

**دانشکده مهندسی کامپیوتر**

**پایان نامه دوره کارشناسی مهندسی کامپیوتر-نرم افزار**

**پیاده سازی و ایجاد یک ارز رمز جدید مبتنی بر بلاک چین**

**نگارش:**

**حامد محمدی**

**استاد راهنما:**

**دکتر سعید صدیقیان کاشی**

**پاییز 1397**

**چکیده**

# فصل اول : مقدمه

در طول تاریخ بشر همواره ردپای معامله به روش های مختلف دیده شده است، این معاملات در ابتدای تاریخ به صورت مبادله کالا با کالا صورت می­گرفتند که به مرور و با گذر زمان به روش های کارآمد تری نظیر انتخاب یک کالا به عنوان مرجع روی اورده شد، تا اینکه در نهایت با ضرب اولین سکه ها از طلا توسط اقوام باستانی در آسیای صغیر مفهموم پول ایجاد شد.

## تاریخچه مختصری از پول

اولین پول ها توسط قوم باستانی لیدی ها ساکن در منطقه آسیاس صغیر تقریبا در قرن 7 قبل از میلاد ضرب شدند این سکه ها اغلب از جنس فلزات گرانبها مانند طلا ،نقره و یا مس ضرب می­شدند و حاوی مهر حکومت ضرب کننده آنها به همراه تصویر پادشاه و یا اشخاص برجسته آن قوم بودند که به این سکه ها رسمیت و اعتبار می­بخشید رفته رفته دیگر اقوام نیز به ضرب سکه روی آوردند و این گونه بود که دوران سکه ها در تاریخ بشر آغاز شد، به طوری که امروزه نیز در اکثر تحقیقات باستان شناسی از سکه های هر قوم و ملیت به عنوان نماد آن قوم و ملیت یاد شده و دارای اهمیت زیادی می­باشند.

### استاندارد طلا [[1]](#footnote-1)

با گذر زمان و افزایش حجم معاملات تجاری لزوم حمل و نقل مقدار زیادی سکه ایجاد می­شد که حمل این سکه ها دردسر های زیادی را به همراه داشت، بنابر این سازمان هایی به وجود آمدند که در ازای تعداد مشخصی سکه حواله هایی صادر میکردند که در اکثر مناطق دنیای آن زمان با مراجعه به دفتر آن سازمان در هر شهر قابل تبدیل شدن به آن مقدار سکه بودند بنابر این این حواله ها دارای ارزش معادلی به سکه طلا بودند که به مرور زمان در بین مردمان رواج پیدا کردند به طوری که امروز نیز در قوانین اساسی اکثر کشور ها میزان مشخصی از طلا به ازای هر واحد پول آن کشور اختصاص داده می­شود [[2]](#footnote-2) . اما در نهایت با توجه به لزوم وجود نقدینگی در کشور ها و با افزایش جمعیت و برخی عوامل دیگر دولت ها مجبور به چاپ مقادیر پول بیشتر از ذخایر طلای خود شدند که به این ترتیب ارز های بی پشتوانه [[3]](#footnote-3) ایجاد شدند.

### پول بی­پشتوانه

پول بی‌پشتوانه ،پول حکمی، پول دستوری یا پول اعتباری پولی است که ارزشش ذاتی نبوده و تنها ناشی از دستور دولتی یا قانون باشد. نام آن از واژه لاتین فیات به معنی بگذارید انجام شود گرفته شده‌است. بنابر این در این نوع پول به دلیل عدم وجود یک پشتوانه محکم ارز پول معادل ارز چاپ کننده آن در نظر گرفته می­شود و با تغییرات شرایط سیاسی یا اقتصادی یک کشور ارزش پول آن کشور نیز تغییر می­کند. همچنین دولت ها در زمان های کمبود نقدینگی در کشور هایشان با اقدام به چاپ بی رویه این نوع پول باعث ایجاد تورم و کاهش ارزش پول خود می­شوند، مجموع عوامل ذکر شده دلیل تغییراتی است که امروزه در قیمت ارز های کشور های مختلف نسبت به یکدیگر شاهد هستیم؛ لازم به ذکر است که تمامی ارز های مرجع امروزی از نوع پول بی پشتوانه می­باشند.

## تراکنش های مالی و نظام بانکی

با گذر زمان و نیاز به انجام تراکنش های مالی با مبالغ سنگین یا انجام پرداخت در زمان مشخصی در آینده بانک های کشور های مختلف اقدام به ایجاد سازکار های مختلفی نظیر دسته چک ها و یا چک های رمز دار بین بانکی و همچنین انتقال از حساب یک شخص به حساب شخص دیگر نمودند که در نهایت با ورود تکنولوژی های جدید مواردی از قبیل کارت های اعتباری [[4]](#footnote-4) و یا کارت های نقدی [[5]](#footnote-5) امروزه به عنوان یکی از روش های اصلی انجام تراکنش های مالی شناخته می­شوند که این کارتها قابلیت انجام انواع تراکنش های مالی مختلف را با کمک دستگاه هایی نظیر خود پرداز ها [[6]](#footnote-6) و یا پایانه های فروشگاهی [[7]](#footnote-7) فراهم می­آوند همچنین به کمک درگاه های پرداخت اینترنتی قابلیت پرداخت با کمک اینترنت نیز فراهم شده است.

### اشکالات تراکنش های مالی فعلی

اگرچه انجام تراکنش های مالی امروزه به راحتی از طریق کارت هایی نظیر Master Card و یا VISA Card در سطح جهانی انجام می­پذیرند اما این سبک انجام تراکنش دارای اشکالاتی است که در ادامه به معرفی آنها میپردازیم.

1. زمان بين انجام تراكنش و تسويه مي­تواند طوﻻني باشد.
2. دوباره كاريها و نياز به شخص سوم براي تاييد اعتبار و حضور واسطه ها.
3. كلاهبرداري، حمله هاي سايبري و حتي اشتباه هاي كوچك به هزينه و پيچيدگي كسب وكار مي افزايند و اگر يك سامانهي مركزي مانند بانك به خطر بيفتد، همگي مشاركت كنندگان در شبكه با مخاطره روبه رو خواهند شد.
4. برای استفاده از خدمات این کارت های اعتباری اغلب نیاز به پرداخت هزینه های اولیه زیاد می­باشد.
5. دریافت این نوع کارت های شامل فرآیند های وقت گیر و کاغذ بازی ها و بررسی سابقه افراد است.
6. این نوع سامانه ها دارای شفافیت کافی در برخی موارد نمی­باشند، در حقیقت هیچ کس نمی­داند که آن سازمان مرکزی صادر کننده کارت ها و حسابها چگونه به انجام این کارها می­پردازد.
7. وجود چنین سامانه های مرکزی با نفوذ افراد و دولت های مختلف رخ می­دهد که در برخی موارد می­تواند باعث حذف برخی افراد از سامانه و قطع سرویس دهی به آنها شود نظیر تحریم های اعمال شده علیه کشور ایران که دسترسی این کشور و مردم آن را به بیشتر سامانه های پرداخت جهانی قطع کرده است.

بنابر این و باتوجه به موارد فوق و همچنین گسترش روز افزون اینترنت در جهان برخی دانشمندان حوزه کامپیوتر اقدام به ایجاد نوع خاصی از ارز ها که ارز های الکترونیکی هستند نمودند که بتواند مشکلات ذکر شده در فوق را برطرف نماید و به عنوان یک سبک پرداخت جهانی با شفافیت عملکرد و بدون نیاز به اعتماد به یک شخص ثالث به عنوان مرجع تراکنش های مالی جهانی در نظر گرفته شوند.

## ارز های دیجیتال [[8]](#footnote-8)

به طور کلی هر ارزی که نمود فیزیکی نداشته باشد و به عنوان واحد های کامپیوتری در شبکه های خاص مورد استفاده قرار گیرد می­تواند نوعی ارز دیجیتالی به حساب آید بنابر این باید توجه داشت که مفهوم ارز دیجیتالی به طور کلی برابر با رمز ارز [[9]](#footnote-9) که در ادامه به بررسی آن خواهیم پرداخت نمی­باشد و هر نوع واحد پولی دیجیتالی حتی سکه ها و یا اعتبارات موجود در اکثر بازی های کامپیوتری را نیز می­توان نوعی ارز دیجیتال دانست.

