دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۴، جلد ۲۳، شماره ۱ (۴۵-۶۳)
https://monadi.isc.org.ir

صورت‌حساب الکترونیکی امن و حافظ حریم خصوصی مبتنی بر زنجیره قالبی

وحیده قانونی شیشوان[۱]، شعبان الهی[۲،*]، صادق دری نوگورانی[۳] و علی یزدیان ورجانی[۴]

[۱]دانشکده مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران
[۲]دانشکده علوم اداری و اقتصاد، دانشگاه ولی‌عصر (عج)، کرمان، ایران
[۳]گروه معماری سیستم‌های کامپیوتری، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران
[۴]گروه قدرت، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۲۴ اسفند ۱۴۰۲
تاریخ پذیرش: ۱۰ اردیبهشت ۱۴۰۴
انتشار آنلاین: ۱۰ خرداد ۱۴۰۴

کلمات کلیدی:
صورت‌حساب الکترونیکی
زنجیره قالبی
هایپرلجر فبریک

نوع مقاله: پژوهشی

چکیده

صدور صورت‌حساب الکترونیکی در سامانه مالیاتی، اگرچه موضوع جدیدی است، اما همچنان نتوانسته سامانه مالیاتی بهینه‌ای را به طور کامل فراهم کند. هدف مقاله حاضر، بهبود صورت‌حساب‌های الکترونیکی از جنبه‌های مختلف، از جمله امنیت و حریم خصوصی با به‌کارگیری فناوری زنجیرهٔ قالبی است. به این منظور، مدلی برای صورت‌حساب‌های الکترونیکی بر مبنای معماری زنجیرهٔ قالبی سازمانی هایپرلجر فبریک ارائه شده است. در این مدل، توزیع شدگی زنجیره قالبی و استفاده از الگوریتم اجماع نامتمرکز باعث شده است از لحاظ امنیت، دسترس‌پذیری و مقاومت نسبت به دستکاری بالایی وجود داشته باشد. همچنین با استفاده از لایه‌بندی مناسب، کانال‌های خصوصی و کنترل دسترسی متناسب توانسته محرمانگی و حریم خصوصی را حفظ کند و جلوی افشای اسرار تجاری را در عین شفافیت و خودکارسازی گرفته شود. ارزیابی مدل از نظر کیفی، امنیت، کارایی، مقایسه با کارهای مرتبط و نظرسنجی از خبرگان انجام گرفته و مناسب بودن آن نشان داده شده است.

© ۱۴۰۴ انجمن رمز ایران

۱ مقدمه

در یک سامانه تبادل مالی مجموعه‌ای از تراکنش‌ها بین خریداران و فروشندگان انجام می‌شود و این تراکنش‌ها معمولاً بر اساس استانداردهای مشخصی در دفاتر کل به‌صورت دستی یا الکترونیکی ثبت می‌شوند [۱]. صورت‌حساب الکترونیکی[۱] رویکرد روز در حوزه تبادل‌های مالی است که متناسب با گسترش مناسب دسترسی به فناوری‌های ارتباطی و موجب کاهش هزینه‌های مبادلاتی است. صورت‌حساب الکترونیکی رسید پرداخت و یا دریافت به شکل الکترونیکی است که در هنگام خرید یا فروش کالا، یا ارائه و پذیرش خدمات توسط سازمان امور مالیاتی صادر یا دریافت می‌شود. حسابرسان به‌عنوان شخص سوم به بررسی صورت‌های مالی می‌پردازند تا صحت اطلاعات مالی را تأیید کنند؛ اما تنها نمونه‌ای از حساب‌ها را بر مبنای مجموعه‌ای از آزمون‌ها کنترل می‌کنند. بنابراین صحت‌سنجی کامل صورت‌های مالی همچنان ضروری است.

در نظام اولیه دفترداری یک‌طرفه، هر تراکنش در یک حساب ثبت می‌شود. اما این روش با اشکال‌هایی مانند خطا و تقلب مواجه است و ردیابی و اصلاح را دشوار می‌کند. نظام دفترداری دوطرفه [۲] جایگزینی مؤثرتر است که از حدود ششصد سال پیش استفاده می‌شود و امکان کنترل دقیق‌تر حساب‌ها را فراهم می‌کند. در این نظام، هر تراکنش دو مدخل مستقل و معکوس دارد که توسط طرفین ثبت می‌شود. این روش خطاهای انسانی را کاهش می‌دهد اما همچنان تضمینی برای صحت

*نویسنده مسئول
آدرس‌های رایانامه: vahideh.ghanooni@modares.ac.ir (وحیده قانونی شیشوان)، elahi@vru.ac.ir (شعبان الهی)، dorri@modares.ac.ir (صادق دری نوگورانی)، yazdian@modares.ac.ir (علی یزدیان ورجانی)
© ۱۴۰۴ تمامی حقوق متعلق به انجمن رمز ایران است.

[1]E-invoice

صورت‌های مالی در صورت تقلب فراهم نمی‌کند.

در سال ۲۰۰۵ گریک [۳] نظام دفترداری سه‌طرفه را به‌منظور بهبود اعتماد به صورت‌های مالی پیشنهاد کرد. در نظام سه‌طرفه [۴] اجازه پردازش تراکنش‌ها به یک شخص سوم بی‌طرف داده می‌شود و این شخص سوم وظیفه تأیید درستی تراکنش‌های ثبت شده را برعهده دارد. در این نظام، فروشنده مسئول ارسال تراکنش و خریدار مسئول بررسی صحت تراکنش ارسال شده و امضای آن است. سازمان امور مالیاتی نیز نقش شخص سوم را در تأیید تراکنش‌ها برعهده گرفته است و همه چیز در پایگاه‌داده مرکزی در قالب صورت‌حساب الکترونیکی ثبت و پردازش می‌گردد.

صورت‌حساب مالیاتی [۵، ۶] مدرکی است که نشان می‌دهد خریدار کالا و خدمات را از فروشنده دریافت نموده است. فروشنده یک صورت‌حساب مالیاتی ما به‌ازای کالا و خدماتی که به خریدار فروخته است، ایجاد می‌کند. هر صورت‌حساب در پایگاه‌داده مرکزی ذخیره می‌شود که توسط سازمان امور مالیاتی مدیریت می‌شود. فرایند ثبت با یک «درخواست»، «پیشنهاد» یا «پیش‌نویس معامله» آغاز می‌شود و طرف مقابل آن را می‌پذیرد [۷]. نظام سه‌طرفه شامل فرایندی برای جمع‌آوری امضاها است؛ به‌طوری که فروشنده امضای خود را به پیش‌نویس تراکنش اضافه می‌کند و خریدار با امضای متقابل آن را می‌پذیرد. قبل از اینکه تراکنش در دفترکل مشترک ثبت شود، شخص سوم اعتبار امضاها را بررسی می‌کند و در صورت تأیید، تراکنش را امضا می‌کند. در نتیجه، یک رسید سه امضایی ایجاد می‌شود که نمی‌توان داده‌های آن را دستکاری یا از بین برد. با وجود بهبودی که صورت‌حساب الکترونیکی در روند صدور صورت‌حساب ایجاد نموده است اما همچنان مشکلاتی [۸–۱۱] وجود دارد که می‌توان آن‌ها را در چهار گروه تقسیم‌بندی نمود:

- جعل اطلاعات تراکنش و یا جعل یک تراکنش
- پیچیدگی و طولانی‌بودن فرایند صدور صورت‌حساب الکترونیکی
- ریسک بسیار بالای نگه‌داری داده در پایگاه‌داده مرکزی
- عدم کدگذاری دقیق کالا و خدمات

در عوض، یک سامانه خودکار [۶] که بتواند میلیون‌ها تراکنش را در زنجیره کسب‌وکار ردیابی کند موردنیاز است تا بر پیچیدگی و طولانی بودن فرایند صدور صورتحساب غلبه کند. این راه‌حل بایستی باعث شفافیت و امنیت نظام مالیاتی شود و فرایند اجرای مالیات را ساده کند. همچنین لازم است فناوری جدیدی به کار گرفته شود که تا جای ممکن نامتمرکز باشد و همچنین اطلاعات تراکنش به‌صورت غیرقابل‌تغییر و شفاف ثبت شوند تا بتواند جلوی جعل اطلاعات را بگیرد و جمع‌آوری مالیات را بهبود بخشد.

معرفی بیت‌کوین و فناوری زنجیره قالبی [1] [۲] نشان داد که نیاز به یک شخص سوم و مورداعتماد ضرورتاً وجود ندارد و می‌توان دفتر مشترک غیر قابل دستکاری و امنی را با استفاده از زنجیره قالبی ایجاد کرد. در مقاله حاضر به‌کارگیری فناوری زنجیره قالبی در صورت‌حساب الکترونیکی مدنظر قرار می‌گیرد. فناوری زنجیره قالبی از طریق طبیعت نامتمرکز، شفافیت، تغییرناپذیری، و خودشمول بودن، در کاربرد مدنظر ما نسبت به سیستم‌های متمرکز برتری دارد. سیستم‌های متمرکز به یک مرجع یا سرور مرکزی برای مدیریت و کنترل داده‌ها و فرآیندها وابسته‌اند. این بدین معناست که تمام تراکنش‌ها و جریان داده‌ها از یک نقطه عبور می‌کنند که این نقطه، نقطه‌ای واحد از شکست است. تغییرات یا به‌روزرسانی‌ها باید از طریق این مرجع مرکزی انجام شوند، که می‌تواند باعث ایجاد گلوگاه، کاهش سرعت تصمیم‌گیری، و احتمال مداخله شود. در عوض، زنجیره قالبی بر روی یک شبکه نامتمرکز از گره‌ها عمل می‌کند، که هرکدام یک نسخه از دفتر کل زنجیره قالبی را دارند. این ویژگی نقطه واحد شکست (یا مداخله) را از بین می‌برد و کنترل را در سراسر شبکه توزیع می‌کند. تغییرات و به‌روزرسانی‌ها از طریق سازوکار اجماع مدیریت می‌شود که در آن همه یا اکثریت گره‌های پردازشی باید توافق کنند، که این موضوع مقاومت و قابلیت اطمینان را افزایش می‌دهد.

