دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی

طراحی و پیاده سازی سامانه زنجیره تأمین مبتنی بر زنجیره بلوکی با بررسی صحت فرادادهها

نگارنده

سید سپهرمیرنصرالهی پارسا

استاد راهنما

دکتر حمیدرضا زرندی

شهریور ۱۴۰۴

دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)

به نام خدا

تعهدنامه اصالت اثر

تاریخ: شهریور ۱۴۰۴

اینجانب **سید سپهرمیرنصرالهی پارسا** متعهد می‌شوم که مطالب مندرج در این پایان‌نامه حاصل کار پژوهشی اینجانب تحت نظارت و راهنمایی اساتید دانشگاه صنعتی امیرکبیر بوده و به دستاوردهای دیگران که در این پژوهش از آنها استفاده شده است مطابق مقررات و روال متعارف ارجاع و در فهرست منابع و مآخذ ذکر گردیده است. این پایان‌نامه قبلاً برای احراز هیچ مدرک هم‌سطح یا بالاتر ارائه نگردیده است.

در صورت اثبات تخلف در هر زمان، مدرک تحصیلی صادر شده توسط دانشگاه از درجه اعتبار ساقط بوده و دانشگاه حق پیگیری قانونی خواهد داشت.

کلیه نتایج و حقوق حاصل از این پایان‌نامه متعلق به دانشگاه صنعتی امیرکبیر می‌باشد. هرگونه استفاده از نتایج علمی و عملی، واگذاری اطلاعات به دیگران یا چاپ و تکثیر، نسخه‌برداری، ترجمه و اقتباس از این پایان نامه بدون موافقت کتبی دانشگاه صنعتی امیرکبیر ممنوع است. نقل مطالب با ذکر مآخذ بلامانع است.

سید سپهرمیرنصرالهی پارسا

امضا

سپاس گزاری

با سپاس فراوان ازجناب آقای دکتر زرندی به عنوان استاد مشاور این پایان نامه و جناب آقای دکترجوادی به عنوان استاد داور، که با راهنمایی ها و نظرات ارزشمند خود نقش بسزایی در پیشبرد این پژوهش داشتند.

سید سپهر میرنصرالهی پارسا
شهریور ۱۴۰۴

چکیده

هدف از پایان‌نامه نگارش شده، گزارشی از ساخت سامانه زنجیره تأمین با هدف حل چالش‌های این حوزه در دنیای واقعی میباشد. هسته اصلی این سامانه، یک قرارداد هوشمند است که با زبان برنامه‌نویسی $Solidity$ بر روی یک شبکه سازگار با ماشین مجازی اتریوم (EVM) پیاده‌سازی شده است. در این قرارداد از استاندارد توکن $ERC1155$ استفاده شده که امکان مدیریت بهینه و همزمان محصولات مثلی و غیرمثلی را با هزینه تراکنش کمتر فراهم می‌کند. یکی از ویژگی‌های کلیدی این پروژه، تضمین صحت فراداده‌ها از طریق تولید هش $Keccak256$ برای هر محصول است. این مکانیزم به تمام ذی‌نفعان زنجیره اجازه می‌دهد تا اصالت و اطلاعات محصول را در هر مرحله اعتبارسنجی کنند. این سیستم شامل نقش‌های دسترسی متفاوتی مانند تولیدکننده، توزیع‌کننده، خرده‌فروش و گمرک است که هر یک مجوزهای خاص خود را برای ثبت، انتقال یا ابطال محصول دارند. علاوه بر این، یک قابلیت نوآورانه برای محاسبه خودکار مالیات در هر مرحله از انتقال مالکیت در قرارداد هوشمند تعبیه شده است. و در نهایت، این پروژه یک راهکار عملی و جامع ارائه می‌دهد که با افزایش شفافیت، قابلیت ردیابی و تضمین اصالت کالا، می‌تواند به طور مؤثری با تقلب مبارزه کرده و اعتماد را به اکوسیستم زنجیره تأمین بازگرداند.

واژه‌های کلیدی:

زنجیره تأمین، قرارداد هوشمند، $ERC1155$، $Solidity$، اصالت کالا

فهرست مطالب

عنوان صفحه

فهرست اشکال

شکل صفحه

فهرست جداول

جدول صفحه

فصل اول

مقدمه

۱-۱ بیان مسئله و اهمیت موضوع

زنجیره تأمین، شبکه‌ای پیچیده و حیاتی از سازمان‌ها، افراد، فعالیت‌ها، اطلاعات و منابع است که در حرکت یک محصول یا خدمت از تأمین‌کننده به مصرف‌کننده نهایی نقش دارد. این زنجیره نه تنها جریان فیزیکی کالاها، بلکه جریان اطلاعات و مالی را نیز در بر می‌گیرد. کارایی و سلامت زنجیره تأمین به عنوان یکی از ارکان اساسی اقتصاد مدرن، نقشی مستقیم در رشد اقتصادی، ثبات بازار و رفاه اجتماعی یک کشور ایفا می‌کند. یک زنجیره تأمین کارآمد، هزینه‌ها را کاهش می‌دهد، دسترسی مصرف‌کنندگان به کالاها را تسهیل می‌کند و مزیت رقابتی برای تولیدکنندگان داخلی در بازارهای جهانی ایجاد می‌نماید.

با وجود این اهمیت استراتژیک، صنعت زنجیره تأمین در ایران و بسیاری از نقاط جهان با چالش‌ها و مشکلات ساختاری عمیقی مواجه است که کارایی و اعتبار آن را به شدت زیر سؤال برده است. این مشکلات صرفاً به ناکارآمدی‌های لجستیکی محدود نمی شود، بلکه یک بحران جدی در شفافیت، اعتماد و امنیت را شامل می‌گردد که تمام بازیگران این اکوسیستم، از تولیدکننده تا مصرف‌کننده، را تحت تأثیر قرار می‌دهد.

۱-۱-۱ بحران اعتماد و شفافیت در زنجیره‌های تأمین سنتی

یکی از بزرگ‌ترین چالش‌های موجود، در فرآیندهای زنجیره تأمین است. این عدم شفافیت، بستری مناسب برای بروز مشکلات متعددی فراهم آورده است که در ادامه به تفصیل بررسی می‌شوند:

گسترش پدیده جعل و تقلب در محصولات

جعل محصولات یکی از مخرب‌ترین پیامدهای یک زنجیره تأمین غیرشفاف است. این معضل دیگر به کالاهای لوکس محدود نیست و دامنه آن به حوزه‌های حیاتی مانند صنایع تولیدی و غذایی نیز کشیده شده است. کالاهای تقلبی نه تنها با ارائه کیفیت نازل به اعتبار برندهای معتبر آسیب می‌زنند و موجب خسارات اقتصادی هنگفت می‌شوند، بلکه در موارد حساس مانند دارو و قطعات صنعتی، می‌توانند سلامت و ایمنی مصرف‌کنندگان را به طور جدی به خطر اندازند. در یک سیستم سنتی، هنگامی که یک محصول از کارخانه خارج می‌شود، ردیابی دقیق آن در هر مرحله از توزیع، انبارداری و فروش تقریبا غیرممکن است. این گسست اطلاعاتی، به عوامل سودجو اجازه می‌دهد تا کالاهای تقلبی را به راحتی وارد چرخه توزیع کرده و به دست مصرف‌کننده برسانند.

نوسانات کیفیت و عدم امکان ریشه‌یابی

فقدان یک سیستم ردیابی یکپارچه، کنترل و تضمین کیفیت محصول در طول زنجیره را به امری دشوار تبدیل کرده است. یک محصول ممکن است در مرحله تولید از کیفیت بالایی برخوردار باشد، اما به دلیل شرایط نگهداری نامناسب در انبار، حمل‌ونقل غیراصولی یا تأخیر در توزیع، کیفیت خود را از دست بدهد. در سیستم‌های سنتی، زمانی که یک مصرف‌کننده با محصولی بی‌کیفیت مواجه می‌شود، ریشه‌یابی دقیق

اینکه کدام حلقه از زنجیره مسئول این افت کیفیت بوده، بسیار پیچیده و گاهی ناممکن است. این امر، پاسخگو نگه داشتن عاملان را دشوار کرده و از بهبود مستمر فرآیندها جلوگیری می‌کند.

عدم شفافیت در مسیر واردات و توزیع

در زنجیره‌های تأمین بین‌المللی، کالاها از مراحل متعددی مانند گمرک، شرکت‌های حمل‌ونقل مختلف و انبارهای متعدد عبور می‌کنند. هر یک از این مراحل می‌تواند نقطه بالقوه‌ای برای بروز فساد، تأخیرهای بی‌دلیل و ورود کالاهای قاچاق باشد. کمبود شفافیت در این مسیر، نظارت دقیق بر اصالت و سلامت کالا را برای نهادهای نظارتی و همچنین واردکنندگان دشوار می‌سازد و به اقتصاد غیررسمی دامن می‌زند.

۱-۱-۲ آسیب‌پذیری‌های معماری در سیستم‌های مدیریت متمرکز

ریشه بسیاری از مشکلات ذکر شده، در معماری فنی سیستم‌های مدیریتی نهفته است که در حال حاضر بر زنجیره‌های تأمین حاکم هستند. این سیستم‌ها غالباً بر پایه پایگاه‌های داده متمرکز طراحی شده‌اند که هر سازمان یا شرکت، داده‌های خود را در سیلوهای اطلاعاتی مجزا نگهداری می‌کند. این معماری دارای نقاط ضعف بنیادینی است:

- **آسیب‌پذیری در برابر دستکاری:** در یک سیستم متمرکز، یک نهاد واحد (صاحب سرور) کنترل کاملی بر روی اطلاعات دارد. این موضوع، داده‌ها را هم در برابر حملات سایبری خارجی و هم در برابر دستکاری‌های داخلی توسط افراد دارای مجوز، به شدت آسیب‌پذیر می‌کند. یک تغییر کوچک و غیرقابل ردیابی در داده‌های مربوط به تاریخ تولید یا مبدأ کالا، می‌تواند کل زنجیره را با اطلاعات نادرست تغذیه کند.
- **عدم وجود یک منبع حقیقت واحد** [1]: هر یک از شرکت‌کنندگان در زنجیره تأمین (تولیدکننده، شرکت حمل‌ونقل، توزیع‌کننده، خرده‌فروش) پایگاه داده و سیستم مدیریتی خود را دارد. این جزیره‌ای بودن اطلاعات باعث می‌شود که هماهنگ‌سازی داده‌ها بین این سیستم‌ها به صورت دستی، با تأخیر و با احتمال بالای خطا انجام شود. این نبود یکپارچگی، منجر به ناکارآمدی‌های عملیاتی و عدم امکان مشاهده یک تصویر کامل و دقیق از وضعیت لحظه‌ای یک محصول می‌شود.
- **پیچیدگی و هزینه بالا:** نگهداری و تأمین امنیت زیرساخت‌های متمرکز، به خصوص برای شرکت‌های کوچک و متوسط، هزینه‌بر و پیچیده است. این در حالی است که تعامل و یکپارچه‌سازی این سیستم‌های ناهمگون نیز خود به پروژه‌های نرم‌افزاری گران‌قیمت و زمان‌بر نیاز دارد.

[1] *Single Source of Truth*

۱-۱-۳ پیامدهای اقتصادی و اجتماعی

مجموعه این چالش‌ها، پیامدهای گسترده‌ای برای اقتصاد و جامعه به همراه دارد. مهم‌ترین پیامد، است. زمانی که مصرف‌کنندگان نتوانند به اصالت و کیفیت کالایی که خریداری می‌کنند اطمینان داشته باشند، تمایل آن‌ها برای خرید محصولات داخلی و حمایت از برندهای معتبر کاهش می‌یابد. این امر مستقیماً به تولید ملی و اعتبار برندها لطمه می‌زند.

از منظر اقتصادی، ناکارآمدی‌های موجود در زنجیره تأمین منجر به افزایش هزینه‌های عملیاتی، اتلاف منابع و کاهش قدرت رقابت‌پذیری کسب‌وکارها در سطح ملی و بین‌المللی می‌شود. در نهایت، این مسائل نشان می‌دهند که مشکلات موجود در زنجیره تأمین، سطحی و قابل حل با راهکارهای مقطعی نیستند، بلکه ریشه در یک ضعف ساختاری عمیق در معماری اعتماد و جریان اطلاعات دارند. بنابراین، برای عبور از این بحران، نیاز به یک تغییر مفهوم اساسی و بهره‌گیری از فناوری‌های نوینی است که بتوانند شفافیت، امنیت و تغییرناپذیری را به اکوسیستم بازگردانند. اهمیت این موضوع، ضرورت تحقیق و توسعه راهکارهای جایگزین، مانند آنچه در این پروژه ارائه خواهد شد را دوچندان می‌کند.

۱-۲ فناوری زنجیره بلوکی به عنوان راهکار

در پاسخ به چالش‌های عمیق و ساختاری حاکم بر زنجیره‌های تأمین سنتی، که در بخش پیشین به تفصیل بررسی شد، نیاز به یک تغییر مفهوم اساسی احساس می‌شود. راهکارهای مقطعی و بهبودهای جزئی در سیستم‌های متمرکز، قادر به حل ریشه‌ای بحران اعتماد و شفافیت نیستند. در این میان، فناوری زنجیره بلوکی [۲] به عنوان یک رویکرد نوین و بنیادین، ظرفیت‌های بی‌نظیری برای بازمهندسی فرآیندهای زنجیره تأمین ارائه می‌دهد. این فناوری صرفاً یک ابزار جدید نیست، بلکه یک معماری کاملاً متفاوت برای ثبت، اشتراک‌گذاری و مدیریت اطلاعات است که می‌تواند شفافیت، امنیت و کارایی را به طور همزمان به اکوسیستم تزریق کند. در ادامه، به بررسی ابعاد مختلف این فناوری، از تاریخچه و مبانی فنی آن گرفته تا کاربرد مستقیم آن در قالب قراردادهای هوشمند، می‌پردازیم تا درک عمیق‌تری از چرایی انتخاب آن به عنوان راهکار اصلی این پروژه حاصل شود.

۱-۲-۱ نگاهی تاریخی به فناوری زنجیره بلوکی

برای درک اهمیت و جایگاه امروزی زنجیره بلوکی، باید به سیر تکاملی اینترنت و نیازهایی که در هر دوره به وجود آمد، نگاهی بیندازیم. این تاریخچه به ما نشان می‌دهد که زنجیره بلوکی، پاسخی طبیعی به محدودیت‌های نسل‌های پیشین وب بوده است.

---

[۲] *Blockchain*

از وب ۰.۱ تا بحران تمرکزگرایی در وب ۰.۲

دوران اولیه اینترنت، معروف به وب ۰.۱ (تقریبا از ۱۹۹۱ تا ۲۰۰۴)، به وب فقط خواندنی شهرت داشت. در این دوره، محتوا عمدتاً ایستا بود و توسط تعداد محدودی از سازمان‌ها و افراد تولید و بر روی وب‌سایت‌ها منتشر می‌شد. کاربران عمدتاً مصرف‌کنندگان غیرفعال اطلاعات بودند و تعامل چندانی وجود نداشت.

با ظهور وب ۰.۲، مفهوم به کلی تغییر کرد و وب تعاملی و اجتماعی متولد شد[۱]. بسترهایی مانند فیسبوک، اینستاگرام و یوتیوب به کاربران عادی این قدرت را دادند که به سادگی و بدون نیاز به دانش فنی، خود به تولیدکنندگان محتوا تبدیل شوند. این تحول، منجر به انفجار تولید محتوا و ایجاد شبکه‌های اجتماعی گسترده شد. با این حال، این آزادی و سهولت، هزینه‌ای پنهان به همراه داشت: تمرکزگرایی شدید قدرت و داده. معماری وب ۰.۲ بر پایه سرورهای متمرکز شرکت‌های بزرگ بنا شده است. این شرکت‌ها با ارائه خدمات رایگان، کاربران را جذب کرده و در ازای آن، به بزرگ‌ترین دارایی آن‌ها، یعنی داده‌های شخصی‌شان، دسترسی پیدا کردند. مدل کسب‌وکار این غول‌های فناوری، عمدتاً بر دو پایه استوار شد: تبلیغات هدفمند یا فروش مستقیم اطلاعات کاربران به اشخاص ثالث[۲]. این ساختار متمرکز، مشکلات بنیادینی را به وجود آورد:

- **مالکیت داده:** کاربران، مالک واقعی داده‌های خود نبودند و کنترلی بر نحوه استفاده از آن نداشتند.
- **سانسور و کنترل:** شرکت‌های متمرکز می‌توانستند به صورت سلیقه‌ای محتوا را حذف کرده یا دسترسی کاربران را مسدود کنند.
- **تک نقطه خرابی** [۳]: تمرکز داده‌ها بر روی سرورهای یک شرکت، آن‌ها را به هدفی جذاب برای حملات سایبری تبدیل کرد و از کار افتادن این سرورها به معنای قطع شدن سرویس برای میلیون‌ها کاربر بود.

ظهور بیت‌کوین و مفهوم عدم تمرکز

در چنین فضایی، نیاز به سیستمی که بتواند اعتماد و تعامل را بدون نیاز به یک واسطه متمرکز فراهم کند، به شدت احساس می‌شد. در سال ۲۰۰۸، فرد یا گروهی ناشناس با نام مستعار ساتوشی ناکاموتو، با انتشار وایت‌پیپر بیت‌کوین، راهکاری انقلابی ارائه داد. بیت‌کوین یک سیستم پول نقد الکترونیکی همتا به همتا بود که به کاربران اجازه می‌داد بدون نیاز به بانک یا هر مؤسسه مالی دیگری، به یکدیگر پول انتقال دهند. هسته اصلی این نوآوری، فناوری زنجیره بلوکی بود؛ یک پایگاه داده خاص که داده‌ها را در بلوک‌هایی ذخیره می‌کند که به صورت رمزنگاری شده به یکدیگر متصل هستند. این ساختار زنجیره‌ای، داده‌ها را به ترتیب زمانی مرتب کرده و مهم‌تر از آن، تغییرناپذیر می‌ساخت. هر تراکنش ثبت‌شده در زنجیره بلوکی بیت‌کوین، برای همیشه در آن باقی می‌ماند و برای همه قابل مشاهده بود، که این شفافیت، امنیت بالایی را در برابر تقلب و کلاهبرداری ایجاد می‌کرد[۳].

[۳] *Single Point of Failure*

عصر اتریوم و تولد وب ۰.۳

بیت‌کوین ثابت کرد که می‌توان اعتماد را به صورت غیرمتمرکز ایجاد کرد، اما کاربرد آن عمدتاً به تراکنش‌های مالی محدود بود. جهش بزرگ بعدی با ظهور اتریوم رخ داد. اتریوم با گسترش ایده زنجیره بلوکی، این امکان را فراهم آورد که نه تنها اعداد (مانند مبالغ تراکنش)، بلکه کد اجرایی نیز بر روی زنجیره بلوکی ذخیره و اجرا شود[۴]. این نوآوری، منجر به پیدایش قراردادهای هوشمند و برنامه‌های غیرمتمرکز [۴]شد[۴، ۵].

این تحول، زمینه را برای شکل‌گیری وب ۰.۳ فراهم کرد. وب ۰.۳ که به آن وب غیرمتمرکز نیز گفته می‌شود، چشم‌اندازی از اینترنت است که در آن کاربران کنترل داده‌ها و هویت دیجیتال خود را پس می‌گیرند. ویژگی‌های اصلی وب ۰.۳ که مستقیماً از فناوری زنجیره بلوکی نشأت می‌گیرند، عبارتند از:

- **غیرمتمرکز بودن** [۵]: کنترل در دست کاربران و جامعه است، نه شرکت‌های بزرگ.
- **بی‌نیاز به اعتماد** [۶]: تعاملات بر اساس قوانین شفاف و تغییرناپذیر کد انجام می‌شود، نه اعتماد به یک واسطه.
- **بی‌نیاز به مجوز** [۷]: هر کسی می‌تواند بدون نیاز به کسب اجازه از یک نهاد مرکزی، در شبکه مشارکت کرده و سرویس ایجاد کند.
- **دارای پرداخت‌های درون‌ساختی** [۸]: تراکنش‌های مالی جزئی جدایی‌ناپذیر از پروتکل است و نیازی به سیستم‌های پرداخت خارجی نیست.

این سیر تکاملی نشان می‌دهد که زنجیره بلوکی، صرفاً یک فناوری برای رمزارزها نیست، بلکه زیرساختی برای نسل بعدی اینترنت و برنامه‌های کاربردی است که می‌توانند صنایع مختلف، از جمله زنجیره تأمین را متحول سازند.

۱-۲-۲ مبانی رمزنگاری در زنجیره بلوکی

امنیت، یکپارچگی و تغییرناپذیری زنجیره بلوکی، بر ستون‌های مستحکم علم رمزنگاری [۹] استوار است. بدون رمزنگاری، اعتماد به یک سیستم غیرمتمرکز که توسط افراد ناشناس اداره می‌شود، غیرممکن بود. دو مفهوم کلیدی رمزنگاری که در قلب زنجیره بلوکی قرار دارند، توابع درهم‌سازی و رمزنگاری کلید عمومی هستند.

---

[۴] *DApps*
[۵] *Decentralized*
[۶] *Trustless*
[۷] *Permissionless*
[۸] *Native Payments*
[۹] *Cryptography*

توابع درهم‌سازی و یکپارچگی داده‌ها

تابع درهم‌سازی، یک الگوریتم ریاضی است که هر ورودی با هر اندازه‌ای را دریافت کرده و یک خروجی با اندازه ثابت تولید می‌کند. این خروجی که به آن متن درهم‌سازی شده گفته می‌شود، مانند اثر انگشت دیجیتال برای داده ورودی عمل می‌کند. توابع درهم‌سازی مورد استفاده در زنجیره بلوکی، مانند $Keccak256$ که در این پروژه نیز به کار گرفته شده است[۶]، دارای سه ویژگی اساسی هستند:

۱. **قطعیت** [۱۰]: یک ورودی مشخص، همواره متن درهم‌سازی شده یکسانی تولید می‌کند.

۲. **مقاومت در برابر پیش‌تصویر** [۱۱]: محاسبه ورودی از روی متن درهم‌سازی شده خروجی، از نظر محاسباتی غیرممکن است.

۳. **اثر بهمنی** [۱۲]: کوچک‌ترین تغییری در داده ورودی، منجر به تولید یک متن درهم‌سازی شده خروجی کاملاً متفاوت می‌شود.

این ویژگی‌ها کاربردهای حیاتی در زنجیره بلوکی دارند. اولاً، برای اطمینان از یکپارچگی داده‌ها به کار می‌روند. در پروژه حاضر، با محاسبه متن درهم‌سازی شده اطلاعات هر محصول و ثبت آن بر روی زنجیره، تضمین می‌شود که این اطلاعات پس از ثبت، به هیچ عنوان دستکاری نشده‌اند. هرگونه تلاشی برای تغییر جزئیات محصول، منجر به تولید یک متن درهم‌سازی شده متفاوت شده و به راحتی قابل تشخیص خواهد بود. ثانیاً، برای ایجاد زنجیره به کار می‌روند. هر بلوک در زنجیره، علاوه بر داده‌های خود، متن درهم‌سازی شده بلوک قبلی را نیز در خود ذخیره می‌کند. این وابستگی زنجیره‌ای باعث می‌شود که تغییر اطلاعات یک بلوک، نیازمند محاسبه مجدد متن درهم‌سازی شده تمام بلوک‌های بعدی باشد که این امر از نظر محاسباتی، دستکاری تاریخچه را غیرممکن می‌سازد و به کل سیستم، خاصیت تغییرناپذیری می‌بخشد.

رمزنگاری کلید عمومی و هویت دیجیتال

یکی دیگر از ارکان رمزنگاری در زنجیره بلوکی، سیستم رمزنگاری نامتقارن یا کلید عمومی است. در این سیستم، هر کاربر دارای یک جفت کلید است: یک کلید خصوصی و یک کلید عمومی.

- **کلید خصوصی** [۱۳]: این کلید باید به صورت کاملاً محرمانه توسط کاربر نگهداری شود. کاربرد اصلی آن، امضای دیجیتال تراکنش‌هاست. وقتی کاربر یک تراکنش (مانند انتقال مالکیت یک کالا) را با کلید خصوصی خود امضا می‌کند، در واقع در حال اثبات مالکیت خود بر آن دارایی و تأیید صحت آن تراکنش است.

---

[۱۰] $Deterministic$
[۱۱] $Pre-imageResistance$
[۱۲] $Avalanche\ Effect$
[۱۳] $Private\ Key$

- **کلید عمومی** [۱۴]: این کلید از روی کلید خصوصی تولید می‌شود و می‌توان آن را به صورت عمومی با دیگران به اشتراک گذاشت. از کلید عمومی، آدرس کاربر در شبکه استخراج می‌شود که برای دریافت دارایی‌ها به کار می‌رود. دیگران می‌توانند با استفاده از کلید عمومی یک کاربر، امضای دیجیتال او را اعتبارسنجی کرده و مطمئن شوند که تراکنش واقعاً توسط مالک کلید خصوصی مربوطه ارسال شده است.

این سازوکار، یک سیستم هویت و احراز هویت دیجیتال قدرتمند و غیرمتمرکز ایجاد می‌کند. کاربران برای تعامل با شبکه، نیازی به ثبت‌نام در یک مرجع مرکزی و ارائه اطلاعات هویتی خود ندارند[۳]. کلیدهای آن‌ها، هویت دیجیتالشان است. این ویژگی، ضمن حفظ حریم خصوصی، امکان تعامل امن و قابل اعتماد بین طرفین ناشناس را فراهم می‌آورد که برای یک زنجیره تأمین جهانی امری ضروری است.

۱-۲-۳ قراردادهای هوشمند: انقلابی در توافقات دیجیتال

اگر زنجیره بلوکی را یک سیستم عامل غیرمتمرکز در نظر بگیریم، قراردادهای هوشمند [۱۵] برنامه‌هایی هستند که بر روی این سیستم عامل اجرا می‌شوند. این مفهوم که با ظهور اتریوم به بلوغ رسید، زنجیره بلوکی را از یک سیستم صرفاً تراکنشی به یک بستر محاسباتی جهانی تبدیل کرد.

تعریف و ماهیت قرارداد هوشمند

یک قرارداد هوشمند، یک برنامه کامپیوتری یا پروتکل تراکنش است که به صورت خودکار، اقدامات و توافقات مشخصی را اجرا، کنترل یا مستند می‌کند. به زبان ساده‌تر، یک قرارداد هوشمند، کدی است که عملیات خاصی را اجرا می‌نماید و می‌تواند با سایر قراردادهای هوشمند تعامل داشته باشد[۷]. این کد، پس از نوشته شدن، بر روی زنجیره بلوکی مستقر [۱۶] می‌شود و از آن پس، به صورت مستقل و خودکار بر اساس منطق برنامه‌ریزی شده خود عمل می‌کند.

جایگزینی واسطه‌های شخص ثالث

قدرت واقعی قراردادهای هوشمند در توانایی آن‌ها برای حذف واسطه‌های شخص ثالث نهفته است[۴]. در دنیای سنتی، اجرای توافقات نیازمند اعتماد به واسطه‌هایی مانند بانک‌ها، دفاتر اسناد رسمی، وکلا یا بسترهای آنلاین است. این واسطه‌ها وظیفه تضمین اجرای صحیح قرارداد و حل اختلافات را بر عهده دارند و در ازای آن، کارمزد دریافت می‌کنند و فرآیند را کند و پیچیده می‌سازند. قراردادهای هوشمند این نقش را به کد منتقل می‌کنند. همان گونه که بیت‌کوین نیاز به نگهداری پول شما توسط بانک را از بین می‌برد، اتریوم نیز با استفاده از قراردادهای هوشمند، نیازی به شخصی برای نظارت بر تراکنش و

[۱۴] *Public Key*
[۱۵] *Smart Contracts*
[۱۶] *Deploy*

یا معامله ندارد[۴]. قوانین توافق (مانند شرایط انتقال مالکیت یک کالا در زنجیره تأمین) یک بار در کد قرارداد نوشته می‌شود و از آن پس، شبکه غیرمتمرکز زنجیره بلوکی، اجرای بی‌طرفانه و دقیق آن قوانین را تضمین می‌کند.

ویژگی‌های کلیدی قراردادهای هوشمند

ویژگی‌های قراردادهای هوشمند مستقیماً از ماهیت زنجیره بلوکی که بر روی آن اجرا می‌شوند، به ارث برده شده است:

- **تغییرناپذیری و قطعیت** [۱۷]: پس از استقرار یک قرارداد هوشمند بر روی زنجیره بلوکی، کد آن دیگر به هیچ عنوان قابل تغییر نیست[۸]. این ویژگی تضمین می‌کند که قوانین بازی در حین اجرا تغییر نخواهد کرد و همه شرکت‌کنندگان می‌توانند با اطمینان کامل به آن تکیه کنند.
- **شفافیت و قابلیت حسابرسی** [۱۸]: کد قرارداد هوشمند و تمام تراکنش‌هایی که با آن انجام می‌شود، به صورت عمومی بر روی زنجیره بلوکی ثبت شده و برای همگان قابل مشاهده است[۸]. این شفافیت، امکان حسابرسی کامل فرآیندها را فراهم کرده و از اقدامات پنهانی جلوگیری می‌کند.
- **عدم تمرکز و پایداری** [۱۹]: قرارداد هوشمند بر روی یک سرور مرکزی اجرا نمی‌شود، بلکه بر روی هزاران گره [۲۰] در سراسر شبکه توزیع شده است. این ساختار غیرمتمرکز باعث می‌شود که قرارداد در برابر سانسور و حملات مقاوم باشد. حذف یک گره، اجرای هیچ یک از قراردادهای هوشمند را مختل نمی‌کند[۹] و سیستم دارای پایداری و در دسترس بودن بسیار بالایی است.

۱-۲-۴ زنجیره بلوکی به عنوان راهکار نوین در زنجیره تأمین

با در نظر گرفتن مباحث مطرح شده، اکنون می‌توانیم تصویر کامل‌تری از چرایی انتخاب زنجیره بلوکی به عنوان راهکار اصلی این پروژه ترسیم کنیم. فناوری زنجیره بلوکی، با ترکیب تاریخچه‌ای تکاملی در جهت عدم تمرکز، مبانی مستحکم رمزنگاری و قابلیت‌های برنامه‌پذیری از طریق قراردادهای هوشمند، مجموعه‌ای از ابزارهای قدرتمند را برای مقابله با چالش‌های زنجیره تأمین فراهم می‌آورد.

ترکیب این مفاهیم، یک راهکار یکپارچه ارائه می‌دهد:

۱. **اصالت تضمین‌شده:** با استفاده از توابع درهم‌سازی رمزنگاری، برای هر محصول یک هویت دیجیتال منحصربه‌فرد و تغییرناپذیر ایجاد می‌شود. این هویت، جعل محصول را تقریبا غیرممکن می‌سازد.

---

[۱۷] *Immutability & Determinism*
[۱۸] *Transparency & Auditability*
[۱۹] *Decentralization & Robustness*
[۲۰] *Node*

۲. **مالکیت امن:** با استفاده از رمزنگاری کلید عمومی، مالکیت هر کالا به صورت امن به آدرس دیجیتال مالک آن گره می‌خورد و انتقال آن تنها با امضای دیجیتال مالک (کلید خصوصی) امکان‌پذیر است.

۳. **فرآیندهای خودکار و شفاف:** با استفاده از قراردادهای هوشمند، قوانین مربوط به انتقال مالکیت، تأیید مراحل و حتی محاسبه مالیات، به صورت کد تعریف شده و به طور خودکار و بدون نیاز به واسطه اجرا می‌شوند. تمام این فرآیندها بر روی یک دفتر کل شفاف و قابل حسابرسی ثبت می‌گردد.

در نتیجه، زنجیره بلوکی بستری را فراهم می‌کند که در آن، اعتماد دیگر به یک نهاد مرکزی وابسته نیست، بلکه در خود معماری سیستم و قوانین ریاضی و رمزنگاری آن نهفته است. این همان تغییری است که می‌تواند بر مشکلات ساختاری زنجیره‌های تأمین سنتی غلبه کرده و عصری جدید از شفافیت، کارایی و اطمینان را برای همه ذی‌نفعان به ارمغان آورد.

۱-۳ اهداف و دستاوردهای پروژه

همانطور که در بخش‌های پیشین تشریح شد، زنجیره‌های تأمین سنتی با بحران‌های عمیقی در حوزه‌های شفافیت، اعتماد و کارایی مواجه هستند. این چالش‌ها که ریشه در معماری متمرکز و گسستگی اطلاعات دارند، نیازمند راهکاری بنیادین هستند که بتواند ساختار تعاملات در این اکوسیستم را بازتعریف کند. پروژه حاضر با درک این نیاز، هدف اصلی خود را طراحی و پیاده‌سازی یک سامانه جامع زنجیره تأمین مبتنی بر فناوری زنجیره بلوکی تعریف کرده است[۱۰]. این هدف کلان، در پی آن است تا با بهره‌گیری از ویژگی‌های منحصربه‌فرد زنجیره بلوکی، راهکاری عملی برای مقابله با تقلب، افزایش قابلیت ردیابی و بازگرداندن اعتماد به اکوسیستم ارائه دهد.

برای نیل به این هدف جامع، مجموعه‌ای از اهداف جزئی، فنی و کاربردی تعریف شده‌اند که هر یک به مثابه یک ستون، شاکله اصلی این سامانه را تشکیل می‌دهند. این اهداف نه تنها مسیر پیاده‌سازی پروژه را مشخص می‌کنند، بلکه در نهایت، دستاوردهای ملموس و قابل سنجش آن را نیز نمایندگی خواهند کرد. در ادامه این بخش، هر یک از این اهداف کلیدی به تفصیل مورد بررسی و تحلیل قرار می‌گیرند تا اهمیت، ضرورت و نحوه تحقق هر یک از آن‌ها به روشنی مشخص گردد.

۱-۳-۱ هدف اول: ایجاد یک سیستم جامع برای ردیابی شفاف محصولات

تشریح هدف و اهمیت آن

اولین و پایه‌ای‌ترین هدف این پروژه، ایجاد یک سیستم یکپارچه برای ردیابی سرتاسری و شفاف محصولات [۲۱] است. در سیستم‌های کنونی، چرخه حیات یک محصول از مجموعه‌ای از مراحل گسسته و جزیره‌ای تشکیل شده است که هر کدام توسط یک نهاد مجزا مدیریت می‌شود. این گسستگی اطلاعاتی باعث ایجاد نقاط کور در زنجیره می‌شود که ردیابی دقیق مسیر حرکت، تاریخچه مالکیت و شرایط نگهداری محصول را ناممکن می‌سازد.

هدف این است که یک شناسنامه دیجیتال برای هر محصول ایجاد شود که از لحظه تولید تا رسیدن به دست مصرف‌کننده نهایی، به صورت پویا و تغییرناپذیر تکمیل گردد. این شناسنامه بر روی یک دفتر کل توزیع‌شده ثبت می‌شود که تمام ذی‌نفعان مجاز (تولیدکننده، توزیع‌کننده، نهادهای نظارتی و مصرف‌کننده) می‌توانند به آن دسترسی داشته باشند[۱۱].