### تاریخچه ارز های دیجیتال

ابتدایی ترین نوع ارز های دیجیتال که در حقیقت مفاهیم استفاده شده در برخی از آنها مبنای کارکرد رمز ارزهای امروزی است اغلب دارای یکاهایی معادل با یکی از ارز های رایج بودند که کاربران با پرداخت میزان معینی ارز دولتی ، ارز دیجیتال معادل آن را دریافت کرده و می­توانستند در معاملات اینترنتی خود از آنها استفاده کنند نمونه این ارز ها رزرو آزادی [[10]](#footnote-10) بود که در دهه 1990 میلادی همزمان با حباب دات-کام ایجاد شد. اگرچه اغلب این ارز های دیجیتال از مفاهیمی نظیر امضا دیجیتال [[11]](#footnote-11) و مکانیزم هایی شبیه به گواهی اثبات کار[[12]](#footnote-12) و یا به اختصار POW نیز استفاده می­کردند و در برخی موارد تا حدی نیز به صورت نظیر به نظیر [[13]](#footnote-13) کار می­کردند اما همه آنها در نهایت برای ایجاد توافق[[14]](#footnote-14) به یک سازمان مرکزی وابسته بودند که در حقیقت این بدان معنی بود که در انجام بزرگترین هدف خود که حذف واسطه ها از انجام تراکنش ها بود نا موفق بودند بنابر این اغلب این ارز های دیجیتال به سرعت به فراموشی سپرده شدند با این حال مفاهیم استفاده شده در بسیاری از آنها به عنوان مبنای رمز ارز های امروزی قرار گرفت. در نهایت در سال 2009 میلادی با معرفی بیت کوین [[15]](#footnote-15) مشکل نیاز به واسطه برای انجام تراکنش ها حل شد و برای انجام توافق از یک الگوریتم قوی کامپیوتری به نام بلاک چین [[16]](#footnote-16) استفاده شد.

# فصل دوم : برخی مفاهیم پایه بکار رفته در رمز ارز ها

برای بررسی بیشتر رمز ارز ها و بلاک چین ابتدا لازم به نظر می­رسد تا با برخی مفاهیم پایه و الگوریتم های به کار رفته در این سامانه ها آشنا شویم.

## رمز نگاری[[17]](#footnote-17)

از ابتدای تاریخ نوع بشر همواره نیاز به رمزکردن پیام های خود را احساس کرده است ،تا به طور مثال در شرایط جنگی و یا موارد خاص بتواند پیامهای خود را بین متحدین خود به گونه ای امن منتقل کند شاید اهمیت رمز نگاری را بتوان با بررسی تاریخ جنگ جهانی دوم مشخص کرد که با شکسته شدن کد های انیگما [[18]](#footnote-18)نوشته شده نازی ها توسط دانشمند انگلیسی و پدر علم کامپیوتر آلن تورینگ [[19]](#footnote-19) سر نوشت جنگ به نفع متحدین تمام شد.

در ابتدا بشر برای رمزنگاری پیام های خود از روش ها مختلفی نظیر قرار دادن سیمبل ها و رمز های خاص استفاده می­کرد تا اینکه پیوند این رمز ها با ریاضیات و الگوریتم های خاص ریاضی پیدا شد و با بررسی رمزنگاری به عنوان شاخه ای از علم ریاضی بشر موفق به ایجاد رمز های پیچده شد و در نهایت با ورود کامپیوتر ها عرصه رمز نگاری نیز توسط این ماشین های قدرتمند دچار تغییراتی شد و الگوریتم های پیچیده رمزنگاری کامپیوتری ایجاد شدند به طوری که امروزه برخی از آنها نطیر الگوریتم AES [[20]](#footnote-20) به قدری امن در نظر گرفته می­شوند که شکستن رمز های آنها تقریبا غیر ممکن به نظر می­رسد.

### رمز نگاری متقارن [[21]](#footnote-21)

این نوع رمزنگاری به نوعی خاصی از رمزنگاری گفته می­شود که در آن برای رمز کردن و رمزگشایی پیام از یک کلید استفاده می­شود ،کلیدها ممکن است مشابه باشند یا ممکن است رابطه‌ای ساده بین دو کلید وجود داشته باشد. کلید، در عمل، نشان دهنده یک راز مشترک بین دو یا چند طرف است که می‌تواند برای حفظ اطلاعات خصوصی مورد استفاده قرار گیرد. این نیاز که هر دو طرف، دسترسی به کلیدهای مخفی داشته باشند یکی از اشکالات اصلی رمزنگاری کلید متقارن است، چرا که در حقیقت با توجه به نیاز دو طرف برای دانستن یک کلید مشخص این نوع رمزنگاری بین دو طرف که به یکدیگر اعتماد ندارند قابل استفاده نیست و دو طرف باید از قبل یکدیگر را بشناسند و آن رمز مشخص را بین خود پذیرفته باشند. برای این نوع رمزنگاری اغلب رو گروه از الگوریتم های جریانی و بلوکی مورد استفاده قرار می­گیرند که الگوریتم های جریانی اغلب به رمز کردن یک واحد کوچک داده یا همان بیت به همان صورت که داده در جریان است می­پردازند و الگوریتم های بلوکی به رمز کردن یک تعداد مشخص از واحد داده ها به عنوان بلوک می­پردازند ، به طور مثال الگوریتم AES به رمزنگاری داده در بلوک های 128 بیتی می­پردازد.

### رمز نگاری نامتقارن [[22]](#footnote-22)

این نوع رمز نگاری در مقابل رمزنگاری متقارن قرار دارد و در آن­ها برای رمز کردن و رمزگشایی پیام از 2 کلید متفاوت استفاده می­شود که یکی از آنها به کلید عمومی [[23]](#footnote-23) و دیگری به کلید خصوصی [[24]](#footnote-24) شهرت دارند و همچنین یک رابطه ریاضی بین این 2 کلید برقرار است به طوری که همواره از کلید خصوصی می­توان کلید عمومی را به دست آور اما از کلید عمومی نمی­توان کلید خصوصی را استخراج کرد.

کارکرد الگوریتم های رمزنگاری نا متقارن به این صورت است است که هر فرد ابتدا با ایجاد یک کلید خصوصی و نگه داشتن آن نظیر خود به صورت امن و به دست آوردن کلید عمومی نظیر آن کلید خصوصی و دراختیار عموم قرار دادن آن کلید عمومی به رد و بدن کردن پیام های رمز شده می­پردازد، به این صورت که هر پیام توسط کلید عمومی که در اختیار همه هست رمز می­شود اما فقط با استفاده از کلید خصوصی که در اختیار خود فرد است قابل رمزگشایی خواهد بود ،بنابر این همه پیام های مورد نظر برای یک نفر فقط و فقط توسط همان فرد قابل رمزگشایی خواهند بود در حالی که همه افرادی که کلید عمومی را در اختیار دارند قادر به رمز کردن پیام های خود خواهند بود از الگوریتم های معروف رمزنگاری نامتقارن می­توان از الگوریتم RSA [[25]](#footnote-25) که بر پایه هم نهشتی و با کمک اعداد اول بزرگ کار می­کند و ECC [[26]](#footnote-26) بر اساس ساختاری جبری از منحنی‌های بیضوی بر روی میدانهای متناهی طراحی شده‌است نام برد البته اغلب این الگوریتم ها با کمک الگوریتم های دیگر مورد استفاده قرار می­گیرند.

#### الگوریتم های تبادل کلید

الگوریتم های رمزنگاری نامقارن اغلب دارای یک مشکل اساسی می­باشند که محدودیت سایز پیام قابل رمزنگاری توسط آن­ها می­باشد به طوری که در صورتی که اندازه پیام از حدی بزرگتر باشد برای رمز نگاری آن نیاز به کلید طولانی تری خواهد بود و طولانی کردن کلید نیز تا حدی ممکن است­ ،بنابر این برای استفاده از آنها یا باید پیام را به قطعا کوچک شکست و رمز نمود و یا از راهکار دیگری بر مبنای الگوریتم های تبادل کلید استفاده نمود ،در حقیقت همانطور که قبلا اشاره شد الگوریتم های رمزنگاری متقارن دارای مشکل اساسی نیاز به دانستن کلید یکسان توسط هر دو طرف قبل از شروع انتقال پیام می­باشند اما در بستر های ناامن که نیاز به رمزنگاری هست در صورتی که دو طرف از قبل با یکدیگر در ارتباط نبوده باشند چطور می­توان کلید مورد نظر را انتقال داد؟ در اینجا با کمک الگوریتم های انتقال کلید و با کمک رمزنگاری نامتقارن می­توان ابتدا به تبادل کلید الگوریتم رمزنگاری متقارن پرداخت و سپس با کمک آن کلید در ادامه پیام هارا به صورت متقارن رمزنگاری کرد از الگوریتم های معروف این دسته می­توان از پروتکل تبادل کلید دیفی-هلمن [[27]](#footnote-27) نام برد الگوریتم استفاده شده در پروتکل امن انتقال ابرمتن[[28]](#footnote-28) ویا به اختصار Https نیز تقریبا کارکردی به همین صورت دارد.