۱.۱ زنجیره قالبی و کاربرد در مالیات

زنجیره قالبی نوع خاصی از دفترکل توزیع شده [۳، ۱۱–۱۳] است که در یک شبکه همتا به همتا مدیریت می‌شود. تراکنش‌ها در بسته‌هایی موسوم به «قالب» [2] با مقدار درهم [3] منحصربه‌فردی که از نظر منطقی به مقدار درهم قالب قبلی متصل است ذخیره می‌شوند و زنجیره‌ای خطی از قالب‌ها را تشکیل می‌دهند؛ بنابراین قالب‌ها متناظر با صفحات متوالی دفترکل هستند و تراکنش‌ها در این صفحات ذخیره می‌شوند. هر قالب تنها در صورتی به این زنجیره اضافه می‌شود که از طریق اجماع [4] در شبکه تأیید شود. در نهایت یک تاریخچه کامل از تراکنش‌ها در دفترکل نگهداری می‌شود.

ساختاری تحت عنوان قرارداد هوشمند [5] بر بستر زنجیره‌های قالبی نسل دوم نظیر اتریوم معرفی شده است که امکان برنامه‌نویسی و اجرای خودکار و بدون مداخله الگوریتم‌های مبتنی بر داده‌های روی زنجیره قالب را فراهم می‌کند. تراکنش‌های ویژه‌ای مربوط به اجرای رویه‌های قراردادهای هوشمند هستند که طی آن، قرارداد مربوطه می‌تواند بر اساس جزئیات تراکنش و داده‌های ذخیره شده روی زنجیره قالب تصمیم‌گیری کند و داده‌هایی را در قالب ذخیره کند. قراردادهای هوشمند به اطلاعاتی به جز ذخیره شده روی زنجیره قالب و فراهم شده در تراکنش دسترسی ندارند. اوراکل [6] یک خدمت [۱۴] است که دسترسی به اطلاعات خارجی را برای یک قرارداد هوشمند فراهم می‌کند.

فناوری زنجیره قالبی در سامانه‌های مالی بسیار پرکاربرد است و نیاز به توجه ویژه‌ای دارد. همچنین به‌کارگیری زنجیره قالبی در صورت‌حساب الکترونیکی [۱۵] از سال ۲۰۱۸ میلادی به عنوان یک رویکرد مهم در حوزه فناوری اطلاعات شناسایی شده اهمیت بالایی برای آن در سامانه‌های

[1] Blockchain

[2] Block [3] Hash [4] Consensus [5] Smart contract [6] Oracle

مالیاتی در نظر گرفته شده است. بااین‌حال، مسائل مربوط به این فناوری در زمینه مالیات هنوز به طور کامل مشخص نشده است [۹] و برای درک بهتر، نیاز به مطالعات بیشتر وجود دارد.

اگرچه فناوری زنجیره قالبی اشتراک اطلاعات را به‌صورت آنی و فراگیر ممکن می‌سازد، اما دولت و تمامی بخش‌های جامعه به حفاظت از داده‌های مالیاتی و حریم خصوصی توجه ویژه‌ای دارند. شفافیت [۱] به معنای آشکارسازی و ارتباط اطلاعات لازم در خصوص یک واقعیت است. در مقابل، محرمانگی داده [۱۶] به معنای آن است که داده‌ها در اختیار اشخاص، نهادها یا فرایندهای غیرمجاز قرار نگیرد. حفاظت از حریم خصوصی ذیل مفهوم کلی حفاظت از محرمانگی قرار می‌گیرد و تمرکز آن بر امکان کنترل و نظارت بر دسترسی به داده‌های شخصی و تجاری توسط مالک داده‌ها است.

محرمانگی و حریم خصوصی به‌عنوان یکی از جنبه‌های امنیت در سامانه مالیاتی و حفاظت از حریم خصوصی مؤدیان بسیار حائز اهمیت است؛ زیرا داده‌های مؤدیان از لحاظ ماهیتی بسیار محرمانه یا خصوصی است. باتوجه‌به همین امر، دسترسی به اطلاعات سامانه مالیاتی باید به حداقل موردنیاز محدود شود و هر موجودیت فقط دسترسی به داده‌هایی داشته باشد که لازم دارد. درعین‌حال از سایر جنبه‌های امنیتی لازم است صحت [۲] داده‌ها حفظ، و جلوی تغییر اطلاعات گرفته شود. نهایتاً دسترس‌پذیری [۳] سامانه نیز بالا باشد.

در یک سامانه اطلاعاتی که بر پایه یک سامانه توزیع شده باشد، موازنه‌ای بین دو هدف مخالف، یعنی شفافیت و محرمانه بودن همواره وجود دارد [۱۷]. هرچند سازمان امور مالیاتی می‌تواند با اتکا به فناوری زنجیره قالبی از افزایش شفافیت مالیاتی بهره‌مند شود؛ اما کسب‌وکارها نگران افشای اطلاعات تجاری حساس هستند [۱۸]. مثلاً هویت کاربران در زنجیره قالبی به طور کامل با استفاده از کلیدهای رمزنگاری محافظت نمی‌شود. این نگرانی تا حدی است که ستیواتی [۱۱] بیان می‌کند زنجیره قالبی تنها برای داده‌هایی از مؤدیان کاربرد دارد که نیازمند حریم خصوصی نباشند. فتز [۸] برای جلوگیری از انتشار اطلاعات حساس در زنجیره قالبی، رمزنگاری داده‌های ذخیره‌شده را پیشنهاد می‌کند. اما ازآنجاکه باید اطلاعات تراکنش‌ها تأیید شود، نمی‌توان کلیه اطلاعات تراکنش را رمزنگاری کرد؛ بنابراین تعادل بین شفافیت و حریم خصوصی ضروری است [۱۹].

۲.۱ روش‌شناسی پژوهش

در این مقاله از روش پژوهش علم طراحی [۴] استفاده می‌شود. منشأ این روش در پژوهش‌های سامانه‌های اطلاعاتی است که در آن یک محصول فنی برای حل یک مشکل ایجاد می‌شود و به طور دقیق ارزیابی می‌شود.

از دیدگاه هونر [۲۰، ۲۱]، علم طراحی در سامانه‌های اطلاعاتی یک رویکرد نظام‌مند و دقیق برای حل مسائل واقعی در حوزه سامانه‌های اطلاعاتی است. در این دیدگاه بر توسعه و ارزیابی مدل‌ها و مصنوع‌های نوآورانه تأکید می‌شود تا درنتیجه مسائل شناسایی شده با راهکارهای عملی حل شوند. با بررسی روش‌شناسی مقاله‌های چاپ شده در حوزه زنجیره قالبی، پژوهش علم طراحی به‌عنوان متداول‌ترین روش‌شناسی، با رویکرد مقاله حاضر مطابقت دارد.

در پژوهش علم طراحی برای پاسخگویی به چالش‌های پیچیده در حوزه سامانه‌های اطلاعاتی از روشی نظام‌مند و مبتنی بر تکرار استفاده می‌شود تا نهایتاً به یک دستاورد قابل‌قبول [۵] رسیده شود. گام‌های پیشنهادی پفرز [۲۲] یکی از پراستنادترین و منسجم‌ترین دستورالعمل‌های اجرای پژوهش در علم طراحی است و شامل مراحل زیر است: (۱) شناسایی مشکل؛ (۲) تعریف اهداف راه‌حل؛ (۳) طراحی و توسعه مدل یا مصنوع؛ (۴) نشان دادن ویژگی‌ها [۶]؛ (۵) ارزیابی دستاورد؛ و (۶) اطلاع‌رسانی [۷].

مقاله حاضر در حقیقت بخشی از اطلاع‌رسانی پژوهش و خروجی رساله دکتری است که در این زمینه انجام شده است. سعی شده است مقاله نیز بر اساس گام‌های فوق سازماندهی شود.

۳.۱ مقاله حاضر

هدف مقاله حاضر، ارائه یک مدل برای به‌کارگیری فناوری زنجیره قالبی در پیاده‌سازی صورت‌حساب‌های الکترونیکی است تا باتوجه‌به ویژگی‌های تمرکززدایی، مقاومت در برابر دستکاری، شفافیت و خودکارسازی زنجیره قالبی [۶، ۹، ۱۱، ۱۵، ۲۳-۲۵] بر مشکلات شناسائی شده فائق آید و صورت‌حساب‌های الکترونیکی را از جنبه‌های مختلف خصوصاً امنیت (دسترس‌پذیری و جلوگیری از دستکاری)، و حریم خصوصی (محدودیت دسترسی تا حداقل ممکن، جلوگیری از افشای اسرار تجاری در عین شفافیت) بهبود دهد. نوآوری‌های مقاله حاضر به شرح ذیل است:

- بهره‌گیری از زنجیره قالبی سازمانی مبتنی بر سکوی هایپرلجر فبریک در صورت‌حساب الکترونیکی
- حفظ محرمانگی و حریم خصوصی اطلاعات تراکنش از طریق لایه‌بندی مناسب در معماری پیشنهادی
- ارائه معماری صورت‌حساب الکترونیکی متناسب با سامانه مالیاتی کشور مبتنی بر هایپرلجر فبریک [۸].