اهمیت این هدف در سه جنبه اصلی نهفته است:

۱. **مقابله با تقلب و جعل:** با داشتن یک تاریخچه کامل و غیرقابل دستکاری، امکان ورود کالای تقلبی به زنجیره اصلی به شدت کاهش می‌یابد. هرگونه عدم تطابق در تاریخچه محصول، به سرعت قابل شناسایی خواهد بود.

۲. **افزایش اعتماد مصرف‌کننده:** مصرف‌کنندگان می‌توانند با اطمینان کامل از اصالت و پیشینه محصولی که خریداری می‌کنند، مطلع شوند. این شفافیت، وفاداری به برند را تقویت کرده و قدرت انتخاب آگاهانه را به مصرف‌کننده می‌دهد.

۳. **مدیریت بحران و فراخوان کارآمد:** در صورت بروز مشکل کیفی یا ایمنی برای یک محصول خاص، می‌توان با مراجعه به تاریخچه دقیق آن، به سرعت منشأ مشکل را شناسایی و محصولات معیوب را از بازار جمع‌آوری [۲۲] کرد. این امر از توزیع گسترده‌تر محصولات مشکل‌دار جلوگیری کرده و خسارات را به حداقل می‌رساند.

نحوه تحقق و پیاده‌سازی فنی

برای دستیابی به این هدف، از یک مدل داده ساختاریافته در قرارداد هوشمند استفاده می‌شود. فرآیند ردیابی در سه مرحله اصلی پیاده‌سازی می‌شود:

- **ثبت محصول** [۲۳]: در ابتدای چرخه حیات، تولیدکننده یا واردکننده محصول جدید را در سیستم ثبت می‌کند. در این مرحله، یک توکن دیجیتال منحصربه‌فرد که نمایانگر آن کالای فیزیکی است،

---

[۲۱] $End-to-End\,Traceability$

[۲۲] $Recall$

[۲۳] $Minting$

بر روی زنجیره بلوکی ضرب یا ساخته می‌شود. تمام اطلاعات اولیه محصول، مانند شماره سریال، تاریخ تولید و مشخصات فنی، به این توکن الصاق می‌گردد. این عمل از طریق فراخوانی یک تابع مشخص در قرارداد هوشمند (مانند [۲۴]) توسط بازیگر دارای مجوز (مثلاً نقش MANUFACTURER_ROLE) انجام می‌شود.

- **ثبت تاریخچه مالکیت:** هر بار که محصول در زنجیره تأمین دست به دست می‌شود (مثلاً از تولیدکننده به توزیع‌کننده)، یک تراکنش انتقال مالکیت بر روی زنجیره بلوکی ثبت می‌گردد. این تراکنش که از طریق توابعی مانند $transferWithTax$ در قرارداد هوشمند مدیریت می‌شود، به صورت خودکار اطلاعات مالک جدید، زمان انتقال و سایر جزئیات مربوطه را به تاریخچه محصول اضافه می‌کند. این فرآیند، یک زنجیره مالکیت [۲۵] شفاف و قابل حسابرسی ایجاد می‌کند که در تابع $getOwnershipHistory$ قابل بازیابی است.
- **دسترسی مصرف‌کننده نهایی:** در نهایت، یک کد QR منحصربه‌فرد بر روی بسته‌بندی محصول فیزیکی قرار می‌گیرد. مصرف‌کنندگان می‌توانند با پویش این کد از طریق یک برنامه کاربردی وب، به شناسنامه دیجیتال آن محصول دسترسی پیدا کرده و تاریخچه کامل آن را از تولید تا قفسه فروشگاه مشاهده نمایند[۱۲]. این فرآیند، پل ارتباطی مستقیم و قابل اعتمادی بین دنیای فیزیکی و دیجیتال ایجاد می‌کند.

۱-۴ هدف دوم: مدیریت بهینه دارایی‌ها با استفاده از استاندارد $ERC1155$

تشریح هدف و اهمیت آن

زنجیره‌های تأمین با طیف گسترده‌ای از محصولات سروکار دارند. برخی از محصولات، مانند یک خودرو با شماره شاسی مشخص، کاملاً منحصربه‌فرد و غیرمثلی [۲۶] هستند. در مقابل، محصولات دیگری مانند یک بچ از هزاران پیچ یکسان، کاملاً مثلی و قابل تعویض [۲۷] هستند. مدیریت این دو نوع دارایی در سیستم‌های سنتی و حتی در استانداردهای اولیه زنجیره بلوکی، نیازمند زیرساخت‌ها و قراردادهای مجزا بود. این امر منجر به افزایش پیچیدگی، هزینه‌های بالا و کاهش کارایی می‌شد.

هدف این بخش از پروژه، بهره‌گیری از یک استاندارد توکن پیشرفته به نام $ERC1155$ است تا بتوان هر دو نوع دارایی مثلی و غیرمثلی را در قالب یک قرارداد هوشمند واحد، به صورت بهینه مدیریت کرد[۶].

[۲۴] $registerProduct$
[۲۵] $Chain\ of\ Custody$
[۲۶] $Non-Fungible$
[۲۷] $Fungible$

این استاندارد که به عنوان یک استاندارد چند-توکنی شناخته می‌شود، به طور خاص برای کاربردهایی مانند بازی‌های کامپیوتری و زنجیره تأمین که با انواع مختلفی از آیتم‌ها سروکار دارند، طراحی شده است. اهمیت استفاده از $ERC1155$ در موارد زیر خلاصه می‌شود:

- **افزایش کارایی و کاهش هزینه:** به جای استقرار چندین قرارداد هوشمند مجزا (مثلاً یک قرارداد $ERC-721$ [۱۳] برای کالاهای منحصربه‌فرد و یک قرارداد $ERC-20$ برای کالاهای مثلی)، تمام منطق مدیریت توکن‌ها[۱۴] در یک قرارداد واحد متمرکز می‌شود. این امر به شدت هزینه‌های استقرار و نگهداری ($GasFee$) را کاهش داده و مدیریت سیستم را ساده‌تر می‌کند[۱۵].
- **انعطاف‌پذیری بالا:** این سامانه قادر خواهد بود تا هر نوع محصولی را، از یک قطعه هنری با اصالت مشخص گرفته تا یک پالت از کالاهای مصرفی، به راحتی مدیریت کند. این انعطاف‌پذیری، کاربردپذیری سیستم را برای طیف وسیعی از صنایع ممکن می‌سازد.
- **تراکنش‌های دسته‌ای** [۲۸]: یکی از قابلیت‌های کلیدی $ERC1155$، امکان انتقال چندین نوع توکن مختلف در یک تراکنش واحد است. برای مثال، یک توزیع‌کننده می‌تواند در یک تراکنش، ۱۰۰ عدد کالای A و ۵۰ عدد کالای B را از تولیدکننده دریافت کند. این قابلیت، تعداد کل تراکنش‌های مورد نیاز شبکه را کاهش داده و به بهینه‌سازی فرآیندهای لجستیکی پیچیده کمک شایانی می‌کند.

نحوه تحقق و پیاده‌سازی فنی

قرارداد هوشمند اصلی این پروژه ($SupplyChainERC1155.sol$) با ارث‌بری از پیاده‌سازی استاندارد $ERC1155$ (که معمولاً توسط کتابخانه‌های معتبری مانند $OpenZeppelin$ ارائه می‌شود[۱۶]) ساخته شده است. هر نوع محصول جدید در سیستم با یک id منحصربه‌فرد تعریف می‌شود. اگر محصول غیرمثلی باشد، تنها یک توکن با آن id ساخته می‌شود. اگر محصول مثلی باشد، می‌توان هر تعداد توکن با همان id ایجاد کرد. توابع اصلی این استاندارد مانند $mint$، $burn$ و $safeTransferFrom$ برای مدیریت ایجاد، ابطال و انتقال این توکن‌ها به کار گرفته می‌شوند. این ساختار فنی، پایه و اساس مدیریت دارایی در کل سامانه را تشکیل می‌دهد.

۱-۴-۱ هدف سوم: تضمین صحت و یکپارچگی فراداده‌ها با $Keccak256$

تشریح هدف و اهمیت آن

ردیابی مالکیت یک کالا تنها نیمی از راه حل است. بخش دیگر و حیاتی‌تر، تضمین این است که اطلاعات و مشخصات آن کالا (فراداده[۲۹]) در طول زمان دستکاری نشده و معتبر باقی مانده است. فراداده شامل

[۲۸] $BatchOperations$
[۲۹] $Metadata$

جزئیاتی مانند تاریخ تولید، شماره سریال، مبدأ جغرافیایی، مواد تشکیل‌دهنده و گواهی‌های کیفیت است. در سیستم‌های سنتی، این اطلاعات معمولاً در پایگاه‌های داده‌ای ذخیره می‌شوند که به راحتی قابل تغییر هستند.

هدف این بخش، پیاده‌سازی یک مکانیزم رمزنگاری قدرتمند برای تضمین صحت و یکپارچگی فراداده‌هاست. در این پروژه، از الگوریتم درهم‌سازی $Keccak256$ برای ایجاد یک اثر انگشت دیجیتال منحصربه‌فرد از فراداده هر محصول استفاده می‌شود[۱۵]. این اثر انگشت متن درهم‌سازی شده بر روی زنجیره بلوکی ذخیره می‌شود که تغییرناپذیر است.

اهمیت این رویکرد در دو نکته کلیدی است:

۱. **ایجاد پیوند تغییرناپذیر بین کالا و اطلاعات آن:** با ثبت متن درهم‌سازی شده فراداده بر روی زنجیره، هرگونه تلاش برای دستکاری اطلاعات اصلی (حتی تغییر یک کاراکتر) منجر به تولید یک متن درهم‌سازی شده کاملاً متفاوت خواهد شد. این عدم تطابق به راحتی قابل تشخیص بوده و تلاش برای تقلب را آشکار می‌سازد.

۲. **بهینه‌سازی هزینه ذخیره‌سازی:** ذخیره‌سازی حجم زیادی از اطلاعات (مانند تصاویر یا اسناد فنی) به صورت مستقیم بر روی زنجیره بلوکی بسیار گران است. این روش به ما اجازه می‌دهد تا فراداده اصلی را در یک سیستم ذخیره‌سازی خارج از زنجیره مانند $IPFS$ یا سرورهای معمولی نگهداری کرده و تنها درهم‌سازی سبک امن آن را بر روی زنجیره ثبت کنیم. این معماری، ضمن حفظ امنیت کامل، هزینه‌ها را به شدت بهینه می‌کند.

نحوه تحقق و پیاده‌سازی فنی

فرآیند تضمین صحت فراداده‌ها در قرارداد هوشمند به شرح زیر پیاده‌سازی می‌شود:

- **تولید متن درهم‌سازی شده در زمان ثبت:** هنگامی که یک محصول جدید از طریق $registerProduct$ ثبت می‌شود، قرارداد هوشمند به صورت داخلی تابع دیگری مانند $generateMetadataHash$ را فراخوانی می‌کند. این تابع، مقادیر کلیدی فراداده (مانند نام، دسته بندی، شماره سریال و غیره) را دریافت کرده، آن‌ها را به یک فرمت استاندارد تبدیل می‌کند و سپس الگوریتم $keccak256$ را بر روی آن اعمال می‌کند.

- **ذخیره‌سازی متن درهم‌سازی شده:** متن درهم‌سازی شده تولید شده در ساختار داده مربوط به آن محصول (مثلاً $Productstruct$) در کنار سایر اطلاعات آن بر روی زنجیره بلوکی ذخیره می‌شود.

- **اعتبارسنجی عمومی:** یک تابع عمومی مانند $verifyProductMetadata$ در قرارداد هوشمند در دسترس قرار می‌گیرد. هر کاربری (مثلاً یک مصرف‌کننده یا بازرس) می‌تواند با ارائه فراداده‌ای که در اختیار دارد، این تابع را فراخوانی کند. قرارداد هوشمند در لحظه، متن درهم‌سازی شده

فراداده ارسالی را محاسبه کرده و آن را با متن درهم‌سازی شده ذخیره‌شده بر روی زنجیره مقایسه می‌کند. نتیجه این مقایسه (که یک مقدار صحیح/غلط است) به کاربر بازگردانده شده و بدین ترتیب، اصالت اطلاعات تأیید یا رد می‌شود[۱۷].

۱-۵ هدف چهارم: خودکارسازی فرآیندهای تجاری و مالی

تشریح هدف و اهمیت آن

زنجیره‌های تأمین سنتی مملو از فرآیندهای دستی، کاغذبازی‌های اداری، تأخیر در پرداخت‌ها و رویه‌های پیچیده مالیاتی هستند. این فرآیندها نه تنها کند و پرهزینه هستند، بلکه به دلیل نیاز به دخالت انسانی، مستعد خطا و فساد نیز می‌باشند. بخش قابل توجهی از این ناکارآمدی‌ها ناشی از نیاز به واسطه‌های متعدد برای تأیید مراحل، پردازش پرداخت‌ها و تضمین اجرای تعهدات است.

هدف این بخش از پروژه، استفاده از قابلیت‌های قراردادهای هوشمند برای خودکارسازی منطق تجاری و مالی زنجیره تأمین است[۸]. با کدنویسی قوانین کسب‌وکار به صورت مستقیم در یک قرارداد هوشمند، می‌توان اجرای آن‌ها را به صورت خودکار، قطعی و بدون نیاز به دخالت یا نظارت انسانی تضمین کرد. اهمیت این هدف عبارت است از:

- **افزایش سرعت و کارایی:** خودکارسازی فرآیندها، تأخیرهای ناشی از هماهنگی‌های انسانی و پردازش‌های دستی را از بین برده و سرعت کل زنجیره را به طور چشمگیری افزایش می‌دهد.
- **کاهش هزینه‌های عملیاتی:** حذف یا کاهش نیاز به واسطه‌هایی که برای اموری مانند خدمات امانی [۳۰] یا پردازش اسناد به کار گرفته می‌شوند، منجر به صرفه‌جویی قابل توجهی در هزینه‌ها می‌شود[۸].
- **شفافیت و سازگاری در اجرا:** وقتی قوانین در قالب کد نوشته می‌شوند، به صورت یکسان و بدون تبعیض برای همه تراکنش‌ها اجرا می‌گردند. این امر از اجرای سلیقه‌ای قوانین جلوگیری کرده و شفافیت را در کل فرآیند حاکم می‌کند.

نحوه تحقق و پیاده‌سازی فنی

دو نمونه برجسته از خودکارسازی در این پروژه پیاده‌سازی شده است:

۱. **انتقال مالکیت خودکار:** تابع $transferWithTax$ در قرارداد هوشمند، فرآیند انتقال توکن از فرستنده به گیرنده را مدیریت می‌کند. این تابع به صورت اتمی عمل می‌کند؛ یعنی انتقال تنها در صورتی انجام می‌شود که تمام شروط لازم (مانند وجود توکن در کیف پول فرستنده) برقرار باشد. این فرآیند جایگزین رویه‌های سنتی مبتنی بر بارنامه و اسناد کاغذی می‌شود.

[۳۰] $Escrow$

۲. **محاسبه خودکار مالیات:** یکی از قابلیت‌های نوآورانه این پروژه، تعبیه منطق محاسبه مالیات به صورت مستقیم در قرارداد هوشمند است[۱۸]. در قرارداد، تابعی مانند $calculateTax$ تعریف شده است که می‌تواند بر اساس پارامترهایی مانند نوع کالا یا ارزش تراکنش، مبلغ مالیات متعلقه را محاسبه کند. این تابع می‌تواند به صورت خودکار در حین فرآیند انتقال مالکیت فراخوانی شود. مبلغ مالیات محاسبه‌شده می‌تواند به یک آدرس از پیش تعیین‌شده (مثلاً کیف پول سازمان امور مالیاتی) ارسال گردد. این مکانیزم، فرآیند محاسبه و جمع‌آوری مالیات را شفاف، دقیق و آنی می‌سازد و بار محاسباتی را از دوش کسب‌وکارها برمی‌دارد.

در مجموع، این چهار هدف کلیدی، یک نقشه راه جامع برای ساختن یک زنجیره تأمین مدرن، شفاف و قابل اعتماد را ترسیم می‌کنند. هر یک از این اهداف، ضمن حل یکی از مشکلات اساسی سیستم‌های سنتی، در ترکیب با یکدیگر، یک راهکار هم‌افزا و قدرتمند را شکل می‌دهند که پتانسیل تحول‌آفرینی در این صنعت حیاتی را داراست.

۱-۶ چالش‌های اصلی پروژه

با وجود پتانسیل عظیم فناوری زنجیره بلوکی برای ایجاد تحول در صنایع مختلف و به‌ویژه در زنجیره تأمین، پیاده‌سازی و استقرار یک سامانه عملیاتی مبتنی بر این فناوری با چالش‌های متعدد و پیچیده‌ای همراه است. این چالش‌ها صرفاً فنی نیستند و ابعاد امنیتی، اقتصادی، قانونی و اجتماعی را نیز در بر می‌گیرند. موفقیت این پروژه در گرو شناسایی دقیق این موانع و ارائه راهکارهای مناسب برای غلبه بر آن‌هاست. در واقع، هر یک از این چالش‌ها، خود یک حوزه پژوهشی و مهندسی مستقل به شمار می‌آید که نیازمند بررسی عمیق و راهکارهای نوآورانه است. در این فصل، به تفصیل به تحلیل چهار چالش اصلی پیش روی این پروژه می‌پردازیم: چالش‌های فنی مرتبط با مقیاس‌پذیری و هزینه، چالش‌های امنیتی در یک محیط غیرمتمرکز، چالش‌های پذیرش و تجربه کاربری، و در نهایت، چالش‌های قانونی و نظارتی.

۱-۶-۱ چالش‌های فنی: مقیاس‌پذیری و هزینه

یکی از برجسته‌ترین و بحث‌برانگیزترین چالش‌ها در دنیای زنجیره بلوکی، مسئله مقیاس‌پذیری [۳۱] و هزینه‌های مرتبط با آن است. در حالی که سیستم‌های متمرکز سنتی می‌توانند ده‌ها هزار تراکنش را در ثانیه پردازش کنند، شبکه‌های زنجیره بلوکی عمومی مانند اتریوم، به دلیل ماهیت غیرمتمرکز و سازوکارهای اجماع خود، دارای توان پردازشی بسیار محدودتری هستند. این محدودیت، به ویژه در کاربردهایی با حجم تراکنش بالا مانند زنجیره تأمین، به یک گلوگاه اساسی تبدیل می‌شود.

[۳۱] $Scalability$

۱-۶-۲ مقدمه‌ای بر معماری ماشین مجازی اتریوم (EVM) و هزینه تراکنش (Gas)

برای درک عمیق چالش هزینه، ابتدا باید با مفهوم گاز (Gas) در شبکه‌های سازگار با ماشین مجازی اتریوم (EVM) آشنا شویم. هر عملیات محاسباتی که بر روی EVM انجام می‌شود، از یک جمع ساده گرفته تا ذخیره‌سازی داده در قرارداد هوشمند، نیازمند مصرف منابع محاسباتی از سوی گره‌های ($Nodes$) شبکه است. این منابع رایگان نیستند[۵]. مفهوم گاز برای اندازه‌گیری میزان این تلاش محاسباتی به کار می‌رود[۵]. هر عملیات یک هزینه گاز ثابت دارد (مثلاً ADD هزینه ۳ گاز و $SSTORE$ برای ذخیره‌سازی داده هزینه ۲۰،۰۰۰ گاز دارد).

هزینه نهایی یک تراکنش از فرمول زیر به دست می‌آید:

$$TransactionFee = TotalGasUsed \times GasPrice$$

در اینجا، $TotalGasUsed$ مجموع گاز مصرفی تمام عملیات‌های یک تراکنش است و $GasPrice$ قیمتی است که کاربر مایل است برای هر واحد گاز بپردازد. این قیمت بر اساس عرضه و تقاضای شبکه تعیین می‌شود و در زمان‌های شلوغی شبکه، به شدت افزایش می‌یابد. پرداخت این هزینه با استفاده از ارز دیجیتال اصلی شبکه، یعنی اتر ($Ether$)، انجام می‌شود[۵]. این سازوکار، ضمن جلوگیری از اجرای کدهای مخرب و حلقه‌های بی‌نهایت، یک مدل اقتصادی برای پاداش‌دهی به اعتبارسنج‌های شبکه فراهم می‌کند. اما همین مدل، چالش هزینه را برای کاربردهای تجاری به وجود می‌آورد.

۱-۶-۳ چالش‌های خاص استاندارد $ERC1155$ در مقیاس بزرگ

پروپوزال این پروژه به درستی به این چالش اشاره می‌کند که استفاده از قرارداد هوشمند مبتنی بر استاندارد $ERC1155$، به ویژه در مقیاس بزرگ، می‌تواند مشکلاتی از جمله مقیاس‌پذیری و هزینه‌های تراکنش ایجاد کند[۱۹]. در یک زنجیره تأمین واقعی، به‌ویژه برای کالاهای تندمصرف ($FMCG$)،ممکن است روزانه هزاران یا حتی میلیون‌ها محصول تولید ،منتقل و مصرف شوند. هر یک از این اقدامات، یک تراکنش مجزا بر روی زنجیره بلوکی است که هزینه گاز به همراه دارد.

فرض کنید هزینه میانگین یک تراکنش انتقال ساده در شبکه اتریوم چند دلار باشد. اگر یک شرکت بخواهد روزانه وضعیت ۱۰۰۰ محصول را به‌روزرسانی کند، هزینه عملیاتی آن به سرعت به هزاران دلار در روز می‌رسد. این هزینه برای بسیاری از کسب‌وکارها، به ویژه در مقایسه با هزینه‌های ناچیز نگهداری یک پایگاه داده متمرکز، غیرقابل قبول است. بنابراین، هرچند $ERC1155$ از نظر فنی برای مدیریت انواع توکن‌ها کارآمد است، اما هزینه اقتصادی استفاده از آن در یک شبکه عمومی پرازدحام، یک مانع جدی برای پذیرش در مقیاس صنعتی محسوب می‌شود.

۱-۶-۴ چالش ذخیره‌سازی داده‌ها بر روی زنجیره

یکی دیگر از ابعاد چالش هزینه، مربوط به ذخیره‌سازی داده است. ذخیره‌سازی داده به صورت مستقیم بر روی زنجیره بلوکی یکی از گران‌ترین عملیات‌ها در EVM است. هر کیلوبایت داده می‌تواند صدها یا هزاران دلار هزینه در بر داشته باشد. برای یک زنجیره تأمین که نیازمند ذخیره اطلاعات جامعی از هر محصول (مانند تصاویر، اسناد فنی، گواهی‌نامه‌ها و غیره) است، ذخیره‌سازی مستقیم این فراداده‌ها بر روی زنجیره، از نظر اقتصادی کاملاً غیرممکن است.

این چالش، تیم پروژه را به سمت یک معماری هوشمندانه سوق داده است که در بخش اهداف نیز به آن اشاره شد: معماری ترکیبی روی زنجیر و خارج از زنجیر. در این مدل، تنها اطلاعات حیاتی و حداقلی که برای تضمین امنیت و یکپارچگی لازم است، بر روی زنجیره ذخیره می‌شود. این اطلاعات شامل فراداده درهم‌سازی شده رمزنگاری شده فراداده است. خود فراداده حجیم، در یک سیستم ذخیره‌سازی خارج از زنجیره خارج از زنجیره مانند $IPFS$ [۳۲] یا سرورهای وب سنتی نگهداری می‌شود. این رویکرد، ضمن حفظ امنیت کامل از طریق درهم‌سازی، هزینه‌های ذخیره‌سازی را هزاران برابر کاهش می‌دهد و سیستم را از نظر اقتصادی عملیاتی می‌سازد.

۱-۶-۵ راهکارهای بالقوه برای غلبه بر چالش فنی

اگرچه این پروژه بر روی یک شبکه تستی و محلی اجرا می‌شود، اما برای استقرار نهایی در دنیای واقعی، باید راهکارهایی برای چالش مقیاس‌پذیری و هزینه اندیشیده شود. برخی از مهم‌ترین راهکارها که در اکوسیستم زنجیره بلوکی در حال توسعه هستند عبارتند از:

- **شبکه‌های لایه ۲** [۳۳]: فناوری‌هایی مانند $Rollups$ ($Optimistic$ و $ZK-Rollups$) تراکنش‌ها را در خارج از زنجیره اصلی پردازش کرده و تنها یک خلاصه فشرده از آن‌ها را به زنجیره اصلی ارسال می‌کنند. این کار هزینه هر تراکنش را به شدت کاهش داده و توان پردازشی را به چندین هزار تراکنش در ثانیه افزایش می‌دهد.
- **زنجیره‌های جانبی** [۳۴]: زنجیره‌های مستقلی که با زنجیره اصلی سازگار هستند و می‌توان دارایی‌ها را بین آن‌ها منتقل کرد. این زنجیره‌ها معمولاً دارای هزینه تراکنش بسیار پایین‌تری هستند.
- **انتخاب شبکه‌های $EVM-Compatible$ با هزینه پایین:** به جای استقرار بر روی شبکه اصلی اتریوم، می‌توان پروژه را بر روی شبکه‌های دیگری که با EVM سازگار هستند اما هزینه تراکنش کمتری دارند (مانند $Polygon$، $Avalanche$، $BNBSmartChain$) مستقر کرد.

انتخاب راهکار مناسب، خود نیازمند تحلیل دقیق نیازمندی‌های پروژه و بررسی مزایا و معایب هر گزینه است که می‌تواند موضوعی برای تحقیقات آینده باشد.

---

[۳۲] $InterPlanetaryFileSystem$

[۳۳] $Layer2Solutions$

[۳۴] $Sidechains$

۱-۷ چالش‌های امنیتی در سیستم‌های غیرمتمرکز

امنیت در سیستم‌های زنجیره بلوکی یک مفهوم کاملاً متفاوت از امنیت در سیستم‌های متمرکز است. در اینجا، دیگر خبری از حفاظت از یک سرور مرکزی با استفاده از فایروال‌ها و کنترل دسترسی‌های فیزیکی نیست. امنیت به خود پروتکل، کد قرارداد هوشمند و مسئولیت‌پذیری کاربران منتقل می‌شود. پروپوزال پروژه به درستی تأکید می‌کند که امنیت اطلاعات در سیستم زنجیره بلوکی باید در بالاترین سطح خود قرار گیرد تا از هرگونه دستکاری داده‌ها جلوگیری شود[۲۰].

۱-۷-۱ امنیت قرارداد هوشمند: کد، قانون است

قراردادهای هوشمند، قلب تپنده برنامه‌های غیرمتمرکز هستند و در عین حال، بزرگ‌ترین سطح حمله [۳۵] را تشکیل می‌دهند. یک آسیب‌پذیری کوچک در کد یک قرارداد هوشمند می‌تواند منجر به سرقت میلیون‌ها دلار دارایی یا از کار افتادن کامل یک سیستم شود. چالش اصلی در اینجا، ویژگی تغییرناپذیری [۳۶] کد است. پس از استقرار یک قرارداد هوشمند، کد آن دیگر قابل تغییر یا اصلاح نیست[۸]. این ویژگی که برای ایجاد اعتماد ضروری است، به این معناست که اگر یک باگ یا حفره امنیتی در کد وجود داشته باشد، نمی‌توان آن را به سادگی وصله کرد. این ماهیت، امنیت قرارداد هوشمند را به امری بسیار حیاتی و پرمخاطره تبدیل می‌کند.

برخی از آسیب‌پذیری‌های رایج در قراردادهای هوشمند عبارتند از:

- **حملات بازگشتی** [۳۷]: حمله‌ای که در آن یک قرارداد مهاجم، قبل از تکمیل یک تراکنش، به صورت مکرر یک تابع را در قرارداد قربانی فراخوانی کرده و موجودی آن را خالی می‌کند.
- **سرریز/زیرریز عدد صحیح** [۳۸]: به دلیل محدودیت در اندازه متغیرهای عددی، انجام محاسباتی که منجر به عبور از حداکثر یا حداقل مقدار ممکن شود، می‌تواند نتایج غیرمنتظره و خطرناکی به همراه داشته باشد.
- **منطق اشتباه در کنترل دسترسی:** عدم پیاده‌سازی صحیح مجوزها و نقش‌ها، که می‌تواند به یک کاربر غیرمجاز اجازه دهد تا اقداماتی مدیریتی مانند تغییر مالکیت یا از بین بردن دارایی‌ها را انجام دهد.

برای مقابله با این چالش‌ها، پروژه حاضر از رویکردهای استاندارد صنعتی بهره می‌برد. اول، استفاده از کتابخانه‌های معتبر و حسابرسی‌شده مانند $OpenZeppelin$[۱۶] برای پیاده‌سازی استانداردهایی مانند $ERC1155$ و مکانیزم‌های کنترل دسترسی. این کتابخانه‌ها توسط متخصصان امنیت بررسی شده و

[۳۵] $Surface\ Attack$
[۳۶] $Immutability$
[۳۷] $Reentrancy$
[۳۸] $Integer\ Overflow/Underflow$

ریسک وجود آسیب‌پذیری‌های رایج را به حداقل می‌رسانند. دوم، پیاده‌سازی یک مجموعه آزمون جامع با استفاده از فریم‌ورک قدرتمند $Foundry$. این آزمون‌ها، تمام توابع و سناریوهای ممکن، از جمله حالت‌های حدی و تلاش برای حملات، را شبیه‌سازی کرده و از صحت عملکرد و امنیت کد اطمینان حاصل می‌کنند.

۱-۸ امنیت فراداده و مکانیزم تأیید متن درهم‌سازی شده

همانطور که قبلاً ذکر شد، معماری این سیستم بر پایه ذخیره متن درهم‌سازی شده فراداده بر روی زنجیره و خود فراداده در یک مکان خارج از زنجیره (مانند $IPFS$) استوار است. این معماری، خود یک چالش امنیتی جدید ایجاد می‌کند: چگونه از صحت و تطابق داده خارج زنجیره با متن درهم‌سازی شده روی زنجیره اطمینان حاصل کنیم؟

۱-۸-۱ بردارهای حمله به فراداده

یک مهاجم نمی‌تواند متن درهم‌سازی شده ثبت‌شده بر روی زنجیره بلوکی را تغییر دهد، اما می‌تواند تلاش کند تا به یکی از روش‌های زیر، سیستم را فریب دهد:

- **حمله مرد میانی** [۳۹]: یک مهاجم می‌تواند در ارتباط بین کاربر و سرور ذخیره‌سازی خارج از زنجیره قرار گرفته و فراداده جعلی را به کاربر نمایش دهد، در حالی که کاربر تصور می‌کند در حال مشاهده اطلاعات اصلی است.
- **دستکاری سرور خارج از زنجیره:** اگر فراداده بر روی یک سرور متمرکز سنتی ذخیره شده باشد، مهاجم می‌تواند با هک کردن آن سرور، اطلاعات را تغییر دهد.
- **عدم دسترسی به داده** [۴۰]: ممکن است سرور خارج از زنجیره از دسترس خارج شود و کاربران دیگر نتوانند به فراداده اصلی دسترسی پیدا کنند، که این امر عملاً اعتبارسنجی را غیرممکن می‌سازد.

مکانیزم دفاعی پروژه

سیستم طراحی‌شده در این پروژه، یک مکانیزم دفاعی قوی برای مقابله با این حملات دارد که مبتنی بر اعتبارسنجی سمت کاربر [۴۱] است. فرآیند به شرح زیر است:

[۳۹] $Man-in-the-Middle$
[۴۰] $Data\,Unavailability$
[۴۱] $Client-SideValidation$

۱. کاربر (مثلاً مصرف‌کننده‌ای که کد QR را اسکن می‌کند) درخواستی برای مشاهده اطلاعات محصول ارسال می‌کند.

۲. برنامه کاربردی [۴۲] دو درخواست موازی ارسال می‌کند: یکی به سیستم ذخیره‌سازی خارج از زنجیره (مثلاً $IPFS$) برای دریافت فایل کامل فراداده، و دیگری به زنجیره بلوکی برای خواندن متن درهم‌سازی شده معتبر و ثبت‌شده آن محصول از قرارداد هوشمند.

۳. پس از دریافت فایل فراداده، برنامه کاربردی در سمت کاربر، تابع درهم‌سازی $Keccak256$ را بر روی آن اجرا کرده و متن درهم‌سازی شده آن را به صورت محلی محاسبه می‌کند.

۴. در نهایت، برنامه، متن درهم‌سازی شده محاسبه‌شده محلی را با متن درهم‌سازی شده دریافت‌شده از زنجیره بلوکی مقایسه می‌کند.

اگر این دو متن درهم‌سازی شده کاملاً یکسان باشند، یک علامت تأیید سبز به کاربر نمایش داده می‌شود که نشان‌دهنده اصالت و یکپارچگی کامل اطلاعات است. اگر حتی یک بیت تفاوت بین دو متن درهم‌سازی شده وجود داشته باشد، به کاربر یک هشدار جدی نمایش داده می‌شود که اطلاعات محصول مورد دستکاری قرار گرفته است. این فرآیند، اعتماد را از سرور خارج از زنجیره سلب کرده و آن را به محاسبات ریاضی و داده‌های تغییرناپذیر زنجیره بلوکی منتقل می‌کند.

نقش $IPFS$ در افزایش امنیت

استفاده از $IPFS$ (که در توضیحات تکمیلی شما به آن اشاره شد) یک لایه امنیتی دیگر به این معماری می‌افزاید. $IPFS$ یک سیستم فایل توزیع‌شده و مبتنی بر محتوا ($Content - Addressed$) است. این بدان معناست که آدرس یک فایل در $IPFS$، خودِ متن درهم‌سازی شدهِ محتوای آن فایل است. بنابراین، اگر محتوای فایل تغییر کند، متن درهم‌سازی شده آن و در نتیجه آدرس آن نیز تغییر خواهد کرد. با ذخیره کردن این آدرس مبتنی بر محتوا (CID) بر روی زنجیره بلوکی، یک پیوند رمزنگاری قوی بین رفرنس آن‌چین و داده آف‌چین ایجاد می‌شود که دستکاری آن را بیش از پیش دشوار می‌سازد.

۱-۸-۲ امنیت کلید خصوصی کاربر

نهایتاً، ضعیف‌ترین حلقه در زنجیره امنیت هر سیستم مبتنی بر زنجیره بلوکی، خود کاربر است. تمام دارایی‌ها و مجوزهای یک کاربر به کلید خصوصی او گره خورده است. اگر کلید خصوصی یک کاربر به سرقت برود یا فاش شود، مهاجم کنترل کاملی بر تمام دارایی‌ها و نقش‌های آن کاربر در سیستم خواهد داشت. این چالشی است که راه حل آن کمتر فنی و بیشتر آموزشی است. کاربران باید در مورد اهمیت نگهداری امن کلیدهای خصوصی خود و استفاده از کیف پول‌های سخت‌افزاری برای دارایی‌های با ارزش، به خوبی آموزش ببینند.