#### امضای دیجیتال

از دیگر کاربرد های رمزنگاری نامتقارن می­توان به امضا دیجیتال اشاره کرد که در حقیقت این الگوریتم امضا دیجیتال است که در ارز رمز ها نیز بسیار کاربرد دارد و در حقیقت به اثبات هویت ارسال کننده یک پیام و یا تراکنش می­پردازد به مانند امضا عادی در سیستم های سنتی که امضا هر طرف در انتهای هر نامه و پیامی به معنی تایید فرد مورد نظر است.

کارکرد امضا دیجیتال به این صورت است که ابتدا فرد نویسنده یک پیام و یا تراکنش برای اثبات هویت خود با کمک توابع درهم سازی یک طرفه [[29]](#footnote-29) با طول ثابت به هش کردن پیام خود می­پردازد و سپس این بار با کمک کلید خصوصی خود رشته به دست آمده را رمز می­کند حال پیام رمز شده نهایی را به انتهای پیام اصلی می افزاید که به این فرایند امضا کردن پیام گفته می­شود حال به ارسال این پیام به شخص یا اشخاص مورد نظر آنها با داشتن کلید عمومی طرف می­توانند امضا فرستاده شده را رمزگشایی کرده و اصل پیام را نیز هش کنند و رشته خروجی را با رشته بدست آمده از رمزگشایی امضا تطبیق دهند در صورت برابر بودن 2 رشته اثبات هویت ارسال کننده پیام صورت می­گیرد که در حقیقت فرد متناظر با ان کلید عمومی است.

#### رمزنگاری ECC

باتوجه به اینکه در اغلب رمز ارزها و سامانه های امروزی از الگوریتم ECC به عنوان الگوریتم رمزنگاری نامتقارن استفاده می­شود به نظر می­رسد لازم است که به اختصار نحوه کارکرد آن را توضیح دهیم.

همانطور که پیش تر ذکر شد این الگوریتم بر اساس ساختاری جبری از منحنی‌های بیضوی بر روی میدانهای متناهی طراحی شده‌است. که این امر باعث نیاز به کلید کوچک تری نسبت به دیگر روش های رمزنگاری نا متقارن می­شود، در حقیقت برای اهداف امروزی رمزنگاری، منحنی بیضوی یک منحنی مسطح است که متشکل از نقاط رضایت بخش معادله می‌باشد.

|  |  |
| --- | --- |
| معادله ‏2‑1: منحنی های بیضوی در 2 بعد |  |

همراه با یک نقطه برجسته در (مختصات در اینجا از یک حوزه ثابت متناهی از مشخصه که با ۲ یا ۳ برابر نیست انتخاب می‌شوند، یا اینکه معادله منحنی تا حدودی پیچیده‌تر خواهد بود) این مجموعه همراه با عملیات گروهی از نظریه گروه بیضوی از گروه Abelian، با نقطه‌ای در بینهایت به عنوان عنصر هویت می‌باشند. ساختار گروه از گروه مقسوم علیه تنوع جبری زیرین ارث بری می‌کند. همان‌طور که برای دیگر سیستم‌های رمزنگاری کلید عمومی محبوب، بدون اثبات ریاضی برای امنیت ECC از سال ۲۰۰۹ منتشر شد.

درنهایت باید دانست که امنیت کاملECC بستگی به توانایی محاسبه ضرب نقطه‌ای و عدم توانایی برای محاسبه حاصلضرب با توجه به نقاط اصلی و نقاط تولید شده دارد.

#### تهدید های متوجه رمزنگاری نامتقارن

امنیت شیوه های امروزی رمز نگاری متقارن اغلب بر پایه سخت بودن حل مسائلی نظیر تجزیه اعداد اول و یا مسئله حل لگاریتم گسسته برای کامپیوتر های امروزی مطرح می­شوند که حل این مسائل به طور عادی از روابط نمایی پیروی می­کند بنابر این برای حل آنها صرف زمان بسیار بسیار زیادی توسط کامپیوتر های امروزی لازم خواهد بود به طوری که می­توان به دست آوردن پاسخ آنهارا عملا غیر قابل دست یابی دانست ، اما نوع دیگر کامپیوتر های که کامپیوتر های کوانتمی [[30]](#footnote-30) معروف هستند. با کمک الگوریتم کوانتمی شور [[31]](#footnote-31) قادر به حل این مسائل در زمان معقولی می­باشند که در حقیقت این مورد این نگرانی را در بین بسیاری از افراد به وجود آورده که این نوع کامپیوتر ها می­توانند تهدیدی برای اغلب روش های رمزنگری و سامانه های مبتنی بر رمزنگاری نامتقارن امروزی باشند ، که از همین رو تلاش هایی برای ایجاد الگوریتم های رمزنگاری نامتقارن کوانتمی [[32]](#footnote-32) شده است ، البته لازم به ذکر است که هنوز کامپیوتر های کوانتمی قدرتمند که توانایی اجرای الگوریتم گفته شده را داشته باشند ساخته نشده اند ، اما تخمین زده می­شود که تا سال 2030 میلادی نمونه اولیه چنین کامپیوتر هایی ساخته شوند ، نکته قابل توجه دیگر آن است که کامپیوتر های کوانتمی تهدیدی برای الگوریتم هایی نظیر AES نمی­باشند.

## توابع درهم سازی یک طرفه

توابع درهم سازی یک طرفه به توابعی گفته می­شود که اغلب با دریافت یک رشته بیتی با درهم ریختن رشته ورودی به ایجاد یک رشته خروجی با طول ثابت می­پردازند به طوری که به دست آوردن رشته ورودی از رشته خروجی امکان پذیر نباشد و همچنین به ازای هر رشته منحصر به فرد در ورودی یک رشته منحصر به فرد در خروجی ایجاد شود. به طوری که با داشتن رشته ورودی همواره به توان به یک رشته خروجی رسید و به ازای هیچ دو رشته ورودی غیر یکسانی ،یک رشته خروجی یکسان حاصل نشود. به طور کلی کاربرد این نوع توابع در شماره گذاری رشته ها و جداول داده درهم [[33]](#footnote-33) کاربردی می­باشند.

### تابع درهم‌سازی رمزنگارانه [[34]](#footnote-34)

این نوع توابع درهم سازی نوع خاصی از توابع در هم سازی می­باشند که یک رشته با طول نا مشخص را به یک رشته با طول ثابت درهم ریزی می­کنند به طوری که رشته خروجی نمایشی از کل محتوای متن یا رشته ورودی است و می‌توان آن را نوعی «اثر انگشت دیجیتالی» برای آن متن به حساب آورد ، این نوع توابع درهم سازی در امضا دیجیتال ، ذخیره اطلاعات حیاتی مانند کلمه عبور کاربران در پایگاه داده ، بلاک چین و بسیاری موارد دیگر کاربرد دارند از معروف ترین توابع درهم سازی رمزنگارانه می­توان از MD4,MD5,SHA-1,SHA-2,SHA-3 نام برد.

از دیگر خصوصیت این توابع که در سیستم های بلاک چینی بسیار قابل توجه است آن است که در حقیقت امکان پیش بینی خروجی از روی وردی به هیچ عنوان امکان پذیر نیست، در حقیقت کارکرد آنها به این صورت نمی­باشد که رشته خروجی به ازای تغییرات مشخص ورودی به یک رشته خاص در خروجی میل کند که بتوان آن را حدس زد و با هر تغییر بسایر کوچک در رشته ورودی، رشته خروجی تغییرات قابل توجهی خواهد کرد.

## درخت مرکله [[35]](#footnote-35)

درخت مرکله و یا درخت درهم سازی به طور معمول یک درخت دودویی [[36]](#footnote-36) و یا یک درخت پیشوندی [[37]](#footnote-37) است که برگ های آن شامل یک سری داده مشخص می­باشند ، سپس در مراحل بالاتر مقدار هر گره از مقدار هش فرزندان خود به دست می­آید به همین صورت از گره های والد برای برگ ها شروع به هش کردن مقادیر میکنیم و سطح به سطح در درخت بالا می­رویم و مقدار هر گره را معادل هش مقدار فرزندان خود می­گذاریم تا به ریشه درخت برسیم.

|  |  |
| --- | --- |
| معادله ‏2‑2: گره های درخت درهم سازی |  |

کاربرد درخت های مرکر به طور معمول در نوع خاصی از امضا دیجیتال به نام امضای لمپورت [[38]](#footnote-38) و یا تایید اعتبار یک فایل و همچنین به طور گسترده در بلاک چین می­باشد.