در خصوص مورد دوم فوق‌الذکر، لازم به توضیح است که زنجیره قالبی مورد استفاده در این مقاله (هایپرلجرفبریک) از طریق ساختار کانال و ویژگی مجموعه‌داده خصوصی، محرمانگی و حریم خصوصی مورد نظر ما را فراهم می‌کند. با استفاده از کانال‌ها، هر گره پردازشی به مجموعه محدودی از تراکنش‌ها دسترسی دارد که باعث ایزوله شدن داده‌ها می‌شود. همچنین مجموعه‌داده خصوصی این امکان را فراهم می‌کند که داده‌ها در یک پایگاه‌داده خصوصی که فقط بر روی گره‌های پردازشی مجاز است، ذخیره شوند و دسترسی به این داده‌ها محدود به یک یا چند سازمان عضو

[1] Transparency [2] Integrity [3] Availability [4] Design Science Research

[5] Satisficing [6] Representation [7] Communication [8] Hyperledger Fabric

کانال است. نهایتاً در لایه حاکمیتی زنجیره قالب برای کنترل دسترسی از گواهی‌های الکترونیکی و زیرساخت کلید عمومی استفاده می‌شود. در بخش‌های بعدی مقاله در این خصوص توضیحات بیشتری داده می‌شود.

بر اساس مدل پفرز، در بخش ۱ مقاله به شناسائی مشکل پرداخته شد و فناوری زنجیره قالبی به‌عنوان یک راه‌حل بالقوه برای حل این چالش‌ها و بهینه‌سازی فرایندهای صورت‌حساب الکترونیکی معرفی شد. به‌منظور ارائه مدل ابتدا در بخش ۲ پیشینه پژوهش بررسی می‌شود و بر اساس آن در بخش ۳ مدل راهکار پیشنهادی ارائه می‌گردد. سپس در بخش ۴ ویژگی‌های راهکار پیشنهادی بررسی و ارزیابی می‌شود. نهایتاً در بخش ۵ جمع‌بندی و پیشنهاد برای کارهای آتی انجام می‌شود.

۲ پیشینه پژوهش

مرور ادبیات نظام‌مند[۲۶] با پاسخ به سه سوال پژوهشی انجام گرفت که فتز، هیک و همکاران [۹] معماری مجوزداری[1] را در سکوی اتریوم پیشنهاد می‌کنند که سه بخش شامل دو قرارداد هوشمند و یک واسط برنامه‌نویسی کاربردی دارد. یک قرارداد نحوه مشارکت بنگاه‌ها را مشخص می‌کند و فقط سازمان امور مالیاتی می‌تواند آن را فراخوانی کند. قرارداد دوم نیز معتبر بودن تراکنش را بررسی می‌کند. هویت خریدار و فروشنده در یک تراکنش باید معتبر باشد. اگر هویت یکی از طرفین نامعتبر باشد و با قرارداد اول تطابق نداشته باشد تراکنش دور ریخته می‌شود. هنگامی‌که اجماع رخ می‌دهد قرارداد یک شناسه منحصر به آن تراکنش اختصاص می‌دهد. واسط برنامه‌نویسی کاربردی سفارشی سومین بخش این معماری است که زنجیره قالبی و فرایندهای کسب‌وکاری را یکپارچه می‌کند.

لیو [۲۷] معماری مبتنی بر زنجیره قالبی را برای فاکتورهای الکترونیکی شامل سه سطح لایه اصلی، خدمات، و برنامه ارائه می‌کند. در این معماری سازمان امور مالیاتی مجری سازوکار قانون‌گذاری در سامانه زنجیره قالبی است و استانداردهای عملیاتی و شرایط قرارداد را تعیین می‌کند. هر گره پردازشی می‌بایست طبق قوانین از پیش تعیین شده عمل کند. در این زنجیره شخص سوم توسط امور مالیاتی تعیین می‌شود که این شخص مسئولیت صحت‌سنجی و تأیید اعتبار فاکتورها را دارد. همچنین از معماری چند زنجیره بهره گرفته شده است تا مشارکت‌کنندگان نامرتبط بتوانند روی زنجیره قالبی‌های موازی چندگانه تراکنش داشته باشند.

انجیون [۲۸] مدل ۱۲ مرحله‌ای را بر مبنای قرارداد هوشمند در سکوی اتریوم ارائه کرده است. در این مدل، فاکتورهای فروش رمزگذاری می‌شود و پس از تأیید توسط خریدار و فروشنده، در یک شبکه ذخیره‌سازی نامتمرکز ثبت می‌شود. سپس به طور خودکار، مالیات بر ارزش‌افزوده محاسبه می‌شود. الخودره و همکاران [۲۳] سامانه مالیات بر ارزش‌افزوده مبتنی بر زنجیره قالبی را با معماری خصوصی و مجوزدار در سکوی فبریک در کشور عربستان سعودی پیشنهاد می‌کنند.

ویجایا، لیو و همکاران [۶] توکنی برای شناسائی مؤدیان، انتقال اعتبار مالیاتی بین آن‌ها و ایجاد فاکتورهای مالیاتی از طریق فناوری زنجیره قالبی معرفی کرده‌اند. اینسورس [۲۹–۳۱] یک واحد پول دیجیتالی را برای پرداخت مالیات بر ارزش‌افزوده ارائه می‌کند. این رمزارز دارای نرخ ثابت است و تراکنش آن توسط مشارکت‌کنندگان دولتی تأیید می‌شود.

ستیواتی [۳۲] پیامدهای احتمالی را برای اجرای زنجیره قالبی در سامانه مالیات بر ارزش‌افزوده اندونزی تحلیل می‌کند. وی معتقد است که اجرای زنجیره قالبی به دلیل خودکارسازی سامانه، عملکرد سامانه صورت‌حساب الکترونیکی را بهبود می‌بخشد. همچنین اگر زنجیره قالبی در یک سامانه مناسب اعمال شود، منافع قابل‌توجهی را فراهم می‌کند؛ بنابراین، ضروری است که قبل از اجرای یک سامانه بر پایه فناوری زنجیره قالبی، عوامل راهبردی در سه بعد سازمانی، محیطی و فناوری مورد تجزیه‌وتحلیل قرار گیرند. عوامل راهبردی سازمانی شامل آمادگی سازمان، حمایت از اطرافیان با مقام بالاتر، آمادگی فناوری، نوآوری، حاکمیت و فرایند پیکربندی داخلی است. عوامل راهبردی محیطی شامل حمایت دولت و شریکان است و عوامل راهبردی فناوری شامل امنیت داده، برنامه‌نویسی قرارداد هوشمند، تعیین معماری، مجوزها و زیرساخت‌های مشترک است.

سوگرد [۳۳] از طریق مصاحبه با چهارده کارشناس از حوزه‌های فناوری اطلاعات و مالی، الزامات طراحی و پیاده‌سازی سامانه مالیات بر ارزش‌افزوده مبتنی بر زنجیره قالبی را برمی‌شمارد. بر اساس بررسی کیم [۱۰]، زنجیره قالبی در بخش‌های عمومی که نیاز به افزونگی داده، شفافیت اطلاعات، تغییرناپذیری و سازوکار اجماع دارد، بسیار مناسب است. زیرا سامانه مالیات حداقل به سه عامل از چهار عامل نیازمند است.

۳ راهکار پیشنهادی

در این بخش راهکار پیشنهادی جهت صورت‌حساب الکترونیکی امن و حافظ حریم خصوصی مبتنی بر زنجیره قالبی ارائه می‌گردد. ابتدا نحوه انتخاب نوع زنجیره قالبی تشریح و سپس مدل پیشنهادی ارائه می‌شود و لایه‌های آن تشریح می‌شود.

۱.۳ زنجیره قالبی انتخابی

امنیت در سامانه مالیاتی و حریم خصوصی مؤدیان بسیار حائز اهمیت است. فتز [۸] مدل خود را بر مبنای زنجیره قالبی عمومی ارائه کرده است تا سایر مشارکت‌کنندگان نیز بتوانند در یک محیط کاملاً نامتمرکز اطلاعات را تبادل و اعتبارسنجی کنند.

زنجیره قالبی ائتلافی [۱۰، ۲۵] نوعی زنجیره قالبی مجوزدار است که تا حدی نامتمرکز است و با مشارکت چند نهاد یا سازمان مجزا از هم شکل می‌گیرد. در این نوع زنجیره قالبی، به‌جای این که همه اعضا تأییدکننده باشند، تنها تعدادی از آن‌ها قالب‌ها را تأیید می‌کنند. زنجیره قالبی ائتلافی برای مشارکت‌کنندگانی که به یکدیگر اعتماد کامل ندارند

[1] Permissioned

اما می‌خواهند با هم کار کنند و همچنین می‌خواهند برخی از اطلاعات را خصوصی نگه دارند، مناسب است. زنجیره قالبی ائتلافی عدم تقارن اطلاعات بین مقامات مالیاتی، مؤدیان و سازمان‌های مالی وابسته را حل می‌کند و شفافیت و کارایی را بهبود می‌بخشد.

ازآنجاکه داده‌های مؤدیان بسیار محرمانه و خصوصی هستند و دسترسی به آن‌ها باید به‌شدت محدود شود، بسیاری از پژوهش‌های پیشین، زنجیره قالبی خصوصی مجوزدار [۸، ۹، ۱۱، ۲۳، ۳۳] را برای سامانه مالیاتی پیشنهاد کرده‌اند. مدل پیشنهادی مبتنی بر یک زنجیره قالبی سازمانی[1] است. این نوع زنجیره قالبی حالت خاصی از زنجیره قالبی خصوصی و مجوزدار است که در آن مشاهده اطلاعات محدود به گره‌های پردازشی است و تنها کاربرانی که احراز هویت شده باشند مجوز دسترسی و فعالیت را بر اساس سطح دسترسی دارند. برای پاسخ به سؤال اینکه آیا واقعاً به یک زنجیره قالبی سازمانی نیاز است، می‌بایست به سؤالات جدول ۱ پاسخ داده شود.