[۴۲] $Front - end$

۱-۹ چالش‌های پذیرش و تجربه کاربری (UX)

یک سیستم هرچقدر هم که از نظر فنی قدرتمند و امن باشد، اگر استفاده از آن برای کاربران نهایی دشوار و پیچیده باشد، هرگز به پذیرش گسترده نخواهد رسید. پروپوزال پروژه به درستی به این موضوع اشاره می‌کند که پذیرش چنین سیستم نوآورانه‌ای در کشور نیازمند آموزش و آگاهی‌رسانی به کاربران است[۲۱]. این چالش، به ویژه در صنعتی مانند زنجیره تأمین که با طیف وسیعی از کاربران با سطوح مختلف دانش فنی سروکار دارد، بسیار پررنگ‌تر است.

۱-۹-۱ فاصله دانش و موانع ذهنی

مفاهیمی مانند زنجیره بلوکی، کیف پول دیجیتال، کلید خصوصی، امضای تراکنش و هزینه گاز، برای اکثر افراد خارج از دنیای فناوری، مفاهیمی بیگانه و ترسناک هستند. انتظار از یک مدیر انبار، یک راننده کامیون یا یک فروشنده خرده‌پا برای درک و کار با این مفاهیم، یک مانع بزرگ برای پیاده‌سازی موفق سیستم است. هدف اصلی در طراحی تجربه کاربری، انتزاع [۴۳] این پیچیدگی‌ها و ارائه یک رابط کاربری ساده، آشنا و بصری است که به کاربران اجازه دهد بدون نیاز به درک جزئیات فنی زیرساخت، وظایف خود را به راحتی انجام دهند.

۱-۹-۲ طراحی تجربه کاربری برای انتزاع پیچیدگی

بر اساس توضیحات تکمیلی شما، پروژه حاضر با طراحی یک تجربه کاربری هدفمند، تلاش کرده است تا این چالش را مرتفع سازد. این طراحی بر اساس نقش‌های مختلف کاربران، شخصی‌سازی شده است:

تجربه کاربری مدیر سیستم / تولیدکننده

برای کاربری که مسئول ثبت محصولات جدید در سیستم است (مثلاً یک مدیر تولید)، یک داشبورد مدیریتی وب طراحی می‌شود. این داشبورد، تمام پیچیدگی‌های فنی را در پس‌زمینه پنهان می‌کند:

- **فرم ثبت محصول ساده:** کاربر با یک فرم وب ساده مواجه می‌شود که در آن فیلدهای آشنایی مانند نام محصول، شماره سریال، دسته‌بندی، تاریخ تولید و امکان بارگذاری تصویر و اسناد را مشاهده می‌کند.
- **فرآیند خودکار در پس‌زمینه:** پس از اینکه کاربر اطلاعات را وارد کرده و بر روی دکمه ایجاد محصول کلیک می‌کند، برنامه کاربردی به صورت خودکار زنجیره‌ای از عملیات پیچیده را انجام می‌دهد:

۱. ابتدا فراداده وارد شده را در یک فرمت استاندارد (مانند $JSON$) بسته‌بندی می‌کند.

[۴۳] $Abstraction$

۲. سپس این فایل فراداده را در سیستم ذخیره‌سازی خارج از زنجیره (مانند $IPFS$) بارگذاری می‌کند.
۳. پس از بارگذاری، آدرس منحصربه‌فرد فایل در $IPFS$ (یعنی CID آن) را دریافت می‌کند.
۴. درهم‌سازی $Keccak256$ فراداده را مطابق منطق قرارداد هوشمند محاسبه می‌کند.
۵. یک تراکنش برای فراخوانی تابع $registerProduct$ در قرارداد هوشمند آماده می‌کند. این تراکنش شامل پارامترهایی مانند متن درهم‌سازی شده فراداده و آدرس $IPFS$ آن است.
۶. در نهایت، از طریق یک کیف پول متصل به مرورگر (مانند $MetaMask$)، از کاربر می‌خواهد تا تراکنش را با یک کلیک ساده، امضا یا تأیید کند.

در تمام این فرآیند، کاربر تنها یک فرم را پر کرده و یک دکمه را فشرده است. او نیازی به دانستن اینکه $IPFS$ یا $Keccak256$ چیست، ندارد. این انتزاع، پذیرش سیستم توسط کاربران سازمانی را به شدت تسهیل می‌کند.

تجربه کاربری مالک توکن (توزیع‌کننده / خرده‌فروش)

یکی از نقاط قوت کلیدی این پروژه، پایبندی به استاندارد جهانی $ERC1155$ است. این پایبندی یک مزیت بزرگ در تجربه کاربری ایجاد می‌کند: محصول ثبت‌شده به عنوان یک توکن استاندارد، به صورت خودکار در تمام کیف پول‌های دیجیتالی که از این استاندارد پشتیبانی می‌کنند (مانند $MetaMask$، $Trust\ Wallet$) قابل مشاهده و مدیریت است. این یعنی یک توزیع‌کننده یا خرده‌فروش، محصول دیجیتال را دقیقاً مانند هر توکن یا NFT دیگری در کیف پول خود مشاهده می‌کند. او می‌تواند موجودی خود را ببیند، آن را به آدرس دیگری منتقل کند و تاریخچه تراکنش‌های آن را مشاهده نماید، همگی با استفاده از رابط کاربری آشنا و استاندارد کیف پول خود. این قابلیت همکاری [۴۴] با اکوسیستم موجود، نیاز به ساخت یک کیف پول اختصاصی را از بین برده و به کاربران اجازه می‌دهد تا از ابزارهایی که از قبل با آن آشنا هستند، استفاده کنند.

تجربه کاربری مصرف‌کننده نهایی

ساده‌ترین و در عین حال مهم‌ترین تجربه کاربری، متعلق به مصرف‌کننده نهایی است. این کاربر نباید با هیچ‌گونه پیچیدگی فنی درگیر شود. فرآیند برای او باید به سادگی یک کلیک باشد:

۱. مصرف‌کننده با دوربین تلفن همراه خود، کد QR روی محصول را اسکن می‌کند.
۲. تلفن به صورت خودکار یک صفحه وب را باز می‌کند.

[۴۴] $Interoperability$

۳. این صفحه وب، که با طراحی بصری و جذاب ساخته شده، اطلاعات کلیدی محصول را نمایش می‌دهد: نام، تصویر، تاریخ تولید و مهم‌تر از همه، یک تأییدیه اصالت واضح (مثلاً یک تیک سبز بزرگ) به همراه تاریخچه کامل مالکیت محصول در یک خط زمانی ساده و قابل فهم.

در پس‌زمینه این فرآیند ساده، برنامه وب در حال انجام همان فرآیند پیچیده اعتبارسنجی متن درهم‌سازی شده است، اما کاربر نهایی هیچ‌کدام از این‌ها را نمی‌بیند. او تنها نتیجه نهایی را دریافت می‌کند: این کالا اصیل است. این سادگی، هدف نهایی پروژه یعنی توانمندسازی مصرف‌کننده و ایجاد اعتماد را محقق می‌سازد.

۱-۹-۳ اهمیت آموزش و پشتیبانی

با وجود تمام تلاش‌ها برای ساده‌سازی تجربه کاربری، ماهیت نوآورانه این فناوری ایجاب می‌کند که فرآیندهای آموزش و پشتیبانی به عنوان بخشی جدایی‌ناپذیر از استقرار سیستم در نظر گرفته شوند[۲۱]. برگزاری کارگاه‌های آموزشی برای کاربران سازمانی، تهیه راهنماهای ویدیویی و متنی، و ایجاد یک کانال پشتیبانی برای پاسخگویی به سؤالات کاربران، نقشی حیاتی در کاهش مقاومت در برابر تغییر و تضمین استفاده صحیح و مؤثر از سامانه خواهد داشت.

۱-۱۰ چالش‌های قانونی و نظارتی

آخرین و شاید پیچیده‌ترین چالش، مربوط به انطباق سیستم با محیط قانونی و نظارتی کشور است. فناوری زنجیره بلوکی و دارایی‌های دیجیتال، مفاهیمی نسبتاً جدید هستند و چارچوب‌های قانونی برای آن‌ها در بسیاری از کشورها، از جمله ایران، هنوز در حال تکامل و بعضاً مبهم است. پروپوزال به درستی اشاره می‌کند که تطابق سیستم با قوانین داخلی کشور چالشی دیگر است چرا که بسیاری از ابزارها و فناوری‌ها در حوزه زنجیره بلوکی با قوانین فعلی ایران سازگاری ندارد[۲۲].

۱-۱۰-۱ ابهام در ماهیت حقوقی توکن‌ها

اولین سؤال قانونی این است که توکن دیجیتالی که نماینده یک کالای فیزیکی است، از نظر حقوقی چه ماهیتی دارد؟ آیا یک دارایی دیجیتال صرف است؟ آیا می‌تواند به عنوان یک سند بهادار [۴۵] تلقی شود؟ پاسخ به این سؤال، تأثیر مستقیمی بر قوانین حاکم بر صدور، انتقال و مالیات‌ستانی از آن خواهد داشت. فقدان یک تعریف قانونی روشن، می‌تواند ریسک حقوقی برای کسب‌وکارهایی که از این سیستم استفاده می‌کنند، به همراه داشته باشد.

[۴۵] *Security*

۱-۱۱ قوانین مربوط به ارزهای دیجیتال و پرداخت

اگرچه در این سیستم، پرداخت هزینه کالاها می‌تواند خارج از زنجیره انجام شود، اما خود تراکنش‌های زنجیره بلوکی نیازمند پرداخت هزینه گاز با استفاده از ارز دیجیتال (مانند اتر) است. قوانین مربوط به نگهداری و استفاده از ارزهای دیجیتال در کشور، همچنان دارای ابهاماتی است که باید در مدل تجاری نهایی پروژه در نظر گرفته شود.

۱-۱۱-۱ حریم خصوصی و حفاظت از داده‌ها

یکی از ویژگی‌های زنجیره بلوکی عمومی، شفافیت آن است. در حالی که این شفافیت برای ردیابی و اعتبارسنجی فوق‌العاده است، می‌تواند چالش‌هایی را برای حریم خصوصی و محرمانگی اطلاعات تجاری ایجاد کند. اطلاعاتی مانند حجم معاملات بین یک تولیدکننده و توزیع‌کننده، یا مسیرهای دقیق توزیع، می‌تواند برای رقبا بسیار ارزشمند باشد. طراحی سیستمی که بتواند بین نیاز به شفافیت برای حسابرسی و نیاز به محرمانگی برای حفظ مزیت رقابتی تعادل برقرار کند، یک چالش مهم است. راهکارهایی مانند استفاده از زنجیره‌های بلوکی خصوصی [۴۶] یا فناوری‌های اثبات با دانش صفر [۴۷] می‌توانند در آینده برای حل این مشکل مورد بررسی قرار گیرند.

۱-۱۱-۲ مسئولیت‌پذیری در یک محیط غیرمتمرکز

در صورت بروز خطا در یک قرارداد هوشمند که منجر به خسارت مالی شود، چه کسی از نظر قانونی مسئول است. قوانین سنتی که بر پایه نهادهای متمرکز بنا شده‌اند، پاسخ روشنی برای این سؤالات در یک محیط غیرمتمرکز ندارند. این ابهام، یکی دیگر از ریسک‌های حقوقی است که کسب‌وکارها در هنگام پذیرش این فناوری با آن روبرو هستند.

رویکرد پروژه در جهت انطباق‌پذیری

پروژه حاضر، با درک این چالش‌ها، یک گام هوشمندانه در جهت افزایش انطباق‌پذیری برداشته است. تعبیه قابلیت محاسبه خودکار مالیات در قرارداد هوشمند[۱۸]، نشان‌دهنده یک رویکرد پیشگیرانه برای همسوسازی سیستم با الزامات مالیاتی کشور است. این قابلیت، به نهادهای نظارتی نشان می‌دهد که این فناوری نه تنها برای فرار از قوانین طراحی نشده، بلکه می‌تواند ابزاری بسیار کارآمد برای افزایش شفافیت مالیاتی و تسهیل فرآیندهای نظارتی باشد. این رویکرد می‌تواند به عنوان یک نقطه قوت در گفتگو با نهادهای قانون‌گذار و جلب اعتماد آن‌ها مورد استفاده قرار گیرد.

---

[۴۶] $Private Blockchains$

[۴۷] $Zero-Knowledge Proofs$

فصل دوم

مرور پژوهش‌های پیشین و سامانه‌های مشابه

هدف اصلی این فصل، قرار دادن پژوهش حاضر در بستر علمی و صنعتی موجود است. برای درک عمیق راهکارها و وجه تمایز این پروژه، ضروری است که ابتدا راهکارهای پیشین و وضعیت فعلی فناوری در حوزه مدیریت زنجیره تأمین را به دقت مورد بررسی و نقد قرار دهیم. این فصل به دو بخش اصلی تقسیم می‌شود. در بخش اول، که در ادامه به تفصیل به آن پرداخته می‌شود، به تحلیل عمیق سامانه‌های مدیریت زنجیره تأمین سنتی و همچنین نسل اول راهکارهای دیجیتال غیرزنجیره بلوکی می‌پردازیم. این تحلیل نشان خواهد داد که چرا این راهکارها، با وجود تمام پیشرفت‌ها، در حل مشکلات بنیادین مربوط به اعتماد و شفافیت ناکام مانده‌اند. در بخش دوم، به صورت متمرکز به بررسی و تحلیل پروژه‌هایی خواهیم پرداخت که از فناوری زنجیره بلوکی در حوزه زنجیره تأمین بهره برده‌اند تا با مقایسه آن‌ها، جایگاه و راهکار پروژه حاضر به روشنی مشخص گردد.

۲-۱ تحلیل سامانه‌های سنتی و راهکارهای دیجیتال غیرزنجیره بلوکی

مفهوم مدیریت زنجیره تأمین [۱] در طول دهه‌های گذشته، تحولات بسیاری را تجربه کرده است. هدف اصلی در نگاه سنتی، همواره بر بهینه‌سازی و کارایی متمرکز بوده است. شرکت‌ها تلاش کرده‌اند تا با استفاده از سیستم‌های اطلاعاتی و مدل‌های ریاضی، هزینه‌های موجودی را کاهش دهند، زمان تحویل را به حداقل برسانند و فرآیندهای لجستیکی خود را بهینه کنند [۲۳]. با این حال، این تمرکز بر بهینه‌سازی داخلی، اغلب به قیمت نادیده گرفتن اهمیت جریان شفاف اطلاعات بین شرکای تجاری تمام شده است. در این بخش، ابتدا معماری سیستم‌های اطلاعاتی متمرکزی که ستون فقرات زنجیره‌های تأمین امروزی را تشکیل می‌ده، بررسی کرده و سپس به تحلیل نسل اول فناوری‌های دیجیتال که برای رفع برخی از این کاستی‌ها به کار گرفته شدند، می‌پردازیم.

۲-۱-۱ معماری سیستم‌های اطلاعاتی متمرکز در زنجیره تأمین

زنجیره تأمین مدرن، بدون سیستم‌های اطلاعاتی پیچیده قابل تصور نیست. این سیستم‌ها وظیفه مدیریت جریان عظیم اطلاعات، از ثبت سفارش یک مشتری تا برنامه‌ریزی تولید و ارسال نهایی کالا را بر عهده دارند. با این حال، معماری غالب این سیستم‌ها، یک معماری متمرکز و درون-سازمانی است که خود ریشه بسیاری از مشکلات امروزی است.

[۱] *Supply Chain Management – SCM*

سیستم‌های برنامه‌ریزی منابع سازمانی (ERP)

سیستم‌های برنامه‌ریزی منابع سازمانی یا ERP [۲]، به عنوان سیستم عصبی مرکزی اکثر شرکت‌های بزرگ و متوسط عمل می‌کنند. بسترهایی مانند SAP، $Oracle$ و $Microsoft Dynamics$، مجموعه‌ای یکپارچه از ماژول‌های نرم‌افزاری را برای مدیریت تمام جنبه‌های یک کسب‌وکار، از منابع انسانی و مالی گرفته تا تولید و فروش، فراهم می‌آورند. ماژول‌های مرتبط با زنجیره تأمین در یک سیستم ERP معمولاً شامل موارد زیر است:

- **مدیریت موجودی** [۳]: ردیابی سطح موجودی مواد اولیه، کالاهای در حال ساخت و محصولات نهایی در انبارها.
- **پردازش سفارش** [۴]: مدیریت چرخه کامل یک سفارش از زمان ثبت توسط مشتری تا تحویل نهایی.
- **مدیریت تدارکات** [۵]: خودکارسازی فرآیندهای مربوط به خرید مواد اولیه از تأمین‌کنندگان.
- **برنامه‌ریزی تولید** [۶]: برنامه‌ریزی و زمان‌بندی فرآیندهای تولید بر اساس پیش‌بینی تقاضا و سطح موجودی.

بزرگ‌ترین مزیت یک سیستم ERP، ایجاد یک منبع حقیقت واحد **درون مرزهای یک سازمان** است. تمام بخش‌های یک شرکت به داده‌های یکسان و به‌روزی دسترسی دارند که این امر هماهنگی داخلی را به شدت افزایش می‌دهد. با این حال، همین نقطه قوت، بزرگ‌ترین نقطه ضعف آن در مقیاس یک زنجیره تأمین است. یک سیستم ERP اساساً برای دنیای داخل یک شرکت طراحی شده و به صورت پیش‌فرض، دیدی نسبت به فرآیندهای تأمین‌کنندگانِ تأمین‌کنندگان یا مشتریانِ مشتریان خود ندارد.

سیستم‌های مدیریت زنجیره تأمین (SCM) و تبادل الکترونیکی داده (EDI)

برای حل مشکل ارتباط بین ERPهای شرکت‌های مختلف، سیستم‌های تخصصی‌تری به نام سیستم‌های مدیریت زنجیره تأمین (SCM) توسعه یافتند. این سیستم‌ها تلاش می‌کنند تا پلی بین سیستم‌های اطلاعاتی شرکای تجاری مختلف ایجاد کنند. یکی از قدیمی‌ترین و رایج‌ترین فناوری‌ها برای این منظور، تبادل الکترونیکی داده یا EDI [۷] است . EDI به شرکت‌ها اجازه می‌دهد تا اسناد تجاری استاندارد (مانند سفارش‌های خرید، فاکتورها و بارنامه‌ها) را به صورت الکترونیکی و با فرمت مشخصی برای یکدیگر ارسال کنند.

---

[۲] *Enterprise Resource Planning*
[۳] *Inventory Management*
[۴] *Order Processing*
[۵] *Procurement*
[۶] *Production Planning*
[۷] *Electronic Data Interchange*

با این حال، EDI نیز دارای محدودیت‌های جدی است:

- **هزینه و پیچیدگی بالا:** راه‌اندازی و نگهداری سیستم‌های EDI پرهزینه و پیچیده است و معمولاً تنها برای شرکت‌های بسیار بزرگ که با تعداد محدودی از شرکای اصلی و بلندمدت کار می‌کنند، مقرون‌به‌صرفه است.
- **عدم کار در زمان واقعی** [۸]: تبادل داده در EDI معمولاً به صورت دسته‌ای و در فواصل زمانی مشخص (مثلاً در پایان هر روز کاری) انجام می‌شود. این تأخیر در جریان اطلاعات، مانع از تصمیم‌گیری‌های سریع و واکنش به موقع به تغییرات بازار می‌شود.
- **ساختار غیرقابل انعطاف:** فرمت‌های EDI بسیار سختگیرانه و استاندارد شده هستند و تغییر یا افزودن اطلاعات جدید به آن‌ها دشوار است.

مشکل بنیادین: سیلوهای اطلاعاتی و اثر شلاقی

نتیجه نهایی معماری متمرکز و سیستم‌های ارتباطی ناکارآمد، پدیده‌ای است که از آن به عنوان سیلوهای اطلاعاتی [۹] یاد می‌شود. در این پدیده، هر شرکت در زنجیره تأمین (تولیدکننده، توزیع‌کننده، عمده‌فروش، خرده‌فروش) داده‌های خود را در یک پایگاه داده مجزا و ایزوله نگهداری می‌کند. جریان اطلاعات بین این سیلوها، کند، غیرقابل اعتماد و اغلب نیازمند ورود دستی داده است که خود منشأ بسیاری از خطاهاست.

یکی از مشهورترین و مخرب‌ترین پیامدهای سیلوهای اطلاعاتی، اثر شلاقی [۱۰] است [۲۴]. این پدیده توصیف می‌کند که چگونه نوسانات کوچک در تقاضای مشتری نهایی (در سطح خرده‌فروشی)، به صورت فزاینده‌ای در حین حرکت به سمت بالای زنجیره تأمین (به سمت تولیدکننده) تقویت می‌شود. برای مثال، یک افزایش ۱۰ درصدی در تقاضای مشتری، ممکن است باعث شود خرده‌فروش سفارش خود به عمده‌فروش را ۲۰ درصد افزایش دهد تا یک موجودی اطمینان برای خود ایجاد کند. عمده‌فروش نیز با مشاهده این افزایش، سفارش خود به تولیدکننده را ۴۰ درصد افزایش می‌دهد و این روند ادامه می‌یابد.

این تقویت نوسانات، ناشی از عدم قطعیت و فقدان دیدپذیری است. هر عضو زنجیره، تنها سفارش دریافتی از عضو پایین‌دستی خود را می‌بیند و دیدی نسبت به تقاضای واقعی مصرف‌کننده نهایی ندارد. این امر منجر به مشکلات زیر می‌شود:

- **موجودی مازاد و هزینه‌های نگهداری بالا:** تولیدکنندگان بر اساس سیگنال‌های تقاضای اغراق‌آمیز، بیش از حد تولید می‌کنند که منجر به انباشت موجودی در انبارها می‌شود.
- **کمبود موجودی:** در جهت معکوس، یک کاهش تقاضای موقتی نیز می‌تواند به صورت اغراق‌آمیز به بالا منتقل شده و باعث شود تولیدکننده تولید خود را بیش از حد کاهش دهد که منجر به کمبود کالا در زمان افزایش مجدد تقاضا می‌شود.

---

[۸] $Real-time$

[۹] $Information\ Silos$

[۱۰] $The\ Bullwhip\ Effect$

- **استفاده ناکارآمد از ظرفیت تولید و حمل‌ونقل:** نوسانات شدید در سفارش‌ها، برنامه‌ریزی پایدار برای تولید و لجستیک را غیرممکن می‌سازد.

اثر شلاقی، نمونه بارزی از این است که چگونه معماری اطلاعاتی یک زنجیره تأمین، تأثیر مستقیمی بر عملکرد مالی و عملیاتی آن دارد. این مشکل، یک مشکل محاسباتی یا لجستیکی صرف نیست، بلکه یک مشکل اطلاعاتی است که ریشه در عدم شفافیت و عدم اشتراک‌گذاری داده‌ها در زمان واقعی دارد.

۲-۱-۲ نسل اول دیجیتالی‌سازی: فناوری‌های ردیابی و شناسایی

در پاسخ به مشکلات دیدپذیری، نسل اول فناوری‌های دیجیتال با هدف بهبود فرآیندهای شناسایی و ردیابی کالاهای فیزیکی پدید آمدند. این فناوری‌ها تلاش کردند تا پلی بین دنیای فیزیکی محصولات و دنیای دیجیتال اطلاعات ایجاد کنند. با این حال، همانطور که خواهیم دید، این راهکارها نیز در نهایت به همان دیوارهای بلند سیلوهای اطلاعاتی برخورد کردند.

بارکدها و کدهای QR

بارکدها، به عنوان یک فناوری بسیار ارزان و فراگیر، انقلابی در مدیریت فروش و موجودی در سطح خرده‌فروشی ایجاد کردند. آن‌ها امکان شناسایی سریع و خودکار یک محصول را در پایانه فروش فراهم آوردند. کدهای QR [۱۱] نیز به عنوان نسل بعدی بارکدهای دوبعدی، قابلیت ذخیره‌سازی اطلاعات بیشتر (مانند یک آدرس وب) را فراهم کرده و استفاده از آن‌ها با دوربین تلفن‌های هوشمند را ممکن ساختند. با این حال، این فناوری‌ها دارای محدودیت‌های ذاتی هستند:

- **ماهیت ایستا و محدودیت داده:** یک بارکد یا کد QR معمولی، تنها یک شناسه ثابت را در خود جای داده است و اطلاعات آن به صورت پویا به‌روز نمی‌شود.
- **آسیب‌پذیری در برابر جعل:** کپی کردن و چاپ مجدد یک بارکد یا کد QR بسیار ساده است. این امر آن‌ها را به ابزاری غیرقابل اعتماد برای کاربردهای ضدجعل تبدیل می‌کند.
- **نیاز به اسکن دستی:** هر عنصر باید به صورت جداگانه و با قرار گرفتن در خط دید اسکنر، خوانده شود که این امر در مقیاس‌های بزرگ (مانند ورودی یک انبار) ناکارآمد است.

تفاوت کلیدی کد QR در پروژه حاضر با یک کد QR معمولی در این است که کد QR ما به یک شناسه ثابت اشاره نمی‌کند، بلکه به یک لینک پویا به یک پایگاه داده امن و تغییرناپذیر (یعنی زنجیره بلوکی) اشاره دارد.

[۱۱] *Quick Response*

۲-۱-۳ شناسایی با فرکانس رادیویی ($RFID$)

فناوری $RFID$ گام بزرگی رو به جلو برای غلبه بر محدودیت‌های بارکد بود. یک سیستم $RFID$ از دو جزء اصلی تشکیل شده است: یک برچسب [۱۲] که به محصول متصل می‌شود و حاوی یک شناسه منحصربه‌فرد است، و یک **خواننده** [۱۳] که با ارسال امواج رادیویی، می‌تواند اطلاعات برچسب‌ها را از راه دور و بدون نیاز به خط دید مستقیم بخواند [۲۵].

مزایای $RFID$ قابل توجه بود:

- **اسکن دسته‌ای و سریع:** یک خواننده $RFID$ می‌تواند صدها برچسب را در چند ثانیه شناسایی کند، که این امر فرآیندهایی مانند شمارش موجودی یا ثبت ورود و خروج کالا از انبار را به شدت تسریع می‌کند.
- **عدم نیاز به خط دید:** برچسب‌ها نیازی به دیده شدن توسط خواننده ندارند و می‌توانند در داخل بسته‌بندی یا کارتن قرار داشته باشند.
- **قابلیت ذخیره داده بیشتر:** برخی از برچسب‌های $RFID$ قابلیت نوشتن و بازنویسی داده را نیز دارند.

شرکت‌های بزرگی مانند والمارت [۱۴] در اوایل دهه ۲۰۰۰، سرمایه‌گذاری عظیمی بر روی این فناوری انجام دادند و تأمین‌کنندگان خود را ملزم به استفاده از برچسب‌های $RFID$ بر روی پالت‌ها و کارتن‌ها کردند. هدف، افزایش دیدپذیری در زنجیره تأمین و کاهش هزینه‌های ناشی از خطای انسانی بود. با وجود موفقیت‌های اولیه، پروژه‌های $RFID$ نیز با چالش‌هایی روبرو شدند، از جمله هزینه بالای برچسب‌ها (در مقایسه با بارکد) و مشکلات مربوط به تداخل امواج رادیویی.

اما مهم‌ترین محدودیت $RFID$، که اغلب نادیده گرفته می‌شود، این است که این فناوری نیز تنها ورودی داده را بهبود می‌بخشد. داده‌های جمع‌آوری شده توسط خواننده‌های $RFID$، در نهایت به همان پایگاه‌های داده متمرکز و ایزوله شرکت مربوطه ارسال می‌شدند. به عبارت دیگر، $RFID$ مشکل جمع‌آوری سریع داده را حل کرد، اما مشکل اشتراک‌گذاری امن و قابل اعتماد داده بین شرکای مختلف را دست‌نخورده باقی گذاشت. داده‌های $RFID$ نیز مانند هر داده دیگری در یک سرور متمرکز، قابل حذف یا دستکاری بودند.

اینترنت اشیاء (IoT) و حسگرهای هوشمند

اینترنت اشیاء یا IoT، تکامل طبیعی فناوری $RFID$ است. در اینجا، به جای یک برچسب غیرفعال، با حسگرهای هوشمند سروکار داریم که می‌توانند به صورت فعال، داده‌های محیطی را جمع‌آوری کرده و از طریق اینترنت ارسال کنند [۲۶]. این حسگرها می‌توانند پارامترهای مختلفی را اندازه‌گیری کنند:

---

[۱۲] Tag

[۱۳] $Reader$

[۱۴] $Walmart$

- **حسگرهای دما و رطوبت:** برای نظارت بر زنجیره سرد [۱۵] در حمل‌ونقل مواد غذایی، داروها و مواد شیمیایی حساس.
- **حسگرهای موقعیت‌یاب** (GPS): برای ردیابی دقیق و لحظه‌ای مکان محموله‌ها.
- **شتاب‌سنج‌ها:** برای تشخیص ضربه یا سقوط که می‌تواند به کالاهای حساس آسیب برساند.
- **حسگرهای باز شدن درب کانتینر:** برای افزایش امنیت و جلوگیری از سرقت.

ترکیب این حسگرها، یک جریان داده بسیار غنی و در زمان واقعی از وضعیت و شرایط یک محصول در طول زنجیره تأمین فراهم می‌کند. این سطح از دیدپذیری، در مدیریت کیفیت و امنیت، بی‌سابقه است. اما بار دیگر، همان مشکل بنیادین پدیدار می‌شود: این داده‌ها به کجا می‌روند؟

داده‌های ارزشمند جمع‌آوری شده توسط حسگرهای IoT، معمولاً به یک بستر ابری [۱۶] متمرکز که توسط ارائه‌دهنده سرویس IoT یا خود شرکت کنترل می‌شود، ارسال می‌گردد. این ساختار، تمام مشکلات یک سیستم متمرکز را به ارث می‌برد:

- **مالکیت و کنترل داده:** داده‌ها در انحصار یک شرکت باقی می‌مانند. شرکت حمل‌ونقل ممکن است به دلایل مختلف، از به اشتراک گذاشتن داده‌های کامل حسگر دما با صاحب کالا یا شرکت بیمه خودداری کند.
- **قابلیت دستکاری:** هیچ تضمین رمزنگاری‌شده‌ای وجود ندارد که داده‌های ثبت‌شده در بستر ابری، پس از ثبت تغییر نکرده باشند.
- **عدم وجود یک تاریخچه یکپارچه:** صاحب کالا ممکن است به داده‌های حسگر شرکت حمل‌ونقل A دسترسی داشته باشد، اما وقتی کالا به شرکت حمل‌ونقل B منتقل می‌شود، این دیدپذیری را از دست بدهد.

۲-۱-۴ جمع‌بندی: علت کافی نبودن راهکارهای سنتی و دیجیتال اولیه

تحلیل ارائه شده در این بخش نشان می‌دهد که با وجود دهه‌ها تلاش برای بهینه‌سازی و دیجیتالی‌سازی، زنجیره‌های تأمین همچنان با یک مشکل اساسی و حل‌نشده دست و پنجه نرم می‌کنند. این مشکل، یک مشکل فنی یا لجستیکی صرف نیست، بلکه یک مشکل اعتماد است. جدول زیر، خلاصه‌ای از محدودیت‌های راهکارهای بررسی شده را در برابر معیارهای کلیدی یک زنجیره تأمین ایده‌آل نشان می‌دهد.

---

[۱۵] $Cold\,Chain$

[۱۶] $Cloud\,Platform$

جدول ۲-۱: مقایسه محدودیت‌های راهکارهای مختلف

راهکار	شفافیت سرتاسری	امنیت/تغییرناپذیری	ایجاد اعتماد	عدم تمرکز
ERP / SCM سنتی	بسیار ضعیف	ضعیف	ضعیف	خیر
کد QR / بارکد	ضعیف	بسیار ضعیف	بسیار ضعیف	خیر
$RFID$	متوسط (درون‌سازمانی)	ضعیف	ضعیف	خیر
IoT / حسگرها	متوسط (بسته به بستر)	ضعیف	ضعیف	خیر

همانطور که در جدول ۲-۱ مشاهده می‌شود، هیچ‌یک از این راهکارها قادر به ارائه ترکیبی از شفافیت، امنیت و عدم تمرکز به صورت همزمان نیستند. مشکل اصلی این است که تمام این فناوری‌ها، در نهایت داده‌های خود را به یک مخزن متمرکز و قابل اعتماد فرضی ارسال می‌کنند، در حالی که در یک زنجیره تأمین که از ده‌ها شرکت مستقل تشکیل شده، چنین مخزن واحد و مورد اعتمادی وجود خارجی ندارد.

هر شرکت به داده‌های سیستم خود اعتماد دارد، اما دلیلی ندارد که به داده‌های ارسال‌شده از سوی شرکای تجاری خود (که ممکن است در فرمت‌های مختلف و با تأخیر ارسال شوند) اعتماد کامل داشته باشد. این عدم اعتماد متقابل، منجر به ایجاد فرآیندهای پرهزینه تطبیق [۱۷] می‌شود. شرکت‌ها تیم‌هایی را استخدام می‌کنند تا فاکتورها، بارنامه‌ها و رسیدهای خود را با اسناد ارسال‌شده از سوی شرکایشان مقایسه و مغایرت‌ها را برطرف کنند. این فرآیندها، منشأ اصلی ناکارآمدی، اتلاف وقت و اختلافات تجاری هستند.

در نهایت، این تحلیل ما را به یک نتیجه‌گیری اساسی می‌رساند: زنجیره تأمین مدرن، بیش از یک سیستم نرم‌افزاری جدید یا یک حسگر هوشمندتر، به یک لایه اعتماد [۱۸] مشترک، بی‌طرف و غیرمتمرکز نیاز دارد. زیرساختی که تمام شرکت‌کنندگان بتوانند داده‌های خود را با اطمینان بر روی آن ثبت کرده و به صحت داده‌های ثبت‌شده توسط دیگران نیز اعتماد کامل داشته باشند، زیرا این زیرساخت توسط هیچ نهاد واحدی کنترل نمی‌شود و قوانین آن توسط ریاضیات و رمزنگاری تضمین شده است.

این نیاز بنیادین به یک لایه اعتماد غیرمتمرکز، دقیقاً همان مسئله‌ای است که فناوری زنجیره بلوکی برای حل آن پدید آمده است. زنجیره بلوکی، با ارائه یک دفتر کل توزیع‌شده، شفاف و تغییرناپذیر، این پتانسیل را دارد که آن لایه اعتماد گمشده را فراهم کرده و مفهوم حاکم بر مدیریت زنجیره تأمین را به کلی دگرگون سازد. مبانی و جزئیات این راهکار نوین، موضوع اصلی بخش بعدی این فصل خواهد بود.

[۱۷] *Reconciliation*
[۱۸] *Trust Layer*

۲-۲ بررسی پروژه‌های زنجیره تأمین مبتنی بر زنجیره بلوکی

در بخش پیشین، به تفصیل نشان داده شد که چرا سامانه‌های سنتی و نسل اول راهکارهای دیجیتال، در حل چالش‌های بنیادین اعتماد و شفافیت در زنجیره تأمین ناکام بوده‌اند. مشخص شد که مشکل اصلی، نه کمبود داده، بلکه فقدان یک لایه اعتماد مشترک و غیرمتمرکز برای اعتبارسنجی و اشتراک‌گذاری امن داده‌ها بین شرکای تجاری ناهمگون است. این تحلیل، زمینه را برای ورود مفهوم نوین زنجیره بلوکی به این حوزه فراهم می‌کند. فناوری زنجیره بلوکی، با ارائه یک دفتر کل توزیع‌شده، شفاف و تغییرناپذیر، دقیقاً همان لایه اعتماد گمشده را ارائه می‌دهد.