تصویر ‏2‑1: نمونه یک درخت درهم سازی

## کدبندی نویسه [[39]](#footnote-39)

باتوجه به اینکه کوچکترین واحد قابل فهم برای کامپیوتر ها یک بیت است که دارای مقاداری معادل 0 یا 1 می­باشد در نتیجه همه مفاهیم از نظر کامیپوتر ها باید دارای یک مقدار عددی باشند­، بنابر این برای نویسه [[40]](#footnote-40) های الفبایی استاندارد هایی در نظر گرفته شده است که هر نویسه را به یک مقدار عددی مشخص نظیر می­کند از نمونه های این استاندارد ها می­توان به مواردی از قبیل ASCII [[41]](#footnote-41) که فقط شامل حروف انگلیسی اعداد و برخی نویسه های خاص است و یا UTF-8 که دارای نویسه های موجود در اغلب زبان های می­باشد اشاره کرد. اما این کدبندی ها اغلب برای داده هایی به کار می­روند که در زبان های طبیعی دارای معنی و مفهوم می­باشند و خروجی یک تابع درهم سازی یک طرفه و یا رشته خروجی حاصل از یک الگوریتم رمزنگاری اشکال سخت و عجیبی در این نوع از کدبندی ها پیدا می­کنند بنابر این برای نمایش خروجی این تابع ها به صورت رشته های حرفی عددی نیز استاندارد های خاصی نظیر Hex, Base64, Base58 ایجاد شده است که Hex در حقیقت نمایش هر بایت از داده در مبنای 16 است که باعث طولانی شدن رشته می­شود بنابر این استاندارد Base64 به طور معمول برای انتقال داده ها استفاده می­شود که این استاندارد نیز به دلیل وجود نویسه هایی مانند عدد 0 و حرف o لاتین و یا حرف l کوچک لاتین و حرف I بزرگ لاتین و عدد 1 و... که در برخی فونت ها شکل یکسان دارند در صورتی که قرار باشد توسط انسانها و نه ماشین ها مورد بررسی قرار گیرند مشکلاتی را ایجاد می­کنند که برای پیشگیری از این مشکلات از استاندارد Base58 در اغلب کریپتو کارنسی ها استفاده می­شود که حروف و اعداد مشابه و غیر قابل تشخیص از یکدیگر در آن مشاهده نمی­شوند.

## شبکه نظیر به نظیر

این شکبه ها در حقیقت در مقابل شبکه های سرویس دهنده-سرویس گیرنده [[42]](#footnote-42) قرار دارند و به جای آنکه یک سرویس دهنده مرکزی وجود داشته باشد که همه سرویس گیرنده ها به آن متصل باشند و فقط بتوانند با سرویس دهنده انتقال پیام انجام دهند ، همه نظیر ها [[43]](#footnote-43) به صورت مستقیم به هم متصل هستند و در حقیقت هر نظیر حکم یک سرویس دهنده و یک سرویس گیرنده کوچک را دارد ، این شبکه در رمز ارزها اهمیت بالایی دارند چراکه به کمک این شبکه ها امکان حذف شخص ثالث در تراکنش ها حذف شده است.



تصویر ‏2‑2 : نمونه یک شبکه سرویس گیرنده-سرویس دهنده



تصویر ‏2‑3 : نمونه یک شبکه نظیر به نظیر

## ماشین مجازی [[44]](#footnote-44)

ماشین مجازی در حقیقت ماشینی است که به طور مجازی روی یک ماشین فیزیکی دیگر اجرا می­شود و یک سری عملیات خاص انجام می­دهد ، نوع خاصی این ماشین های مجازی آنهایی هستند که در زبان های برنامه نویسی سطح بالا مانند جاوا [[45]](#footnote-45) و یا زبان های خانواده دانت نت [[46]](#footnote-46) به ترتیب با نام های JVM [[47]](#footnote-47)و CLR [[48]](#footnote-48) استفاده می­شوند . این ماشین های مجازی اغلب مانند ریز پردازنده ها [[49]](#footnote-49) دارای یک زبان اسمبلی مانند [[50]](#footnote-50) مخصوص به خود می­باشند که کد های زبان سطح بالاتر به این زبان ها ترجمه می­شوند و سپس کد های خروجی حاصل در ماشین مجازی مورد نظر اجرا می­شوند در حقیقت این ماشین های مجازی رفتار شبیه به یک پردازنده را شبیه سازی می­کنند.



تصویر ‏2‑4 : نحوه کارکرد CLR

اغلب رمز ارزها نیز برای انجام کارهای خود دارای یک ماشین مجازی می­باشند که تراکنش ها مورد نظر به صورت کد های این ماشین مجازی در آمده و برای تایید کد های مورد نظر اجرا می­شوند به طور مثال می­توان از EVM [[51]](#footnote-51) در این زمینه نامبرد.

# فصل سوم : بلاک چین

همانطور که گفته شد در سال 2009 میلادی با معرفی بیت کوین به عنوان اولین رمز ارز توسط فرد یا افرادی با نام مستعار ساتوشی ناکاماتو [[52]](#footnote-52) مفهوم رمز ارزها پابه عرصه وجود گذاشتند به طوری که امروزه بیش از بیش از 1000 رمز ارز مختلف در دنیا وجود دارد ، بیت کوین برخلاف ارز دیجیتال قبل از خود توانست مشکل نیاز به طرف سوم قابل اعتماد را با کمک یک مکانیزم انقلابی به نام بلاک چین حل کند که در این فصل به بررسی این سیستم می­پردازیم.

در حقیقت بلاک چین را می­توان به مانند یک سیستم عامل در نظر گرفت و رمز ارزهارا به عنوان برنامه هایی که بر روی این سیستم عامل بزرگ و توزیع شده اجرا می­شوند.

## تعریف مفهومی بلاک چین

بلاک چین یک دفتر کل بزرگ و توزیع شده می­باشد که کار ثبت و رهگیری دارایی هارا به صورت تراکنش [[53]](#footnote-53) محور انجام می­دهد به طوری که امکان تغییر یا حذف اطلاعات درج شده در این دفتر کل وجود ندارد و فقط می­توان اطلاعات جدیدی را به آن افزود ، بلاک چین كار فرآيند ثبت تراكنشها و ردگيري داراييها را در يك شبكه­ي كسب­وكار ساده ميكند. يك دارايي ميتواند ملموس مانند خانه، خودرو، پول نقد، زمين و يا ناملموس مانند مالكيت معنوي نظیر حق اختراع، حق چاپ يا نام اعتباري باشد. تقريباً هرچيز ارزشمندي ميتواند در يك شبكهي بلاک چین ردگيري و معامله شود و مخاطرات و هزينه­ها را براي همه­ي طرفهاي درگير كاهش دهد.

## تعریف ساختاری بلاک چین

در ساده ترین حالت ساختار بلاک چین را همانطور که از نامش پیداست می­توان به صورت زنجیره ای از بلاک های داده ای دانست که به طور متوالی پشت یکدیگر قرار می­گیرند و هر بلاک به طوری به بلاک قبلی خود وابسته است.



تصویر ‏3‑1: شمای کلی یک بلاک چین

## ساختار هر بلاک

باتوجه به اینکه بلاک چین از زنجیره ای از بلاک ها ساخته شده است بنابر این ضروری به نظر می­رسد که ابتدا به بررسی ساختار هر بلاک به صورت جز به جز بپردازیم تا در ادامه بتوانیم کاربرد هر یک از این بخش هارا در یک بلاک چین بررسی کنیم.

هر بلاک به طور معمول حداقل دارای 3 بخش زیر است:

1. بخش داده ای
2. نماد بلاک
3. نماد بلاک قبل از خود

حال به بررسی هر کدام از این بخش ها می­پردازیم:

### بخش داده ای بلاک

بخش داده ای یک بلاک در ساده ترین حالت ممکن می­تواند یک رشته متنی حاوی یک پیام باشد و یا اطلاعات تراکنش های مالی مختلف به همراه اطلاعات دیگری نذیر یک مقدار متغییر ، زمان ساخت بلاک ، شماره بلاک و ... که در رمز ارزها استفاده می­شود.

### نماد یا امضا بلاک

برای هر بلاک نماد یا امضا آن بلاک برابر است با خروجی تابع درهم ریزی یک طرف از همه بخش های به غیر از خود بخش نماد بلاک یا به عبارت دیگر مقدار هش بخش های مختلف بلاک.

### نماد بلاک قبل از خود

هر بلاک شامل نماد بلاک قبلی خود نیز می­شود. که در حقیقت این بخش باعث ایجاد زنجیره و مرتبط شدن بلاک ها به یکدیگر می­شود.