اگر پاسخ هر یک از پرسش‌های جدول ۱ بله باشد، استفاده از یک راه‌حل زنجیره قالبی سازمانی می‌تواند گزینه خوبی باشد. باتوجه‌به پاسخ‌های جدول ۱، زنجیره قالبی سازمانی مدل مناسبی برای پژوهش است.

چندین راه‌حل زنجیره قالبی سازمانی در چند سال گذشته توسعه یافته و در دسترس قرار گرفته است که مهم‌ترین آن‌ها عبارت‌اند از [۳۴]:

(۱) **کوروم**[2]: یک سکوی زنجیره قالبی سازمانی منبع‌باز و یک شاخه سبک از اتریوم است. ویژگی‌های تجاری بسیار عالی در کوروم ارائه حفظ حریم خصوصی در سطح سازمانی، عملکرد و کنترل دسترسی است.

(۲) **فبریک:** یکی از پروژه‌های هایپرلجر است. یک دفتر توزیع شده در سطح سازمان است که اجازه می‌دهد راه‌حل‌های زنجیره قالبی با یک معماری پیمانه‌ای توسعه یابند. فبریک معماری مجوزدار دارد، از قراردادهای هوشمند پشتیبانی می‌کند و سازوکار اجماع در آن قابل‌تعویض است.

(۳) **کوردا آرتری**[3]: یک سکوی زنجیره قالبی منبع‌باز است که اجازه می‌دهد شبکه‌های زنجیره قالبی قابل‌تعاملی ساخته شوند که حفظ حریم خصوصی اعضا در آن مهم است. فناوری قرارداد هوشمند به کسب‌وکارها اجازه می‌دهد تا با ویژگی‌های امنیتی پیشرو در صنعت به طور مستقیم معامله کنند.

با درنظرگرفتن عملکرد هر یک از پروژه‌ها، می‌توان فبریک را از نظر معیارهای تعامل‌پذیری با شبکه‌ها و زنجیره‌های مختلف، پشتیبانی از الگوریتم‌های اجماع، پیشرفت عرضه در صنایع مختلف، آسانی پیاده‌سازی، قابلیت سفارشی‌سازی و معیارهای غیرفنی مانند تجربه کاری، اعتبار [۳۵]، دردسترس‌بودن توسعه‌دهندگان، سطح پشتیبانی، تاریخچه و شهرت در صنعت، پشتیبانی از رابط برنامه‌نویسی و به‌روزرسانی یا انتشار نسخه‌ها [۳۶]، پذیرش، حریم خصوصی و محرمانگی، و مقیاس‌پذیری [۳۷] نسبت به سکوهای دیگر ارجحیت داد؛ بنابراین، فبریک به‌عنوان سکوی زنجیره قالبی سازمانی و نسخه Fabric v x.2.5 که پشتیبانی بلندمدت (LTS[4]) دارد، انتخاب گردید.

[1] Enterprise Blockchain [2] Quorum [3] Corda R3

۲.۳ مدل پیشنهادی

مدل پیشنهادی در شکل ۱ نمایش داده شده است. در این مدل، خریدار و فروشنده به‌عنوان مؤدی، اتاق اصناف، و جامعه حسابداران رسمی در خارج از شبکه زنجیره قالبی قرار می‌گیرند و سازمان امور مالیاتی و بانک‌ها به‌عنوان سازمان‌های عضو عمل می‌کنند. تعدادی قرارداد هوشمند و منبع داده مربوط به آن‌ها نیز جهت خودکارسازی عملیات پیش‌بینی شده است که در توضیحات لایه مربوطه تشریح می‌شوند. همچنین به‌منظور ارتباط داده‌ای بین زنجیره قالبی، سازمان امور مالیاتی و بانک‌ها، دو گره پردازشی[5] تحت عنوان اوراکل به منابع داده‌ای متصل هستند و آن‌ها را تغذیه می‌کنند.

شروع فرایند ثبت صورت‌حساب با برنامه کاربردی مشتری است. اتصال این برنامه با زنجیره قالبی از طریق گره پردازشی هدف است که به‌عنوان دروازه برای انتخاب گره‌های پردازشی تأییدکننده عمل می‌کند و پس از امضای تراکنش، پیشنهاد تراکنش را به سرویس سفارش دهی ارجاع می‌دهد. قراردادهای هوشمند توسط گره‌های پردازشی تأییدکننده اجرا می‌شوند.

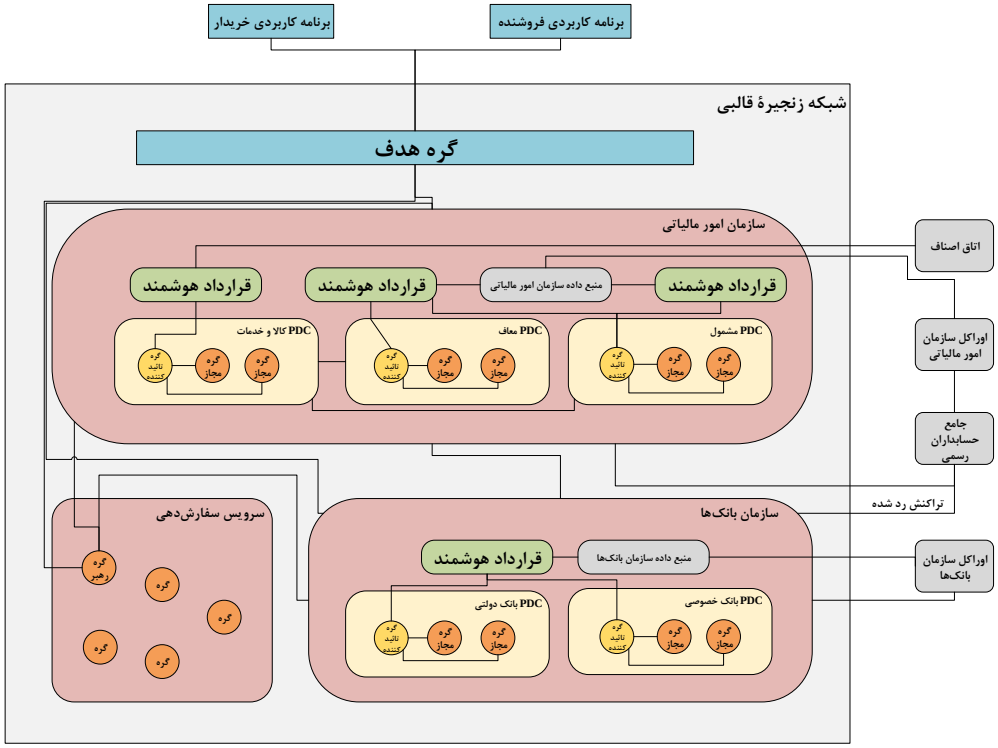
لازم به توضیح است که سازمان‌ها به طور مستقیم بر روی زنجیره قالبی پیاده‌سازی نمی‌شوند. بلکه، سازمان‌ها از طریق گره‌ها با شبکه نامتمرکز تعامل دارند. این امر اجازه می‌دهد که داده‌ها به صورت امن اعتبارسنجی شوند و امکان تعامل با آنها وجود داشته باشند، بدون اینکه نیاز باشد کل زیرساخت سازمان بر روی زنجیره قرار گیرد. در یک سیستم زنجیرة قالبی، «گره» به نقطه‌ای اشاره دارد که با زنجیره قالبی ارتباط برقرار می‌کند، داده‌ها را ذخیره، اعتبارسنجی و به شبکه انتقال می‌دهد. این گره‌ها نماینده کامل ساختار سازمان نیستند. سازمان‌ها از طریق این گره‌ها با زنجیره قالبی برای انجام وظایف خاص مانند اعتبارسنجی تراکنش‌ها یا اجرای قراردادهای هوشمند تعامل دارند.

به طور کلی، گره‌های زنجیره قالبی وظیفه اعتبارسنجی تراکنش‌ها و حفظ دفترکل توزیع‌شده را بر عهده دارند، بدون اینکه ساختار داخلی کامل یک سازمان بر روی زنجیره قالبی وجود داشته باشد. این بدین معناست که در حالی که یک سازمان ممکن است از زنجیره قالبی برای فرآیندهای خاص (مانند مدیریت زنجیره تأمین یا تراکنش‌های مالی امن) استفاده کند، خود سازمان در خارج از زنجیره فعالیت می‌کند و از شبکه زنجیره قالبی به عنوان ابزاری برای انجام خدمات استفاده می‌کند. بنابراین، نشان دادن سازمان به عنوان یک «گره» در زنجیره قالبی یک مدل ساده برای پیاده‌سازی وظایف خاص است، در حالی که ساختار و عملیات کلی سازمان در خارج از زنجیره حفظ می‌شود.

[4] Long Term Support [5] Node

جدول ۱. معیارهای انتخاب زنجیره قالبی سازمانی

پرسش	پاسخ
آیا نیاز به داده‌های مشترک بین شرکت‌کنندگان دارد؟	برای ایجاد شفافیت، لازم است داده‌های سازمان امور مالیاتی بین سازمان‌های مختلف به اشتراک گذاشته شود.
آیا می‌توان به شرکت‌کنندگان از سایر سازمان‌ها اعتماد کرد یا آیا دارای منافع متضاد هستند؟	امکان سو استفاده از داده‌های محرمانه وجود دارد.
نیاز به حسابرسی سخت‌گیرانه و دقیق وجود دارد؟	باتوجه‌به احتمال وقوع تقلب و فرار مالیاتی، لازم است حسابرسی صورت بگیرد.
آیا لازم است محرمانگی معاملات حفظ شود؟	بله
آیا لازم است هویت شرکت‌کنندگان ناشناس باقی بماند؟	اطلاعات مؤدیان و تراکنش‌های آن‌ها باید ناشناس باقی بمانند.
آیا نیاز به به‌روزرسانی‌های کنترل شده، اما شفاف، وجود دارد؟	بله – امکان دستکاری اطلاعات حسابداری دوطرفه یکی از علل فرار مالیاتی است.
آیا نیاز به یک مقام مورداعتماد واحد وجود دارد؟	خیر – سازمان حسابرسی، بانک‌ها، اتحادیه، همراه با سازمان امور مالیاتی می‌توانند ائتلاف تشکیل دهند.