در این بخش، به صورت عمیق به بررسی و تحلیل پروژه‌ها، بسترها و استانداردهایی می‌پردازیم که تلاش کرده‌اند از این پتانسیل عظیم برای متحول ساختن زنجیره تأمین بهره ببرند. این بررسی یک مسیر تکاملی را دنبال می‌کند: از نسل اول راهکارها که بر بسترهای خصوصی و افزایش شفافیت متمرکز بودند، تا نسل دوم که با بهره‌گیری از شبکه‌های عمومی و مفهوم نیزه‌سازی، قابلیت‌های جدیدی را به این عرصه افزودند. هدف نهایی این بررسی، شناسایی دقیق نقاط قوت و ضعف رویکردهای مختلف و در نهایت، مشخص کردن جایگاه راهکارمندانه و منحصربه‌فرد پروژه حاضر در این چشم‌انداز گسترده است.

۲-۲-۱ نسل اول راهکارها: تمرکز بر شفافیت و بسترهای خصوصی

در سال‌های اولیه معرفی زنجیره بلوکی به دنیای کسب‌وکار (تقریباً بین سال‌های ۲۰۱۴ تا ۲۰۱۸)، هیجان زیادی پیرامون این فناوری وجود داشت. بسیاری آن را به عنوان یک گلوله نقره‌ای [۱۹] برای حل تمام مشکلات زنجیره تأمین می‌دیدند. با این حال، استفاده از شبکه‌های زنجیره بلوکی عمومی و بدون نیاز به مجوز [۲۰] مانند بیت‌کوین یا اتریوم برای کاربردهای سازمانی، با موانع جدی روبرو بود:

- **مقیاس‌پذیری و هزینه:** این شبکه‌ها دارای توان پردازشی پایین و هزینه تراکنش گاز بالا و غیرقابل پیش‌بینی بودند.
- **حریم خصوصی:** تمام داده‌های ثبت‌شده بر روی یک زنجیره بلوکی عمومی، برای همه افراد در سراسر جهان قابل مشاهده است. این سطح از شفافیت برای اطلاعات حساس تجاری (مانند قیمت‌گذاری، حجم معاملات و هویت شرکا) غیرقابل قبول بود.
- **حاکمیت و کنترل:** در یک شبکه عمومی، هیچ نهاد مرکزی برای مدیریت شبکه، حل اختلافات یا کنترل دسترسی شرکت‌کنندگان وجود ندارد. این عدم کنترل برای محیط‌های تجاری که نیازمند قوانین و مقررات مشخص هستند، یک نقطه ضعف بزرگ محسوب می‌شد.

این چالش‌ها منجر به ظهور دسته‌ای جدید از بسترهای زنجیره بلوکی شد که به طور خاص برای نیازهای

[۱۹] *silver bullet*
[۲۰] *Permissionless*

سازمانی طراحی شده بودند: زنجیره‌های بلوکی خصوصی یا کنسرسیومی [۲۱]. در این مدل، به جای یک شبکه باز، یک شبکه بسته و نیازمند مجوز [۲۲] ایجاد می‌شود که تنها اعضای تأییدشده (مانند چند شرکت در یک زنجیره تأمین) می‌توانند در آن مشارکت کنند. این رویکرد، ضمن حفظ برخی از مزایای زنجیره بلوکی (مانند تغییرناپذیری و دفتر کل مشترک)، مشکلات مربوط به حریم خصوصی و حاکمیت را برطرف می‌کرد. برجسته‌ترین و تأثیرگذارترین بستر در این نسل از راهکارها، بدون شک $Hyperledger\ Fabric$ است.

معرفی و تحلیل عمیق بستر $Hyperledger\ Fabric$

$Hyperledger$ یک پروژه چتر [۲۳] متن‌باز است که در سال ۲۰۱۵ توسط بنیاد لینوکس [۲۴] با هدف ترویج و توسعه فناوری‌های زنجیره بلوکی برای کاربردهای سازمانی آغاز شد. این پروژه شامل چندین فریم‌ورک و ابزار مختلف است که مشهورترین آن‌ها، $Hyperledger\ Fabric$ است. $Fabric$ که توسعه آن توسط شرکت IBM رهبری می‌شد، با یک معماری کاملاً ماژولار و متفاوت از اتریوم طراحی شد تا به نیازهای خاص کسب‌وکارها پاسخ دهد.

معماری منحصربه‌فرد $Hyperledger\ Fabric$: برخلاف معماری یکپارچه اتریوم، $Fabric$ از یک رویکرد ماژولار بهره می‌برد که در آن وظایف مختلف شبکه (مانند اجرای تراکنش، اجماع و به‌روزرسانی دفتر کل) بین مؤلفه‌های مختلف تقسیم شده است [۲۷]. این معماری به انعطاف‌پذیری و مقیاس‌پذیری بیشتر کمک می‌کند. مؤلفه‌های کلیدی آن عبارتند از:

- **همتاها** ($Peers$): گره‌هایی در شبکه هستند که میزبان دفتر کل ($Ledger$) و قراردادهای هوشمند (که در $Fabric$ به آن کد زنجیره[۲۵] گفته می‌شود) هستند. همتاها تراکنش‌ها را اجرا و اعتبارسنجی می‌کنند.
- **سرویس ترتیب‌دهی** [۲۶]: این مؤلفه مسئول ایجاد اجماع بر روی ترتیب تراکنش‌ها و بسته‌بندی آن‌ها در بلوک‌های جدید است. $Fabric$ از الگوریتم‌های اجماع مختلفی مانند $Solo$ (برای توسعه) و $Raft$ یا $Kafka$ (برای تولید) پشتیبانی می‌کند که برخلاف اثبات کار [۲۷] در اتریوم، نیازی به استخراج پرمصرف ندارند.
- **کانال‌ها** [۲۸]: این یکی از نوآورانه‌ترین ویژگی‌های $Fabric$ است. کانال یک مکانیزم ارتباطی

[۲۱] $Blockchains\ Consortium/Private$
[۲۲] $Permissioned$
[۲۳] $umbrella\ project$
[۲۴] $Foundation\ Linux$
[۲۵] $Chaincode$
[۲۶] $Ordering\ Service$
[۲۷] $Proof-of-Work$
[۲۸] $Channels$

خصوصی بین زیرمجموعه‌ای از اعضای شبکه است. هر کانال، دفتر کل مخصوص به خود را دارد و تراکنش‌های انجام‌شده در یک کانال، تنها برای اعضای همان کانال قابل مشاهده است. این ویژگی، راهکاری قدرتمند برای حل مشکل حریم خصوصی داده‌ها ارائه می‌دهد. برای مثال، در یک زنجیره تأمین، تولیدکننده و یک توزیع‌کننده خاص می‌توانند یک کانال خصوصی برای ثبت معاملات و قیمت‌گذاری‌های محرمانه خود داشته باشند، در حالی که سایر اعضای شبکه از آن بی‌اطلاع هستند.

- **کد زنجیره:** منطق کسب‌وکار در $Fabric$ در قالب کد زنجیره نوشته می‌شود. برخلاف اتریوم که تنها از زبان $Solidity$ پشتیبانی می‌کند، کد زنجیره را می‌توان با زبان‌های برنامه‌نویسی عمومی مانند Go، $Node.js$ و $Java$ نوشت که این امر توسعه را برای برنامه‌نویسان وب آسان‌تر می‌کند.
- **سیاست‌های تأیید** [۲۹]: برای هر کد زنجیره می‌توان یک سیاست تأیید تعریف کرد که مشخص می‌کند یک تراکنش برای معتبر بودن، باید توسط کدام یک از همتاهای شبکه تأیید (امضا) شود. برای مثال، می‌توان سیاستی تعریف کرد که طبق آن، یک تراکنش انتقال مالکیت باید هم توسط فروشنده و هم توسط خریدار تأیید شود.

مزایا و معایب $Hyperledger\ Fabric$ در زنجیره تأمین:

این معماری منحصربه‌فرد، مزایای قابل توجهی برای کاربردهای زنجیره تأمین به همراه داشت:

- **محرمانگی داده‌ها:** قابلیت ایجاد کانال‌های خصوصی، بزرگ‌ترین مزیت $Fabric$ بود که به شرکت‌ها اجازه می‌داد تا داده‌های حساس خود را تنها با شرکای مورد نظر به اشتراک بگذارند.
- **توان پردازشی بالا:** به دلیل استفاده از الگوریتم‌های اجماع سبک‌تر و عدم نیاز به مشارکت تمام گره‌ها در تمام تراکنش‌ها، $Fabric$ می‌تواند به توان پردازشی بسیار بالاتری (هزاران تراکنش در ثانیه) نسبت به شبکه‌های عمومی دست یابد.
- **عدم وجود هزینه گاز:** در $Fabric$، هزینه تراکنش به صورت مستقیم (مانند گاز در اتریوم) وجود ندارد. هزینه‌ها بیشتر مربوط به زیرساخت‌های محاسباتی برای اجرای گره‌ها و مدیریت شبکه است.
- **شبکه نیازمند مجوز:** امکان کنترل دقیق اینکه چه کسی می‌تواند به شبکه بپیوندد و چه مجوزهایی داشته باشد، برای محیط‌های تجاری که نیازمند حاکمیت مشخص هستند، یک مزیت کلیدی بود.

[۲۹] $Endorsement\ Policies$

با این حال، این رویکرد با چالش‌ها و معایبی نیز همراه بود:

- **پیچیدگی در راه‌اندازی و مدیریت:** راه‌اندازی یک شبکه $Fabric$ با چندین سازمان، کانال و سیاست‌های مختلف، بسیار پیچیده‌تر از استقرار یک قرارداد هوشمند بر روی شبکه اتریوم است.
- **ریسک تمرکزگرایی مجدد:** در یک شبکه کنسرسیومی، اگر تعداد اعضا کم باشد یا قدرت در دست چند عضو بزرگ متمرکز شود، ریسک تبانی و بازگشت به نوعی از تمرکزگرایی وجود دارد. اعتماد در اینجا از کد به حاکمیت کنسرسیوم منتقل می‌شود.
- **فقدان قابلیت همکاری با اکوسیستم عمومی:** شبکه‌های $Fabric$ ایزوله هستند و به صورت پیش‌فرض نمی‌توانند با دارایی‌ها و پروتکل‌های موجود در شبکه‌های عمومی مانند اتریوم (مانند پروتکل‌های مالی غیرمتمرکز یا $DeFi$) تعامل داشته باشند.

مطالعات موردی برجسته با $Hyperledger\ Fabric$

برای درک بهتر تأثیر عملی این بستر، دو مورد از بزرگ‌ترین و مشهورترین پروژه‌های زنجیره تأمین که بر پایه $Fabric$ ساخته شده‌اند را بررسی می‌کنیم.

مطالعه موردی اول: $IBM\ Food\ Trust$ صنعت مواد غذایی یکی از اولین و مستعدترین حوزه‌ها برای پذیرش فناوری زنجیره بلوکی بود. شیوع بیماری‌های ناشی از مواد غذایی آلوده و نیاز به فراخوان سریع محصولات از بازار، هزینه‌های هنگفتی را به شرکت‌ها تحمیل کرده و جان مصرف‌کنندگان را به خطر می‌انداخت. مشکل اصلی این بود که ردیابی منشأ یک محصول آلوده در یک زنجیره تأمین پیچیده، ممکن بود روزها یا حتی هفته‌ها طول بکشد.

شرکت IBM با همکاری غول‌های خرده‌فروشی مانند $Walmart$، پروژه $Trust\ Food$ را بر پایه $Hyperledger\ Fabric$ راه‌اندازی کرد [۲۸]. هدف این بستر، ایجاد یک دفتر کل مشترک و تغییرناپذیر برای ثبت تمام رویدادهای مربوط به یک محصول غذایی، از مزرعه تا قفسه فروشگاه، بود.

- **نحوه عملکرد:** هر شرکت‌کننده در زنجیره (کشاورز، فرآوری‌کننده، شرکت حمل‌ونقل، خرده‌فروش) یک گره در شبکه $Fabric$ اجرا می‌کند. اطلاعات مربوط به هر بچ از محصول (مانند تاریخ برداشت، گواهی‌های ارگانیک، اطلاعات حمل‌ونقل و...) به عنوان یک دارایی [۳۰] در دفتر کل ثبت می‌شود. هر مرحله از انتقال، به عنوان یک تراکنش جدید ثبت شده و یک تاریخچه کامل و قابل ردیابی ایجاد می‌کند.
- **دستاورد اصلی:** بزرگ‌ترین دستاورد $Food\ Trust$، کاهش چشمگیر زمان ردیابی بود. در یکی از پایلوت‌های اولیه با $Walmart$، زمان لازم برای ردیابی منشأ یک بسته انبه از ۶ روز و ۱۸ ساعت به تنها ۲.۲ ثانیه کاهش یافت. این سرعت، امکان واکنش سریع در مواقع بحرانی و جلوگیری از توزیع گسترده محصولات آلوده را فراهم می‌کند.

[۳۰] $Asset$

- **چالش‌ها و درس‌آموخته‌ها:** با وجود موفقیت فنی، $Food\ Trust$ با چالش پذیرش نیز روبرو شد. متقاعد کردن هزاران کشاورز و تأمین‌کننده کوچک برای پیوستن به بستر و ثبت دقیق داده‌ها، یک چالش بزرگ بود. همچنین، مدل کسب‌وکار مبتنی بر حق عضویت، برای بازیگران کوچک‌تر جذابیت کمتری داشت. این پروژه نشان داد که موفقیت یک راهکار زنجیره بلوکی، تنها به فناوری آن بستگی ندارد، بلکه به شدت به مدل کسب‌وکار، حاکمیت شبکه و ایجاد انگیزه برای تمام شرکت‌کنندگان وابسته است.

مطالعه موردی دوم: $TradeLens$ صنعت حمل‌ونقل کانتینری بین‌المللی، یکی از پیچیده‌ترین زنجیره‌های تأمین در جهان است. یک محموله ساده ممکن است در طول سفر خود توسط ۳۰ نهاد مختلف (از جمله گمرک، مقامات بندری، شرکت‌های حمل‌ونقل زمینی و دریایی) و با استفاده از بیش از ۲۰۰ تعامل و تبادل سند مختلف، جابجا شود. این فرآیند که عمدتاً مبتنی بر کاغذبازی و سیستم‌های ارتباطی قدیمی است، مملو از ناکارآمدی، تأخیر و ریسک خطا است. برای حل این مشکل، دو غول این صنعت، شرکت کشتیرانی $Maersk$ و شرکت فناوری IBM، با یکدیگر همکاری کرده و بستر $TradeLens$ را بر پایه $Hyperledger\ Fabric$ ایجاد کردند. هدف $TradeLens$، دیجیتالی کردن و ایجاد یک منبع حقیقت واحد برای تمام اسناد و رویدادهای مربوط به یک محموله کانتینری بود.

- **نحوه عملکرد:** بستر به تمام طرف‌های درگیر اجازه می‌دهد تا به صورت آنی و امن، به اسناد حمل‌ونقل، اطلاعات گمرکی و وضعیت لحظه‌ای کانتینرها دسترسی داشته باشند. این دیدپذیری سرتاسری، هماهنگی بین نهادهای مختلف را به شدت بهبود بخشیده و نیاز به ارسال فیزیکی یا فکس اسناد را از بین می‌برد.
- **چالش اصلی: اثر شبکه‌ای** [۳۱]: بزرگ‌ترین چالش $TradeLens$، متقاعد کردن رقبای $Maersk$ (یعنی سایر خطوط کشتیرانی بزرگ) برای پیوستن به یک بستر بود که توسط رقیب اصلی آن‌ها رهبری می‌شد. بسیاری از شرکت‌ها نگران بودند که $Maersk$ به داده‌های حساس آن‌ها دسترسی پیدا کند. اگرچه معماری $Fabric$ با استفاده از کانال‌ها می‌توانست این نگرانی را از نظر فنی برطرف کند، اما چالش اصلی، یک چالش اعتماد تجاری بود، نه یک مشکل فنی.
- **درس‌آموخته‌ها:** $TradeLens$ نشان داد که در یک کنسرسیوم، حاکمیت باید کاملاً بی‌طرف و غیرمتمرکز باشد. در نهایت، این بستر با پیوستن سایر غول‌های کشتیرانی مانند $CGM\ CMA$ و MSC توانست بر این چالش غلبه کند، اما این فرآیند سال‌ها طول کشید. این مورد تأکید می‌کند که موفقیت یک شبکه کنسرسیومی، نیازمند یک مدل حاکمیتی قوی و مورد اعتماد همه اعضاست.

در مجموع، نسل اول راهکارها با استفاده از بسترهای خصوصی مانند $Fabric$، توانستند با موفقیت مشکل حریم خصوصی را حل کرده و کاربردهای عملی و تأثیرگذار زنجیره بلوکی را در مقیاس سازمانی به نمایش

[۳۱] $Effect\ Network$

بگذارند. با این حال، پیچیدگی و ماهیت ایزوله این شبکه‌ها، زمینه را برای ظهور نسل دومی از راهکارها فراهم کرد که تلاش می‌کردند از قدرت و قابلیت همکاری اکوسیستم‌های عمومی بهره ببرند.

۲-۲-۲ نسل دوم راهکارها: استفاده از شبکه‌های عمومی و نشانه‌سازی

با بلوغ اکوسیستم زنجیره بلوکی، محدودیت‌های اولیه شبکه‌های عمومی تا حد زیادی برطرف یا کمرنگ شد. ظهور راهکارهای مقیاس‌پذیری لایه ۲ و زنجیره‌های جانبی سازگار با EVM، هزینه و سرعت تراکنش‌ها را به سطحی رساند که برای کاربردهای تجاری قابل قبول بود. این تحول، همراه با درک عمیق‌تر از مزایای شبکه‌های عمومی، منجر به یک تغییر مفهوم به سمت استفاده از این شبکه‌ها برای کاربردهای زنجیره تأمین شد.

مزایای کلیدی شبکه‌های عمومی عبارتند از:

- **عدم تمرکز واقعی:** امنیت شبکه توسط هزاران اعتبارسنج ناشناس در سراسر جهان تأمین می‌شود که این امر، ریسک تبانی یا کنترل توسط یک نهاد واحد را تقریباً به صفر می‌رساند.
- **قابلیت همکاری:** دارایی‌های ایجاد شده بر روی یک شبکه عمومی (مانند توکن‌های نماینده محصولات)، می‌توانند به راحتی با هزاران برنامه و پروتکل دیگر در همان اکوسیستم تعامل داشته باشند. برای مثال، می‌توان یک دارایی زنجیره تأمین را در یک پروتکل مالی غیرمتمرکز ($DeFi$) به عنوان وثیقه برای دریافت وام استفاده کرد.
- **دسترسی بدون نیاز به مجوز:** هر کسی می‌تواند بدون نیاز به کسب اجازه، یک قرارداد هوشمند را بر روی شبکه مستقر کرده و یک برنامه کاربردی ایجاد کند. این امر نوآوری را به شدت تسریع می‌کند.

مفهوم محوری که این نسل از راهکارها را به پیش می‌راند، نشانه‌سازی دارایی‌ها [۳۲] است.

نشانه‌سازی دارایی‌ها در زنجیره تأمین

نشانه‌سازی، فرآیند ایجاد یک نماینده دیجیتال (یک نشانه) برای یک دارایی واقعی یا دیجیتال بر روی یک شبکه زنجیره بلوکی است. این نشانه، مالکیت آن دارایی را نمایندگی می‌کند و می‌تواند بر اساس قوانین تعریف‌شده در یک قرارداد هوشمند، منتقل، معامله یا مدیریت شود.

نشانه‌سازی، دارایی‌های سنتی و غیرنقدشونده را به دارایی‌هایی برنامه‌پذیر تبدیل می‌کند. وقتی یک کالای فیزیکی در زنجیره تأمین به یک نشانه دیجیتال تبدیل می‌شود، مزایای زیر حاصل می‌گردد:

- **مالکیت شفاف و قابل تأیید:** مالکیت نشانه به صورت شفاف بر روی زنجیره بلوکی ثبت شده و هر کسی می‌تواند با اطمینان، مالک فعلی آن را شناسایی کند.

[۳۲] $Asset\ Tokenization$

- **انتقال آنی و همتا به همتا:** انتقال مالکیت، به سادگی انتقال نشانه از یک کیف پول دیجیتال به دیگری است. این فرآیند در چند ثانیه و بدون نیاز به هیچ واسطه‌ای انجام می‌شود.
- **قابلیت تقسیم‌پذیری** [۳۳]: می‌توان مالکیت یک دارایی گران‌قیمت (مانند یک محموله بزرگ) را به چندین نشانه کوچک‌تر تقسیم کرد و به چندین نفر فروخت.
- **دسترسی به بازارهای جهانی:** نشانه‌ها می‌توانند به راحتی در بازارهای دیجیتال جهانی لیست شده و با نقدینگی بسیار بالاتری نسبت به دارایی فیزیکی معامله شوند.

برای پیاده‌سازی نشانه‌سازی، مجموعه‌ای از استانداردهای فنی توسعه یافته‌اند که اطمینان می‌دهند نشانه‌های ایجاد شده توسط برنامه‌های مختلف، با یکدیگر سازگار و قابل تعامل هستند. در اکوسیستم اتریوم، این استانداردها به نام ERC [۳۴] شناخته می‌شوند.

تحلیل عمیق استانداردهای نشانه ERC در زنجیره تأمین

انتخاب استاندارد نشانه مناسب، یکی از مهم‌ترین تصمیمات معماری در طراحی یک سیستم زنجیره تأمین مبتنی بر زنجیره بلوکی است. هر استاندارد، برای نوع خاصی از دارایی طراحی شده و دارای مزایا و محدودیت‌های خود است.

استاندارد نشانه‌های مثلی $ERC-20$: $ERC-20$ [۳۵]اولین و مشهورترین استاندارد نشانه در اتریوم است که در سال ۲۰۱۵ معرفی شد. این استاندارد، یک رابط کاربری مشترک برای نشانه‌هایی تعریف می‌کند که مثلی هستند؛ یعنی هر واحد از آن‌ها با هر واحد دیگری از همان نشانه، قابل تعویض و دارای ارزش یکسان است. بهترین مثال برای یک دارایی مثلی، پول است: یک اسکناس ۱۰ دلاری با هر اسکناس ۱۰ دلاری دیگری ارزش یکسانی دارد.
توابع کلیدی استاندارد $ERC-20$ عبارتند از:

- $totalSupply()$: تعداد کل نشانه‌های موجود را برمی‌گرداند.
- $balanceOf(address account)$: موجودی نشانه یک آدرس خاص را نشان می‌دهد.
- $transfer(address recipient, uint256 amount)$: تعداد مشخصی نشانه را به یک آدرس دیگر منتقل می‌کند.
- $approve(address spender, uint256 amount)$: به یک آدرس دیگر اجازه می‌دهد تا از طرف شما، تا سقف مشخصی نشانه خرج کند.

[۳۳] $Fractionalization$
[۳۴] $Ethereum\ Request\ for\ Comment$
[۳۵] $Fungible\ Tokens$

- $transferFrom(address\,sender,\ address\,recipient,\ uint256\,amount)$: توسط آدرس $spender$ برای انتقال نشانه از $sender$ به $recipient$ استفاده می‌شود.

$ERC-20$ برای نمایندگی کالاهای انبوه و قابل تعویض بسیار مناسب است. برای مثال، یک شرکت کشاورزی می‌تواند موجودی گندم خود را در قالب نشانه‌های $ERC-20$ (مثلاً هر نشانه نماینده یک کیلوگرم گندم) نشانه کند. این نشانه‌ها می‌توانند به راحتی بین تولیدکنندگان، توزیع‌کنندگان و کارخانه‌ها منتقل و معامله شوند ولی این استاندارد به هیچ عنوان قادر به نمایندگی دارایی‌های منحصربه‌فرد نیست. تمام نشانه‌های یک قرارداد $ERC-20$ یکسان هستند و راهی برای تمایز قائل شدن بین آن‌ها وجود ندارد. این امر استفاده از آن را برای ردیابی عنصرهای خاص و غیرمثلی غیرممکن می‌سازد.

استاندارد نشانه‌های غیرمثلی $ERC-721$: برای حل محدودیت $ERC-20$، استاندارد $ERC-721$[۳۶] در سال ۲۰۱۸ و با الهام از پروژه محبوب $CryptoKitties$ معرفی شد. این استاندارد برای نمایندگی دارایی‌هایی طراحی شده که هر کدام منحصربه‌فرد و غیرقابل تعویض هستند. هر نشانه در یک قرارداد $ERC-721$ دارای یک شناسه یکتا است که آن را از تمام نشانه‌های دیگر متمایز می‌کند.
ویژگی‌های کلیدی $ERC-721$ عبارتند از:

- هر نشانه یک شناسه منحصربه‌فرد و یک مالک مشخص دارد.
- تابعی مانند $ownerOf(uint256\,tokenId)$ وجود دارد که مالک یک نشانه خاص را برمی‌گرداند.
- انتقال مالکیت به صورت یک به یک انجام می‌شود؛ یعنی یک نشانه خاص از یک مالک به مالک دیگر منتقل می‌گردد.

$ERC-721$ راهکاری ایده‌آل برای ردیابی کالاهای با ارزش و منحصربه‌فرد است. هر NFT می‌تواند به عنوان شناسنامه دیجیتال یک عنصر خاص عمل کند. برخی از کاربردهای آن عبارتند از:

- **کالاهای لوکس:** ردیابی یک ساعت سوئیسی یا یک کیف دستی برند با شماره سریال مشخص.
- **صنعت خودروسازی:** ایجاد یک NFT برای هر خودرو که تاریخچه تعمیرات، تصادفات و مالکیت آن را ثبت می‌کند.
- **هنر و کلکسیون:** اثبات اصالت و تاریخچه مالکیت یک اثر هنری.
- **اسناد رسمی:** نشانه کردن اسناد مالکیت املاک یا گواهی‌های تحصیلی.

ولی از محدودیت های آن باید اشاره به این کرد که در حالی که $ERC-721$ برای عنصرهای منحصربه‌فرد عالی است، برای مدیریت کالاهای مثلی یا نیمه‌مثلی بسیار ناکارآمد است. فرض کنید یک شرکت بخواهد ۱۰۰۰ عدد از یک قطعه یدکی یکسان را منتقل کند. با استفاده از $ERC-721$، باید ۱۰۰۰ نشانه مجزا (با شماره شناسه متفاوت) ساخته شود و انتقال آن‌ها نیازمند ۱۰۰۰ تراکنش جداگانه خواهد بود. این فرآیند از نظر هزینه گاز و سرعت، بسیار ناکارآمد و غیراقتصادی است.

[۳۶] $NFTs - Tokens\ Non-Fungible$

استاندارد چند-نشانه ای $ERC-1155$: با توجه به محدودیت‌های دو استاندارد قبلی، مشخص شد که بسیاری از کاربردها (به ویژه بازی‌های کامپیوتری و زنجیره تأمین) نیازمند یک راهکار ترکیبی هستند که بتواند هر دو نوع دارایی مثلی و غیرمثلی را به صورت همزمان و کارآمد مدیریت کند. این نیاز منجر به توسعه استاندارد $ERC-1155$ توسط تیم پروژه $Enjin$ در سال ۲۰۱۸ شد. $ERC-1155$[۳۷] یک استاندارد چند-نشانهی است که به یک قرارداد هوشمند واحد اجازه می‌دهد تا تعداد نامحدودی از انواع نشانه‌های مختلف (اعم از مثلی و غیرمثلی) را مدیریت کند.

نوآوری کلیدی $ERC-1155$: ایده اصلی در این استاندارد، تفکیک نوع نشانه از تعداد آن است. در حالی که در $ERC-721$ هر نشانه یک موجودیت مستقل بود، در $ERC-1155$ ما با کلاس‌های نشانه سروکار داریم که هر کدام با یک شناسه (id) مشخص می‌شوند. سپس برای هر آدرس، موجودی آن از هر کلاس نشانه به صورت یک عدد ($amount$) ذخیره می‌شود.

- برای نمایندگی یک **نشانه غیرمثلی** (NFT)، یک کلاس نشانه جدید با یک id منحصربه‌فرد ایجاد کرده و تنها یک واحد ($amount = 1$) از آن را به یک مالک اختصاص می‌دهیم.
- برای نمایندگی یک **نشانه مثلی** [۳۸]، یک کلاس نشانه با یک id مشخص ایجاد کرده و می‌توانیم هر تعداد از آن را بین مالکان مختلف توزیع کنیم.

این معماری، قدرت و انعطاف‌پذیری بی‌نظیری را فراهم می‌کند. توابع اصلی این استاندارد نیز این ماهیت دوگانه را بازتاب می‌دهند:

- balanceOf(address account, uint256 id): موجودی یک آدرس خاص از یک کلاس نشانه مشخص را برمی‌گرداند.
- safeTransferFrom(address from,... bytes data): تعداد مشخصی ($amount$) از یک کلاس نشانه (id) را منتقل می‌کند.
- balanceOfBatch(address[] accounts, uint256[] ids): موجودی چندین آدرس از چندین کلاس نشانه را در یک فراخوانی واحد برمی‌گرداند.
- safeBatchTransferFrom(address from,... bytes data): این تابع، قابلیت کلیدی و انقلابی این استاندارد است. این تابع اجازه می‌دهد تا چندین نوع نشانه مختلف با مقادیر متفاوت، همگی در یک تراکنش واحد منتقل شوند.

این استاندارد، پاسخی مستقیم به نیازهای پیچیده زنجیره تأمین مدرن است. پروژه حاضر با انتخاب هوشمندانه این استاندارد[۱۵]، از مزایای زیر بهره‌مند می‌شود:

---

[۳۷] $The\ Multi-Token\ Standard$

[۳۸] $Fungible$

۱. **کارایی بی‌نظیر:** فرض کنید یک کارخانه خودروسازی، یک خودروی جدید را به یک نمایندگی ارسال می‌کند. این محموله شامل خود خودرو (یک عنصر غیرمثلی)، ۴ حلقه لاستیک (یک دسته از عنصرهای مثلی) و ۱۰ لیتر روغن موتور (یک دسته دیگر از عنصرهای مثلی) است. با استفاده از استانداردهای قدیمی، این فرآیند نیازمند چندین تراکنش مجزا بود. اما با $ERC-1155$، تمام این دارایی‌ها را می‌توان با فراخوانی تابع $safeBatchTransferFrom$ در یک تراکنش واحد و بهینه منتقل کرد. این امر به شدت هزینه گاز را کاهش داده و توان عملیاتی سیستم را بالا می‌برد.

۲. **انعطاف‌پذیری کامل:** سیستم طراحی‌شده در این پروژه، محدود به یک نوع کالا نیست. این سیستم می‌تواند به صورت همزمان یک قطعه ماشین‌آلات سنگین و منحصربه‌فرد را به عنوان یک NFT و هزاران پیچ و مهره استاندارد را به عنوان نشانه‌های مثلی، همگی در یک قرارداد واحد مدیریت کند.

۳. **سادگی در توسعه و مدیریت:** به جای نگهداری و مدیریت ده‌ها قرارداد هوشمند مختلف برای انواع محصولات، تمام منطق در یک قرارداد واحد متمرکز شده است. این امر، توسعه، تست و به‌روزرسانی سیستم را در آینده بسیار آسان‌تر می‌کند.

انتخاب $ERC-1155$ نشان‌دهنده بلوغ معماری پروژه و درک عمیق از نیازهای عملیاتی یک زنجیره تأمین واقعی است.

مطالعات موردی با استفاده از شبکه‌های عمومی

با جذاب‌تر شدن شبکه‌های عمومی، پروژه‌های متعددی تلاش کرده‌اند تا از این بسترها برای کاربردهای زنجیره تأمین استفاده کنند.

- **بستر $VeChain$ (VET):** $VeChain$ یک زنجیره بلوکی عمومی است که از ابتدا به طور خاص با هدف کاربردهای سازمانی و زنجیره تأمین طراحی شده است. این بستر از یک مدل دو-نشانه ای استفاده می‌کند (VET برای ارزش و $VTHO$ برای پرداخت هزینه تراکنش‌ها) تا هزینه گاز را برای شرکت‌ها قابل پیش‌بینی‌تر کند. $VeChain$ با شرکت‌های بزرگی در صنایع مختلف از جمله کالاهای لوکس ($LVMH$) و ایمنی مواد غذایی همکاری کرده و با ترکیب برچسب‌های $RFID/NFC$ با زنجیره بلوکی، راهکارهای ردیابی جامعی ارائه داده است.
- **پروژه‌های اصالت‌سنجی کالاهای لوکس:** شرکت‌هایی مانند $Arianee$ از NFTها بر روی شبکه اتریوم برای ایجاد یک پاسپورت دیجیتال برای کالاهای لوکس استفاده می‌کنند. هر محصول دارای یک NFT منحصربه‌فرد است که تاریخچه مالکیت آن را ثبت کرده و اصالت آن را تضمین می‌کند. این NFT می‌تواند به همراه کالای فیزیکی به مالک بعدی منتقل شود.

این پروژه‌ها نشان‌دهنده روند رو به رشد استفاده از شبکه‌های عمومی و نشانه‌سازی برای حل مشکلات زنجیره تأمین هستند.

۲-۲-۳ تحلیل ساختار پروژه و استاندارد انتخابی

پس از بررسی دقیق نسل‌های مختلف راهکارهای زنجیره بلوکی، از بسترهای خصوصی مانند $Hyperledger\ Fabric$ گرفته تا راهکارهای مبتنی بر استانداردهای مختلف نشانه در شبکه‌های عمومی، اکنون می‌توانیم جایگاه پروژه حاضر را در این چشم‌انداز مشخص کنیم. جدول زیر یک مقایسه کیفی بین رویکردهای اصلی ارائه می‌دهد:

جدول ۲-۲: مقایسه کیفی رویکردهای مختلف زنجیره بلوکی برای زنجیره تأمین

معیار	$Hyperledger\ Fabric$	$ERC-721$	$ERC-1155$
حریم خصوصی داده	عالی	ضعیف	ضعیف
توان پردازشی	بالا	پایین	متوسط
قابلیت همکاری	بسیار ضعیف	عالی	عالی
انعطاف‌پذیری دارایی	متوسط	ضعیف	عالی
هزینه تراکنش	پایین	بالا	متوسط
عدم تمرکز	متوسط	کامل	کامل

تحلیل جدول ۲-۲:

- بسترهای خصوصی مانند $Fabric$، با قربانی کردن عدم تمرکز و قابلیت همکاری، به حریم خصوصی و توان پردازشی دست یافتند، اما در یک اکوسیستم ایزوله باقی ماندند.
- راهکارهای مبتنی بر $ERC-721$ بر روی شبکه‌های عمومی، قابلیت همکاری را فراهم کردند، اما برای مدیریت زنجیره‌های تأمین با محصولات متنوع، ناکارآمد و گران بودند.