## بررسی ساختار بلاک چین

همانطور که گفته شد بلاک چین زنجیره ای از بلوک های داده ای به هم وابسته است اما این بلاک ها چگونه به هم وابسته می­شوند؟

در حقیقت وظیفه ایجاد وابستگی بلاک های یک بلاک چین فارغ از بخش داده ای و بخش های دیگر آن بر عهده بخش شامل نماد بلاک قبلی می­باشد، به این صورت که با قرار دادن نماد بلاک قبلی در هر بلاک آن بلاک را به بلاک قبلی خود وابسته می­کنیم و باتوجه به اینکه بخش نماد بلاک قبلی برای محاسبه نماد بلاک جدید استفاده می­شود در حقیقت با ایجاد هر بلاک ،این بلاک جدید به همه بلاک های قبل از خود وابسته است به طوری که برای ایجاد تغییر در یک بلاک نماد آن بلاک تغییر می­کند در نتیجه نماد بلاک بعد از آن نیز تغییر می­کند و این تغییر تا جدید ترین بلاک انتشار می­یابد ،حال اگر بلاک چین یک بلاک چین پویا باشد به طوری که پیوسته به بلاک های آن افزوده شود عملا ایجاد تغییر در یکی از بلاک های قبلی امکان پذیر نخواهد بود و یا حداقل بسیار بسیار سخت خواهد بود بنابر این همه افرادی که در یک بلاک چین مشارکت می­کنند می­توانند بر روی صحیح بودن اطلاعات بلاک چین توافق کنند و به این صورت توافق مورد نظر بدون نیاز به فرد سومی ایجاد می­شود و در حقیقت همه افراد مشارکت کننده بر روی صحت داده های داخل بلاک چین توافق دارند.



تصویر ‏3‑2: ساختار بلاک چین

## خواص بلاک چین

هر بلاک چین باید شامل خواص زیر باشد:

1. تغییر ناپذیری: تغییر ناپذیری در بلاک چین باتوجه به ساختار آن به وجود می­آید.
2. اصل بودن : مشاركت كنندگان ميدانند دارايي از كجا ميآيد و مالكيت آن در طول زمان چگونه تغییر کرده است.
3. قطعیت : هر بلاک دارای قطعیت است در حقیقت داده های آن قطعی و صحیح و پذیرفته شده هستند.
4. شفافیت : نحوه ساز و کار بلاک چین دارای شفافیت است و داده های موجود در آن برای همه افراد موجود در شبکه قابل دسترسی است.

## بررسی کارکرد شبکه های بلاک چین

اغلب شبکه های مبتنی بر بلاک چین مانند رمز ارز ها بر بستر شبکه های کامپیوتری نظیر به نظیر به فعالیت می­پردازند به طوری که هر یک از نظیر های موجود در شبکه که اینجا ند [[54]](#footnote-54) نامیده می­شوند یک نسخه از بلاک چین را در سیستم خود نگه می­دارند و قابلیت خواندن اطلاعات بلاک چین و افزودن بلاک جدید در شبکه را دارا می­باشند و به ازای افزوده شدن هر بلاک جدید ،ندی که آن بلاک را به بلاکچین افزوده است موظف است که این موضوع را به همه نظیر های دیگر اعلام کند تا آنها نیز اطلاعات بلاک چین خود را به روز رسانی [[55]](#footnote-55) کنند تا شبکه دچار خطا نشود.

## انواع بلاک چین

بلاک چین ها دارای انواع مختلفی می­باشند اما به صورت کلی به دو دسته خصوصی و عمومی تقسیم می­شوند که بلاک چین های عمومی اطلاعاتشان در اختیار همه افراد قرار دارد و هر کسی می­تواند در هر زمان به عنوان یک ند جدید وارد این شبکه شود و یا اطلاعات آن­هارا مورد بررسی قرار دهد نظیر بلاک چین های ارز رمز ها، در مقابل نیز بلاک چین های خصوصی قرار دارند که یک سازمان و یا کسب و کار می­تواند برای افراد موجود در شبکه خود آن­را ایجاد کند و بر بستر شبکه های داخلی خود سازمان به اجرای آن بپردازد و یا با رمزگذاری همه داده های آن از دسترسی افراد غیر قابل اعتماد به داده ها جلوگیری به عمل آورد.

## اثبات کار

اثبات کار یا POW در حقیقت یک مکانیزم در شبکه های بلاک چین است که ویژگی تغییر ناپذیری بلاک چین را تقویت می­کند و همچنین از افزوده شدن بلاک های زیاد و غیر ضروری به سادگی در شبکه جلوگیری می­کند، در حقیقت همان­طور که از نامش پیداست POW یک مکانیزم است که باعث می­شود هر فرد برای افزودن هر بلاک در شبکه موظف باشد میزان معینی کار انجام دهد.

سازکار این مکانیزم به این صورت است که برای هر بلاک چین مقدار مشخصی به نام سختی [[56]](#footnote-56) در نظر گرفته می­شود و حال یک شرط جدید برای به دست آوردن بلاک هش به سازوکار شبکه افزوده می­شود به طوری که مقدار عددی هش به دست آمده باید از مقدار سختی کمتر باشد برای ساده شدن کار می­توان این شرط را به صورت ظاهر شدن تعداد معینی 0 در ابتدای مقدار هش بلاک دانست.

همانطور که گفته شد هش بلاک شامل مقدار هش بخش مختلف بلاک می­باشد اما این بخش اغلب از داده های ثابتی تشکیل شده اند که قابل تغییر نمی­باشد بنابر این به ازای داده های بلاک فقط و فقط یک مقدار هش تولید می­شود که ممکن است شرط مورد نظر برای POW را نداشته باشد، برای حل این مشکل یک مقدار متغییر به نام nonce نیز به داده های بلاک افزوده می­شود این مقدار متغییر فارغ از دیگر بخش های بلاک است و می­تواند هر مقداری داشته باشد حال با کمک این مقدار جدید و تغییر دادن آن و محاسبه مجدد هش بلاک می­توان هش های مختلف برای یک بلاک به دست آورد و درحقیقت مکانیزم POW مشارکت کنندگان را مجبور می­کند تا مکررا به محاسبه مقدار هش های مختلف برای یک بلاک با nonce های مختلف بپردازند تا یک مقدار هش با شرط کوچکتر بودن از سختی یافته شود؛ به محض یافته شدن این مقدار ،ندی که هش را پیدا کرده است این مقدار جدید را و مقدار nonce ای که به ازای آن مقدار هش را به دست آورده است به دیگر ند ها اعلام می­کند و دیگر ند ها نیز حال به سادگی با یکبار هش کردن با nonce اعلام شده می­توانند صحت ادعای ند اعلام کننده را راستی آزمایی کنند و درصورت درست بودن ادعا آن را به عنوان بلاک جدید بپذیرند.

### حمله 51 درصد

با افزوده شدن POW به بلاک چین حال تغییر دادن داده های بلاک بیش از بیش سخت می­شود به طوری که برای تغییر داده های یک بلاک این بار فرد مورد نظر باید به ازای همه بلاک های بعدی نیز الگوریتم POW را نیز اجرا کند و مقدار هشی کمتر از سختی برای همه بلاک ها بیاید، که بسیار زمانگیر خواهد بود همچنین در شبکه های پویا که همواره به بلاک های آن افزوده می­شود ند خاطی باید بتواند به قدری سریع به محاسبه POW بلاک های قبلی بپردازد که بتواند به آخرین بلاک برسد و بلاک آخر را نیز خود بدست بیاورد و به شبکه اعلام کند تا همه آن­را بپذیرند که این اتفاق فقط در حالتی ممکن است که ند مورد نظر حداقل 51 درصد قدرت محاسباتی شبکه را داشته باشد یعنی قدرت محاسباتی آن از مجموع قدرت محاسباتی همه ند های دیگر موجود در شبکه بیشتر باشد.

### تغییرات سختی

از دیگر کاربرد های POW آن است که شبکه های بلاک چینی شلوغ می­توانند زمان ایجاد شدن بلاک های خود را کنترل کنند تا به این صورت از رشد بی رویه بلاک چین جلو گیری به عمل آورند به این ترتیب که با افزوده شدن هر ند شانس یافته شدن بلاک جدید بیشتر می­شود چرا که ند های بیشتری برای بدست آوردن بلاک جدید به رقابت می­پردازند حال پس از افزوده شدن تعداد زیادی ند می­توان با افزایش دادن مقدار سختی زمان مورد نیاز برای بدست آوردن بلاک جدید را بیشتر کرد و درحقیقت انجام مکانیزم POW را سخت تر نمود و زمان میانگین برای به دست آمدن تعداد معینی ای بلاک را کنترل نمود.



تصویر ‏3‑3: نمودار تغییرات سختی شبکه بیت کوین

## استخراج [[57]](#footnote-57) رمز ارز

در شبکه های بلاک چینی رمز ارزهایی نظیر بیت کوین که تعداد زیادی ند برای بدست آوردن بلاک بعدی رقابت می­کنند مقداری از توکن های شبکه به عنوان جایزه [[58]](#footnote-58) به هر فردی که موفق به یافتن بلاک بعدی شود اختصاص داده می­شود تا به این صورت انگیزه برای پیاده کردن بلاک های جدید در بین افراد ایجاد شود چرا که هر فرد با پیدا کردن بلاک جدید و انجام عملیات POW در حقیقت به میزان امنیت شبکه می­افزاید ،به این ترتیب به تعداد کوین های شبکه افزوده می­شود و در حقیقت مکانیزمی مانند استخراج کردن ایجاد می­شود.