شکل ۱. مدل پیشنهادی سیستم صورت‌حساب الکترونیکی مبتنی بر زنجیره قالبی سازمانی (گره پردازشی به اختصار گره ذکر شده است.)

۳.۳ لایه‌های مدل

بر مبنای لایه‌های معرفی شده توسط بشیر [۳۴]، لایه‌های معماری سازمانی پیشنهادی برای صورت‌حساب الکترونیکی مبتنی بر فبریک شامل شش‌لایه شبکه، پروتکل، کنترل داده، حاکمیتی، یکپارچه‌سازی و برنامه است که در شکل ۲ در کنار هم‌نشان داده شده‌اند. در سمت راست نمودار امنیت، مقیاس‌پذیری، عملکرد و نظارت نمایش داده شده‌اند. این امر به این دلیل است که هر لایه در زنجیره قالبی به امنیت، مقیاس‌پذیری و عملکرد نیاز دارد. نظارت نیز نقش مهمی در هر راه‌حل سازمانی دارد.

در لایه شبکه، مشارکت‌کنندگان سامانه صورت‌حساب الکترونیکی اعم از سازمان امور مالیاتی، بانک‌ها، مودیان، اتاق اصناف و جامع حسابداران رسمی قرار می‌گیرند. لایه پروتکل شامل تراکنش فروش، دفترکل و وضعیت سراسری است. لایه کنترل داده شامل مجموعه‌داده خصوصی کالاها و خدمات، معاف، مشمول، و بانک‌های دولتی و خصوصی است. در لایه حاکمیتی، عواملی مانند مرکز صدور گواهی الکترونیکی، کلیدهای خصوصی و عمومی، گواهی‌های الکترونیکی، فراهم‌کننده خدمات عضویت، و کنترل دسترسی تعریف می‌شوند. در لایه یکپارچه‌سازی، gRPC، رویداد و اوراکل قرار می‌گیرند. لایه برنامه شامل برنامه‌های کاربردی مشتری، کیت توسعه نرم‌افزار، و قراردادهای هوشمند که می‌بایست منطق با قانون مالیات باشند، است. در ادامه هر

لایه به‌تفصیل توضیح داده می‌شود.

۱.۳.۳ لایه شبکه

زنجیره قالبی از تعدادی گره پردازشی تشکیل شده است که هر کدام از آن‌ها نسخه‌ای از دفتر را نگه‌داری می‌کنند. هر شبکه زنجیره قالبی سازمانی شامل سازمان، خدمت سفارش دهی و گره‌های پردازشی آن‌ها و کاربران است. اعضای اصلی شناسائی شده این لایه در شکل ۴ نشان داده شده‌اند و عبارت‌اند از: مؤدیان، سازمان امور مالیاتی، بانک‌ها، اتاق اصناف و جامع حسابداران رسمی. مؤدی آغازگر تراکنش‌های سامانه است. سازمان امور مالیاتی و بانک‌ها به‌عنوان مجریان سامانه مالیات و اتاق اصناف به‌عنوان مرکز نظارت بر کالا و خدمات عرضه شده بر مبنای مجوز و جامع حسابداران رسمی، حسابرسان سامانه هستند.

بنابراین، اعضای زنجیره قالبی، در داخل شبکه سازمان امور مالیاتی و سازمان بانک‌ها هستند که یک ائتلاف را تشکیل می‌دهند و در خارج از شبکه مؤدیان (خریدار و فروشنده) و سازمان جامعه حسابداران رسمی و اتاق اصناف قرار می‌گیرند. در داخل شبکه، سازمان امور مالیاتی شامل نه گره پردازشی و سازمان بانک‌ها شامل شش گره پردازشی می‌باشند. خدمت سفارش دهی شامل سه گره پردازشی از سازمان امور مالیاتی و دو گره پردازشی از بانک است که در این صورت، حداکثر دو گره پردازشی می‌تواند بدون ازکارافتادن سامانه از کار بیفتد. کاربران هم مؤدیان هستند.

۲.۳.۳ لایه پروتکل

لایه پروتکل یا لایهٔ زنجیره قالبی، جایی است که مدیریت تراکنش، اجماع و ذخیره‌سازی در آن انجام می‌گیرد. در هر تراکنش فروش، فروشنده تراکنشی را با ذکر مشخصات شناسه کالا و خدماتی که مجاز به معامله است با تکمیل مشخصات حساب بانکی و جزئیات پرداخت ایجاد می‌کند. جزئیات تراکنش به شرح شکل ۳ است.

در زنجیره قالبی، سازوکار اجماع، وظیفه ایجاد وحدت بین گره‌های پردازشی را بدون شخص سوم انجام می‌دهد. زمانی که شبکه تحت‌نظر یک شرکت یا یک سازمان قابل‌اعتماد باشد، اجماع در برابر خطاهای غیرقابل‌پیش‌بینی (بیزانسی) به طور کامل مقاوم است. در چنین شرایطی، یک پروتکل اجماع مقاوم در برابر خطاهای فروپاشی کافی است.

چون سازمان امور مالیاتی و سازمان بانک‌ها که شبکه را تشکیل می‌دهند قابل‌اعتماد می‌باشند، الگوریتم Raft که یکی از معروف‌ترین الگوریتم‌های اجماع در برابر خطای فروپاشی است، در مدل انتخاب می‌گردد.

اجزای داخلی [۳۸، ۳۹] در دفتر هر گره پردازشی شامل دفتر و قالب‌ها و وضعیت سراسری است. وضعیت سراسری نماینده وضعیت فعلی زنجیره قالبی در هر لحظه زمانی است. برای مثال نشان می‌دهد شخص الف، ۱۰۰۰ عدد از کالای ب را دارد. برای رعایت حریم خصوصی، مدل طوری طراحی شده است که از خواندن غیرمجاز جلوگیری کند و از آنجا که انتظار می‌رود عملکرد مدل با افزایش حجم داده‌ها در شبکه کاهش نیابد و کند نگردد، پایگاه داده LevelDB به‌جای پایگاه داده CouchDB برای وضعیت سراسری انتخاب گردیده است. تفاوت اصلی این دو پایگاه داده، در شکل اصلی نگهداری داده در آن‌هاست. به طور خاص، CouchDB یک پایگاه داده مستند محور[1] است، در حالی که LevelDB یک پایگاه داده کلیدی- مقداری[2] است.

۳.۳.۳ لایه کنترل داده

پروتکل فبریک از طریق ساختار کانال و ویژگی مجموعه‌داده خصوصی، محرمانگی را فراهم می‌کند.

کانال: در کانال‌ها [۳۸] اعضای شبکه فبریک یک زیرشبکه را ایجاد می‌کنند که هر گره پردازشی به یک مجموعه خاص از تراکنش‌ها دسترسی دارد که باعث ایزوله شدن داده‌ها می‌شود.

کانال سازمان امور مالیاتی و بانک‌ها (TaxationBanks) شامل پیکربندی زیر است:

سازمان‌ها: سازمان‌های امور مالیاتی (Taxation) و بانک‌ها (Banks) اعضای کانال هستند که توسط MSP اختصاصی و MSP کانال که در لایه حاکمیتی توضیح داده می‌شود، شناخته می‌شوند.

خدمت سفارش دهی[3]: شامل پنج گره پردازشی می‌باشند که سازوکار اجماع در آن Raft است.

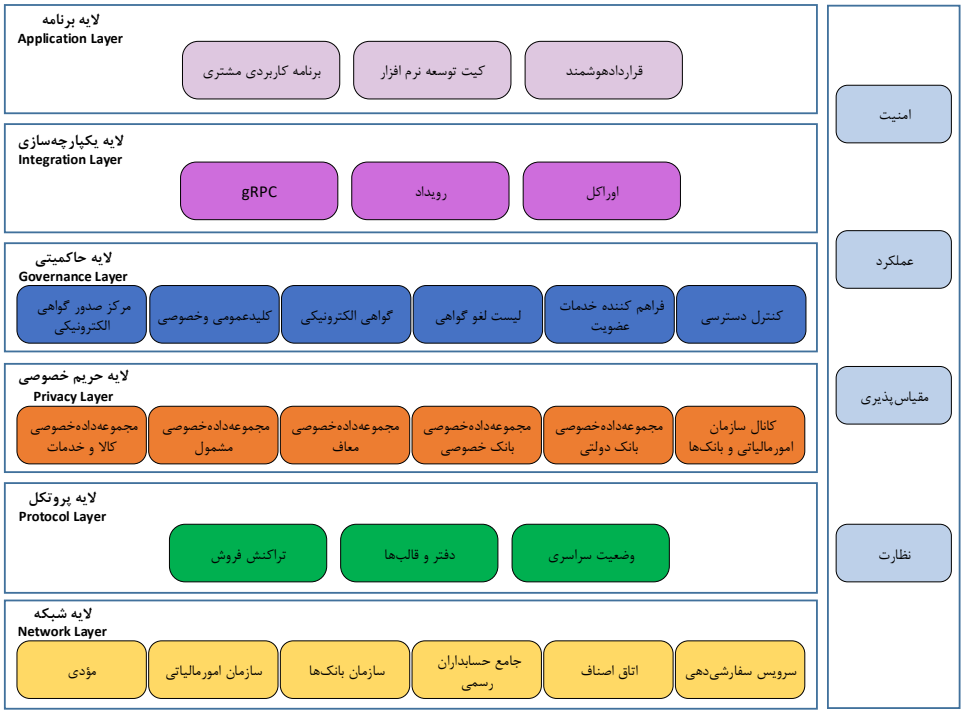
پروفایل: یک ائتلاف با نام TaxationBanksConsortium ایجاد می‌شود که دو سازمان Taxation و Banks را شامل می‌شود. شکل ۴ شبکه فبریک را با دو سازمان امور مالیاتی و بانک که به کانال می‌پیوندند، نمایش می‌دهد.