راهکار های پروژه در برطرف سازی نیاز ها. این پروژه با اتخاذ یک رویکرد چندلایه و هوشمندانه، تلاش می‌کند تا بهترین ویژگی‌های هر دو جهان را با یکدیگر ترکیب کند:

۱. **انتخاب استراتژیک** $ERC-1155$: همانطور که به تفصیل شرح داده شد، این استاندارد به تنهایی مشکل مدیریت دارایی‌های متنوع را به کارآمدترین شکل ممکن حل می‌کند و پایه و اساس یک زنجیره تأمین انعطاف‌پذیر را فراهم می‌آورد.

۲. **معماری هوشمند برای مدیریت فراداده:** این پروژه به جای نادیده گرفتن مشکل هزینه ذخیره‌سازی، با ارائه یک راهکار مبتنی بر تابع درهم سازی $Keccak256$ و ذخیره‌سازی خارج از زنجیره، یک معماری اقتصادی و در عین حال امن را برای مدیریت فراداده‌ها پیاده‌سازی می‌کند. این مکانیزم، یکپارچگی داده‌ها را بدون تحمیل هزینه‌های گزاف زنجیره بلوکی تضمین می‌نماید.

۳. **نگاه آینده‌نگر به انطباق‌پذیری:** با تعبیه قابلیت‌هایی مانند محاسبه خودکار مالیات، این پروژه از یک راهکار صرفاً فنی فراتر رفته و به چالش‌های دنیای واقعی کسب‌وکار، یعنی انطباق با قوانین نظارتی و مالی، پاسخ می‌دهد. این ویژگی، پذیرش عملیاتی سیستم توسط شرکت‌ها را تسهیل می‌کند.

بنابراین، پروژه حاضر نه تنها یک پیاده‌سازی دیگر از زنجیره بلوکی در زنجیره تأمین نیست، بلکه یک سنتز راهکارمندانه از بهترین فناوری‌ها و معماری‌های موجود است. این پروژه با یادگیری از محدودیت‌های نسل‌های پیشین، یک راهکار جامع، کارآمد و عملیاتی ارائه می‌دهد که یک گام مهم رو به جلو در تکامل سامانه‌های زنجیره تأمین غیرمتمرکز محسوب می‌شود.

۲-۳ تحلیل چالش های پروژه و راهکار های مقابله با آن

در بخش‌های پیشین این فصل، یک تحلیل جامع از سیر تکاملی سیستم‌های مدیریت زنجیره تأمین ارائه گردید. این تحلیل از سیستم‌های برنامه‌ریزی منابع سازمانی (ERP) متمرکز آغاز شد، به بررسی نسل اول فناوری‌های دیجیتالی مانند $RFID$ و IoT پرداخت و در نهایت، به ارزیابی دو نسل اصلی از راهکارهای مبتنی بر زنجیره بلوکی منتهی شد: نسل اول مبتنی بر بسترهای خصوصی و نیازمند مجوز مانند $Hyperledger\ Fabric$، و نسل دوم مبتنی بر شبکه‌های عمومی و استانداردهای نشانه‌سازی مانند $ERC-721$. هر یک از این مفهوم‌ها، گامی مهم در جهت حل مشکلات پیچیده زنجیره تأمین بوده‌اند، اما در عین حال، هر کدام با محدودیت‌ها و چالش‌های خاص خود روبرو شدند.

هدف اصلی این بخش، انجام یک ارزیابی انتقادی و عمیق بر روی این چالش‌ها است. ما با سنتز یافته‌های بخش‌های قبل، به صورت نظام‌مند نشان خواهیم داد که راهکارهای پیشین در پاسخگویی به نیازهای چندوجهی یک زنجیره تأمین مدرن، دچار کاستی بوده‌اند. این تحلیل، بستری را فراهم می‌آورد تا بتوانیم جایگاه راهکارمندانه و منحصربه‌فرد پروژه حاضر را به روشنی مشخص کنیم. در نهایت، استدلال خواهد شد که این پروژه، با ارائه یک معماری سنتز شده و هوشمندانه، نه تنها به چالش‌های شناسایی‌شده پاسخ می‌دهد، بلکه نماینده یک نسل سوم از راهکارهای زنجیره تأمین غیرمتمرکز است که یک گام به پیاده‌سازی عملیاتی و پذیرش گسترده نزدیک‌تر شده است.

۲-۳-۱ شناسایی چالش‌های کلیدی

پس از مرور گسترده راهکارهای موجود، می‌توان سه چالش اصلی و بنیادین را شناسایی کرد که اکثر پروژه‌های پیشین به صورت جامع به آن‌ها نپرداخته‌اند. این چالش‌ها در سه حوزه کلیدی قرار دارند: مدیریت دارایی‌های ناهمگون، یکپارچگی داده‌های خارج از زنجیره، و انطباق‌پذیری با محیط‌های واقعی تجاری و نظارتی.

چالش اول: چالش مدیریت دارایی‌های ناهمگون

یک زنجیره تأمین واقعی، اکوسیستمی بسیار متنوع از دارایی‌هاست. این دارایی‌ها از نظر ماهیت، ارزش و نحوه مدیریت، تفاوت‌های بنیادینی با یکدیگر دارند. می‌توان آن‌ها را در یک طیف، از کاملاً مثلی تا کاملاً غیرمثلی، دسته‌بندی کرد:

- **دارایی‌های کاملاً مثلی** [۳۹]: این‌ها مواد اولیه یا کالاهای انبوهی هستند که هر واحد از آن‌ها با واحد دیگر قابل تعویض است. به عنوان مثال، یک کیلوگرم گندم از یک دسته مشخص، با کیلوگرم دیگری از همان دسته تفاوتی ندارد. مدیریت این دارایی‌ها مبتنی بر تعداد و مقدار است.
- **دارایی‌های کاملاً غیرمثلی** [۴۰]: این‌ها عنصرهای منحصربه‌فردی هستند که هر کدام هویت و تاریخچه مختص به خود را دارند. یک خودرو با شماره شاسی مشخص، یک الماس با گواهی اصالت، یا یک قطعه هنری، نمونه‌هایی از این دارایی‌ها هستند. مدیریت این‌ها مبتنی بر هویت یکتا است.
- **دارایی‌های نیمه‌مثلی** [۴۱]: این دسته که اغلب نادیده گرفته می‌شود، دارایی‌هایی هستند که در یک دوره زمانی مثلی بوده و در دوره‌ای دیگر به غیرمثلی تبدیل می‌شوند. برای مثال، یک بلیط کنسرت برای یک جایگاه مشخص، قبل از شروع رویداد با بلیط دیگری از همان جایگاه قابل تعویض است (مثلی)، اما پس از استفاده و تبدیل شدن به یک یادگاری، منحصربه‌فرد و غیرمثلی می‌شود.

اکثر راهکارهای زنجیره بلوکی پیشین، در ارائه یک مدل یکپارچه برای مدیریت این طیف گسترده از دارایی‌ها دچار مشکل بوده‌اند.

محدودیت‌های راهکارهای تک-استانداردی: راهکارهای نسل دوم که بر روی شبکه‌های عمومی ساخته شده‌اند، معمولاً خود را به یکی از دو استاندارد اصلی محدود کرده‌اند:

۱. **رویکرد مبتنی بر** $ERC-20$: این پروژه‌ها بر روی مدیریت مواد اولیه و کالاهای انبوه تمرکز کرده‌اند. در حالی که این رویکرد برای زنجیره‌های تأمین کالاهای اساسی (مانند محصولات کشاورزی) کارآمد است، اما به کلی از ردیابی عنصرهای منحصربه‌فرد و محصولات نهایی که نیازمند شناسنامه دیجیتال یکتا هستند، عاجز است.

۲. **رویکرد مبتنی بر** $ERC-721$: این پروژه‌ها که محبوبیت بیشتری داشته‌اند، بر روی تضمین اصالت کالاهای لوکس، داروها و قطعات صنعتی متمرکز شده‌اند. هر محصول به یک NFT منحصربه‌فرد تبدیل می‌شود که تاریخچه آن را ثبت می‌کند. مشکل این رویکرد، ناکارآمدی شدید

[۳۹] $Fungible$
[۴۰] $Non-Fungible$
[۴۱] $Semi-Fungible$

آن در مدیریت اجزای تشکیل‌دهنده یا مواد اولیه آن محصول است. برای مثال، در زنجیره تأمین یک خودرو، ردیابی خود خودرو با یک NFT منطقی است، اما ردیابی هزاران پیچ و مهره یا لیترها روغن موتور که در تولید آن به کار رفته، با استفاده از NFTهای مجزا، از نظر هزینه و سرعت، یک فاجعه عملیاتی خواهد بود. این امر منجر به ایجاد یک دید ناقص از زنجیره تأمین می‌شود که در آن، تنها محصول نهایی قابل ردیابی است و نه مواد اولیه آن.

محدودیت‌های بسترهای خصوصی: بسترهای سازمانی مانند $Hyperledger\ Fabric$ مدل دارایی انعطاف‌پذیرتری را ارائه می‌دهند که در آن می‌توان هر نوع ساختار داده‌ای را به عنوان یک دارایی تعریف کرد. با این حال، این بسترها فاقد یک استاندارد مورد توافق جهانی برای تمایز بین دارایی‌های مثلی و غیرمثلی هستند. این امر منجر به ایجاد راهکارهای جزیره‌ای و سفارشی می‌شود که قابلیت همکاری با یکدیگر یا با اکوسیستم گسترده‌تر دارایی‌های دیجیتال را ندارند. یک دارایی تعریف‌شده در یک شبکه $Fabric$، نمی‌تواند به راحتی در یک بازار NFT عمومی لیست شود یا به عنوان وثیقه در یک پروتکل $DeFi$ استفاده گردد.

چالش دوم: مسئله یکپارچگی داده‌های خارج از زنجیره

همانطور که در بخش چالش‌ها ذکر شد، ذخیره‌سازی داده‌های حجیم بر روی زنجیره بلوکی از نظر اقتصادی غیرعملی است. این یک واقعیت فنی است که تمام پروژه‌های جدی زنجیره تأمین باید با آن روبرو شوند. در نتیجه، یک معماری ترکیبی که در آن، داده‌های اصلی (فراداده) در خارج از زنجیره و تنها یک اثبات یا ارجاع به آن در داخل زنجیرهامری اجتناب‌ناپذیر است. با این حال، نحوه پیاده‌سازی این معماری، خود یک چالش بزرگ و یک چالش مهم در پژوهش‌های پیشین است.

بسیاری از پروژه‌های اولیه، این چالش را به سادگی نادیده گرفته یا راهکارهای ضعیفی برای آن ارائه داده‌اند:

- **نادیده گرفتن مشکل:** برخی پروژه‌های آکادمیک، صرفاً بر روی منطق روی زنجیره تمرکز کرده و فرض می‌کنند که فراداده به نوعی در دسترس و معتبر است، بدون اینکه معماری مشخصی برای آن ارائه دهند.
- **استفاده از سرورهای متمرکز:** بسیاری از راهکارهای تجاری، برای ذخیره‌سازی فراداده از سرورهای وب سنتی ($Web2$) و پایگاه‌های داده متمرکز استفاده می‌کنند. در این مدل، یک URL به سرور مربوطه در قرارداد هوشمند ذخیره می‌شود. این رویکرد، کل فلسفه زنجیره بلوکی را زیر سؤال می‌برد. زیرا با این کار، ما مجدداً تک نقطه خرابی و یک مرجع قابل اعتماد مرکزی را به سیستم وارد کرده‌ایم. اگر آن سرور هک شود و داده‌ها تغییر کنند، یا اگر شرکت مالک سرور ورشکست شود و سرور از دسترس خارج گردد، ارجاع ثبت‌شده بر روی زنجیره بلوکی بی‌معنی و بی‌ارزش خواهد شد. این راهکار، مشکل اعتماد را حل نمی‌کند، بلکه صرفاً آن را به مکانی دیگر منتقل می‌نماید.

مفهوم گسترده‌تر مشکل اوراکل: این چالش، نمونه‌ای از یک مسئله بزرگ‌تر در دنیای زنجیره بلوکی است که به آن مشکل اوراکل [۴۲] گفته می‌شود. قراردادهای هوشمند، محیط‌های اجرایی بسته‌ای هستند که به صورت بومی، به داده‌های دنیای خارج از خود دسترسی ندارند. اوراکل‌ها، سرویس‌هایی هستند که به عنوان پل عمل کرده و داده‌های دنیای واقعی را به صورت قابل اعتماد به داخل زنجیره بلوکی وارد می‌کنند. در مسئله ما، سیستم ذخیره‌سازی خارج زنجیره نقش یک نوع اوراکل را برای فراداده ایفا می‌کند. اگر این اوراکل متمرکز و غیرقابل اعتماد باشد، کل امنیت و اعتبار سیستم به خطر می‌افتد.

چالش سوم: فقدان انطباق‌پذیری با محیط‌های نظارتی و تجاری بزرگ‌ترین مانع بر سر راه پذیرش گسترده فناوری زنجیره بلوکی در سطح سازمانی، صرفاً فنی نیست. بسیاری از پروژه‌های زنجیره بلوکی در یک خلأ تجاری و قانونی توسعه می‌یابند. آن‌ها بر روی جنبه‌های الگوریتمی و رمزنگاری تمرکز می‌کنند و واقعیت‌های پیچیده دنیای کسب‌وکار و الزامات قانونی را نادیده می‌گیرند. یک شرکت نمی‌تواند سیستمی را به کار گیرد که با قوانین مالیاتی، گمرکی و تجاری که ملزم به رعایت آن‌هاست، در تضاد باشد. اکثر پروژه‌های زنجیره تأمین پیشین، در این حوزه سکوت کرده‌اند. آن‌ها نشان می‌دهند که چگونه می‌توان یک کالا را ردیابی کرد، اما به سؤالات حیاتی زیر پاسخ نمی‌دهند:

- چگونه مالیات بر ارزش افزوده (VAT) در هر مرحله از انتقال مالکیت محاسبه و پرداخت می‌شود؟
- چگونه اسناد مورد نیاز گمرک به صورت دیجیتال و قابل تأیید تولید و ارائه می‌گردد؟
- چگونه می‌توان بین شفافیت مورد نیاز برای حسابرسی و محرمانگی لازم برای حفظ مزیت رقابتی، تعادل برقرار کرد؟
- در صورت بروز اختلاف تجاری، وضعیت حقوقی تراکنش‌های ثبت‌شده بر روی زنجیره بلوکی چیست؟

این بی‌توجهی به الزامات دنیای واقعی، باعث شده است که بسیاری از این پروژه‌ها در حد یک طرح آزمایشی ($Pilot$) باقی بمانند و به مرحله تولید انبوه نرسند. زیرا ادغام آن‌ها با فرآیندهای مالی و قانونی موجود شرکت‌ها، بسیار دشوار و پرهزینه است.

۲-۳-۲ ارائه راهکار مورد استفاده در پروژه: یک معماری سنتز شده

پروژه حاضر، با شناسایی دقیق این سه چالش کلیدی، یک راهکار جامع و چندلایه ارائه می‌دهد که هدف آن، نه تنها پیاده‌سازی یک قابلیت فنی جدید، بلکه ارائه یک سنتز راهکارمندانه از بهترین رویکردها برای پر کردن این چالش‌هاست. معماری این پروژه، پاسخی مستقیم به هر یک از چالش‌های مطرح‌شده است.

[۴۲] $The\ Oracle\ Problem$

نوآوری اول: مدیریت یکپارچه دارایی‌ها با استاندارد $ERC-1155$

این پروژه به صورت مستقیم به چالش مدیریت دارایی‌های ناهمگون پاسخ می‌دهد. با انتخاب استراتژیک استاندارد $ERC-1155$، این سیستم از ابتدا با این فرض طراحی شده است که یک زنجیره تأمین واقعی، با ترکیبی از دارایی‌های مثلی و غیرمثلی سروکار دارد. این انتخاب، یک تصمیم فنی صرف نیست، بلکه یک تصمیم معماری بنیادین با پیامدهای عملی گسترده است.

فراتر از یک استاندارد فنی: یک مدل عملیاتی انعطاف‌پذیر قدرت واقعی $ERC-1155$ در توانایی آن برای مدل‌سازی فرآیندهای لجستیکی پیچیده در دنیای واقعی نهفته است. در ادامه با چند مثال، این قابلیت تشریح می‌شود:

- **صنعت داروسازی:** یک شرکت داروسازی را در نظر بگیرید. این شرکت می‌تواند یک دسته کامل از یک داروی خاص را که شامل هزاران ویال یکسان است، به عنوان یک دسته از نشانه‌های مثلی با شناسه مثلاً $ID = 101$ و تعداد $Amount = 10000$ نشانه کند. سپس، هر یک از این ویال‌ها را در حین بسته‌بندی نهایی، به یک نشانه غیرمثلی منحصربه‌فرد با شماره سریال مشخص تبدیل نماید. استاندارد $ERC-1155$ این قابلیت تبدیل بین حالت مثلی و غیرمثلی را نیز تسهیل می‌کند. این فرآیند، امکان ردیابی هم در سطح دسته (برای کنترل کیفیت کلی) و هم در سطح عنصر (برای جلوگیری از فروش داروی تقلبی) را فراهم می‌آورد.
- **صنعت الکترونیک:** یک شرکت تولیدکننده لپ‌تاپ را تصور کنید. این شرکت می‌تواند هر لپ‌تاپ تولید شده را با شماره سریال منحصربه‌فرد خود، به عنوان یک NFT (مثلاً $ID = 202$، $Amount = 1$) در سیستم ثبت کند. همزمان، می‌تواند قطعات یدکی استاندارد مانند باتری یا شارژر را به عنوان نشانه‌های مثلی (مثلاً $ID = 203$، $Amount = 5000$) مدیریت نماید. زمانی که یک مشتری لپ‌تاپ را به همراه یک شارژر اضافی خریداری می‌کند، تابع $safeBatchTransferFrom$ به فروشنده اجازه می‌دهد تا هر دو عنصر (یک NFT و یک نشانه مثلی) را در یک تراکنش واحد و بهینه به مشتری منتقل کند.

این سطح از انعطاف‌پذیری و کارایی، که مستقیماً از قابلیت‌های استاندارد $ERC-1155$ نشأت می‌گیرد، پاسخی قدرتمند به چالش اول است و سیستم را برای کاربرد در طیف وسیعی از صنایع آماده می‌سازد.

راهکار دوم: تضمین صحت فراداده با معماری ترکیبی خارج و روی زنجیره

این پروژه برای پاسخ به چالش یکپارچگی داده‌های خارج از زنجیره، یک معماری دقیق و امن ارائه می‌دهد که بر پایه دو فناوری کلیدی استوار است: سیستم فایل بین‌سیاره‌ای ($IPFS$) و تابع درهم سازی رمزنگاری $Keccak256$.

چرخه حیات کامل فراداده در معماری پیشنهادی: برای درک کامل این راهکار، باید چرخه کامل ثبت و اعتبارسنجی فراداده را دنبال کنیم:

۱. **مرحله اول: ایجاد و بسته‌بندی فراداده:** هنگامی که یک تولیدکننده قصد ثبت محصول جدیدی را دارد، اطلاعات کامل آن را در داشبورد مدیریتی وارد می‌کند. برنامه کاربردی، این اطلاعات را در یک فایل با ساختار استاندارد (مانند $JSON$) بسته‌بندی می‌کند. این فایل شامل تمام جزئیات محصول است.

۲. **مرحله دوم: بارگذاری در $IPFS$ و دریافت شناسه محتوا (CID):** برنامه کاربردی، این فایل $JSON$ را در شبکه $IPFS$ بارگذاری می‌کند. $IPFS$ یک شبکه ذخیره‌سازی همتا به همتا و غیرمتمرکز است. برخلاف سرورهای وب سنتی که در آن، محتوا بر اساس مکان آدرس‌دهی می‌شود ($addressing\ Location-based$ - مانند یک URL)، در $IPFS$ محتوا بر اساس متن درهم سازی خود آدرس‌دهی می‌شود ($addressing\ Content-based$). پس از بارگذاری، $IPFS$ یک شناسه منحصربه‌فرد به نام CID ($Identifier\ Content$) به فایل اختصاص می‌دهد که در واقع متن درهم ساخته شده محتوای آن فایل است. این ویژگی دو مزیت بزرگ دارد:

- **تغییرناپذیری:** اگر حتی یک بیت از محتوای فایل تغییر کند، CID آن نیز کاملاً تغییر خواهد کرد.
- **عدم تمرکز و در دسترس بودن:** فایل در چندین گره در شبکه $IPFS$ توزیع می‌شود که این امر، ریسک از دسترس خارج شدن به دلیل خرابی یک سرور واحد را از بین می‌برد.

۳. **مرحله سوم: محاسبه متن درهم ساخته شده تأیید و ثبت بر روی زنجیره:** برنامه کاربردی، به صورت موازی، محتوای فایل $JSON$ را با استفاده از الگوریتم $Keccak256$ (که الگوریتم تابع درهم سازی استاندارد در اتریوم است) درهم سازی می‌کند. سپس، در حین فراخوانی تابع $registerProduct$، هر دو مقدار، یعنی CID دریافت شده از $IPFS$ و تابع درهم سازی $Keccak256$ محاسبه‌شده، به عنوان پارامتر به قرارداد هوشمند ارسال و بر روی زنجیره بلوکی ذخیره می‌شوند.

۴. **مرحله چهارم: فرآیند اعتبارسنجی غیرمتمرکز:** زمانی که یک مصرف‌کننده کد QR را اسکن می‌کند، برنامه کاربردی او فرآیند اعتبارسنجی زیر را به صورت خودکار انجام می‌دهد:

(آ) ابتدا CID و متن درهم ساخته شده $Keccak256$ معتبر را از قرارداد هوشمند بر روی زنجیره بلوکی می‌خواند.

(ب) سپس با استفاده از CID، فایل فراداده اصلی را از شبکه غیرمتمرکز $IPFS$ بازیابی می‌کند.

(ج) به صورت محلی، متن درهم سازی شده $Keccak256$ محتوای فایل بازیابی‌شده را مجدداً محاسبه می‌کند.

(د) در نهایت، متن درهم ساخته شده محاسبه‌شده محلی را با متن درهم ساخته شده معتبر خوانده‌شده از زنجیره بلوکی مقایسه می‌کند.

تنها در صورتی که این دو متن درهم ساخته شده کاملاً یکسان باشند، اصالت اطلاعات تأیید می‌شود. این معماری چندلایه، یک راهکار بسیار قوی، غیرمتمرکز و اقتصادی برای حل چالش دوم ارائه می‌دهد.

راهکار سوم: پل زدن به دنیای واقعی با محاسبه خودکار مالیات

مهم‌ترین و شاید جسورانه‌ترین راهکار این پروژه، پاسخگویی مستقیم به چالش انطباق‌پذیری با محیط‌های نظارتی است. این پروژه، به جای نادیده گرفتن الزامات دنیای واقعی، تلاش می‌کند تا از ویژگی‌های منحصربه‌فرد زنجیره بلوکی برای ایجاد راهکارهای نوین در حوزه فناوری‌های نظارتی [۴۳] بهره ببرد. در این راستا، یک راهکار قابل اجرا برای محاسبه و پرداخت خودکار مالیات به عنوان بخشی از پروتکل ارائه می‌شود.

دلایل ایده‌آل بودن زنجیره بلوکی برای مالیات هوشمند زنجیره بلوکی، به دلیل سه ویژگی کلیدی خود، یک زیرساخت بی‌نظیر برای مدرن‌سازی سیستم‌های مالیاتی فراهم می‌کند:

۱. **شفافیت و قابلیت حسابرسی آنی:** هر تراکنشی که منجر به انتقال ارزش یا مالکیت می‌شود (و بالقوه مشمول مالیات است)، به صورت شفاف و تغییرناپذیر بر روی یک دفتر کل عمومی ثبت می‌گردد. این امر به نهادهای نظارتی اجازه می‌دهد تا به جای حسابرسی‌های دوره‌ای و مبتنی بر اسناد کاغذی، به یک حسابرسی آنی و مستمر دسترسی داشته باشند.

۲. **داده‌های قابل اعتماد و قطعی:** زمان، مبلغ و طرفین هر تراکنش به صورت رمزنگاری‌شده تأیید و ثبت می‌شوند. این قطعیت، اختلافات مربوط به زمان و مبلغ معاملات را که بخش بزرگی از فرآیندهای حسابرسی سنتی را تشکیل می‌دهد، از بین می‌برد و فرصت‌های فرار مالیاتی را به شدت کاهش می‌دهد.

۳. **قابلیت برنامه‌پذیری و خودکارسازی:** با استفاده از قراردادهای هوشمند، می‌توان قوانین مالیاتی را به صورت مستقیم در قالب کد پیاده‌سازی کرد. این کد می‌تواند به صورت خودکار و بدون دخالت انسان، در زمان وقوع هر تراکنش اجرا شود.

معماری پیشنهادی برای ماژول مالیات هوشمند راهکار قابل اجرای ارائه شده در این پروژه، مبتنی بر گسترش منطق تابع $transferWithTax$ است. این تابع، علاوه بر انتقال مالکیت نشانه، زنجیره‌ای از اقدامات مرتبط با مالیات را نیز به صورت اتمی انجام خواهد داد:

۱. **فراخوانی منطق محاسبه مالیات:** در حین اجرای تابع انتقال، یک تابع داخلی به نام $calculateTax$ فراخوانی می‌شود.

۲. **پیاده‌سازی قوانین مالیاتی:** منطق این تابع می‌تواند به صورت‌های مختلفی پیاده‌سازی شود:

[۴۳] $RegTech$

- **مدل ساده (نرخ ثابت):** ساده‌ترین مدل، اعمال یک نرخ مالیات ثابت (مثلاً درصد مشخصی به عنوان مالیات بر ارزش افزوده) بر ارزش اسمی معامله است.
- **مدل پویا (مبتنی بر اوراکل):** در یک مدل پیشرفته‌تر، قرارداد هوشمند می‌تواند از طریق یک اوراکل، اطلاعاتی مانند قیمت روز کالا یا نرخ‌های مالیاتی متغیر را از منابع خارجی دریافت کرده و محاسبات خود را بر اساس آن انجام دهد.
- **مدل چندنرخی (مبتنی بر دسته‌بندی):** قوانین مالیاتی می‌توانند بر اساس دسته‌بندی محصول (که در فراداده آن مشخص شده) متفاوت باشند. قرارداد هوشمند می‌تواند این دسته‌بندی را خوانده و نرخ مناسب را اعمال کند.

۳. **انتقال خودکار مبلغ مالیات:** پس از محاسبه مبلغ مالیات، قرارداد هوشمند به صورت خودکار آن مبلغ را از حساب فروشنده کسر کرده و مستقیماً به یک آدرس کیف پول از پیش تعیین‌شده که متعلق به سازمان امور مالیاتی است، واریز می‌کند.

۴. **ثبت رویداد مالیاتی:** یک رویداد [۴۴] مشخص برای ثبت جزئیات تراکنش مالیاتی (مبلغ، مبنای محاسبه، آدرس پرداخت) بر روی زنجیره بلوکی ثبت می‌شود تا برای حسابرسی‌های بعدی به راحتی قابل استناد باشد.

تمام این مراحل در یک تراکنش واحد و به صورت اتمی انجام می‌شود؛ یعنی یا تمام مراحل با موفقیت اجرا می‌شوند، یا کل تراکنش ناموفق خواهد بود. این ویژگی، تضمین می‌کند که هیچ معامله‌ای بدون پرداخت مالیات متعلقه انجام نخواهد شد. این رویکرد راهکارمندانه، نه تنها یک قابلیت فنی، بلکه یک پل استراتژیک بین دنیای غیرمتمرکز زنجیره بلوکی و دنیای ساختاریافته نظارتی است و به چالش سوم به صورت مستقیم پاسخ می‌دهد.

۲-۳-۳ جمع‌بندی: جایگاه پروژه به عنوان یک راهکار نسل سوم

با توجه به تحلیل جامع ارائه شده، می‌توان ادعا کرد که پروژه حاضر، نماینده یک نسل سوم از راهکارهای زنجیره تأمین مبتنی بر زنجیره بلوکی است. این نسل، با یادگیری از تجربیات و محدودیت‌های دو نسل پیشین، به یک رویکرد سنتز شده و جامع‌تر دست یافته است:

- **نسل اول (مبتنی بر بستر خصوصی):** تمرکز اصلی بر حریم خصوصی و توان پردازشی بود، اما به قیمت از دست دادن قابلیت همکاری و عدم تمرکز واقعی.
- **نسل دوم (مبتنی بر نشانه‌سازی اولیه):** تمرکز بر قابلیت همکاری و مالکیت دیجیتال بود، اما با چالش‌های جدی در کارایی (به دلیل استفاده از استانداردهای تک‌منظوره) و یکپارچگی داده روبرو بود.

---

[۴۴] *Event*

- **نسل سوم (رویکرد سنتز شده پروژه حاضر):** این نسل با ترکیب هوشمندانه فناوری‌ها، تلاش می‌کند تا به صورت همزمان به چندین هدف کلیدی دست یابد:

۱. **انعطاف‌پذیری دارایی:** با استفاده از استاندارد قدرتمند $ERC-1155$.

۲. **یکپارچگی داده:** با استفاده از معماری امن و اقتصادی $Keccak256 + IPFS$.

۳. **انطباق‌پذیری تجاری:** با ارائه راهکارهای قابل اجرا برای نیازمندی‌های دنیای واقعی مانند مالیات.

۴. **قابلیت همکاری:** با پایبندی به استانداردهای شبکه عمومی اتریوم.

بنابراین، این پروژه صرفاً یک پیاده‌سازی دیگر از یک ایده موجود نیست، بلکه یک گام رو به جلو در جهت بلوغ و عملیاتی‌سازی فناوری زنجیره بلوکی برای یکی از مهم‌ترین و پیچیده‌ترین صنایع جهان است. این پایان‌نامه، یک نقشه راه دقیق و یک نمونه اولیه قوی برای ساختن نسل آینده زنجیره‌های تأمین ارائه می‌دهد؛ زنجیره‌هایی که نه تنها کارآمدتر، بلکه به صورت قابل اثباتی، شفاف‌تر، امن‌تر و عادلانه‌تر خواهند بود.

فصل سوم

معماری و روش پیاده‌سازی سامانه

پس از بررسی مبانی نظری و تحلیل شکاف‌های موجود در پژوهش‌های پیشین در فصل دوم، این فصل به صورت کاملاً عملی و فنی به تشریح «معماری و روش پیاده‌سازی سامانه پیشنهادی» می‌پردازد. هدف این فصل، ارائه یک نقشه راه دقیق و شفاف از تمامی اجزای تشکیل‌دهنده سیستم، از قرارداد هوشمند در لایه زنجیره بلوکی گرفته تا واسطهای کاربری در لایه کاربری است. در این بخش، نه تنها «چه چیزی» ساخته شده، بلکه «چرا» و «چگونه»ی آن نیز با استناد به انتخاب‌های فنی و نمایش قطعه کدهای کلیدی، به تفصیل مورد بحث و بررسی قرار خواهد گرفت.

این فصل به مثابه قلب فنی پایان‌نامه عمل می‌کند و به چهار بخش اصلی تقسیم می‌شود: ابتدا، به معرفی و توجیه پشته فناوری [۱] انتخاب شده برای پروژه می‌پردازیم. سپس، معماری کلان و چندلایه سیستم را تشریح می‌کنیم. در ادامه، به صورت عمیق وارد جزئیات پیاده‌سازی هر یک از لایه‌های اصلی سیستم، یعنی لایه زنجیره بلوکی [۲]، لایه ذخیره‌سازی خارج از زنجیره و لایه کاربری خواهیم شد.

۳-۱ مقدمه و انتخاب فناوری‌ها

انتخاب مجموعه مناسبی از فناوری‌ها، یکی از حیاتی‌ترین مراحل در موفقیت هر پروژه نرم‌افزاری، به ویژه در حوزه‌های نوظهوری مانند زنجیره بلوکی است. پشته فناوری این پروژه با در نظر گرفتن اهداف کلیدی مانند امنیت، عدم تمرکز، کارایی، تجربه کاربری مدرن و قابلیت توسعه در آینده، به دقت انتخاب شده است. هر یک از ابزارهای به کار رفته، نقشی کلیدی در تحقق یکی از اهداف پروژه ایفا می‌کند.

۳-۱-۱ توجیه انتخاب فناوری‌های لایه زنجیره بلوکی

لایه زنجیره بلوکی، به عنوان هسته امنیتی و منطقی سیستم، نیازمند فناوری‌هایی است که بالاترین سطح از بلوغ، امنیت و پشتیبانی جامعه توسعه‌دهندگان را داشته باشند.

- **زبان برنامه‌نویسی $Solidity$ و ماشین مجازی اتریوم (EVM):** $Solidity$ به عنوان زبان برنامه‌نویسی پیشرو برای نوشتن قراردادهای هوشمند و EVM به عنوان پلتفرم اجرایی آن، به دلیل بلوغ، مستندات گسترده، جامعه توسعه‌دهندگان فعال و اکوسیستم وسیعی از ابزارها و کتابخانه‌ها، به عنوان استاندارد صنعتی شناخته می‌شوند. انتخاب این پلتفرم، قابلیت همکاری با هزاران برنامه غیرمتمرکز دیگر را نیز تضمین می‌کند.

- **کتابخانه‌های $OpenZeppelin$:** امنیت در قراردادهای هوشمند از اهمیت فوق‌العاده‌ای برخوردار است. به جای اختراع مجدد چرخ، این پروژه از قراردادهای پایه ارائه شده توسط $OpenZeppelin$ بهره می‌برد[۱۶]. این قراردادها توسط متخصصان امنیت به صورت دقیق حسابرسی [۳] شده و

---

[۱] $Technology\ Stack$

[۲] $Blockchain$

[۳] $audited$

پیاده‌سازی‌های استانداردی برای توکن‌هایی مانند $ERC-1155$ و مکانیزم‌هایی مانند کنترل دسترسی [۴] و توقف اضطراری [۵] ارائه می‌دهند که ریسک بروز آسیب‌پذیری‌های رایج را به حداقل می‌رساند.

- **چارچوب توسعه و آزمون** $Foundry$: برای توسعه، کامپایل، استقرار و آزمون قرارداد هوشمند، از چارچوب مدرن $Foundry$ استفاده شده است. برخلاف ابزارهای قدیمی‌تر مانند $Truffle$ که نیازمند نوشتن آزمون‌ها به زبان $JavaScript$ هستند، $Foundry$ به توسعه‌دهندگان اجازه می‌دهد تا آزمون‌های خود را مستقیماً به زبان $Solidity$ بنویسند. این ویژگی، فرآیند آزمون را سریع‌تر، کارآمدتر و برای توسعه‌دهندگان $Solidity$ طبیعی‌تر می‌سازد. ابزارهای همراه آن مانند $Anvil$ (یک نود محلی برای توسعه) و $Forge$ (موتور آزمون)، چرخه توسعه را به شدت تسریع می‌کنند.