به طور مثال برای شبکه بیت کوین در ابتدا جایزه هر بلاک 50 بیت کوین در نظر گرفته شده بود که به ازای ایجاد شدن هر 210 هزار بلاک این میزان نصف می­شود تا در نهایت به 0 میل کند به طوری که پیش بینی می­شود در نهایت تعدادی نزدیک به 21 ملیون بیت کوین وجود خواهند داشت که این مقدار تا سال 2140 میلادی کاملا استخراج می­شود ، لازم به ذکر است که با افزایش تعداد ند ها به مرور زمان سرعت به استخراج بیت کوین ها افزایش نمی­یابد چرا که همانطور که اشاره شد مقدار سختی مکررا افزوده می­شود به طوری که تقریبا هر 210 هزار بلاک زمانی معادل 4 سال برای ایجاد شدن نیاز خواهند داشت.

## دیگر اثبات ها[[59]](#footnote-59)

علی رغم تمام مزایای اثبات کار این مکانیزم دارای مشکلاتی نیز می­باشد یکی از بزرگترین ایرادات مکانیزم POW مصرف مقدار زیادی انرژی توسط کامپیوتر های ند هایی است که به اجرای آن می­پردازند به طوری که گفته می­شود به طور مثال شبکه بیت کوین در حال حاظر انرژی الکتریکی به اندازه انرژی مورد نیاز برای کل کشور ایرلند می­باشد، درحالی که این انرژی برای امن کردن شبکه استفاده می­شود اما تعداد زیادی هش تولید شده برای هر بلاک بی استفاده است و عملا این حجم عظیم انرژی به هدر می­رود ، همچنین از دیگر اشکالات این مکانیزم آن است که برخی افراد با ایجاد مدارات مجتمع خاص و یا asics قادر به استخراج بیت کوین با سرعت زیاد­ می­باشند به طوری که امروزه استخراج با cpu های معمولی عملا امکان پذیر نمی­باشد بنابر این تعداد اثبات دیگر نیز برای ارز رمز ها مطرح شده است که در اینجا به معرفی برخی از آنها می­پردازیم.

### اثبات سهام [[60]](#footnote-60) (POS)

در این روش یکی از ند های موجود در شبکه به طور تصادفی برای ایجاد بلاک جدید توسط شبکه انتخاب می­شود اما با این شرط که افرادی که دارای سهم بیشتری از توکن های شبکه می­باشند شانس بیشتری برای انتخاب شدن دارند، که داشتن تعداد زیادی از توکن های شبکه مانع از تقلب فرد مورد نظر می­شود چرا که اگر این ند اقدام به تقلب کند ارزش توکن های شبکه که خود مالک تعداد زیادی از آنها است کاهش می­یابد.

### اثبات حافظه [[61]](#footnote-61)

این اثبات به مانند اثبات کار می­باشد با این تفاوت که در آن از توابع در هم سازی حافظه سخت می­باشد که فرد مورد نظر برای استخراج بلاک جدید به جای داشتن قدرت محاسباتی بیشتر باید سیستمی با حافظه بیشتر داشته باشد که باتوجه به سخت بودن ساخت حافظه و گرانتر بودن آن ها شانس استفاده از مدارهای مجتمی محاسباتی درآنها کمتر است.

### گواهی سوزاندن [[62]](#footnote-62)

این گواه نوعی گواهی است که در آن هر ند برای ایجاد کردن بلاک جدید باید تعدادی از توکن های خود را از بین ببرد بنابر این لزوم از بین بردن مانع از تقلب می­شود.

همچنین برخی روش های دیگر نیز که گاها ترکیبی از روش های فوق است نیز استفاده می­شود.

## بلاک چین های نسل دوم [[63]](#footnote-63)

همانطور که پیش­تر اشاره شد یکی از بخش های ارز رمز ها و برنامه های مبتنی بر بلاک چین یک ماشین مجازی است که به اجرای برخی دستورات شبه اسمبلی مختص آن ارز رمز و بلاک چین می­پردازد. این زبان شبه اسمبلی در نسخه های اولیه ارز رمز ها شامل دستورات بسیار محدودی می­شد و به اصطلاح دارای خاصیت کامل بودن تورینگ [[64]](#footnote-64) نبود، به این معنی که دارای دستورات پرش نبود اما با گذر زمان برخی از فعالان حوزه ارز رمز با بررسی پتانسیل های نهفته در این زبان، به استفاده از دستورات کامل تر و زبان های کامل تورینگ روی آوردند که به این ترتیب نسل دوم بلاک چین ها شروع شدند، یکی از نمونه های ارز رمز های با بلاک چین نسل دوم اتریوم [[65]](#footnote-65)می­باشد.

### قرار داد های هوشمند [[66]](#footnote-66)

قرار داد های هوشمند برخلاف آنچه که ممکن است از نام ظاهری آن­ها برداشت شود، قطعه کد هایی با زبان های کامل تورینگ ماشین های مجازی ارز رمز ها هستند که به ارسال یک تراکنش به سمت آن­ها قادر به انجام یک کار مشخص و ثبت نتیجه آن در بلاک چین می­باشند. بنابر این، این قطعه کد ها در محیط یک شبکه بلاک چین اجرا می­شوند و همه مشارکت کنندگان شبکه می­توانند با آن­ها ارتباط برقرار کرده و انجام سرویس خاصی را مدنظر داشته باشند.

## قاعده طولانی ترین زنجیره [[67]](#footnote-67)

همانطور که گفته شد در بلاک چین های شلوغ مانند بلاک چین های رمز ارز ها تعداد زیادی ند برای به دست آوردن بلاک بعدی با یکدیگر به رقابت می­پردازند و هر ندی که بتواند زودتر از بقیه ند ها پاسخ مسئله POW را بیابد به عنوان برنده برای استخراج آن بلاک معرفی می­شود اما اگر 2 ند همزمان موفق به این کار شوند چه می­شود؟ در این حالت هر 2 ند در یک زمان پاسخ درستی برای POW بدست آورده اند و هر دو می­توانند بلاک خود را به انتهای بلاک چین بی افزایند که این اتفاق در عمل باعث 2 شاخه شدن بلاک چین می­شود، اما در نهایت باید یکی از این شاخه به عنوان شاخه صحیح پذیرفته شود و به حیات خود ادامه دهد. راه حل بیت کوین و دیگر رمز ارز ها برای چنین حالتی آن است که ابتدا میگذارند هر 2 بلاک به انتهای بلاک چین افزوده شود چرا که در مرحله اولیه هر دو بلاک برابر هستند اما با گذر و افزوده شدن بلاک های بعدی در انتهای این 2 بلاک 2 شاخه متفاوت از بلاک چین ایجاد می­شود که در نهایت همه ند ها طولانی ترین شاخه ایجاد شده را به عنوان شاخه درست می­پذیرند و کار کردن بر روی شاخه دیگر را رها می­کنند.



تصویر ‏3‑4 : قاعده طولانی ترین شاخه

همانطور که در تصویر 3-4 دیده می­شود در هر مرحله پس از 2 شاخه شدن بلاک چین بلاک چین زنجیره سیاه که طولانی تر بوده است را به عنوان زنجیره اصلی انتخاب کرده و بلاک های بنفش راه شده اند، به این بلاک های رها شده در اصطلاح یتیم شده [[68]](#footnote-68) می­گویند.

## فورک [[69]](#footnote-69) در بلاک چین

شبکه های بلاک چین نیز مانند دیگر برنامه های کامپیوتری هموراه دستخور تغییرات و به روز رسانی هایی می­شوند اما با توجه به این که این شبکه ها کار حساس تری را نسبت به دیگر برنامه ها انجام می­دهند و همچنین پایگاه داده آنها که بلاک چین می­باشد همواره در حال افزودن بلاک جدید است در برخی موارد ممکن است این تغییرات باعث ایجاد بلاک هایی با قواعد جدید شوند که با بلاک های قبل از آن تفاوت هایی دارد به چنین حالتی فورک در بلاک چین گفته می­شود. در چنین حالتی ند هایی که نسخه نرم افزار خود را به روز رسانی [[70]](#footnote-70) کرده اند بلاک هایی با خصوصیات متفاوتی از ند هایی که به روز رسانی را انجام نداده اند تولید می­کنند.

### فورک نرم [[71]](#footnote-71)

فورک نرم زمانی رخ می­دهد که تغییرات ایجاد شده اساسی نباشند و بنابر این علی رغم این که 2 نسخه مختلف از بلاک ها در حال ایجاد شد هستند اما این بلاک ها می­توانند بدون رخ دادن مشکل خاصی پشت یکدیگر قرار بگیرند و شبکه کلی دچار مشکل نمی­شود بنابر این ند هایی که به روز رسانی کرده اند و ند هایی که به روز رسانی نکرده اند می­توانند کار کردن بر روی یک بلاک چین رو ادامه دهند.