مجموعه‌داده خصوصی (PDC): داده‌های خصوصی [۳۸] در یک پایگاه‌داده خصوصی بر روی هر گره پردازشی مجاز ذخیره می‌شوند و دسترسی به این داده‌ها محدود به یک یا چند سازمان در یک کانال است که از طریق تعریف مجموعه‌داده خصوصی انجام می‌شود. مجموعه‌داده خصوصی در سازمان امور مالیاتی شامل «کالا و خدمات»، «معاف» و «مشمول» می‌گردد.

مجموعه‌داده خصوصی در سازمان بانک‌ها شامل «خصوصی» و «دولتی» است. برای نمونه از میان مجموعه‌های داده خصوصی، مجموعه‌داده خصوصی «معاف» با ویژگی‌های زیر انتخاب شده است:

- نام: «معاف»
- خط‌مشی: گره پردازشی تأییدکننده پیشنهاد «تراکنش فروش» را برای دو گره پردازشی مجاز در همان PDC ارسال می‌کند و سپس گره پردازشی تأییدکننده پیشنهاد «تراکنش فروش» را امضا می‌کند.
- تعداد حداقل گره پردازشی موردنیاز: حداقل یک گره پردازشی مجاز باید پیشنهاد تراکنش را دریافت کند.

[1] Document-based [2] Key-value [3] Ordering Service



شکل ۲. معماری صورت‌حساب الکترونیکی مبتنی بر فبریک

بدنه- سرآمد	بدنه - مشخصات کالا	بدنه - پرداخت
شماره منحصر به فرد	شناسه کالا و خدمات	شماره شبا خریدار
تاریخ و زمان ایجاد صورت حساب	شرح کالا و خدمت	شماره شبا فروشنده
نرخ مالیات بر ارزش افزوده	واحد اندازه گیری	روش پرداخت (نقدی- نسیه- بدون پرداخت)
شناسه بانک شبا خریدار	تعداد/مقدار	مبلغ پرداختی
شناسه فروشنده	مبلغ واحد	تاریخ و زمان پرداخت
شناسه خریدار	مبلغ قبل از تخفیف	مجموع مبلغ پس از کسر تخفیف
	مبلغ تخفیف	مجموع مالیات بر ارزش افزوده
	مبلغ بعد از تخفیف	
	نرخ مالیات بر ارزش افزوده	
	مبلغ مالیات بر ارزش افزوده	

شکل ۳. محتوای تراکنش فروش

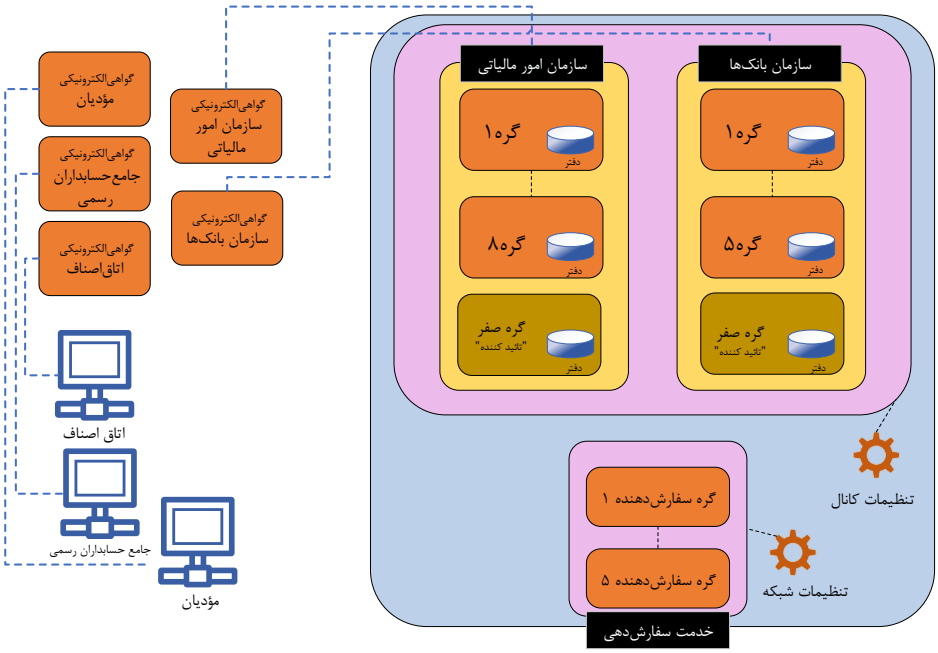
- تعداد حداکثر گره پردازشی: حداکثر دو گره پردازشی مجاز در PDC هستند که پیشنهاد تراکنش را از گره پردازشی تأییدکننده دریافت می‌کنند.
- تعداد قالب برای نگهداشت: داده‌ها در پایگاه‌داده خصوصی حداقل تا پنج سال تا زمان مرور طبق ماده ۱۵۷ قانون مالیات مستقیم باقی بمانند و پس از آن پاک شوند.
- گره پردازشی فقط خواندنی: دو گره پردازشی مجاز دیگر به جز گره پردازشی تأییدکننده در PDC فقط مجاز به خواندن داده‌های خصوصی هستند.
- گره پردازشی فقط نوشتنی: گره پردازشی تأییدکننده در PDC تنها مجاز به نوشتن در مجموعه‌داده خصوصی است.
- خط‌مشی تأیید: برای هر پیشنهاد «تراکنش فروش» گره پردازشی تأییدکننده در PDC مشمول یا معاف و گره پردازشی تأییدکننده در PDC خصوصی یا دولتی باید موافقت کنند تا تراکنش به‌عنوان معتبر تأیید شود.

۴.۳.۳ لایه حاکمیتی

لایه حاکمیتی جهت مدیریت و به‌کارگیری گواهی‌های الکترونیکی و ارائه خدمت‌های امنیتی در مدل زیرساخت کلید عمومی مورداستفاده قرار می‌گیرد که شامل ۴ بخش است:

گواهی الکترونیکی: گواهی الکترونیکی نمونه شرکت توسعه ایده نوین که در حوزه تولید قطعات کامپیوتری فعالیت می‌کند، به شرح شکل ۵ است. شرکت توسعه ایده نوین مالک گواهی (بخش ۱ در شکل) با نقش "seller/buyer" و ویژگی‌های منتسب شده نوع مؤدی "manufacture"، سریال محصول "۷۳۹۶" و شماره شبا "IR010170123789...." است. گواهی الکترونیکی از الگوریتم امضای ecdsa-with-SHA256 بهره می‌گیرد (بخش ۲ در شکل).

کلیدهای عمومی و خصوصی: هر گره پردازشی در داخل شبکه و مؤدیان به‌عنوان اعضای خارج از شبکه یک جفت کلید عمومی و خصوصی مخصوص خود را دارند. کلیدهای عمومی به‌صورت آشکار همان‌طور که در شکل ۵ بخش ۳ مشاهده می‌شود به اشتراک گذاشته می‌شوند تا به دیگر سازمان‌ها اجازه رمزگذاری پیام‌ها یا بررسی امضا را بدهد. کلیدهای



شکل ۴. لایه شبکه مدل پیشنهادی (مبتنی بر فبریک)

Certificate:

Version: 3 (0x2)
Serial Number:
41:01:de:fj:5d:b2-94:18:79:91-26:31:d8:0c:b0:9h:6b:88
Signature Algorithm: ecdsa-with-SHA256 (2) (4)
Issuer. O-Hyperledger, OU-Fabric, CN-public-intermediate-ca-server
Validity
Not Before: October 15 08:00:00 2023 GMT
Not After: October 15 07:59:00 2024 GMT (1)
Subject :OU seller/buyer ,OU-ToseIdeNovin ,OU manufacture, OU IR, OU CN-user!
X509v 3extensions:
X509v3 Key Usage: critical
Digital Signature
X509v3 Basic Constraints: critical
CA:FALSE
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit) (3)
pub:
04:29:ec:d5:53:3e:03:9d:64:a4:a4:28:a5:fe:12:
e2:f0:dd:e4:ee:b9:3f:3e:01:b2:3a:d4:68:b1:b2:
4f:82:1a:3a:33:db:92:6d:10:c9:c2:3b:3d:fc:7a:
f0:fa:cc:8b:44:e8:03:cb:a1:6e:eb:b3:6c:05:a2:
f8:fc:3c:af:24

شکل ۵. نمایش متنی یک گواهی الکترونیکی نمونه (۱: مشخصات مالک گواهی، ۲: تابع درهم و الگوریتم رمزنگاری، ۳: کلید عمومی، ۴: مرکز صدور گواهی الکترونیکی)

خصوصی محرمانه نگهداری می‌شوند و برای رمزگشایی پیام‌های دریافتی و امضای تراکنش‌های خروجی استفاده می‌شوند.

مرکز صدور گواهی الکترونیکی: بر اساس آیین‌نامه اجرائی ماده ۳۲ قانون تجارت الکترونیکی [۴۰] به‌منظور به‌رسمیت‌شناختن امضای الکترونیکی، یک مدل سلسله‌مراتبی متشکل از شورای سیاست‌گذاری گواهی الکترونیکی کشور، مرکز دولتی صدور گواهی الکترونیکی ریشه به‌عنوان نقطه اعتماد و مراکز صدور گواهی الکترونیکی میانی به‌عنوان معماری زیرساخت کلید عمومی کشور به تصویب رسیده است که از همین مدل استفاده شد.

