افزایش پیچیدگی و مقیاس‌پذیری‌اش به احتمال زیاد نرم‌افزارهای بیشتری نیز بر روی آن ایجاد خواهند شد و همین مسئله آن را به حاکم مطلق در این زمینه بدل خواهد کرد. تقاضا برای تراکنش‌های اتریوم بیشتر خواهد شد و این موضوع باعث افزایش قیمت این ارز می‌شود. همچنین او بیان میکند، اتریوم تنها در صورتی با پذیرش گسترده‌تر مواجه می‌شود که کارمزدهای شبکه کاهش یابد و ظرفیت آن 100 برابر شود. اتر سوخت شبکه اتریوم به حساب می‌آید و به همین دلیل استفاده از آن نباید برای کاربران بیش از اندازه گران باشد. از همین رو می‌توان گفت که یک محدودیت ذاتی برای ارزشش وجود دارد. مثلا این طور در نظر بگیرید که اگر قیمت بنزین و گازوئیل بیش از اندازه گران باشد، مردم به سمت استفاده از انرژی الکتریکی سوق پیدا می‌کنند.

۳. پیش‌بینی جف رد (Jeff Reed) یکی از برجسته‌ترین‌ها در نوع خود است. به گفته وی قیمت اتریوم در بلندمدت با جهش همراه خواهد بود، تا جایی که به راحتی بیت کوین را از پیش رو خواهد برداشت. آقای رد، قابلیت‌های بیشتر اکوسیستم اتریوم را دلیلی بر فائق آمدن بر این چالش می‌داند (مقیاس‌پذیری، راحتی استفاده و بخش‌پذیری). به گفته وی، این مسائل باعث می‌شود تا اتریوم در مقایسه با دیگر ارزها جهش بیشتری را تجربه کند. همچنین قراردادهای هوشمند این پلتفرم را دلیل دیگری بر برتری اتریوم می‌داند و آن را «بدیع» توصیف می‌کند. به گفته رد، همین مسئله به تنهایی می‌تواند مهر تاییدی بر برتری اتریوم نسبت به بیت کوین باشد.

۴. شوستر (Brian Schuster) به عنوان بنیان‌گذار شرکت سرمایه‌گذاری آرک(Ark) ، معتقد است که اتریوم نیز مانند بیت کوین در بلند مدت دارای ذخیره ارزش است. به عقیده وی رسیدن ارزش بازار اتریوم به رقم 10 تریلیون دلار دور از ذهن نیست؛ در این صورت هر واحد اتر قیمتی معادل 100000 دلار خواهد داشت. شوستر همچنین می‌افزاید که اتریوم این پتانسیل را دارد تا جایگزین تمام ارزهای دیجیتالی شود که در حال حاضر وجود دارد. به گفته او، اتریوم یکی از معدود پلتفرم‌های غیر متمرکزی است که در مقیاس بزرگ به کار گرفته شده است و می‌تواند از پس مشکلات مقیاس‌پذیری که گریبان بسیاری از بزرگان این صنعت را گرفته است، بر بیاید.

منابع:

۱.نوری، مهدی و نواب پور، علیرضا،(۱۳۹۶) طراحی چارچوب مفهومی سیاستگذاری ارزهای مجازی در اقتصاد ایران ، فصلنامه علمی-پژوهشی سیاستگذاری عمومی، ، دوره ۳ ، شماره ۴ زمستان ۱۳۹۶ ، صفحات ۷۸-۵۱

۲. رحیمی، فتح الله و شریفیان، سحر (۱۳۹۹) موقعیت رمزارزهای دیجیتال در نظام ملی و بین المللـــی، دوفصلنامه حقوق قراردادها و فناوری های نوین، دوره اول، شماره ۱ ،بهار و تابستان ۱۳۹۹ ،صفحه ۱-۲۲

۳. سید حسینی، میرمیثم و دعایی، میثم (۱۳۹۳)بیتکوین، نخستین پول مجازی، ماهنامه بورس، شماره ۱۱۴ و ۱۱۵.

۴. ماروین نیوفیند، مارچین کاسپرچیک. ترجمه ابوالفضل آدرسی و امید خیاط (1398) ارز دیجیتال؛ راهنمای جامع چگونگی دادوستد با بیتکوین ها و آلتکوین ها، نشر نوین توسعه، ۱-۴۰

۵. ناصر، مهدی و رضوی پور، سید محمد حسن (۱۳۹۷) ، تحلیل حقوقی کارکرد قراردادهای هوشمند در نقل و انتقالات دیجیتالی در بازارهای مالی ، فصلنامه پژوهشنامه بازرگانی، شماره ۹۳ ،زمستان ۱۳۹۸ ، ۷۰-۳۳

۶. شاکری ، ابوالقاسم (۱۳۹۸) ارز دیجیتال (Cryptocurrency) ، چاپ نشده

۷. بهاری بندری، بهاره و احمدی جشفقانی، حسین علی (۱۳۹۷) ، ابزار مالی رمزدار ، بررسی مروری ارز رمزی با تکیه بر نیازهای محلی و ابزار جهانی پرداخت ، چاپ نشده

۸. .arzdigital.com

9 . Vitalik Buterin , (2014) Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, {https://github.com/ethereum/wiki/ wiki/White-Paper}

10 . Gavin Wood , (2017), Ethereum: A Secure Decentralised Generalised Transaction Ledgre, EIP-150 Revision (1e18248 - 2017-04-12)

11. Sebastián E. Peyrott , (2017) An Introduction to Ethereum and Smart Contracts