### فورک سخت [[72]](#footnote-72)

این نوع فورک زمانی رخ می­دهد که تغییرات مذکور بسیار اساسی باشند به طوری که بلاک های تولید شده با هر نسخه نمی­توانند کنار یکدیگر قرار گیرند و از نقطه ایجاد به روز رسانی عملا بلاک چین به 2 بلاک چین مجزا تبدیل می­شود در چنین حالتی ند هایی که به روز رسانی را دریافت کرده اند روی یک بلاک چین و ند هایی که به روز رسانی را دریافت نکرده اند روی یک بلاک چین دیگر کار می­کنند که به هیچ عنوان سازگار [[73]](#footnote-73) نمی­باشند و عملا در چنین حالتی ممکن است توکن های ارز رمز به 2 توکن متفاوت تجزیه شوند، به طور مثال پس از یکی از اپدیت های شبکه بیت کوین در سال 2016 میلادی با ایجاد فورک سخت توکن های شبکه به 2 نوع بیت کوین معمولی و بیت کوین کلاسیک [[74]](#footnote-74) تقسیم شدند به طوری که دارندگان کیف پول هریک نمی­توانند توکن های نوع دیگر را داشته باشند.



تصویر ‏3‑5: نمونه فورک سخت در بلاک چین

همانطور که در تصویر 3-5 مشاهده می­شود پس از یک فورک سخت بلاک چین به 2 بلاک چین متفاوت تبدیل می­شود و برخلاف حالت طولانی ترین زنجیره اینجا هر 2 زنجیره قابل قبول هستند اما نه توسط همه ند ها بلکه برخی ند ها یک زنجیره و برخی ند ها زنجیره دیگر را قبول کرده و روی زنجیره مورد نظر خود مشغول به کار می­شوند.

## مشکلات بلاک چین ها

شبکه های بلاک چینی نیز علی رغم همه مزیت هایی که به ارمغان می­آورند خالی از اشکال نیستند که در اینجا به برخی از اشکالات این شبکه ها اشاره مختصری می­کنیم.

یکی از ایرادات این شبکه به دلیل مکانیزم POW و مصرف انرژی بیش از حد رخ می­دهد که تلاش هایی برای حل این مشکل با سعی بر ایجاد کردن اثبات های متفاوت انجام شده است اما هیچکدام به کارآمدی اثبات کار یا POW نمی­باشند.

در بسیاری از بلاک چین ها امکان پرداخت های با مبلغ بسیار کم وجود ندارد[[75]](#footnote-75) که این خود می­تواند ناشی از عوامل مختلفی باشد، به طور مثال در شبکه بیت کوین برای هر تراکنش مبلغی نیز به عنوان هزینه تراکنش [[76]](#footnote-76) دریافت می­شود که اگر این مبلغ کمتر از حد معینی باشد ماینر ها رقبتی به پردازش آن تراکنش نخواهند داشت حال اگر فردی بخواهد تراکنشی با مبلغی کمتر از هزینه آن انجام دهد عملا غیر منطقی می­باشد.

یکی از مهمترین مشکلات نیز مشکل مقیاس پذیری [[77]](#footnote-77) در شبکه های بلاک چینی می­باشد. که در این حالت باتوجه به نیاز انجام کار مشخصی و سپری شدن زمانی برای افزوده شدن هر بلاک و همچنین محدودیتی که در حجم اطلاعاتی که بلاک می­تواند ذخیره کند وجود دارد باعث می­شود عملا در هر زمان بیش از تعداد معینی تراکنش قابل پردازش نباشند به طور مثال در شبکه بیت کوین تقریبا در هر ثانیه فقط 7 ترنزکشن قابلیت پردازش شدن را دارند که این باعث ایجاد محدودیت بسیاری در ساختار این شبکه و قابلیت های آن می­شود. همچنین به دلیل محدودیت تعداد تراکنش ها افراد مجبور می­شوند پیوسته هزینه پردازش تراکنش بیشتری پرداخت کنند تا استخراج کنندگان [[78]](#footnote-78) رغبت بیشتری به پردازش ترکنش آن­ها داشته باشند.

### هش گراف [[79]](#footnote-79)

باتوجه به مشکل مقیاس پذیری بسیاری از فعالات حوزه بلاک چین تلاش هایی برای حل این مشکل کردند یکی از راه حل های پیشنهاد شده برای مشکل مقیاس پذیری ایجاد هش گراف ها به جای هش چین ها یا همان بلاک چین ها می­باشد که در این حالت مشکل مقیاس پذیری تا حد زیادی حل می­شود و تعداد هزاران تراکنش در ثانیه قابلیت پردازش شدن خواهند داشت همچنین امکان انجام پرداخت های با مقادیر بسیار کم نیز وجود خواهد داشت.



تصویر ‏3‑6: مقایسه هش گراف با بلاکچین

همانطور که در تصویر 3-6 مشاهده می­شود در هش گراف به جای استفاده از قاعده طولانی ترین زنجیره سعی بر آن است تا بلاک های یتیم شده به صورتی مجدادا به شبکه بازگردانده شوند در این حالت به جای یک زنجیره یک گراف ایجاد می­شود که ند های آن با هش به یکدیگر مرتبط می­باشند.

## بلاک چین های نسل سوم [[80]](#footnote-80)

بلاک چین های نسل سوم نوع دیگری از بلاک چین های هستند که در پاسخ به مشکل مقیاس پذیری بلاک چین ایجاد شده اند به طوری که با حل این مشکل امکان پردازش تعداد نامحدود تراکنش با هر مبلغ را فراهم می­آورند. همچنین کاربرد دیگر آنها در موارد مرتبط به اینترنت اشیا [[81]](#footnote-81) می­باشد یکی از نمونه های موفق پیاده سازی بلاک چین های نسل سوم IOTA می­باشد.

### نحوه کارکرد بلاک چین های نسل سوم

در این بلاک چین ها به جای ذخیره کردن تعدادی تراکنش در یک بلاک و سپس پشت هم قرار دادن بلاک ها پشت یکدیگر تلاش می­شود تا تراکنش های بعدی به صورت مستقیم به تراکنش های قبل از خود متصل شوند، به طور دقیق تر هر تراکنش به 2 تراکنش تصادفی از تراکنش های قبلی خود متصل می­شود و بنابر این یک گراف از تراکنش ها ایجاد می­شود که این گراف در حقیقت یک گراف جهت دار رو به جلو در زمان خواهد بود چرا که هر تراکنش فقط به تراکنش های قبل از خود در زمان می­تواند متصل شود بنابر این یال های متصل کننده این تراکنش ها در گراف جهت دار هستند و همچنین به دلیل جهت دار بودن امکان ایجاد دور [[82]](#footnote-82) نیز در این گراف موجود نمی­باشد از این رو به آنها گراف های جهت دار بدون دور [[83]](#footnote-83) ویا به اختصار DAG گفته می­شود.



تصویر ‏3‑7: نمونه یک DAG

### پردازش تراکنش ها در بلاک چین های نسل سوم

در این نوع بلاک چین ها در حقیقت هر فرد برای ارسال تراکنش خود به جای پرداخت هزینه تراکنش به استخراج کنندگان تا آن­ها تراکنش فرد را تایید و پردازش و به شبکه اعلام کنند خود اقدام به اعلام کردن تراکنش خود ­می­کند با این تفاوت که برای افزودن تراکنش خود به شبکه موظف است 2 تراکنش قبل از خود را تایید کند و پس از تایید صحت آن 2 تراکنش، تراکنش خود را به انتهای آن­ها می­افزاید به این صورت ساختار DAG گفته شده از اتصال هر تراکنش به 2 تراکنش قبل از خود به وجود می­آید به این ترتیب و به دلیل عدم وجود هزینه تراکنش تراکنش های با هر مقدار ناچیز قابلیت افزوده شدن به شبکه را دارا می­باشند. همچنین به افزایش تعداد تراکنش ها مشکل ایجاد ترافیک برای تراکنش ها رخ نمی­دهد چرا که افزایش تعداد تراکنش ها به معنی افزایش تعداد ند های فعال در شبکه است که خود موظف به تایید تراکنش های قبل از خود می­باشند، بنابر این همواره با افزایش تعداد تراکنش ها تعداد تایید کنندگان تراکنش نیز افزایش می­یابد و شبکه دچار کندی نمی­شود.



تصویر ‏3‑8 : وضعیت تراکنش ها در یک DAG

همانطور که در تصویر 3-8 نشان داده شده است تراکنش ها در این نوع شبکه ها به 3 نوع مختلف تقسیم می­شوند تراکنش های کاملا تایید شده تراکنش های در دست تایید و تراکنش های جدید که به ترتیب با رنگ های سبز قرمز و خاکستری در تصویر قابل مشاهده می­باشند.