۳-۱-۲ توجیه انتخاب فناوری‌های لایه ذخیره‌سازی و کاربری

برای لایه‌هایی که مستقیماً با کاربر در تعامل هستند، انتخاب فناوری‌هایی که تجربه کاربری مدرن، سریع و امنی را فراهم کنند، در اولویت قرار داشته است.

- **ذخیره‌سازی خارج از زنجیر با** $IPFS$ **و** $Pinata$: همانطور که در فصل قبل تشریح شد، برای حل چالش هزینه ذخیره‌سازی، از معماری ترکیبی استفاده می‌شود. $IPFS$ [۶] به دلیل ماهیت غیرمتمرکز و آدرس‌دهی مبتنی بر محتوا، به عنوان راهکار ایده‌آل برای ذخیره‌سازی فراداده انتخاب شد. برای تضمین در دسترس بودن دائمی فایل‌ها، از یک سرویس پینینگ به نام $Pinata$ استفاده شده است (که در فایل $ipfs.ts$ پیکربندی شده[۲۹]) که نیاز به اجرای یک گره $IPFS$ توسط خود کاربر را مرتفع می‌سازد.

- **کتابخانه** $React$ **و ابزار ساخت** $Vite$: برای توسعه لایه کاربری، از کتابخانه محبوب $React$ استفاده شده است که به دلیل معماری مبتنی بر عنصر سازنده، مدیریت حالت قدرتمند و اکوسیستم وسیع، امکان ساخت رابط‌های کاربری پیچیده و در عین حال قابل نگهداری را فراهم می‌کند. ابزار ساخت $Vite$ نیز به دلیل سرعت بسیار بالا در فرآیندهای توسعه و ساخت نهایی پروژه، جایگزین ابزارهای قدیمی‌تر مانند $Create-React-App$ شده است.

- **کتابخانه** $Wagmi$ [۳۰] **برای تعامل با زنجیره بلوکی:** $Wagmi$ مجموعه‌ای از قلاب‌های [۷] $React$ برای تعامل با اتریوم است. این کتابخانه، فرآیندهای پیچیده‌ای مانند اتصال به کیف پول، خواندن داده از قراردادهای هوشمند، ارسال تراکنش و مدیریت وضعیت شبکه را به شدت

[۴] $AccessControl$
[۵] $Pausable$
[۶] $InterPlanetary\ File\ System$
[۷] $Hooks$

ساده‌سازی می‌کند. استفاده از $Wagmi$ (که در $main.tsx$ و $wagmi.ts$ پیکربندی شده) به توسعه‌دهنده اجازه می‌دهد تا به جای درگیر شدن با جزئیات سطح پایین پروتکل RPC، بر روی منطق اصلی برنامه تمرکز کند.

- **کتابخانه $TailwindCSS$ برای طراحی واسط کاربری:** برای استایل‌دهی، از رویکرد $utility-first$ کتابخانه $TailwindCSS$ استفاده شده است (فایل $index.css$). این رویکرد، به جای نوشتن فایل‌های CSS جداگانه، امکان استایل‌دهی سریع و مستقیم در خود عنصرهای سازنده را فراهم کرده و منجر به ایجاد یک سیستم طراحی منسجم و قابل نگهداری می‌شود.

این پشته فناوری مدرن و یکپارچه، زیربنای لازم برای ساخت یک سامانه قوی، امن و کاربرپسند را فراهم می‌آورد.

۳-۲ معماری کلان سامانه

سامانه پیشنهادی بر اساس یک معماری چندلایه طراحی شده است که در آن، هر لایه مسئولیت مشخصی را بر عهده دارد. این تفکیک مسئولیت‌ها، به توسعه، نگهداری و مقیاس‌پذیری سیستم در آینده کمک می‌کند. همانطور که در نمودار بلوکی پروپوزال نیز نشان داده شده، می‌توان سه لایه اصلی را برای این سیستم متصور شد. در ادامه، این معماری با جزئیات بیشتری تشریح شده و جریان داده در یک سناریوی کلیدی (ثبت محصول جدید) ردیابی می‌شود.

۳-۲-۱ معماری سه لایه سیستم

۱. **لایه زنجیره بلوکی:** این لایه، هسته غیرمتمرکز و قابل اعتماد سیستم است که به آن «لایه اعتماد» ($Layer\ Trust$) نیز گفته می‌شود. این لایه مسئولیت‌های زیر را بر عهده دارد:

- تعریف و مدیریت هویت دیجیتال محصولات از طریق توکن‌های $ERC-1155$.
- اجرای منطق کسب‌وکار به صورت تغییرناپذیر از طریق قرارداد هوشمند.
- ثبت تاریخچه کامل و قابل حسابرسی تمام تراکنش‌های مالکیت.
- نگهداری ارجاع‌های امن (هش‌ها) به داده‌های خارج از زنجیره.
- مدیریت کنترل دسترسی و مجوزهای بازیگران مختلف شبکه.

این لایه، منبع حقیقت واحد و غیرقابل انکار سیستم است.

۲. **لایه ذخیره‌سازی خارج از زنجیره** [۸]: این لایه برای نگهداری داده‌های حجیم و غنی که ذخیره‌سازی آن‌ها بر روی زنجیره بلوکی اقتصادی نیست، به کار می‌رود. مسئولیت اصلی این لایه،

[۸] $Off-chain\ Storage\ Layer$

ذخیره‌سازی فایل‌های فراداده محصولات (در فرمت $JSON$) و فایل‌های چندرسانه‌ای مرتبط (مانند تصاویر و اسناد) است. در این پروژه، این لایه با استفاده از شبکه غیرمتمرکز $IPFS$ پیاده‌سازی شده تا همراستا با فلسفه عدم تمرکز کل سیستم باشد.

۳. **لایه کاربری** [۹]: این لایه که به آن $Frontend$ یا لایه ارائه نیز گفته می‌شود، نقطه تعامل کاربران با سیستم است. این لایه مسئولیت‌های زیر را بر عهده دارد:

- ارائه واسط‌های کاربری گرافیکی (GUI) ساده و کاربرپسند برای نقش‌های مختلف (داشبورد نگهدارنده سیستم، داشبورد مشتری).
- جمع‌آوری داده‌ها از کاربران (مانند اطلاعات محصول جدید).
- تعامل با لایه ذخیره‌سازی خارج از زنجیر برای بارگذاری و بازیابی فراداده.
- تعامل با کیف پول دیجیتال کاربر (مانند $MetaMask$) برای امضای تراکنش‌ها.
- ساخت و ارسال تراکنش‌ها به لایه زنجیره بلوکی.
- خواندن داده‌ها از زنجیره بلوکی و نمایش آن‌ها به صورت قابل فهم برای کاربر.

جریان داده در سناریوی ثبت محصول جدید

برای درک بهتر تعامل بین این سه لایه، فرآیند ثبت یک محصول جدید را به صورت گام به گام دنبال می‌کنیم:

۱. **شروع در لایه کاربری:** یک کاربر با نقش «تولیدکننده» (MANUFACTURER_ROLE) وارد داشبورد نگهدارنده سیستم شده و فرم «ایجاد محصول جدید» را با اطلاعاتی مانند نام، شماره سریال، و فایل‌های تصویری پر می‌کند (صفحه $CreateProduct.tsx$).

۲. **تعامل با لایه ذخیره‌سازی خارج از زنجیر:** پس از فشردن دکمه ثبت، برنامه کاربردی ابتدا با لایه خارج از زنجیر تعامل می‌کند. منطق موجود در $ipfs.ts$، فایل‌های تصویری و فراداده محصول را در شبکه $IPFS$ بارگذاری کرده و یک شناسه محتوای منحصربه‌فرد (CID) برای فایل فراداده دریافت می‌کند.

۳. **آماده‌سازی تراکنش در لایه کاربری:** برنامه کاربردی سپس متن درهم سازی شده $Keccak256$ فراداده را به صورت محلی محاسبه می‌کند. سپس یک تراکنش برای فراخوانی تابع $registerProduct$ در قرارداد هوشمند آماده می‌کند. این تراکنش شامل پارامترهایی مانند نام، شماره سریال، CID دریافت شده از $IPFS$ (به عنوان $metadataUrl$) و متن درهم سازی شده $Keccak256$ محاسبه‌شده است.

[۹] $User\ Layer$

۴. **امضای تراکنش:** لایه کاربری، از طریق کتابخانه $Wagmi$، از کیف پول کاربر می‌خواهد تا این تراکنش را امضا کند. این امضا با استفاده از کلید خصوصی کاربر انجام شده و اثبات می‌کند که درخواست واقعاً از طرف او ارسال شده است.

۵. **ارسال به لایه زنجیره بلوکی:** پس از امضا، تراکنش به یک گره در شبکه زنجیره بلوکی ارسال می‌شود.

۶. **اجرا در لایه زنجیره بلوکی:** قرارداد هوشمند، تابع $registerProduct$ را اجرا می‌کند. این تابع، پس از بررسی مجوز کاربر، یک توکن $ERC-1155$ جدید می‌سازد، اطلاعات ومتن های درهم سازی شده را در متغیرهای حالت خود ذخیره می‌کند و یک رویداد $ProductRegistered$ را منتشر می‌نماید.

۷. **بازخورد به لایه کاربری:** لایه کاربری منتظر تأیید تراکنش در شبکه می‌ماند. پس از تأیید، یک پیام موفقیت به کاربر نمایش داده شده (با استفاده از $react-hot-toast$) و او به داشبورد نگهدارنده سیستم هدایت می‌شود، جایی که محصول جدید ثبت‌شده اکنون قابل مشاهده است.

این جریان کار نشان می‌دهد که چگونه این سه لایه به صورت هماهنگ با یکدیگر کار می‌کنند تا یک فرآیند پیچیده را به یک تجربه کاربری ساده و امن تبدیل نمایند.

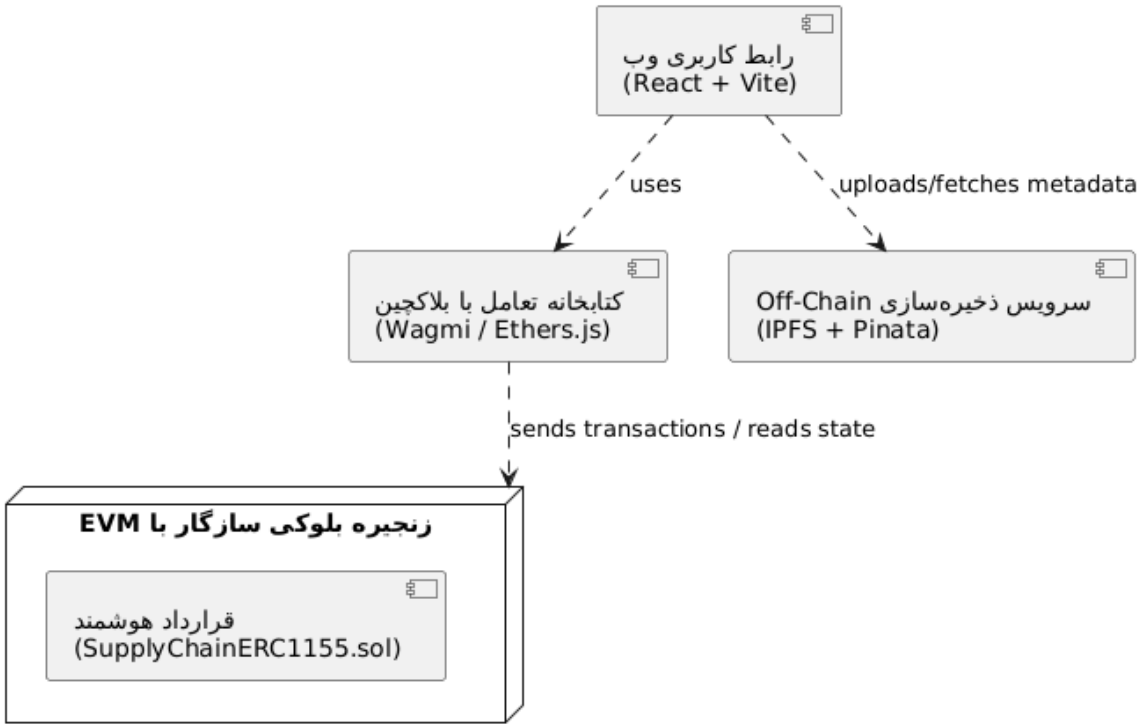
۳-۳ پیاده‌سازی لایه زنجیره بلوکی

این بخش به تشریح عمیق و خط به خط قرارداد هوشمند $SupplyChainERC1155.sol$ می‌پردازد که هسته اصلی منطق و امنیت کل سامانه را تشکیل می‌دهد.

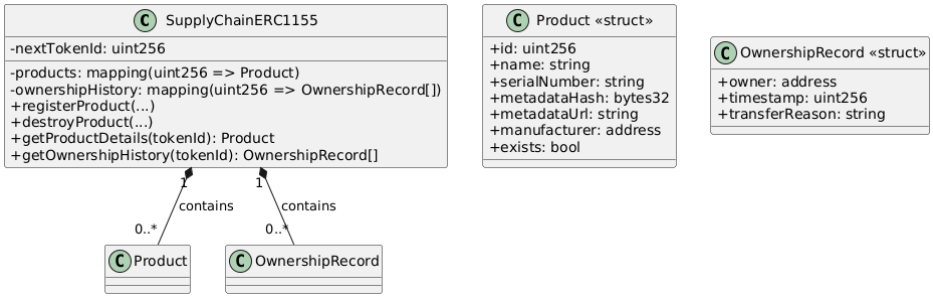
۳-۳-۱ ساختار کلی و وراثت قرارداد

قرارداد هوشمند این پروژه، با ارث‌بری از چندین قرارداد استاندارد و حسابرسی‌شده از کتابخانه $OpenZeppelin$، بر پایه‌ای محکم و امن بنا شده است. این رویکرد، ضمن کاهش حجم کدهای نوشته شده، از بهترین شیوه‌های ($practices\ best$) امنیتی بهره می‌برد.

```
contract SupplyChainERC1155 is ERC1155,
    AccessControl,
    Pausable,
    ERC1155Supply {
    // ...
}
```



شکل ۳-۱: نمودار معماری سامانه و ارتباط بین اجزای اصلی



شکل ۳-۲: مدل داده قرارداد هوشمند و ساختارهای اصلی آن

- $ERC1155$: این قرارداد پایه، تمام منطق اصلی استاندارد چند-توکنی $ERC-1155$ را پیاده‌سازی می‌کند، از جمله توابع $balanceOf$، $mint$، $burn$ و $safeTransferFrom$.
- $AccessControl$: این قرارداد یک مکانیزم قدرتمند و انعطاف‌پذیر برای مدیریت کنترل دسترسی مبتنی بر نقش $RBAC$ [۱۰] فراهم می‌کند. این ماژول به ما اجازه می‌دهد تا نقش‌های مختلفی تعریف کرده و دسترسی به توابع حساس را تنها به نقش‌های مجاز محدود کنیم.
- $Pausable$: این ماژول یک قابلیت ایمنی حیاتی را اضافه می‌کند: امکان توقف اضطراری تمام

[۱۰] $Role-Based\ Access\ Control$

فعالیت‌های اصلی قرارداد (مانند انتقالات) توسط یک مدیر. این ویژگی می‌تواند در صورت کشف یک آسیب‌پذیری، از بروز خسارات بیشتر جلوگیری کند.

- $ERC1155Supply$: این یک افزونه برای $ERC-1155$ است که تعداد کل توکن‌های موجود از هر نوع ($totalSupply$) را ردیابی می‌کند. این قابلیت برای حسابرسی و نظارت بر کل سیستم مفید است.

۳-۳-۲ نقش‌ها و کنترل دسترسی

یکی از مهم‌ترین جنبه‌های یک سیستم زنجیره تأمین، تعریف دقیق نقش‌ها و مسئولیت‌های هر یک از بازیگران است. قرارداد هوشمند این پروژه با استفاده از ماژول $AccessControl$، چهار نقش اصلی را تعریف و مدیریت می‌کند:

```
bytes32 constant MANUFACTURER_ROLE = keccak256("MANUFACTURER_ROLE");
bytes32 constant DISTRIBUTOR_ROLE = keccak256("DISTRIBUTOR_ROLE");
bytes32 constant RETAILER_ROLE = keccak256("RETAILER_ROLE");
bytes32 constant CUSTOMS_ROLE = keccak256("CUSTOMS_ROLE");
```

- MANUFACTURER_ROLE: این نقش مجوز ثبت (ساخت) محصولات جدید را دارد. تنها آدرس‌هایی این نقش به آن‌ها اعطا شده، می‌توانند تابع $registerProduct$ را فراخوانی کنند.
- DISTRIBUTOR_ROLE و RETAILER_ROLE: اگرچه در نسخه فعلی قرارداد، توابع خاصی برای این نقش‌ها تعریف نشده، اما وجود آن‌ها زیرساخت لازم برای افزودن منطق‌های تجاری آینده (مانند ثبت مراحل توزیع خاص) را فراهم می‌کند.
- CUSTOMS_ROLE: این نقش، مجوز ابطال یا از بین بردن یک محصول (مثلاً به دلیل شناسایی به عنوان کالای تقلبی یا تاریخ مصرف گذشته) را دارد. این نقش، کنترل تابع حساس $destroyProduct$ را در اختیار دارد.
- DEFAULT_ADMIN_ROLE: این نقش که در سازنده ($constructor$) به آدرس مستقرکننده قرارداد اعطا می‌شود، بالاترین سطح دسترسی را دارد و می‌تواند نقش‌های دیگر را به سایر آدرس‌ها اعطا یا از آن‌ها سلب کند (از طریق توابعی مانند $grantRole$ و $revokeRole$).

استفاده از اصلاح‌گر $onlyRole$ در توابع حساس، این سیاست‌های دسترسی را به صورت قاطع اعمال می‌کند. برای مثال، تعریف تابع $registerProduct$ تضمین می‌کند که هیچ بازیگر دیگری جز یک تولیدکننده تأییدشده، قادر به افزودن محصول به سیستم نخواهد بود:

```
function registerProduct(
    // ...
) external onlyRole(MANUFACTURER_ROLE) whenNotPaused returns (uint256) {
    // ...
}
```

۳-۳-۳ ساختارهای داده اصلی

قرارداد هوشمند از چندین ساختار داده و نگاشت [۱۱] برای ذخیره‌سازی وضعیت سیستم به صورت کارآمد و ساختاریافته استفاده می‌کند.

۳-۳-۴ ساختار داده محصول

این ساختار، شناسنامه دیجیتال هر محصول را تعریف می‌کند و تمام اطلاعات کلیدی آن را در خود جای داده است:

```
struct Product {
    uint256 id;
    string name;
    string category;
    string serialNumber;
    uint256 productionDate;
    string geographicalOrigin;
    bytes32 metadataHash; // Keccak256 hash of metadata content
    string metadataUrl;  // IPFS URL for full metadata
    address manufacturer;
    bool exists;
}
```

است. $ERC-1155$ توکن شناسه id است. شده انتخاب دقت با ساختار این فیلدهای از یک هر $exists$ فیلد می‌دهند. تشکیل را اعتبارسنجی مکانیزم اصلی هسته $metadataUrl$ و $metadataHash$

[۱۱] $mapping$

شده» «باطل عنوان به تاریخچه، از آن اطلاعات کامل حذف بدون را محصول یک تا می‌دهد اجازه ما به اصلی نگاشت یک در ساختارها این است. مهم بسیار حسابرسی اهداف برای که کنیم علامت‌گذاری می‌شوند: ذخیره

```
mapping(uint256 => Product) public products;
```

۳-۳-۵ ساختار داده تاریخچه مالکیت

برای ردیابی کامل زنجیره مالکیت، از این ساختار استفاده می‌شود:

```
struct OwnershipRecord {
    address owner;
    uint256 timestamp;
    string transferReason; // "manufactured", "sold", etc.
}
```

ابتدا از را آن انتقالات کامل تاریخچه که می‌شود نگهداری رکوردها این از آرایه‌ای محصول، هر برای می‌کند. ثبت کنون تا

۳-۳-۶ مدیریت چرخه حیات محصول

قرارداد هوشمند، توابع اصلی برای مدیریت چرخه کامل حیات یک محصول را فراهم می‌کند.

ثبت محصول (تابع $registerProduct$**)**

این تابع، نقطه ورود محصولات به اکوسیستم زنجیره بلوکی است.

```
function registerProduct(
    address to,
    string memory name,
    string memory category,
    string memory serialNumber,
    string memory geographicalOrigin,
    string memory metadataUrl,
    bytes32 metadataHash,
    uint256 amount
```

```
) external onlyRole(MANUFACTURER_ROLE) whenNotPaused returns (uint256) {
    uint256 tokenId = nextTokenId;
    nextTokenId++;

    metadataRegistry[tokenId] = metadataUrl;
    urlToTokenId[metadataUrl] = tokenId;

    products[tokenId] = Product({
        id: tokenId,
        name: name,
        category: category,
        serialNumber: serialNumber,
        productionDate: block.timestamp,
        geographicalOrigin: geographicalOrigin,
        metadataHash: metadataHash,
        metadataUrl: metadataUrl,
        manufacturer: msg.sender,
        exists: true
    });

    _mint(to, tokenId, amount, "");

    ownershipHistory[tokenId].push(OwnershipRecord({
        owner: to,
        timestamp: block.timestamp,
        transferReason: "manufactured"
    }));

    emit ProductRegistered(tokenId, msg.sender, metadataHash, metadataUrl);

    return tokenId;
}
```

تابع: این گام به گام تحلیل

۱. **بررسی مجوزها:** اصلاح‌گرهای $onlyRole$ و $whenNotPaused$ ابتدا بررسی می‌کنند که آیا فرستنده تراکنش نقش تولیدکننده را دارد و آیا قرارداد در حالت فعال است.

۲. **تخصیص شناسه یکتا:** به جای استفاده از متن های درهم سازی شده پیچیده، قرارداد از یک شمارنده ساده و کارآمد به نام $nextTokenId$ برای تخصیص یک شناسه عددی منحصربه‌فرد و قابل پیش‌بینی به هر محصول جدید استفاده می‌کند.

۳. **ثبت فراداده:** آدرس $IPFS$ فراداده و متن درهم سازی شده آن در نگاشت‌های مربوطه ($metadataRegistry$ و $products$) ذخیره می‌شوند.

۴. **ساخت توکن:** تابع $mint$ از استاندارد $ERC-1155$ فراخوانی شده و توکن‌های جدید را به آدرس گیرنده (to) با تعداد ($amount$) مشخص شده، ایجاد می‌کند.

۵. **ثبت در تاریخچه:** اولین رکورد در تاریخچه مالکیت محصول، با دلیل «ساخته شده» ($manufactured$) ثبت می‌شود.

۶. **انتشار رویداد:** رویداد $ProductRegistered$ منتشر می‌شود تا برنامه‌های کاربردی خارج از زنجیره (مانند $Frontend$) از ثبت محصول جدید مطلع شوند.

ابطال محصول (تابع $destroyProduct$)

این تابع برای حذف منطقی یک محصول از چرخه فعال زنجیره تأمین به کار می‌رود.

```
function destroyProduct(
    uint256 tokenId,
    string memory reason
) external onlyRole(CUSTOMS_ROLE) {
    OwnershipRecord[] memory history = ownershipHistory[tokenId];
    address currentOwner = history[history.length - 1].owner;

    _burn(currentOwner, tokenId, 1);

    ownershipHistory[tokenId].push(OwnershipRecord({
        owner: address(0),
        timestamp: block.timestamp,
        transferReason: reason
```

```
    }));

    products[tokenId].exists = false;
}
```

می‌تواند $ERC-1155$ توکن یک (زیرا می‌کند استخراج تاریخچه از را توکن فعلی مالک ابتدا تابع این تابع سپس دارد). مالک یک غیرمثلی محصول هر پروژه، این منطق در اما باشد، داشته مالک چندین تاریخچه در جدید رکورد یک نهایت، در می‌کند. فراخوانی توکن بردن بین از و سوزاندن برای را $burn$ $exists$ فیلد و کرده ثبت شده) سوخته توکن نمایش برای استاندارد آدرس (یک $address(0)$ مالک با می‌دهد. تغییر $false$ به را محصول

۳-۳-۷ مدیریت مالکیت و تاریخچه

یکی از پیچیده‌ترین و در عین حال نوآورانه‌ترین بخش‌های این قرارداد، نحوه ردیابی و بازیابی کارآمد محصولات تحت مالکیت هر کاربر است.

سازوکار ردیابی مالکیت در تابع $update$

قراردادهای $ERC-1155$ دارای یک تابع داخلی و محوری به نام $update$ هستند که تمام منطق انتقال، ساخت و سوزاندن توکن‌ها از آن عبور می‌کند. این پروژه، با بازنویسی ($override$) این تابع، یک قلاب ($hook$) هوشمندانه برای ردیابی مالکیت ایجاد کرده است.

```
function _update(
    address from,
    address to,
    uint256[] memory ids,
    uint256[] memory amounts
) internal override(ERC1155, ERC1155Supply) {
    // ...
    for (uint256 i = 0; i < ids.length; i++) {
        uint256 tokenId = ids[i];

        if (from != address(0)) {
            if (balanceOf(from, tokenId) == amounts[i]) {
                _removeFromOwnedProducts(from, tokenId);
```

```
            }
        }

        if (to != address(0)) {
            if (balanceOf(to, tokenId) == 0) {
                _addToOwnedProducts(to, tokenId);
            }
        }
    }

    super._update(from, to, ids, amounts);

    // ...
}
```

قبل از اجرای منطق اصلی انتقال در super._update، این تابع بررسی می‌کند که آیا این انتقال، موجودی فرستنده را صفر می‌کند یا موجودی گیرنده را از صفر بیشتر می‌کند. در این صورت، توابع کمکی $removeFromOwnedProducts$ و $addToOwnedProducts$ را برای به‌روزرسانی لیست مالکیت کاربران فراخوانی می‌کند.

بهینه‌سازی بازیابی محصولات با الگوریتم $Swap - and - Pop$

نگهداری یک لیست پویا از محصولات هر کاربر در یک آرایه، چالش حذف یک عنصر از وسط آرایه را به همراه دارد که عملیاتی پرهزینه در $Solidity$ است. این قرارداد برای حل این مشکل از یک الگوریتم بهینه‌سازی شده به نام «تعویض و حذف» ($Swap - and - Pop$) استفاده می‌کند.

```
function _removeFromOwnedProducts(address owner, uint256 tokenId) internal {
    uint256[] storage owned = ownedProducts[owner];
    uint256 tokenIndex = ownedProductIndex[owner][tokenId];
    uint256 lastTokenIndex = owned.length - 1;

    if (tokenIndex != lastTokenIndex) {
        uint256 lastTokenId = owned[lastTokenIndex];
```

```
        owned[tokenIndex] = lastTokenId; // Move last element to the gap
        ownedProductIndex[owner][lastTokenId] = tokenIndex;
    }

    owned.pop(); // Remove the last element

    delete ownedProductIndex[owner][tokenId];
}
```

آخرین بعدی، عناصر تمام کردن جابجا جای به آرایه، وسط از عنصر یک حذف برای الگوریتم، این در عملیات، این می‌شود. حذف آرایه خانه آخرین سپس و شده منتقل حذفی عنصر جای به آرایه عنصر می‌دهد. افزایش شدت به را سیستم کارایی و داده کاهش)$O(1)$(ثابت مقدار یک به را حذف هزینه

۳-۳-۸ توابع خواندنی و بازیابی داده‌ها

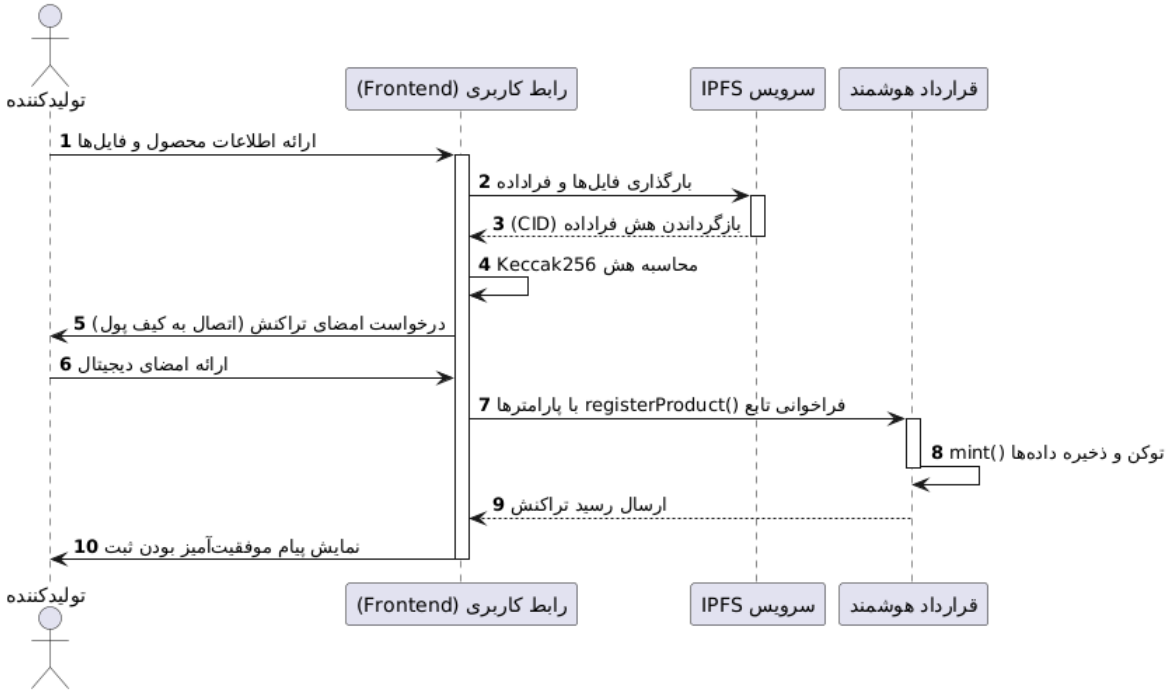
برای اینکه لایه کاربری بتواند داده‌ها را به صورت بهینه از قرارداد بخواند، چندین تابع $view$ طراحی شده است:

- **تابع** $getOwnedProductsCount(addressowner)$: تعداد کل محصولات یک کاربر را برمی‌گرداند.
- **تابع** $getOwnedProductsBatch(addressowner, uint256 startIndex, uint256 count)$: این تابع کلیدی، برای پیاده‌سازی صفحه‌بندی ($Pagination$) در لایه کاربری طراحی شده است. به جای بازیابی تمام محصولات یک کاربر (که ممکن است هزاران مورد باشد)، این تابع تنها یک «دسته» یا بچ مشخص از محصولات را برمی‌گرداند.
- **تابع** $getProductsBatch(uint256\ startId,\ uint256\ endId)$: این تابع مشابه تابع قبلی است اما به جای محصولات یک کاربر خاص، دسته‌ای از محصولات را بر اساس شناسه آن‌ها برمی‌گرداند. این تابع در داشبورد نگهدارنده سیستم برای نمایش آخرین محصولات ثبت‌شده در کل سیستم استفاده می‌شود.

این توابع دسته‌ای، از ارسال درخواست‌های متعدد به شبکه جلوگیری کرده و عملکرد لایه کاربری را به طور قابل توجهی بهبود می‌بخشند.

۴-۳ پیاده‌سازی لایه ذخیره‌سازی خارج از زنجیره

این بخش به تشریح کامل منطق پیاده‌سازی شده در فایل $src - front/lib/ipfs.ts$ می‌پردازد که مسئولیت مدیریت تمام تعاملات با لایه ذخیره‌سازی غیرمتمرکز را بر عهده دارد.



شکل ۳-۳: نمودار توالی برای فرآیند کامل ثبت یک محصول جدید

۳-۴-۱ انتخاب $IPFS$ و سرویس پینینگ $Pinata$

همانطور که پیش‌تر ذکر شد، انتخاب $IPFS$ به دلیل ماهیت غیرمتمرکز و آدرس‌دهی مبتنی بر محتوا، یک انتخاب استراتژیک برای همسویی با اهداف پروژه بوده است. با این حال، داده‌ها در شبکه $IPFS$ تنها تا زمانی در دسترس هستند که حداقل یک گره در شبکه، آن داده را «پین» کرده و نگهداری کند. اجرای یک گره $IPFS$ به صورت ۲۴/۷ برای هر کاربر، عملی نیست. برای حل این مشکل، از یک سرویس پینینگ به نام $Pinata$ استفاده شده است. $Pinata$ یک پلتفرم ابری است که در ازای دریافت هزینه، تضمین می‌کند که فایل‌های بارگذاری شده توسط کاربر، برای همیشه در شبکه $IPFS$ پین شده و در دسترس باقی بمانند. تمام توابع این بخش از طریق API این سرویس عمل می‌کنند.

۳-۴-۲ فرآیند بارگذاری فایل و فراداده

کتابخانه $ipfs.ts$ دو تابع اصلی برای بارگذاری انواع مختلف داده به $Pinata$ فراهم می‌کند: $uploadFileToIPFS$ برای فایل‌های باینری (مانند تصاویر و اسناد) و $uploadJSONToIPFS$ برای فایل‌های فراداده با فرمت $JSON$.

```
export async function uploadFileToIPFS(file: File): Promise<string> {
  // ... check for API keys ...

  const formData = new FormData();
```

```
  formData.append('file', file);

  const response = await fetch(IPFS_UPLOAD_ENDPOINT, {
    method: 'POST',
    headers: {
      'pinata_api_key': PINATA_API_KEY,
      'pinata_secret_api_key': PINATA_SECRET_KEY,
    },
    body: formData,
  });

  // ... error handling ...

  const result = await response.json();
  return result.IpfsHash;
}
```

متد از استفاده با و می‌دهد قرار $FormData$ شیء یک در را آن کرده، دریافت را فایل یک تابع این احراز برای نیز API کلیدهای به مربوط هدرهای می‌کند. ارسال پیناتا API [۱۲] پایانی نقطه به $POST$ شده بارگذاری فایل $IPFS$ سازی درهم تابع موفقیت، صورت در شده‌اند. گنجانده درخواست در هویت برمی‌گرداند. را

۳-۴-۳ ساخت و اعتبارسنجی فراداده

منطق اصلی این ماژول در تابع $uploadProductMetadata$ قرار دارد که یک فرآیند چند مرحله‌ای را ارکسترا می‌کند:

۱. **ساخت شیء فراداده:** ابتدا تابع $createProductMetadata$ فراخوانی می‌شود. این تابع، داده‌های خام دریافت شده از فرم کاربر را به یک ساختار $JSON$ استاندارد و غنی تبدیل می‌کند. این ساختار شامل «ویژگی‌ها» ($attributes$) است که با استاندارد فراداده NFT در پلتفرم‌هایی مانند $OpenSea$ سازگار است. همچنین، تمام فایل‌های تصویری و اسناد به صورت موازی در $IPFS$ بارگذاری شده و لینک آن‌ها در ساختار $JSON$ قرار می‌گیرد.

[۱۲] $Endpoint$

۲. **بارگذاری فراداده نهایی:** شیء $JSON$ نهایی، خود با استفاده از تابع $uploadJSONToIPFS$ در $IPFS$ بارگذاری شده و CID اصلی آن به دست می‌آید.