مرکز صدور گواهی الکترونیکی[1] میانی دولتی عام کشور [۴۱] (بخش ۴ در شکل) بر اساس استاندارد X509 و به استناد مصوبه شورای سیاست‌گذاری گواهی الکترونیکی کشور، مرکز منحصربه‌فردی است که برای هر یک از سازمان امور مالیاتی، بانک، اتاق اصناف ایران، جامعه حسابداران رسمی و مؤدیان و هر یک از گره‌های پردازشی آن‌ها یک گواهی صادر می‌کند. مرکز صدور گواهی الکترونیکی میانی دولتی عام کشور، به‌ازای هر شناسه، رمز احراز هویتی را برای مدیر گواهی الکترونیکی ارسال می‌کند. شناسه و رمز احراز هویت به هر گره پردازشی ارسال می‌شود که با ارسال آن به مرکز صدور گواهی الکترونیکی، کلید عمومی و خصوصی و یک گواهی Ecert دریافت می‌کنند.

لیست‌های لغو گواهی: لیست‌های لغو گواهی، گواهی‌های الکترونیکی هستند که پیش از تاریخ انقضا، توسط صادرکننده گواهی باطل شده‌اند.

فراهم‌کننده خدمات عضویت: هر فراهم‌کننده خدمات عضویت[2] [۳۸] مسئول تعریف و مدیریت هویت‌ها، نقش‌ها و مجوزهای مرتبط با مشارکت اعضا است. برای هر گره پردازشی و سازمان امور مالیاتی و بانک MSP محلی برای کانال "TaxationBanks" و خدمت سفارش

[1]Certificate Authority [2]Membership Service Provider (MSP)

دهی MSP در سطح کانال تعریف می‌گردد.

کنترل دسترسی: سازوکار کنترل دسترسی مبتنی بر ویژگی[1] [۴۲] قوانین، ویژگی‌های عامل، موضوع و شرایط محیطی را ارزیابی می‌کند تا تصمیم‌گیری کند که آیا عامل مجاز به دسترسی به موضوع هست یا خیر. کنترل دسترسی مؤدی، گره پردازشی تأییدکننده، گره پردازشی سفارش‌دهنده و گره پردازشی با درنظرگرفتن خط‌مشی امضا و سایر خط‌مشی‌ها به شرح جدول ۲ است.

۵.۳.۳ لایه یکپارچه‌سازی

لایه یکپارچه‌سازی به‌منظور یکپارچه‌سازی با سامانه‌های موجود خارج از زنجیره شامل gRPC، رویداد و اوراکل است. gRPC یک چارچوب است که توسط گوگل توسعه یافته است [۳۴] و برای ارتباط بین سامانه‌های مختلف استفاده می‌شود تا امکان مکالمه بین برنامه مشتری و گره‌های پردازشی را فراهم کند. اعضای شبکه می‌توانند با مشترک‌شدن در رویدادهای ذیل در جریان اتفاقات زنجیره قالبی باقی بمانند [۳۸]:

- **رویداد ثبت تراکنش:** سازمان‌ها ثبت تراکنش را در قالب رویداد به اطلاع خریدار و فروشنده می‌رسانند.
- **رویداد برداشت وجه:** پس از ثبت تراکنش، برداشت وجه را به بانک عامل ارسال می‌کنند.

در مدل پیشنهادی، یک منبع داده در شبکه وجود دارد که هر یک از گره‌های پردازشی برای ارتباط با اوراکل درخواست داده را به منبع داده می‌دهند و منبع داده با اوراکل ارتباط می‌گیرد. اوراکل داده‌های درخواستی را فراهم می‌کند و امضا می‌کند. منبع داده صحت امضا را بررسی می‌کند و در صورت تأیید آن، داده‌های دریافتی از اوراکل را در اختیار گره پردازشی قرار می‌دهند.

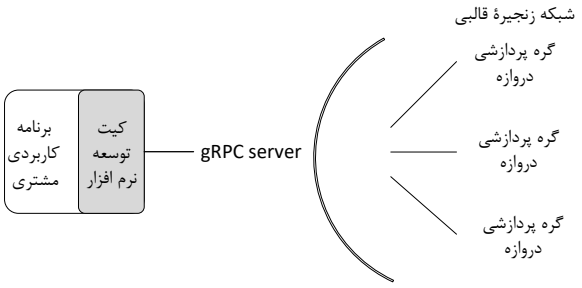
زمانی که تراکنشی در مدل ما امضا می‌شود، یک رویداد به اوراکل بانک ارسال می‌شود تا مبلغ مذکور را تا زمان تسویه نهایی، مسدود نماید و در صورت لغو تراکنش، مبلغ مسدودی آزاد می‌گردد.

۶.۳.۳ لایه برنامه

لایه برنامه شامل برنامه کاربردی مشتری مبتنی بر کیت توسعه نرم‌افزار و ارتباط با قراردادهای هوشمند است. ارتباط این لایه با شبکه زنجیره قالبی در شکل ۶ نمایش‌داده‌شده است:

- برنامه کاربردی مشتری: رابط کاربری است که با شبکه فبریک ارتباط برقرار می‌کند و تراکنش‌ها را شروع می‌کند.
- کیت توسعه نرم‌افزار: مجموعه‌ای از ابزارها و کتابخانه‌هاست که توسعه‌دهندگان برای ساخت برنامه استفاده می‌کنند.

[1] Attribute Based Access Control (ABAC)



شکل ۶. لایه برنامه و نحوه ارتباط آن با زنجیره قالب‌ها

۴ ارزیابی

در این بخش، ارزیابی راهکار پیشنهادی به چهار روش انجام می‌شود. نخست، ابتدا به‌صورت کیفی از لحاظ مناسب بودن از دید خبرگان ارزیابی می‌شود و نشان داده می‌شود که از لحاظ فنی و سازمانی راهکار مناسبی است. سپس از لحاظ امنیتی باتوجه‌به سه جنبه محرمانگی، صحت و دسترس‌پذیری بررسی می‌شود. پس از آن از لحاظ کارایی و نهایتاً با کارهای مرتبط مقایسه می‌شود و نشان داده می‌شود که مدل بهتر از کارهای گذشته به این نیازمندی‌ها پرداخته است.

۱.۴ ارزیابی کیفی مدل

ازآنجاکه راهکار پیشنهادی یک مدل و معماری ارائه می‌کند، مؤثرترین روش سنجش کیفی آن، مصاحبه با خبرگان [۴۳] است که در کارهای مشابه و در روش‌شناسی پژوهش علم طراحی به‌کارگرفته می‌شود. باتوجه‌به همین امر، خبرگانی انتخاب شده‌اند که به‌صورت حرفه‌ای در حوزه زنجیره قالبی در سازمان‌ها فعالیت می‌کنند و باتوجه‌به نو بودن موضوع، حداقل سه سال فعالیت حرفه‌ای در این زمینه دارند.

این مصاحبه‌ها به شکل نیمه‌ساختارمند از بهمن ۱۴۰۲ تا فروردین ۱۴۰۳ با پنج خبره برگزار شد. پیش از مصاحبه، فایل‌های مدل برای ایشان ارسال گردید و در شروع مصاحبه، مدل برای خبرگان شرح داده شد. مصاحبه به صورت حضوری یا برخط انجام گرفت. جمع‌آوری داده‌ها و کدگذاری داده‌های نظرسنجی نیز با استفاده از یک نرم‌افزار تخصصی تحلیل محتوا صورت گرفت. پرسش‌های مصاحبه و پاسخ‌ها در پیوست مقاله ارائه شده است.

پرسش‌های مصاحبه بر اساس الزامات پیاده‌سازی یک فناوری مبتنی بر چارچوب TOE[2] [۴۰] انتخاب شدند. این چارچوب به تحلیل فرایندپذیرش و استفاده از نوآوری‌های فناورانه در سه جنبه سازمان، فناوری و محیط می‌پردازد. خلاصه نظرات ارائه شده خبرگان به شرح زیر است:

- از جنبه فنی،

[2] Technical-Organizational-Environmental

جدول ۲. کنترل دسترسی

عامل	خطمشی امضا	سایر خطمشی
مؤدی	می‌تواند «پیشنهاد تراکنش فروش» را امضا کند.	همه مؤدیان می‌توانند پیشنهاد تراکنش فروش را ایجاد کنند. اگر خریدار یا فروشنده گمرک باشد فقط روش «بدون پرداخت» را می‌تواند انتخاب کند.
گره پردازشی تأییدکننده	همه گره‌های پردازشی تأییدکننده می‌توانند پیشنهاد تراکنش فروش را امضا کنند. یک گره پردازشی تأییدکننده از سازمان امور مالیاتی و یک گره پردازشی تأییدکننده از سازمان بانک‌ها باید پیشنهاد تراکنش فروش را امضا کنند.	
گره پردازشی سفارش‌دهنده	گره پردازشی رهبر از میان سفارش‌دهنده‌ها می‌تواند تراکنش‌های امضا شده را مرتب کند و به همه گره‌های پردازشی ارسال کند.	هر گره پردازشی سفارش‌دهنده می‌تواند طی الگوریتم اجماع به‌عنوان رهبر انتخاب شود.
گره پردازشی	اگر اکثریت گره‌های پردازشی سازمان امور مالیاتی و بانک‌ها قالب را تأیید کنند، قالب ثبت می‌شود.	