تراکنش های تایید شده تراکنش هایی اند که از هر تراکنش جدید شبکه پس از طی چند مرحله در گراف می­توان به آن­ها رسید، در حقیقت این بدان معنی است که این تراکنش ها سابقیه کاملی از تراکنش های قبلی را در خود دارند، تراکنش های تایید نشده که به رنگ قرمز هستند فقط به تعدادی از تراکنش های جدید متصل اند و تراکنش های جدید تراکنش هایی هستند که در انتظار افزوده شدن تراکنش جدید به انتهای خود و پردازش شدن توسط یک ند می­باشند.

## بلاک چین های نسل چهارم [[84]](#footnote-84)

این نوع بلاک چین ها که بلاک چین های هوشمند نیز معروفیت دارند در حقیقت تلاشی برای ایجاد اتصال میان حوزه های هوش مصنوعی [[85]](#footnote-85) و به خصوص یادگیری عمیق [[86]](#footnote-86) با بلاک چین می­باشند از پروژه های معروف بلاک چین های نسل چهارمی می­توان به SingularityNet و Deep Brain Chain اشاره کرد.

## بلاک چین در خارج از رمز ارزها

همانطور که پیشتر گفته شد بلاک چین فقط مختص به رمز ارزها نمی­شود و قابلیت های این تکنولوژی انقلابی می­تواند در بسیاری از صنایع دیگر نیز مورد استفاده قرار گیرد به طور مثال در اینجا به بررسی کاربرد بلاک چین در یک شبکه فروش اقساطی خودرو می­پردازیم.

كارخانه­هاي سازنده­ي خودرو خريد قسطي خودرو را ساده جلوه ميدهند، اما اين كار در واقعيت ميتواند كاملا پيچيده باشد. چالش مهمي كه اين روزها شبكه­هاي خريد قسطي خودرو با آن روبهرو هستند اين است كه هرچند زنجیه تامین فیزیکی معمولا یک­پارچه است ، اما هر مشارکت کننده در شبکه و سامانه های پشتیبان از هم جدا هستند که هرکدام از این­ها باید دفتر کل مخصوص به خود را نگه داری کنند همچنین از طرفی نیز مراجع حقوقی که وظیفه ثبت مالکیت و سند را بر عهده دارند دفتر کل خود را دارند و پلیس نیز باید دفتر کل خود را برای شماره گذاری خودرو ها داشته باشد و از طرفی بانک ها نیز دفتر کل خود را برای پرداخت اقساط دارند با وجود این همه سازمان مختلف و دفتر کل های متفاوت هماهنگی میان این مراجعه بسیار سخت صورت می­گیرد و گاها بسیار دردسر ساز است اما درصورت استفاده از بلاک چین بسیاری از مشکلات حل می­شوند. به طوری که هریک از مشارکت کنندگان می­توانند به راحتی بلاک چین را رسد کرده و اطلاعات مورد نظر خود را از آن برداشته و تراکنش های مورد نظر خود را بی افزایند.



تصویر ‏3‑9: رهگیری مالکیت خودرو بدون بلاک چین



تصویر ‏3‑10: رهگیری مالکیت خودرو با بلاک چین

# فصل چهارم : بررسی کارکرد چند رمز ارز مهم

باتوجه به این که شبکه های بلاک چین اغلب برای رمز ارز ها استفاده می­شوند برای درک کامل مدل کارکرد آن­ها لازم به نظر می­رسد تا ابتدا به بررسی کارکرد چند رمز ارز مهم دنیای فناوری بپردازیم.

## بیت کوین

1. Gold Standard [↑](#footnote-ref-1)
2. به طور مثال هر یک ریال ایران برابر یکصدوهشت‌هزاروپنجاه‌وپنج‌ده‌میلیونیم (۰٫۰۱۰۸۰۵۵) گرم [طلای](https://fa.wikipedia.org/wiki/%D8%B7%D9%84%D8%A7) خالص است. [↑](#footnote-ref-2)
3. Fiat Currency [↑](#footnote-ref-3)
4. Credit Card [↑](#footnote-ref-4)
5. Debit Card [↑](#footnote-ref-5)
6. ATM [↑](#footnote-ref-6)
7. POS [↑](#footnote-ref-7)
8. Digital Currency [↑](#footnote-ref-8)
9. Crypto Currency [↑](#footnote-ref-9)
10. Liberty Reserve [↑](#footnote-ref-10)
11. Digital signature [↑](#footnote-ref-11)
12. Proof-of-Work [↑](#footnote-ref-12)
13. Peer-To­-Peer [↑](#footnote-ref-13)
14. consensus [↑](#footnote-ref-14)
15. BitCoin [↑](#footnote-ref-15)
16. Block Chain [↑](#footnote-ref-16)
17. cryptography [↑](#footnote-ref-17)
18. Enigma Machine [↑](#footnote-ref-18)
19. Alan Mathison Turing [↑](#footnote-ref-19)
20. Advanced Encryption Standard [↑](#footnote-ref-20)
21. [Symmetric-key](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) [↑](#footnote-ref-21)
22. Public-key cryptography, or asymmetric cryptography [↑](#footnote-ref-22)
23. Public Key [↑](#footnote-ref-23)
24. Private Key [↑](#footnote-ref-24)
25. Rivest–Shamir–Adleman [↑](#footnote-ref-25)
26. elliptic curve cryptography [↑](#footnote-ref-26)
27. Diffie–Hellman key exchange [↑](#footnote-ref-27)
28. Hypertext Transfer Protocol Secure [↑](#footnote-ref-28)
29. Hash Function [↑](#footnote-ref-29)
30. Quantum computer [↑](#footnote-ref-30)
31. Shor's algorithm [↑](#footnote-ref-31)
32. Quantum cryptography [↑](#footnote-ref-32)
33. Hash Table [↑](#footnote-ref-33)
34. Cryptographic hash function [↑](#footnote-ref-34)
35. Merkle tree [↑](#footnote-ref-35)
36. Binary Tree [↑](#footnote-ref-36)
37. Trie [↑](#footnote-ref-37)
38. Lamport Signature [↑](#footnote-ref-38)
39. Character encoding [↑](#footnote-ref-39)
40. Character [↑](#footnote-ref-40)
41. American Standard Code for Information Interchange [↑](#footnote-ref-41)
42. Client-Server [↑](#footnote-ref-42)
43. Peer [↑](#footnote-ref-43)
44. Virtual Machine [↑](#footnote-ref-44)
45. Java [↑](#footnote-ref-45)
46. .Net [↑](#footnote-ref-46)
47. Jave Virtual Machine [↑](#footnote-ref-47)
48. Common Language Runtime [↑](#footnote-ref-48)
49. CPU [↑](#footnote-ref-49)
50. Assembly [↑](#footnote-ref-50)
51. Ethereum Virtual Machine [↑](#footnote-ref-51)
52. Satoshi Nakamoto [↑](#footnote-ref-52)
53. Transaction [↑](#footnote-ref-53)
54. Node [↑](#footnote-ref-54)
55. Sync [↑](#footnote-ref-55)
56. Difficulty [↑](#footnote-ref-56)
57. Mining [↑](#footnote-ref-57)
58. Block Reward [↑](#footnote-ref-58)
59. Proofs [↑](#footnote-ref-59)
60. Proof Of Stake [↑](#footnote-ref-60)
61. Proof Of Capacity [↑](#footnote-ref-61)
62. Proof Of Burn [↑](#footnote-ref-62)
63. Block chain 2.0 [↑](#footnote-ref-63)
64. Turing completeness [↑](#footnote-ref-64)
65. Ethereum [↑](#footnote-ref-65)
66. Smart Contract [↑](#footnote-ref-66)
67. Longest Chain Is Valid [↑](#footnote-ref-67)
68. Orphaned Blocks [↑](#footnote-ref-68)
69. Fork [↑](#footnote-ref-69)
70. Update [↑](#footnote-ref-70)
71. Soft Fork [↑](#footnote-ref-71)
72. Hard Fork [↑](#footnote-ref-72)
73. Compatible [↑](#footnote-ref-73)
74. Bitcoin Classic [↑](#footnote-ref-74)
75. Micro Payment [↑](#footnote-ref-75)
76. Transaction Fee [↑](#footnote-ref-76)
77. Scalability [↑](#footnote-ref-77)
78. Miners [↑](#footnote-ref-78)
79. HashGraph [↑](#footnote-ref-79)
80. Block Chain 3.0 [↑](#footnote-ref-80)
81. IOT [↑](#footnote-ref-81)
82. Cycle [↑](#footnote-ref-82)
83. Directed Acyclic Graph [↑](#footnote-ref-83)
84. Block Chain 4.0 [↑](#footnote-ref-84)
85. artificial intelligence [↑](#footnote-ref-85)
86. Deep Learning [↑](#footnote-ref-86)