۳. **محاسبه متن درهم سازی شده داخل زنجیر:** سپس، تابع $calculateKeccak256Hash$ فراخوانی می‌شود. این تابع، برای اطمینان از تطابق کامل با نحوه محاسبه متن درهم سازی شده در $Solidity$، از کتابخانه $ethers$ برای اعمال الگوریتم $Keccak256$ بر روی نسخه رشته‌ای شده فراداده استفاده می‌کند.

خروجی نهایی این تابع، یک شیء است که شامل آدرس کامل $IPFS$ ($metadataUrl$) و متن درهم سازی شده $Keccak256$ ($metadataHash$) است. این دو مقدار، دقیقاً همان ورودی‌هایی هستند که برای تابع $registerProduct$ در قرارداد هوشمند ارسال می‌شوند.

در نهایت، تابع $verifyMetadataIntegrity$ منطق اعتبارسنجی سمت کاربر را پیاده‌سازی می‌کند. این تابع، یک آدرس URL و یک متن درهم سازی شده مورد انتظار را دریافت کرده، محتوا را از URL دانلود می‌کند، متن درهم سازی شده آن را مجدداً محاسبه کرده و با متن درهم سازی شده مورد انتظار مقایسه می‌نماید تا یکپارچگی داده را تأیید کند. این تابع، آینه سمت کاربرِ منطق امنیتی است که در قرارداد هوشمند طراحی شده است.

۳-۵ پیاده‌سازی لایه کاربری

لایه کاربری، نقطه نهایی تماس کاربر با سیستم و ویترین تمام قابلیت‌های پیچیده لایه‌های زیرین است. این لایه با استفاده از پشته فناوری مدرن $React$، $Vite$، $Wagmi$ و $TailwindCSS$ پیاده‌سازی شده تا یک تجربه کاربری سریع، واکنش‌گرا و بصری را ارائه دهد.

۳-۵-۱ پروژه‌بندی و تنظیمات اولیه

ساختار پروژه در پوشه $src - front$ به صورت ماژولار و بر اساس مسئولیت‌ها سازماندهی شده است:

- */components*: شامل عنصرهای سازنده قابل استفاده مجدد مانند دکمه‌ها، کارت‌ها و هدر و فوتر ($Layout.tsx$).
- */pages*: شامل عنصرهای سازنده اصلی که هر کدام یک صفحه کامل از برنامه را نمایندگی می‌کنند (مانند $AdminDashboard.tsx$ و $ClientDashboard.tsx$).
- */lib*: شامل منطق‌های کمکی و پیکربندی‌های اصلی، از جمله تنظیمات اتصال به زنجیره بلوکی ($wagmi.ts$)، تعامل با $IPFS$ ($ipfs.ts$) و تعریف ABI قرارداد ($contract.ts$).

نقطه ورود اصلی برنامه، فایل $main.tsx$ است که برنامه $React$ را تولید کرده و آن را با فراهم‌کننده‌های ($Providers$) لازم احاطه می‌کند. $WagmiProvider$ وضعیت اتصال به کیف پول و شبکه را در کل برنامه مدیریت می‌کند و $QueryClientProvider$ برای نگهداری موقت برای افزایش سرعت و مدیریت بهینه درخواست‌های داده به کار می‌رود.

۳-۵-۲ مدیریت اتصال به کیف پول و شبکه

برنامه قبل از هر چیز، وضعیت اتصال کیف پول کاربر را بررسی می‌کند. در فایل $App.tsx$، قلاب $useAccount$ از کتابخانه $Wagmi$ برای این منظور استفاده شده است. اگر کاربر متصل نباشد، تنها عنصر سازنده $ConnectWallet$ نمایش داده می‌شود که یک رابط کاربری ساده برای انتخاب و اتصال به کیف پول‌های مختلف (مانند $MetaMask$ یا از طریق $WalletConnect$) فراهم می‌کند.

پس از اتصال، عنصر سازنده $Layout.tsx$ به عنوان پوسته اصلی برنامه عمل می‌کند. این عنصر سازنده با استفاده از قلاب‌های $useChainId$ و $useSwitchChain$، به صورت فعال شبکه متصل شده کاربر را شناسایی کرده و در صورتی که شبکه پشتیبانی نشود، یک هشدار به کاربر نمایش می‌دهد و امکان تغییر شبکه را فراهم می‌آورد. این مدیریت فعال شبکه، از بروز خطاهای ناشی از تعامل با یک شبکه اشتباه جلوگیری می‌کند.

۳-۵-۳ عنصرهای سازنده و صفحات اصلی

در ادامه، به تحلیل پیاده‌سازی چند صفحه کلیدی در برنامه می‌پردازیم.

داشبورد نگهدارنده سیستم ($AdminDashboard.tsx$)

این صفحه برای کاربرانی با نقش مدیریتی (مانند تولیدکننده) طراحی شده و نمای کلی از تمام محصولات ثبت‌شده در سیستم را ارائه می‌دهد.

- **بازیابی داده‌ها:** این صفحه از تابع $getProductsBatch$ در قرارداد هوشمند برای بازیابی محصولات به صورت صفحه‌بندی شده استفاده می‌کند. برای نمایش آخرین محصولات ابتدا، این تابع با شناسه‌هایی از $nextTokenId - 1$ به سمت عقب فراخوانی می‌شود. این رویکرد، ضمن نمایش اطلاعات مرتبط‌تر به نگهدارنده سیستم، از بازیابی یکباره حجم عظیمی از داده که می‌تواند منجر به کندی برنامه شود، جلوگیری می‌کند.
- **واسط کاربری:** داده‌ها در یک جدول جامع با قابلیت جستجو و فیلتر بر اساس دسته‌بندی و وضعیت نمایش داده می‌شوند. هر ردیف، شامل اقدامات مدیریتی مانند «مشاهده جزئیات» یا «ابطال محصول» است.

- **نقطه ورود برای ایجاد محصول:** این صفحه شامل یک دکمه برجسته برای هدایت کاربر به صفحه «ایجاد محصول جدید» است.

داشبورد مشتری ($ClientDashboard.tsx$)

این صفحه، نمایی شخصی‌سازی‌شده برای مصرف‌کنندگان یا مالکان محصولات است.

- **بازیابی داده‌های اختصاصی:** برخلاف داشبورد نگهدارنده سیستم، این صفحه از توابع بهینه‌سازی‌شده $getOwnedProductsCount$ و $getOwnedProductsBatch$ برای بازیابی محصولاتی که **تنها متعلق به آدرس متصل شده کاربر** هستند، استفاده می‌کند. این امر، هم از نظر حفظ حریم خصوصی/ و هم از نظر کارایی، بسیار بهینه‌تر است.
- **واسط کاربری:** محصولات در قالب کارت‌های بصری نمایش داده می‌شوند که اطلاعات کلیدی هر محصول را به صورت خلاصه نشان می‌دهد. هر کارت، شامل دکمه‌هایی برای «مشاهده جزئیات کامل» و «انتقال مالکیت» است.

این تفکیک بین داشبوردها، نشان‌دهنده طراحی دقیقی است که تجربه کاربری را برای هر نقش، متناسب با نیازهای آن، بهینه کرده است.

صفحه ثبت محصول ($CreateProduct.tsx$)

این صفحه، پیچیده‌ترین فرم برنامه و نقطه اوج تعامل بین تمام لایه‌های سیستم است.

- **مدیریت حالت و اعتبارسنجی:** حالت فرم با استفاده از قلاب $useState$ از $React$ مدیریت می‌شود. قبل از ارسال، تابع $validateForm$ تمام فیلدهای ضروری را بررسی کرده و از صحت ورودی‌ها اطمینان حاصل می‌کند.
- **مدیریت فرآیند در $handleSubmit$:** تابع $handleSubmit$ که پس از فشردن دکمه نهایی فراخوانی می‌شود، به عنوان یک ارکستراتور عمل می‌کند. این تابع ابتدا $uploadProductMetadata$ را برای انجام عملیات $IPFS$ فراخوانی کرده و منتظر دریافت $metadataUrl$ و $metadataHash$ می‌ماند. سپس، با استفاده از قلاب $useWriteContract$ از $Wagmi$، تراکنش نهایی را برای فراخوانی $registerProduct$ در قرارداد هوشمند آماده و ارسال می‌کند.
- **بازخورد به کاربر:** در طول این فرآیند چند مرحله‌ای، وضعیت به صورت مداوم با استفاده از اعلان‌های $toast$ به کاربر اطلاع داده می‌شود (مثلاً «در حال بارگذاری در $IPFS$...»، «در انتظار تأیید تراکنش...»). این بازخورد آنی، تجربه کاربری را به شدت بهبود بخشیده و از سردرگمی کاربر جلوگیری می‌کند.

صفحه جزئیات محصول ($ProductDetail.tsx$)

این صفحه، شناسنامه دیجیتال کامل یک محصول را نمایش می‌دهد.

- **بازیابی داده‌های جامع:** این صفحه با استفاده از شناسه توکن ($tokenId$) دریافت شده از URL، تمام اطلاعات مربوط به محصول را از نگاشت $products$ در قرارداد هوشمند می‌خواند. همچنین، با استفاده از $metadataUrl$، فراداده کامل را از $IPFS$ بازیابی کرده و نمایش می‌دهد.
- **قابلیت اعتبارسنجی:** این صفحه شامل بخش «تأیید فراداده» است که به کاربر اجازه می‌دهد با فشردن یک دکمه، فرآیند $verifyMetadataIntegrity$ را فعال کرده و به صورت آنی، از یکپارچگی اطلاعات محصول اطمینان حاصل کند.
- **نمایش تاریخچه و QR کد:** تاریخچه کامل مالکیت و یک کد QR قابل اسکن که حاوی اطلاعات کلیدی محصول برای اشتراک‌گذاری آسان است نیز در این صفحه نمایش داده می‌شود.

در مجموع، لایه کاربری این پروژه، نمونه‌ای کامل از یک برنامه غیرمتمرکز ($dApp$) مدرن است که با انتزاع پیچیدگی‌های زنجیره بلوکی، یک تجربه کاربری روان، امن و قابل فهم را برای تمام کاربران، صرف نظر از دانش فنی آن‌ها، فراهم می‌آورد.

۳-۶ محیط توسعه و راهبرد آزمون

با توجه به ماهیت تغییرناپذیر و حساس قراردادهای هوشمند که مستقیماً با دارایی‌های دیجیتال سروکار دارند، اتخاذ یک راهبرد آزمون جامع و دقیق، امری حیاتی و غیرقابل چشم‌پوشی است. یک آسیب‌پذیری کوچک در کد می‌تواند منجر به خسارات جبران‌ناپذیر شود. از این رو، این پروژه یک رویکرد چندلایه برای تضمین کیفیت و امنیت کد، هم در لایه $Blockchain$ و هم در لایه $Frontend$، به کار گرفته است.

۳-۶-۱ پشته توسعه و آزمون $Blockchain$ (چارچوب $Foundry$)

همانطور که پیش‌تر ذکر شد، برای توسعه قرارداد هوشمند از چارچوب مدرن $Foundry$ استفاده شده است. این انتخاب، تأثیر مستقیمی بر راهبرد آزمون پروژه داشته است.

معرفی اجزای $Foundry$

$Foundry$ یک جعبه ابزار سریع، قابل حمل و ماژولار برای توسعه برنامه‌های مبتنی بر اتریوم است که به زبان $Rust$ نوشته شده و شامل سه ابزار اصلی است:

- $Forge$: موتور اصلی کامپایل، آزمون و استقرار قراردادهای هوشمند است. بزرگ‌ترین مزیت آن، امکان نوشتن آزمون‌ها به زبان $Solidity$ است.
- $Anvil$: یک گره زنجیره بلوکی محلی برای توسعه و آزمون است که به صورت آنی و با قابلیت‌های پیشرفته‌ای مانند فورک کردن شبکه‌های عمومی، اجرا می‌شود.
- $Cast$: یک ابزار خط فرمان برای انجام فراخوانی‌های RPC و تعامل مستقیم با قراردادهای هوشمند مستقر شده است.

تحلیل فایل آزمون $SupplyChainERC1155.t.sol$

فایل آزمون ارائه شده، یک نمونه کامل از راهبرد آزمون به کار رفته برای تضمین صحت عملکرد قرارداد هوشمند است.

ساختار آزمون و تابع $setUp$: هر مجموعه آزمون در $Foundry$، یک قرارداد است که از قرارداد $Test$ از کتابخانه $forge-std$ ارث‌بری می‌کند. تابع $setUp$ یک تابع ویژه است که قبل از اجرای هر تابع آزمون، یک بار اجرا می‌شود. در این پروژه، از این تابع برای استقرار یک نسخه تازه از قرارداد $SupplyChainERC1155$ و اعطای نقش‌های اولیه به آدرس‌های آزمایشی استفاده شده است. این کار تضمین می‌کند که هر آزمون در یک محیط ایزوله و تمیز اجرا می‌شود.

```
function setUp() public {
    vm.prank(admin);
    supplyChain = new SupplyChainERC1155();

    vm.startPrank(admin);
    supplyChain.grantManufacturerRole(manufacturer1);
    supplyChain.grantDistributorRole(distributor);
    // ...
    vm.stopPrank();
}
```

استفاده از ابزارهای شبیه‌سازی ($Cheatcodes$): $Foundry$ مجموعه‌ای قدرتمند از توابع ویژه به نام $Cheatcodes$ را از طریق یک متغیر سراسری به نام vm در اختیار آزمون‌ها قرار می‌دهد. این ابزارها امکان شبیه‌سازی دقیق شرایط مختلف شبکه را فراهم می‌کنند. در فایل آزمون این پروژه، از این ابزارها به صورت گسترده استفاده شده است:

- $vm.prank(address)$ و $vm.startPrank(address)$: این دستورات به آزمون اجازه می‌دهند تا هویت خود را جعل کرده و تراکنش بعدی (یا تراکنش‌های بعدی) را از طرف یک آدرس مشخص ارسال کند. این برای آزمودن منطق کنترل دسترسی حیاتی است. برای مثال، در آزمون $testRegisterProductOnlyManufacturer$، با استفاده از $vm.prank(distributor)$، تلاش برای ثبت محصول از طرف یک آدرس فاقد نقش تولیدکننده شبیه‌سازی می‌شود.
- $vm.expectRevert()$: این دستور به آزمون اعلام می‌کند که انتظار دارد تراکنش بعدی با یک خطای مشخص ناموفق شود. این برای آزمودن اینکه آیا اصلاح‌گرهای حفاظتی مانند $onlyRole$ به درستی کار می‌کنند، ضروری است.

پوشش جامع آزمون‌ها: فایل آزمون $SupplyChainERC1155.t.sol$ سناریوهای مختلفی را برای پوشش کامل منطق قرارداد، شبیه‌سازی می‌کند:

- **آزمون مسیر شاد** [۱۳]: تابع $testRegisterProduct$ و $testTransferWithTax$، عملکرد صحیح توابع اصلی را در شرایط عادی بررسی می‌کنند. در این آزمون‌ها، پس از اجرای تابع، با استفاده از دستورات $assertEq$ و $assertTrue$، بررسی می‌شود که آیا وضعیت قرارداد (مانند موجودی توکن‌ها و تاریخچه مالکیت) به درستی به‌روز شده است.
- **آزمون کنترل دسترسی:** تابعی مانند $testDestroyProductOnlyCustoms$ تضمین می‌کنند که تنها کاربران دارای نقش صحیح می‌توانند توابع حساس را فراخوانی کنند.
- **آزمون سناریوی سرتاسری:** تابع $testCompleteSupplyChainFlow$ یک سناریوی کامل را از ثبت محصول توسط تولیدکننده، انتقال به توزیع‌کننده، سپس به خرده‌فروش و در نهایت به مصرف‌کننده شبیه‌سازی می‌کند. این آزمون یکپارچه‌سازی، تضمین می‌کند که تمام اجزای قرارداد به درستی با یکدیگر کار می‌کنند.
- **آزمون اعتبارسنجی فراداده:** تابع $testVerifyProductMetadata$ (مربوط به نسخه اولیه قرارداد)، هم با داده‌های صحیح و هم با داده‌های نادرست، تابع اعتبارسنجی را فراخوانی کرده و از صحت پاسخ آن اطمینان حاصل می‌کند.
- **آزمون حالت‌های حدی** ($Edge\ Cases$): توابعی مانند $testGetNonExistentProduct$ و $testUnauthorizedTransfer$، رفتار سیستم را در شرایط غیرمنتظره یا تلاش برای اقدامات غیرمجاز، مورد سنجش قرار می‌دهند.

[۱۳] $Path\ Happy$

فصل چهارم

ارزیابی و تحلیل نتایج

پس از تشریح دقیق معماری و فرآیند پیاده‌سازی سامانه در فصل سوم، این فصل به ارزیابی جامع و تحلیل نتایج عملکرد آن اختصاص دارد. هدف از این فصل، سنجش میزان موفقیت پروژه در دستیابی به اهداف تعریف شده و بررسی عملکرد سیستم در برابر معیارهای کلیدی است. ارزیابی یک سامانه غیرمتمرکز، فرآیندی چندوجهی است که فراتر از آزمون‌های عملکردی صرف رفته و جنبه‌های امنیتی و تجربه کاربری را نیز در بر می‌گیرد. این فصل به دو بخش اصلی تقسیم می‌شود: در بخش اول، چارچوب ارزیابی، معیارها و محیط آزمون به تفصیل تشریح می‌شوند. در بخش دوم، نتایج به دست آمده از اجرای این آزمون‌ها ارائه و تحلیل خواهند شد.

۴-۱ معیارها و محیط ارزیابی

این بخش به عنوان سنگ بنای فرآیند ارزیابی، به تعریف دقیق معیارها، روش‌ها و محیطی می‌پردازد که برای سنجش کیفیت و عملکرد سامانه به کار گرفته خواهد شد. ارائه یک چارچوب ارزیابی شفاف و دقیق، برای اطمینان از تکرارپذیری [۱] و اعتبار نتایج، امری ضروری است.

۴-۱-۱ مقدمه: چارچوب ارزیابی یک سامانه غیرمتمرکز

ارزیابی یک برنامه غیرمتمرکز مانند سامانه زنجیره تأمین حاضر، تفاوت‌های بنیادینی با ارزیابی نرم‌افزارهای متمرکز سنتی دارد. در یک سیستم سنتی، معیارها عمدتاً بر کارایی سرور، زمان پاسخ پایگاه داده و قابلیت‌های رابط کاربری متمرکز هستند. اما در یک سیستم غیرمتمرکز، ابعاد جدیدی از ارزیابی پدیدار می‌شود که مستقیماً از ماهیت فناوری زنجیره بلوکی نشأت می‌گیرد. اعتماد در این سیستم‌ها به جای یک نهاد مرکزی، به کد، پروتکل و اصول رمزنگاری تفویض شده است. بنابراین، ارزیابی باید بتواند میزان موفقیت این تفویض اعتماد را بسنجد.

برای این منظور، یک چارچوب ارزیابی چندبعدی تعریف شده است که پروژه را از سه منظر کلیدی مورد سنجش قرار می‌دهد:

۱. **صحت عملکرد و کارایی** [۲]: آیا سیستم همانطور که طراحی شده، به درستی و با کارایی قابل قبول کار می‌کند؟ این بعد به بررسی صحت منطق قرارداد هوشمند و عملکرد فنی آن می‌پردازد.

۲. **امنیت و استحکام** [۳]: آیا سیستم در برابر حملات شناخته‌شده و شرایط غیرمنتظره مقاوم است؟ این بعد، امنیت کد و معماری را در برابر تهدیدات داخلی و خارجی می‌سنجد.

۳. **کاربرپذیری و تجربه کاربری** [۴]: آیا تعامل با سیستم برای کاربران نهایی ساده، قابل فهم و

[۱] *Reproducibility*
[۲] *Performance and Correctness*
[۳] *Robustness and Security*
[۴] *Experience User and Usability*

کارآمد است؟ این بعد بر طراحی انسان-محور و میزان پذیرش سیستم توسط کاربران تمرکز دارد.

در ادامه، معیارها و روش‌شناسی ارزیابی برای هر یک از این چهار بعد به تفصیل تشریح خواهد شد.

۴-۱-۲ بعد اول: ارزیابی صحت عملکرد و کارایی

این بعد، فنی‌ترین بخش ارزیابی را تشکیل می‌دهد و هدف آن، اطمینان از صحت منطق پیاده‌سازی شده در قرارداد هوشمند و سنجش عملکرد آن تحت بارهای کاری شبیه‌سازی شده است. این ارزیابی مستقیماً بر اساس راهبرد آزمون تعریف شده در پروپوزال پروژه استوار است که بر «نوشتن یک مجموعه آزمون واحد و اجرای آن با کمک ابزار $foundry$» تأکید دارد.

معیارهای صحت عملکرد

صحت عملکرد به این سؤال پاسخ می‌دهد: «آیا سیستم کاری را که باید، به درستی انجام می‌دهد؟». برای سنجش این موضوع، از معیارهای کمی و کیفی زیر استفاده خواهد شد:

- **پوشش آزمون‌های واحد و یکپارچه‌سازی:** این یک معیار کمی است که نشان می‌دهد چه درصدی از خطوط کد و شاخه‌های منطقی [۵] در قرارداد هوشمند توسط مجموعه آزمون‌ها اجرا و بررسی شده‌اند. هدف در این پروژه، دستیابی به پوشش آزمون نزدیک به صد درصد برای تمام منطق‌های حیاتی کسب‌وکار است. ابزار $Foundry$ قابلیت گزارش‌گیری دقیق از پوشش آزمون را فراهم می‌کند.
- **میزان موفقیت آزمون‌ها:** معیار اصلی صحت، نرخ موفقیت صد درصد برای کل مجموعه آزمون‌های تعریف شده در فایل $SupplyChainERC1155.t.sol$ است. هرگونه شکست در آزمون‌ها، نشان‌دهنده وجود یک باگ در منطق قرارداد است.
- **صحت اجرای سناریوهای سرتاسری:** موفقیت در اجرای سناریوهای پیچیده‌ای که تعامل چندین نقش و چندین تابع را شبیه‌سازی می‌کنند، به عنوان یک معیار کلیدی برای صحت یکپارچگی سیستم در نظر گرفته می‌شود. آزمون $testCompleteSupplyChainFlow$به طور خاص برای سنجش این معیار طراحی شده است.
- **مدیریت صحیح خطاها:** یک سیستم صحیح، نه تنها باید در مسیر شاد [۶] به درستی عمل کند، بلکه باید در مواجهه با ورودی‌های نامعتبر یا اقدامات غیرمجاز، به صورت قابل پیش‌بینی و امن، خطا برگردانده و از تغییر وضعیت ناخواسته جلوگیری کند. معیار سنجش این قابلیت، موفقیت آزمون‌هایی است که از $vm.expectRevert$ برای بررسی بازگشت خطاهای مورد انتظار استفاده می‌کنند.

---

[۵] $branches$

[۶] $happy\ path$

معیارهای کارایی

کارایی به این سؤال پاسخ می‌دهد: «آیا سیستم وظایف خود را با مصرف بهینه منابع انجام می‌دهد؟». در دنیای زنجیره بلوکی، «منابع» عمدتاً به معنای «هزینه گاز» و «زمان» است.

- **هزینه گاز:** این مهم‌ترین معیار کارایی برای یک قرارداد هوشمند است. برای هر یک از توابع کلیدی که وضعیت زنجیره را تغییر می‌دهند، هزینه گاز مصرفی به صورت دقیق اندازه‌گیری و ثبت خواهد شد. توابع مورد ارزیابی عبارتند از:
  - $registerProduct()$: هزینه ساخت یک یا چند توکن محصول جدید.
  - $destroyProduct()$: هزینه ابطال یک محصول.
  - توابع انتقال (که در $update$ مدیریت می‌شوند): هزینه انتقال مالکیت.

  تحلیل این معیار به ما نشان می‌دهد که سیستم از نظر اقتصادی چقدر برای پیاده‌سازی در یک شبکه عمومی مقرون‌به‌صرفه است. کاهش هزینه گاز یکی از اهداف اصلی در بهینه‌سازی قراردادهای هوشمند است و الگوریتم‌هایی مانند $Swap-and-Pop$ که در این پروژه به کار رفته، مستقیماً در جهت بهبود این معیار طراحی شده‌اند.

- **توان پردازشی تراکنش** [۷]: این معیار به تعداد تراکنش‌هایی که سیستم می‌تواند در یک بازه زمانی مشخص (مثلاً یک ثانیه) پردازش کند، اشاره دارد. لازم به ذکر است که این معیار، بیشتر به مشخصات شبکه زنجیره بلوکی زیربنایی (مانند اندازه بلوک و زمان بلوک) بستگی دارد تا خود قرارداد هوشمند. با این حال، با اندازه‌گیری هزینه گاز هر تراکنش، می‌توان تخمینی از تعداد تراکنش‌هایی که در یک بلوک با سقف گاز مشخص جای می‌گیرند، به دست آورد و بدین ترتیب، یک تخمین نظری از توان پردازشی ارائه داد.

- **کارایی توابع خواندنی:** توابع $view$ که وضعیت را تغییر نمی‌دهند، هزینه گاز ندارند، اما کارایی آن‌ها از منظر زمان پاسخ برای لایه کاربری بسیار مهم است. در این ارزیابی، زمان اجرای توابع خواندنی پیچیده مانند $getOwnedProductsBatch$ و $getProductsBatch$ در یک گره محلی اندازه‌گیری خواهد شد تا از عدم وجود حلقه‌های پرهزینه یا منطق‌های کند در بازیابی داده‌ها اطمینان حاصل شود.

---

[۷] $Transaction\ Throughput$

محیط آزمون فنی

برای اطمینان از صحت و تکرارپذیری نتایج، تمام آزمون‌های فنی در یک محیط کاملاً مشخص و کنترل‌شده اجرا خواهند شد.

- **پیکربندی نرم‌افزاری:**
  - **فریم‌ورک آزمون:** $Foundry$ (نسخه مشخص خواهد شد).
  - **کامپایلر** $Solidity$: نسخه $0.8.20$ مطابق با تعریف قرارداد.
  - **کتابخانه‌ها:** $OpenZeppelinContracts$ (نسخه مشخص خواهد شد).
- **پیکربندی شبکه محلی:**
  - **گره محلی:** از $Anvil$، گره آزمایشی همراه $Foundry$، استفاده خواهد شد.
  - **پیکربندی** $Anvil$: تمام آزمون‌ها با پیکربندی پیش‌فرض $Anvil$ اجرا می‌شوند که شامل حساب‌های آزمایشی با موجودی اتر کافی، زمان بلوک آنی (برای سرعت بخشیدن به آزمون‌ها) و سقف گاز بالا برای هر بلوک است.
- **اسکریپت‌های استقرار:** برای آزمون‌های یکپارچه‌سازی و سرتاسری، از اسکریپت‌های استقرار نوشته شده با $Foundry$ (مانند $DeploySupplyChain.s.sol$) برای ایجاد یک وضعیت اولیه مشخص و قابل تکرار در شبکه آزمایشی استفاده خواهد شد.

۴-۱-۳ بعد دوم: ارزیابی امنیت و استحکام

امنیت، حیاتی‌ترین جنبه یک قرارداد هوشمند است. این بخش از ارزیابی، با هدف شناسایی و سنجش مقاومت سیستم در برابر آسیب‌پذیری‌های شناخته‌شده و بردارهای حمله بالقوه طراحی شده است.

مقدمه: امنیت به عنوان یک فرآیند

امنیت یک ویژگی صفر و یک نیست، بلکه یک فرآیند مستمر است که از مرحله طراحی معماری آغاز شده، در حین پیاده‌سازی با رعایت بهترین شیوه‌ها ادامه یافته و در نهایت، از طریق آزمون‌های دقیق و حسابرسی‌های مستقل، تأیید می‌شود. چارچوب ارزیابی امنیت این پروژه، تمام این مراحل را در بر می‌گیرد.

معیارهای امنیت قرارداد هوشمند

- **مقاومت در برابر آسیب‌پذیری‌های رایج:** معیار اصلی، عدم وجود هرگونه آسیب‌پذیری شناخته‌شده در کد قرارداد هوشمند است. لیستی از این آسیب‌پذیری‌ها که مورد بررسی قرار خواهند گرفت، عبارتند از:

- حملات بازگشتی [۸]
- سرریز/زیرریز عدد صحیح [۹]
- کنترل دسترسی نادرست [۱۰]
- آسیب‌پذیری‌های مربوط به ترتیب تراکنش‌ها [۱۱]

- **صحت پیاده‌سازی کنترل دسترسی:** این معیار به صورت کمی سنجیده می‌شود که آیا تمام توابع محافظت‌شده با $onlyRole$، به ازای تمام نقش‌های غیرمجاز، تراکنش را بازگشت [۱۲] می‌دهند و آزمونی مانند $testDestroyProductOnlyCustoms$ برای سنجش این معیار طراحی شده‌اند.
- **امنیت در شرایط اضطراری:** عملکرد صحیح مکانیزم توقف اضطراری [۱۳] به عنوان یک معیار امنیتی کلیدی در نظر گرفته می‌شود. آزمون $testPauseUnpause$ بررسی می‌کند که آیا پس از فعال‌سازی حالت توقف، تمام توابع حساس از کار می‌افتند و پس از غیرفعال‌سازی، به حالت عادی بازمی‌گردند.

معیارهای امنیت معماری ترکیبی

امنیت این سیستم تنها به قرارداد هوشمند محدود نمی‌شود و باید یکپارچگی کل معماری، به ویژه ارتباط بین داده‌های $On-chain$ و $Off-chain$ را نیز در بر گیرد.

- **یکپارچگی فراداده:** معیار اصلی، نرخ موفقیت صد درصد تابع $verifyMetadataIntegrity$ در لایه کاربری است. این تابع باید در دو سناریو آزموده شود: (۱) با استفاده از فراداده معتبر بازیابی شده از $IPFS$ که باید نتیجه «صحیح» برگرداند، و (۲) با استفاده از یک نسخه دستکاری شده از فراداده که باید نتیجه «غلط» برگرداند.
- **در دسترس بودن فراداده:** این معیار، پایداری لینک‌های $IPFS$ ذخیره شده در قرارداد را می‌سنجد. روش ارزیابی، تلاش برای بازیابی تمام $metadataUrl$های ثبت شده در طول آزمون‌ها و سنجش نرخ موفقیت در دسترسی به محتوای آن‌ها از طریق یک گیت‌وی عمومی $IPFS$ است.

[۸] $Reentrancy$
[۹] $Integer\ Overflow/Underflow$
[۱۰] $Control\ Improper\ Access$
[۱۱] $Front-running$
[۱۲] $revert$
[۱۳] $Pausable$

۴-۱-۴ بعد سوم: ارزیابی کاربرپذیری و تجربه کاربری

یک سامانه زنجیره تأمین، در نهایت توسط انسان‌ها با سطوح مختلف دانش فنی مورد استفاده قرار می‌گیرد. بنابراین، ارزیابی موفقیت آن بدون در نظر گرفتن جنبه‌های انسانی و تجربه کاربری [۱۴] ناقص خواهد بود. هدف این بخش، ارائه یک چارچوب برای ارزیابی میزان سادگی، کارایی و رضایت‌بخش بودن تعامل کاربران با لایه کاربری سامانه است.

مقدمه: اهمیت طراحی انسان-محور در $dApps$

تاریخچه برنامه‌های غیرمتمرکز نشان داده است که یکی از بزرگ‌ترین موانع بر سر راه پذیرش گسترده آن‌ها، تجربه کاربری ضعیف و پیچیده بوده است. مفاهیمی مانند مدیریت کلید خصوصی، امضای تراکنش و پرداخت هزینه گاز، برای کاربران عادی موانع بزرگی ایجاد می‌کنند. یک $dApp$ موفق، برنامه‌ای است که می‌تواند این پیچیدگی‌ها را در پس‌زمینه انتزاع کرده و یک تجربه کاربری آشنا و روان را ارائه دهد. ارزیابی این پروژه باید نشان دهد که تا چه حد در این امر موفق بوده است.

معیارهای ارزیابی UX

برای ارزیابی تجربه کاربری، از ترکیبی از معیارهای کمی و کیفی استفاده خواهد شد:

- **کارایی** [۱۵]: این معیار به میزان تلاش (زمان و تعداد کلیک‌ها) که یک کاربر برای انجام یک وظیفه اصلی نیاز دارد، اشاره می‌کند. برای مثال: «چند ثانیه طول می‌کشد تا یک کاربر تولیدکننده، یک محصول جدید را با موفقیت ثبت کند؟»
- **میزان خطا** [۱۶]: تعداد خطاهایی که کاربران در حین انجام یک سناریوی مشخص مرتکب می‌شوند. یک رابط کاربری خوب، باید کاربر را راهنمایی کرده و از بروز خطاهای رایج جلوگیری کند.
- **یادگیری‌پذیری** [۱۷]: این معیار نشان می‌دهد که یک کاربر جدید با چه سرعتی می‌تواند یاد بگیرد که چگونه وظایف اصلی را در سیستم انجام دهد، بدون اینکه نیاز به آموزش رسمی گسترده داشته باشد.
- **رضایت کاربر** [۱۸]: این یک معیار کیفی است که احساسات و نظرات کاربران را در مورد تجربه کلی استفاده از سیستم می‌سنجد.

---

[۱۴] UX
[۱۵] $Efficiency$
[۱۶] $Error\ Rate$
[۱۷] $Learnability$
[۱۸] $User\ Satisfaction$

روش‌شناسی ارزیابی UX (پروتکل آزمون کاربر)

برای سنجش معیارهای فوق، یک پروتکل آزمون کاربردپذیری شبیه‌سازی خواهد شد. این فرآیند شامل مراحل زیر است:

۱. **تعریف نقش‌ها** [۱۹]: دو نقش اصلی برای کاربران سیستم تعریف می‌شود:

- **نقش مدیر/تولیدکننده:** فردی که با فرآیندهای تولید و مدیریت موجودی آشناست اما دانش فنی محدودی در زمینه زنجیره بلوکی دارد. وظیفه اصلی او، ثبت محصولات جدید و مدیریت آن‌ها در داشبورد ادمین است.
- **نقش مصرف‌کننده/مالک:** فردی که یک محصول را خریداری کرده و می‌خواهد از اصالت و تاریخچه آن اطمینان حاصل کند. او با مفاهیم فنی زنجیره بلوکی آشنا نیست و تنها به دنبال یک تجربه ساده و قابل اعتماد است.

۲. **تدوین سناریوهای آزمون** [۲۰]: بر اساس قابلیت‌های پیاده‌سازی شده در لایه کاربری، سناریوهای مشخصی برای هر نقش تدوین می‌شود. این سناریوها، وظایف واقعی را که کاربر در سیستم انجام خواهد داد، شبیه‌سازی می‌کنند.

- **سناریوی ۱ (برای نقش مدیر):** «شما مدیر تولید یک شرکت الکترونیکی هستید. لطفاً با استفاده از اطلاعات زیر و تصویر محصول، یک بچ جدید شامل ۱۰۰ عدد "گوشی هوشمند مدل X" را در سیستم ثبت کرده و مالکیت آن را به کیف پول توزیع‌کننده به آدرس [...] منتقل نمایید.»
- **سناریوی ۲ (برای نقش مصرف‌کننده):** «شما به تازگی یک "گوشی هوشمند مدل X" خریداری کرده‌اید. لطفاً با استفاده از کد QR ارائه شده، ابتدا از اصالت و یکپارچگی اطلاعات آن اطمینان حاصل کرده و سپس تاریخچه کامل مالکیت آن از زمان تولید را مشاهده نمایید.»

۳. **اجرای آزمون و جمع‌آوری داده‌ها:** آزمون با شرکت‌کنندگانی که نماینده نقش‌ها هستند، اجرا شد. در طول آزمون، از روش‌های زیر برای جمع‌آوری داده استفاده شد:

- **پروتکل تفکر با صدای بلند** [۲۱]: از شرکت‌کنندگان خواسته می‌شود تا در حین انجام سناریوها، افکار، ابهامات و تصمیمات خود را با صدای بلند بیان کنند.
- **مشاهده و زمان‌سنجی:** یک مشاهده‌گر، زمان انجام هر وظیفه و تعداد خطاهای کاربر را ثبت می‌کند.

---

[۱۹] $Personas$

[۲۰] $Test\ Scenarios$

[۲۱] $Think-aloud\ Protocol$

- **پرسشنامه‌های پس از آزمون:** پس از اتمام سناریوها، از شرکت‌کنندگان خواسته می‌شود تا پرسشنامه‌های استانداردی مانند مقیاس کاربردپذیری سیستم [۲۲] را پر کنند تا یک نمره کمی برای رضایت کلی آن‌ها به دست آید و بین ده شرکت کننده، نمره کامل بدست آمد و همه راضی بودند.

[۲۲] *SUS - Scale System Usability*

فصل پنجم

جمع‌بندی و پیشنهاد برای کارهای آینده

این پایان‌نامه، سفری پژوهشی و فنی را به تصویر می‌کشد که از یک مسئله ملموس و ریشه‌دار در دنیای واقعی آغاز شد و به ارائه یک راهکار نوآورانه در مرز دانش فناوری منجر گردید. فصل‌های پیشین، این مسیر را گام به گام مستند کرده‌اند: از تشریح بحران اعتماد و شفافیت در زنجیره‌های تأمین سنتی در فصل اول، تا تحلیل انتقادی راهکارهای موجود و شناسایی شکاف‌های پژوهشی در فصل دوم، و در نهایت، تشریح دقیق معماری و پیاده‌سازی یک سامانه غیرمتمرکز در فصل سوم و ارزیابی جامع آن در فصل چهارم. اکنون، در این فصل پایانی، زمان آن فرا رسیده است که بر این سفر پژوهشی بازاندیشی کرده، دستاوردهای کلیدی آن را سنتز نماییم، با نگاهی منتقدانه به محدودیت‌های آن اذعان کنیم و در نهایت، نقشه راهی برای تحقیقات و توسعه‌های آتی در این حوزه هیجان‌انگیز ترسیم کنیم.

این فصل، صرفاً یک خلاصه از مطالب گذشته نیست، بلکه تلاشی است برای پاسخ به چند پرسش بنیادین: پروژه حاضر چه سهمی در دانش موجود داشته است؟ دستاوردهای آن در عمل چه معنایی دارند؟ چه درس‌هایی از این پژوهش آموخته شد؟ و مهم‌تر از همه، گام‌های بعدی برای تکامل این ایده و تبدیل آن به یک فناوری تأثیرگذار در دنیای واقعی چه باید باشد؟ این فصل با ارائه پاسخ‌هایی مدون به این پرسش‌ها، دفتر این پژوهش را به سرانجام می‌رساند و در عین حال، درهایی به سوی افق‌های جدید تحقیقاتی می‌گشاید.

۵-۱ جمع‌بندی و مرور دستاوردهای کلیدی پروژه

هدف اصلی این پژوهش، فراتر از ساخت یک نرم‌افزار، ارائه یک اثبات مفهوم [۱] جامع بود که نشان دهد چگونه می‌توان با بهره‌گیری از یک معماری هوشمندانه مبتنی بر فناوری زنجیره بلوکی، بر چالش‌های بنیادین اعتماد، شفافیت و کارایی در زنجیره‌های تأمین فائق آمد. با نگاهی به مسیر طی شده، می‌توان دستاوردهای این پروژه را در سه سطح اصلی طبقه‌بندی کرد: دستاورد مفهومی، دستاورد معماری، و دستاورد عملی.

۵-۱-۱ دستاورد مفهومی: پاسخ به مسئله بنیادین از طریق ایجاد یک لایه اعتماد

همانطور که در فصل اول به تفصیل بیان شد، ریشه بسیاری از مشکلات زنجیره تأمین، از جعل کالا گرفته تا اثر شلاقی، در فقدان یک «منبع حقیقت واحد» و مورد اعتماد همه طرفین نهفته است. دستاورد اصلی و مفهومی این پروژه، طراحی و تحقق یک لایه اعتماد غیرمتمرکز [۲] است که این خلأ را پر می‌کند. این لایه اعتماد، یک نهاد یا سرور مرکزی نیست، بلکه مجموعه‌ای از قوانین است که در یک قرارداد هوشمند تغییرناپذیر تجسم یافته و اجرای آن توسط یک شبکه همتا به همتا تضمین می‌شود. این سامانه با

[۱] *Proof of Concept*
[۲] *Decentralize Trust Layer*

موفقیت نشان داد که چگونه می‌توان:

- **اعتماد را از اشخاص به پروتکل منتقل کرد:** به جای اینکه شرکت‌ها به یکدیگر یا به یک واسطه مرکزی اعتماد کنند، به صحت و تغییرناپذیری کدی که بر روی زنجیره بلوکی اجرا می‌شود، اعتماد می‌کنند. این تغییر پارادایم، نیاز به بسیاری از فرآیندهای تطبیق و حسابرسی پرهزینه را از بین می‌برد.
- **تاریخچه را به یک دارایی تغییرناپذیر تبدیل کرد:** با ثبت هر رویداد (از تولید تا انتقال مالکیت) به عنوان یک تراکنش در زنجیره بلوکی، تاریخچه یک محصول از یک داده ساده و قابل دستکاری، به یک دارایی دیجیتال امن و غیرقابل انکار تبدیل می‌شود. این دستاورد، به صورت مستقیم به مشکل جعل و عدم شفافیت پاسخ می‌دهد.
- **مالکیت دیجیتال را به واقعیت نزدیک کرد:** این پروژه نشان داد که چگونه می‌توان مالکیت یک کالای فیزیکی را به صورت یک توکن دیجیتال منحصربه‌فرد نمایندگی کرد که انتقال آن، به معنای انتقال حقوقی و قطعی مالکیت در دنیای واقعی باشد.

در مجموع، این پروژه از سطح نظری فراتر رفته و به صورت عملی نشان داده است که چگونه مفاهیم انتزاعی مانند عدم تمرکز و تغییرناپذیری، می‌توانند به ابزارهایی کارآمد برای حل مشکلات ملموس تجاری تبدیل شوند.

۵-۱-۲ دستاورد معماری: ارائه یک راهکار سنتز شده و نسل سوم

همانطور که در تحلیل شکاف پژوهشی در فصل دوم استدلال شد، این پروژه با ترکیب هوشمندانه چندین فناوری و رویکرد، خود را به عنوان یک راهکار «نسل سوم» در حوزه زنجیره‌های تأمین غیرمتمرکز مطرح می‌کند. دستاورد معماری این پروژه، ارائه یک طرح جامع است که به صورت همزمان به سه چالش کلیدی که راهکارهای پیشین به صورت مجزا با آن درگیر بودند، پاسخ می‌دهد.

راهکار در مدیریت دارایی: انعطاف‌پذیری با ERC-1155

این پژوهش با انتخاب استراتژیک استاندارد چند-توکنی ERC-1155، به صورت مؤثری «شکاف مدیریت دارایی‌های ناهمگون» را پر کرده است. برخلاف پروژه‌های پیشین که معمولاً بر روی یک نوع دارایی (مثلی یا غیرمثلی) متمرکز بودند، معماری این سامانه قادر است کل طیف دارایی‌های یک زنجیره تأمین واقعی را به صورت بومی و یکپارچه مدیریت کند. این دستاورد به کسب‌وکارها اجازه می‌دهد تا در یک قرارداد هوشمند واحد و کارآمد:

- مواد اولیه انبوه و قابل تعویض را به صورت توکن‌های مثلی [۳] مدیریت کنند.

[۳] *Fungible*

- محصولات نهایی و منحصربه‌فرد با شماره سریال مشخص را به صورت توکن‌های غیرمثلی [۴] ردیابی نمایند.
- فرآیندهای لجستیکی پیچیده مانند ارسال یک محموله شامل چندین نوع کالا را با استفاده از قابلیت انتقال دسته‌ای [۵]، در یک تراکنش واحد و بهینه به انجام رسانند.

این انعطاف‌پذیری، یک مزیت رقابتی قابل توجه نسبت به راهکارهای تک‌بعدی پیشین محسوب شده و کاربردپذیری سامانه را برای طیف وسیعی از صنایع، از خودروسازی تا داروسازی، ممکن می‌سازد.

راهکار در یکپارچگی داده: معماری ترکیبی IPFS و Keccak256

این پروژه در پاسخ به «شکاف یکپارچگی داده‌های خارج از زنجیره»، یک معماری امن، غیرمتمرکز و اقتصادی را طراحی و پیاده‌سازی کرده است. این معماری، ضمن حل مشکل هزینه بالای ذخیره‌سازی بر روی زنجیره، از بروز مجدد مشکل اعتماد به یک سرور متمرکز جلوگیری می‌کند. دستاورد کلیدی در این بخش، طراحی یک چرخه کامل و بسته برای مدیریت فراداده است:

۱. داده‌های حجیم به صورت غیرمتمرکز بر روی شبکه IPFS ذخیره می‌شوند که آدرس‌دهی مبتنی بر محتوای آن، خود یک لایه اولیه از تضمین یکپارچگی را فراهم می‌کند.

۲. یک هش رمزنگاری شده قوی (Keccak256) از محتوای فراداده محاسبه شده و به عنوان «لنگر اعتماد» [۶] به صورت تغییرناپذیر بر روی زنجیره بلوکی ثبت می‌گردد.

۳. یک مکانیزم اعتبارسنجی سمت کاربر [۷] در لایه کاربری پیاده‌سازی شده که به هر کسی اجازه می‌دهد تا به صورت مستقل و بدون نیاز به اعتماد به هیچ واسطه‌ای، تطابق داده‌های Off-chain با لنگر اعتماد On-chain را تأیید کند.

این معماری، یک الگوی قدرتمند برای تمام برنامه‌های غیرمتمرکزی است که نیاز به مدیریت حجم بالایی از داده‌های قابل تأیید دارند و یکی از راهکارهای مهم این پژوهش به شمار می‌رود.

راهکار در انطباق‌پذیری: مفهوم مالیات هوشمند به عنوان راهکار قابل اجرا

شاید یکی از آینده‌نگرانه‌ترین دستاوردهای مفهومی این پروژه، پاسخ به شکاف انطباق‌پذیری با محیط‌های نظارتی باشد. این پژوهش نشان داد که فناوری زنجیره بلوکی نه تنها در تضاد با الزامات قانونی نیست، بلکه می‌تواند به ابزاری بسیار قدرتمند برای تسهیل و خودکارسازی فرآیندهای نظارتی تبدیل شود. با

---

[۴] $NFTs$

[۵] $batch\ transfer$

[۶] $Trust\ Anchor$

[۷] $Client-Side\ Validation$

ارائه طرح مفهومی و قابل اجرای مالیات هوشمند [۸]، این پروژه نشان داد که چگونه می‌توان از شفافیت و تغییرناپذیری زنجیره بلوکی برای موارد زیر بهره برد:

- **محاسبه خودکار و دقیق مالیات:** با کدنویسی قوانین مالیاتی در قرارداد هوشمند، محاسبات به صورت خودکار و بدون خطای انسانی در لحظه وقوع تراکنش انجام می‌شود.
- **پرداخت آنی و شفاف:** مبلغ مالیات می‌تواند در همان تراکنش انتقال مالکیت، به صورت مستقیم به کیف پول دیجیتال نهاد نظارتی واریز شود.
- **تسهیل حسابرسی:** تمام تراکنش‌های مالیاتی به صورت شفاف و غیرقابل انکار بر روی دفتر کل ثبت شده و فرآیند حسابرسی را برای نهادهای نظارتی به امری آنی و بسیار کارآمد تبدیل می‌کند.

این رویکرد، یک پل استراتژیک بین دنیای نوآورانه فناوری‌های غیرمتمرکز و دنیای ساختاریافته کسب‌وکار و قانون‌گذاری ایجاد کرده و مسیر پذیرش گسترده این فناوری توسط سازمان‌ها را هموارتر می‌سازد.

۵-۱-۳ دستاورد عملی: ارائه یک نمونه اولیه جامع و قابل ارزیابی

این پژوهش در سطح تئوری و مفهومی باقی نمانده و به یک دستاورد عملی و ملموس منتهی شده است: یک سامانه کامل و سرتاسری [۹] که تمام اجزای معماری پیشنهادی را پیاده‌سازی کرده است. این نمونه اولیه شامل موارد زیر است:

- **یک قرارداد هوشمند امن و بهینه:** قرارداد $SupplyChainERC1155.sol$ با رعایت بهترین شیوه‌های امنیتی و با استفاده از الگوهای بهینه‌سازی پیشرفته (مانند $Swap-and-Pop$) پیاده‌سازی شده است.
- **یک مجموعه آزمون جامع:** با استفاده از فریم‌ورک $Foundry$، مجموعه‌ای کامل از آزمون‌های واحد و یکپارچه‌سازی برای قرارداد هوشمند نوشته شده که صحت عملکرد و امنیت آن را در سطح بالایی تضمین می‌کند.
- **یک لایه کاربری مدرن و کاربرپسند:** با استفاده از پشته فناوری $React/Wagmi/Vite$، یک برنامه وب کامل با واسط‌های کاربری مجزا برای نقش‌های مختلف و با تمرکز بر انتزاع پیچیدگی‌های فنی، توسعه یافته است.

وجود این نمونه اولیه جامع، امکان ارزیابی عملی و اعتبارسنجی تمام ادعاهای مطرح شده در این پژوهش را فراهم آورده و آن را از یک کار صرفاً نظری متمایز می‌سازد. نتایج ارزیابی فصل چهارم، صحت عملکرد، امنیت پایه و کارایی این نمونه اولیه را به اثبات رسانده است.

---

[۸] $Smart\ Tax$

[۹] $End-to-End$

۵-۲ محدودیت‌های پژوهش و تحلیل انتقادی

بخشی از صداقت علمی، اذعان به محدودیت‌های یک پژوهش است. هیچ پروژه‌ای، به ویژه در حوزه‌های نوظهور، نمی‌تواند ادعای کمال داشته باشد. شناسایی و تحلیل انتقادی این محدودیت‌ها، نه تنها به درک بهتر محدوده اعتبار نتایج کمک می‌کند، بلکه خود زمینه‌ساز اصلی برای تعریف کارهای آینده است. محدودیت‌های این پژوهش را می‌توان در سه حوزه اصلی دسته‌بندی کرد.

۵-۲-۱ محدودیت‌های مربوط به محیط ارزیابی

اگرچه ارزیابی‌های فنی گسترده‌ای در فصل چهارم انجام شد، اما این ارزیابی‌ها در یک محیط کنترل‌شده و شبیه‌سازی شده صورت گرفته‌اند. این موضوع، محدودیت‌های زیر را به همراه دارد:

- **عدم وجود شرایط شبکه واقعی:** تمام آزمون‌ها بر روی یک گره محلی *Anvil* اجرا شده‌اند. در این محیط، تأخیر شبکه [۱۰] نزدیک به صفر است، هزینه گس ثابت و قابل پیش‌بینی است و هیچ‌گونه ازدحام [۱۱] یا رقابتی برای ورود تراکنش‌ها به بلوک وجود ندارد. عملکرد سیستم در یک شبکه عمومی واقعی مانند اتریوم یا یک شبکه لایه دو، به دلیل نوسانات شدید قیمت گس و زمان تأیید متغیر تراکنش‌ها، می‌تواند تفاوت‌های قابل توجهی داشته باشد.
- **فقدان محیط خصمانه واقعی:** اگرچه آزمون‌های امنیتی، سناریوهای حمله شناخته‌شده را شبیه‌سازی کرده‌اند، اما یک شبکه آزمایشی محلی، فاقد انگیزه اقتصادی واقعی برای هکرها و بازیگران مخرب است. استحکام واقعی یک سیستم غیرمتمرکز، تنها در مواجهه با تهدیدات یک شبکه عمومی زنده و با ارزش اقتصادی واقعی، به طور کامل سنجیده می‌شود.

۵-۲-۲ محدودیت‌های مربوط به جامعیت مدل کسب‌وکار و حاکمیت

نمونه اولیه پیاده‌سازی شده، برخی از فرآیندهای پیچیده دنیای واقعی را به منظور تمرکز بر روی هسته اصلی پژوهش، ساده‌سازی کرده است.

- **ساده‌سازی منطق مالیاتی:** ماژول محاسبه خودکار مالیات، به عنوان یک اثبات مفهوم طراحی شده و از یک مدل ساده (مثلاً نرخ ثابت) پیروی می‌کند. یک سیستم مالیاتی واقعی، نیازمند منطق‌های بسیار پیچیده‌تری است که شامل نرخ‌های متغیر، معافیت‌ها، قوانین بین‌المللی و... می‌شود. پیاده‌سازی کامل چنین سیستمی، خود یک پروژه تحقیقاتی مستقل است.
- **مدل حاکمیتی متمرکز:** در این نسخه، اعطای نقش توسط آدرس DEFAULT_ADMIN_ROLE به صورت متمرکز انجام می‌شود. این مدل برای شروع کار مناسب است، اما در یک اکوسیستم

[۱۰] *network latency*
[۱۱] *congestion*

غیرمتمرکز واقعی، این سؤال پیش می‌آید که «چه کسی ادمین را کنترل می‌کند؟». یک مدل حاکمیتی پایدار، نیازمند مکانیزم‌های غیرمتمرکزتری برای تصمیم‌گیری و مدیریت نقش‌ها است.

۵-۲-۳ محدودیت‌های مفهومی و چالش‌های حل‌نشده بنیادین

برخی از محدودیت‌ها، نه تنها به این پروژه، بلکه به کل حوزه زنجیره بلوکی در زنجیره تأمین مربوط می‌شوند و همچنان به عنوان چالش‌های باز پژوهشی مطرح هستند.

- **چالش حریم خصوصی داده‌ها:** شفافیت، شمشیر دولبه زنجیره بلوکی است. در حالی که این ویژگی برای حسابرسی و ردیابی عالی است، اما افشای عمومی تمام اطلاعات تراکنش‌ها (حتی به صورت نام مستعار) برای بسیاری از کسب‌وکارها که اطلاعاتی مانند حجم معاملات، قیمت‌گذاری و هویت شرکای تجاری‌شان برایشان حیاتی است، غیرقابل قبول است. این پروژه، راهکار جامعی برای این چالش ارائه نداده و این موضوع به عنوان مهم‌ترین محدودیت معماری آن باقی می‌ماند.
- **مشکل اوراکل و ورود داده‌های اولیه:** این سامانه، یکپارچگی و تغییرناپذیری داده‌ها را «پس از ثبت» بر روی زنجیره تضمین می‌کند. اما هیچ تضمینی در مورد صحت اولیه داده‌هایی که توسط تولیدکننده وارد سیستم می‌شود، ارائه نمی‌دهد. این مشکل که به مشکل اوراکل یا آشغال ورودی، آشغال خروجی [۱۲] معروف است، یک چالش بنیادین در تمام سیستم‌هایی است که تلاش می‌کنند دنیای فیزیکی را به دنیای دیجیتال متصل کنند. اگر یک تولیدکننده از ابتدا اطلاعات نادرستی را ثبت کند، زنجیره بلوکی آن اطلاعات نادرست را به صورت تغییرناپذیر برای همیشه ثبت خواهد کرد.

اذعان به این محدودیت‌ها، به هیچ وجه از ارزش دستاوردهای پروژه نمی‌کاهد، بلکه با مشخص کردن مرزهای دانش فعلی، نقشه راهی واضح برای گام‌های بعدی پژوهش فراهم می‌آورد.

۵-۳ پیشنهاد برای کارهای آینده: ترسیم نقشه راه توسعه

بر اساس دستاوردهای این پژوهش و با در نظر گرفتن محدودیت‌های شناسایی شده، می‌توان یک نقشه راه جامع و هیجان‌انگیز برای تحقیقات و توسعه‌های آتی ترسیم کرد. این نقشه راه در سه مسیر اصلی قابل پیگیری است: مسیر حرکت به سمت تولید، مسیر گسترش قابلیت‌های پروتکل، و مسیر توسعه مدل حاکمیتی و اقتصادی.

[۱۲] *Garbage In، Garbage Out*

۵-۳-۱ مسیر اول: حرکت از نمونه اولیه به محصول واقعی

برای تبدیل نمونه اولیه فعلی به یک سامانه قابل استقرار در محیط عملیاتی، چندین گام کلیدی باید برداشته شود:

- **استقرار و ارزیابی بر روی شبکه‌های لایه دو** [۱۳]: اولین و مهم‌ترین گام، استقرار و آزمون کامل سامانه بر روی یکی از شبکه‌های مقیاس‌پذیری لایه دو اتریوم مانند Arbitrum، Optimism یا zkEVM Polygon است. این کار به ما اجازه می‌دهد تا عملکرد سیستم را در یک محیط واقعی‌تر و با هزینه تراکنش بسیار پایین‌تر ارزیابی کنیم. این مرحله باید شامل تحلیل مقایسه‌ای هزینه گس در شبکه‌های مختلف برای یافتن بهینه‌ترین پلتفرم برای استقرار باشد.
- **انجام حسابرسی امنیتی حرفه‌ای** [۱۴]: قبل از اینکه هرگونه دارایی با ارزش واقعی بر روی قرارداد هوشمند مدیریت شود، انجام یک حسابرسی کامل توسط یک شرکت امنیتی معتبر و شخص ثالث، امری مطلقاً ضروری است. این فرآیند، به شناسایی آسیب‌پذیری‌های پنهانی که ممکن است در آزمون‌های داخلی نادیده گرفته شده باشند، کمک می‌کند.
- **توسعه و بهبود UX/UI بر اساس بازخورد کاربران:** اجرای آزمون‌های کاربردپذیری رسمی (که در فصل چهارم تشریح شد) با کاربران واقعی از صنعت، و استفاده از بازخوردهای آن‌ها برای بهبود مستمر رابط‌های کاربری، افزایش سادگی و کاهش موانع پذیرش.

۵-۳-۲ مسیر دوم: گسترش قابلیت‌های پروتکل و معماری

این مسیر، بر روی حل چالش‌های مفهومی باقی‌مانده و افزودن قابلیت‌های نوآورانه جدید به هسته پروتکل تمرکز دارد.

- **ادغام با اینترنت اشیاء** [۱۵] **برای خودکارسازی ورود داده:** برای مقابله با مشکل اوراکل، می‌توان سامانه را با سنسورهای IoT ادغام کرد. در این معماری، سنسورهای معتبر (مثلاً سنسورهای دما و رطوبت در یک کانتینر یخچال‌دار) می‌توانند به صورت خودکار و مستمر، داده‌های محیطی را امضا کرده و به یک قرارداد هوشمند اوراکل ارسال کنند. قرارداد اصلی زنجیره تأمین سپس می‌تواند این داده‌های تأییدشده را خوانده و به تاریخچه محصول الصاق نماید. این کار، ضمن خودکارسازی ورود داده، وابستگی به صداقت انسان را کاهش داده و اعتبار داده‌های اولیه را به شدت افزایش می‌دهد.
- **پیاده‌سازی مکانیزم‌های پیشرفته حریم خصوصی:** برای حل چالش حریم خصوصی، می‌توان از فناوری‌های پیشرفته‌ای مانند «اثبات با دانش صفر» [۱۶] بهره برد. با استفاده از تکنیک‌هایی مانند

---

[۱۳] $Layer\ 2$

[۱۴] $Professional\ Security\ Audit$

[۱۵] IoT

[۱۶] $Zero-Knowledge\ Proofs$

zk-SNARKs یا zk-STARKs، می‌توان یک لایه حریم خصوصی بر روی سیستم ایجاد کرد. در این مدل، شرکت‌ها می‌توانند صحت یک ادعا را بدون افشای داده‌های زیربنایی آن اثبات کنند. برای مثال، یک شرکت حمل‌ونقل می‌تواند به صورت رمزنگاری شده اثبات کند که «دمای محموله در تمام طول سفر بین ۰ تا ۵ درجه سانتی‌گراد بوده است»، بدون اینکه نیاز باشد مقادیر دقیق دما در هر لحظه را به صورت عمومی فاش کند. این حوزه، یکی از فعال‌ترین و مهم‌ترین زمینه‌های تحقیقاتی در حال حاضر است.

- **توسعه یک سیستم اوراکل غیرمتمرکز برای اعتبارسنجی اولیه:** می‌توان یک شبکه اوراکل غیرمتمرکز [۱۷] مانند *Chainlink* را برای تأیید داده‌های اولیه به کار گرفت. در این مدل، قبل از ثبت نهایی یک محصول، چندین گره مستقل و از نظر اقتصادی جریمه‌پذیر، صحت اطلاعات ارائه شده توسط تولیدکننده را (مثلاً با تطبیق با اسناد رسمی) تأیید می‌کنند. این اجماع اولیه، اعتبار داده‌های ورودی به سیستم را به طور قابل توجهی تقویت می‌کند.

۵-۳-۳ مسیر سوم: توسعه مدل حاکمیتی و اقتصادی

برای پایداری بلندمدت و پذیرش گسترده، سیستم باید دارای یک مدل حاکمیتی شفاف و یک مدل اقتصادی انگیزه‌بخش باشد.

- **ایجاد یک سازمان خودگردان غیرمتمرکز** *DAO*: برای حل مشکل حاکمیت متمرکز، می‌توان مدیریت پروتکل را به یک *DAO* [۱۸] واگذار کرد. در این مدل، ذی‌نفعان اصلی سیستم (مانند تولیدکنندگان، توزیع‌کنندگان و حتی نمایندگان مصرف‌کنندگان) می‌توانند با در اختیار داشتن «توکن‌های حاکمیتی» [۱۹]، در مورد تصمیمات کلیدی مانند به‌روزرسانی قرارداد هوشمند، تغییر نرخ‌های مالیاتی یا افزودن نقش‌های جدید، رأی‌گیری کرده و به صورت جمعی پروتکل را مدیریت نمایند.
- **طراحی مدل‌های پخش توکن** [۲۰]: می‌توان یک «توکن کاربردی» [۲۱] بومی برای این پلتفرم طراحی کرد. این توکن می‌تواند کاربردهای مختلفی داشته باشد:
  - **پرداخت هزینه‌ها:** استفاده از این توکن برای پرداخت هزینه‌های عملیاتی در پلتفرم (با تخفیف).
  - **سپرده‌گذاری** [۲۲]: شرکت‌کنندگان می‌توانند با سپرده‌گذاری توکن، به عنوان یک وثیقه برای

[۱۷] *DON - Decentralized Oracle Network*
[۱۸] *Decentralized Autonomous Organization*
[۱۹] *Governance Tokens*
[۲۰] *Tokenomics*
[۲۱] *Utility Token*
[۲۲] *Staking*

تضمین رفتار صادقانه خود عمل کنند. در صورت تقلب، بخشی از توکن‌های سپرده‌گذاری شده آن‌ها به عنوان جریمه کسر می‌شود.

- **پاداش‌دهی:** می‌توان به کاربرانی که داده‌های دقیق و با کیفیتی را به سیستم وارد می‌کنند، با این توکن پاداش داد.

یک مدل پخش توکن دقیق، می‌تواند انگیزه‌های اقتصادی تمام شرکت‌کنندگان را در جهت حفظ سلامت و رشد کل اکوسیستم همسو سازد.

در نهایت، این پژوهش با ارائه یک نمونه اولیه قوی و یک نقشه راه جامع، نشان می‌دهد که ما در آستانه یک تحول بزرگ در نحوه مدیریت زنجیره‌های تأمین قرار داریم. مسیر پیش رو پر از چالش‌های فنی، اقتصادی و اجتماعی است، اما دستاوردهای بالقوه آن ایجاد زنجیره‌های تأمینی که به صورت قابل اثباتی شفاف، کارآمد و عادلانه هستند ارزش پیمودن این مسیر را دارد. این پایان‌نامه، امیدوار است که به عنوان یک گام کوچک اما محکم در این راه طولانی، به شمار آید.

منابع و مراجع

[1] O'Reilly, Tim. What is web 2.0: Design patterns and business models for the next generation of software. O'Reilly Media, 2005.

[2] Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019.

[3] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system, 2008.

[4] Buterin, Vitalik. Ethereum white paper: A next-generation smart contract and decentralized application platform, 2014.

[5] Wood, Gavin. Ethereum: A secure decentralised generalised transaction ledger. Yellow paper, Ethereum Project, 2014.

[6] National Institute of Standards and Technology (NIST). Sha-3 standard: Permutation-based hash and extendable-output functions, 2015.

[7] Szabo, Nick. Smart contracts: Building blocks for digital markets. Extropy: The Journal of Transhumanist Thought, (18), 1996.

[8] Christidis, Konstantinos and Devetsikiotis, Michael. Blockchains and smart contracts for the internet of things. IEEE Access, 4:2292–2303, 2016.

[9] Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014.

[10] OECD/EUIPO. Trade in counterfeit and pirated goods: Mapping the economic impact. tech. rep., OECD Publishing, Paris, 2018.

[11] Kshetri, Nir. Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39:80–89, 2018.

[12] Kamath, Ramya, K, Jamsheedha, Shet, Sujaya, and R, Suneetha. Qr code based smart tracking and tracing system in supply chain management. International Journal of Applied Engineering Research, 13(10):7986–7990, 2018.

[13] Entriken, William, Shirley, Dieter, Evans, Jacob, and Sachs, Nastassia. Eip-721: Non-fungible token standard, 2018. Ethereum Improvement Proposals, No. 721.

[14] Vogelsteller, Fabian and Buterin, Vitalik. Eip-20: Token standard, 2015. Ethereum Improvement Proposals, No. 20.

[15] Radomski, Witek, Entriken, Andrew, Shirley, Phillippe, and Falticeanu, Nastassia. Eip-1155: Multi token standard, 2018. Ethereum Improvement Proposals, No. 1155.

[16] OpenZeppelin. Openzeppelin contracts: A library for secure smart contract development, 2024. Accessed August 2024.

[17] Benet, Juan. Ipfs - content addressed, versioned, p2p file system, 2014. arXiv preprint arXiv:1407.3561.

[18] The World Bank. Govtech: The new frontier in digital government transformation. tech. rep., The World Bank Group, 2020.

[19] Xu, Xiwei, Pautasso, Cesare, Dutra, Ines, Weber, Ingo, He, Qing, and Lu, Qing. A taxonomy of blockchain-based systems for architecture design. 2018 IEEE International Conference on Services Computing (SCC), pp. 243–250, 2018.

[20] Luu, Loi, Chu, Duc-Hiep, Olickel, Hrishi, Saxena, Prateek, and Hobor, Aquinas. Making smart contracts smarter. in Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 254–269, 2016.

[21] Zavolokina, Liudmila, Zani, Nicolò, Tessone, Claudio J, and Schweitzer, Frank. Ux challenges of blockchain-based decentralized applications: The case of 'uport'. in 2016 IEEE 18th International Conference on Business Informatics (CBI), vol. 1, pp. 375–381, 2016.

[22] De Filippi, Primavera and Wright, Aaron. The rise of blockchain technology: A legal analysis. Harvard Journal of Law & Technology, 29(2), 2016.

[23] Chopra, Sunil and Meindl, Peter. Supply Chain Management: Strategy, Planning, and Operation. Pearson, 7th ed. , 2019.

[24] Lee, Hau L, Padmanabhan, V, and Whang, Seungjin. The bullwhip effect in supply chains. Sloan Management Review, 38(3):93–102, 1997.

[25] Wamba, Samuel Fosso, Lefebvre, Louis A, Bendavid, Ygal, and Lefebvre, Élisabeth. Rfid-enabled supply chain management: a literature review. Production Planning & Control, 26(12):1031–1050, 2015.

[26] Gubbi, Jayavardhana, Buyya, Rajkumar, Marusic, Slaven, and Palaniswami, Marimuthu. Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):1645–1660, 2013.

[27] Androulaki, Elli, Barger, Artem, Borkowski, Vita, Cachin, Christian, Christidis, Konstantinos, De Caro, Angelo, Enyeart, David, Ferris, Christopher, Laventman, Gennady, Mane, Yacov, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. in Proceedings of the thirteenth EuroSys conference, pp. 1–15, 2018.

[28] Kamilaris, Andreas, Fonts, Angels, and Prenafeta-Boldú, Francesc X. The rise of blockchain technology in agriculture and food supply chains. Trends in Food Science & Technology, 91:640–652, 2019.

[29] Pinata. Pinata: The ipfs pinning service, 2024. Accessed August 2024.

[30] Wagmi. Wagmi: React hooks for ethereum, 2024. Accessed August 2024.

Abstract

Modern supply chains face significant challenges, including a lack of transparency, product counterfeiting, and difficult traceability. These issues erode consumer trust and inflict considerable economic losses on legitimate producers. This project addresses these challenges by designing and implementing a decentralized supply chain system using blockchain technology. The proposed solution establishes a distributed, transparent, and immutable ledger for complete end-to-end tracking of the product lifecycle, from manufacturing to the final consumer.

The system's core is a Solidity smart contract deployed on an Ethereum Virtual Machine (EVM) compatible network. It uniquely leverages the ERC-1155 token standard to efficiently manage both fungible and non-fungible assets within a single contract, reducing complexity and transaction costs. A key feature is the guarantee of metadata integrity, achieved by generating and storing a Keccak256 hash for each product on-chain. This allows any stakeholder to cryptographically verify the authenticity of product information at any stage.

The system architecture includes role-based access control for various participants (e.g., Manufacturer, Distributor, Customs) and an innovative function for the automated calculation of taxes during ownership transfers. The user-facing application is a modern web interface built with React, allowing consumers to scan a QR code to instantly view a product's complete, tamper-proof history. The contract's robustness and security are validated through a comprehensive test suite developed using the Foundry framework. By enhancing transparency, traceability, and authenticity, this project provides a practical solution to combat fraud and restore trust within the supply chain ecosystem.

Key Words:

Blockchain, Supply Chain Management, Smart Contract, ERC-1155, Solidity, Product Authenticity, Metadata Verification, Foundry, React

Amirkabir University of Technology
(Tehran Polytechnic)

Department of Computer Engineering

Bachelor Thesis

Design and Implementation of a Blockchain-Based Supply Chain with Metadata Validity Verification

By

Seyed Sepehr Mirnasrollahi parsa

Supervisor

Dr. Hamidreza Zarandi

October 2025