- (قوت) با استفاده از پروتکل‌های پیشنهادی مکانیزم اجماع می‌تواند امنیت را تأمین کند.
- (قوت) وضعیت نهائی تراکنش و تشخیص آن که معتبر یا غیرمعتبر است، قابل شناسائی است.
- (قوت) داده‌های حساس در شبکه به‌درستی ذخیره می‌شوند.
- (قوت) زنجیره قالبی در کل مقیاس‌پذیر نیست، اما به دلیل تعداد کمی از گره‌های پردازشی و بودن در محیط سازمانی خصوصی، این مدل از زنجیره قالب‌های عمومی بهتر عمل می‌کند.
- (کاستی) بررسی اینکه داده‌های وارد شده با داده‌های دنیای واقعی تطابق دارند، نیاز به یک نهاد ناظر یا یک توکن دارد که احراز حقیقت و صحه‌گذاری بر اطلاعات را انجام دهد.

• از جنبه سازمانی،

- (قوت) در خصوص سازگاری با سامانه‌های سنتی، مدل می‌تواند در بستر نرم‌افزارها و سخت‌افزارهای موجود عمل کند و از سوی دیگر لزومی هم برای سازگاری وجود ندارد.
- (قوت) استفاده از زنجیره قالبی در مدل، اطمینان از امنیت ذخیره داده را فراهم می‌کند.
- (قوت) برای ذخیره‌کردن داده‌ها، دو بخش داده‌های داغ که به آن‌ها مراجعه می‌شود و داده‌های بیات شده که آرشیو می‌شوند، وجود دارد.
- (قوت) از دسترسی غیرمجاز، از طریق گواهی الکترونیکی و مجوزدار بودن زنجیره قالبی جلوگیری می‌گردد. همچنین، هیچ گره پردازشی وجود ندارد که دسترسی کامل داشته باشد.
- (کاستی) باید بین اسناد و مدارک دیجیتال و کاغذی همبستگی ایجاد شود تا آن را انکارناپذیر کند. برای مثال تصویری از اسناد و مدارک کد شود و در دفتر ذخیره شود.

• از جنبه محیطی، بحث قوانین و منطق تراکنش نیاز به اشراف به قوانین و فرایندهای مالیاتی دارد، بنابراین، نمی‌توان در این بخش اظهارنظر نمود.

بنابراین، با استناد به نظر خبرگان می‌توان تأیید کرد که راهکار پیشنهادی، یک راهکار مناسب است و البته جنبه‌هایی هم هست که می‌تواند به کار اضافه شود و آن را بهبود دهد.

۲.۴ امنیت

امنیت از ابتدایی‌ترین نیازمندی‌های یک سامانه مالیاتی است و در این بخش نشان می‌دهد که در راه‌حل پیشنهادی این مقاله چطور در نظر گرفته شده است. در این خصوص بر سه نیازمندی اصلی محرمانگی، صحت و دسترس‌پذیری [۴۴] تمرکز می‌شود.

۱.۲.۴ محرمانگی

از لحاظ جنبه محرمانگی، باید توجه داشت که داده‌ی مطلقاً محرمانه (نظیر گذرواژه یا کلیدهای رمزنگاری و امضای دیجیتالی) اصولا در سامانه پیشنهادی نگهداری نمی‌شود. اطلاعاتی که در خصوص تراکنش‌های مالی و غیره در سامانه نگهداری می‌شود، همگی در یک زنجیره قالبی خصوصی (سازمانی) مجوزدار ذخیره می‌شود که توسط گره‌های پردازشی از قبل تعریف شده و محدود سازمانی مدیریت می‌شود. احراز اصالت گره‌های پردازشی و کاربران سامانه همگی با گواهی‌های دیجیتالی و زیرساخت کلید عمومی انجام می‌شود و اصولاً گره یا کاربر غیرمجاز امکان دسترسی ندارد. پس از احراز اصالت، با استفاده از سازوکار کانال، دسترسی به داده‌ها فقط به افراد و سازمان‌هایی داده می‌شود که مجاز باشند. همچنین با اتکا به سازوکار مجموعه‌داده خصوصی در زنجیره قالبی فبریک، فقط گره‌های پردازشی مجاز، و نه همه‌ی گره‌های پردازشی، اطلاعات را در پایگاه‌داده خود ذخیره می‌کنند. بنابراین حریم‌خصوصی اطلاعات و دسترسی به مطالبی که ممکن است اسرار تجاری را فاش کند، طبق اصل حداقل مجوزها، در حداقل ممکن نگه‌داشته شده است.

۲.۲.۴ صحت

در خصوص جنبه صحت، اولاً زیرساخت زنجیرة قالبی مورد استفاده ذاتاً توزیع شده و نامتمرکز است و با اتکا به سازوکار اجماع، از یکسان بودن

اطلاعات در همه گره‌ها اطمینان حاصل می‌شود. بنابراین اطلاعات بر روی یک گره پردازشی متمرکز یا فقط در یک بخش از سازمان نگهداری نمی‌شوند که آن گره بتواند اطلاعات را جعل، دستکاری یا حذف کند. ثانیاً همه تغییرات و ثبت اطلاعات در قالب تراکنش و فراخوانی قرارداد هوشمند انجام می‌شود. تراکنش‌ها امضای دیجیتالی دارند و با اتکا به زیرساخت کلید عمومی و امنیت امضا، امکان دستکاری یا جعل آن‌ها وجود ندارد. همچنین قراردادهای هوشمند همه عملیات را به صورت خودکار و فقط با رعایت ضوابط انجام می‌دهند که جلوی هرگونه خرابکاری یا دورزدن مقررات را می‌گیرد. با توجه به ساختار و فرایند ثبت تراکنش‌ها در کانال‌ها، همه گره‌های عضو کانال ضمن حفظ محدودیت‌های دسترسی، بر روند تراکنش‌ها نظارت دارند و این راهکار در عین ایجاد شفافیت، نسبت به صحت هم اطمینان ایجاد می‌کند.

پروتکل Raft مورد استفاده برای اجماع زنجیره قالبی پیشنهادی، یک پروتکل قطعی است و امکان لغو تراکنش در آن وجود ندارد؛ در حالی که اجماع بعضی زنجیره‌های قالبی نظیر بیتکوین غیرقطعی، و ممکن است به علت شکل‌گیری یک زنجیره بلندتر موازی، تراکنشی که قبلاً تایید شده بوده، لغو شود.

۳.۲.۴ دسترس‌پذیری

در جنبه دسترس‌پذیری، زنجیره قالبی به عنوان زیرساخت مهم برای پردازش داده‌ها و ذخیره‌سازی آن‌ها، ذاتاً یک سامانه توزیع شده است. در این خصوص با توجه به شکل ۱، در هر بخشی از معماری، چندین گره مضاعف[1] در نظر گرفته شده‌اند. اگر یکی یا چند گره پردازشی از کار بیافتند، اطلاعات همچنان بر روی سایر گره‌ها موجود است و می‌توانند به پردازش خود ادامه دهند. همچنین اگر به هر دلیل، کاربری نتواند به یکی از گره‌ها متصل شود، سایر گره‌ها به عنوان جایگزین قابل استفاده هستند.

میزان تاب آوری نسبت به خرابی گره‌ها کاملاً وابسته به سازوکار اجماع Raft است. به طور خاص، تعداد گره‌ها باید به اندازه کافی زیاد باشد که با توجه به احتمال از کار افتادن تعدادی از گره‌ها، همواره یک جمع غالب از گره‌ها فعال باقی بمانند. بر اساس توضیحات لایه شبکه در معماری پیشنهادی، نُه گره پردازشی برای سازمان امور مالیاتی و شش گره برای بانک‌ها در نظر گرفته شده است. بنابراین پانزده گره دارد که نسبت به خرابی حداکثر هفت گره مقاوم است. خدمت سفارش‌دهی هم شامل جمعاً پنج گره است که نسبت به خرابی حداکثر دو گره مقاوم است.

پروتکل Raft یک پروتکل سریع است و زمانی در مقیاس یک رفت و برگشت پیام در شبکه[2] (RTT) برای ثبت یک تراکنش در آن کافی است. لذا از لحاظ سرعت عملکرد نیز، زنجیره قالبی مورد استفاده تأخیری مشابه سامانه‌های متداول شبکه‌ای دارد. این در حالی است که مثلاً در پروتکل اجماع اثبات کار (PoW) مورد استفاده بیتکوین، حداقل ۱۰ دقیقه برای ثبت تراکنش روی زنجیره قالبی زمان لازم است.

[1]Redundant [2]Round trip time

۳.۴ کارایی

از آنجا که سامانه مالیاتی یک سامانه زیرساختی در اقتصاد کشور است و همه‌ی کسب و کارهای کشور با آن در ارتباط هستند، لازم است از کارایی بالایی برخوردار باشد و کشش پاسخگویی به درخواست‌ها در مقیاس ملی را داشته باشد. در این خصوص دو نکته حائز اهمیت است. اولاً در راهکار پیشنهادی کسب و کارها به صورت پیوسته و در طول سال صورت‌حساب‌های خود را در سامانه ثبت می‌کنند. بنابراین اوج حجم کاری این سامانه نسبت به سامانه سنتی مالیاتی بسیار پایین‌تر است. ثانیاً در مقاله حاضر یک معماری و راهکار پیشنهاد شده است و هنوز پیاده‌سازی نشده است.

بر اساس مستندات رسمی هایپرلجر فبریک، استفاده از پایگاه داده LevelDB در گره‌ها می‌تواند سرعت پردازش را تا دو برابر افزایش دهد. شاخص‌های دیگر نظیر تعداد کانال‌ها، تعداد گره‌های دخیل در اجماع، مقدار حافظه، سرعت پردازنده مرکزی، اندازه حافظه کش، پهنای باند شبکه، و سایر مشخصات و تنظیمات گره‌های پردازشی بر کارایی فبریک اثرگذار است. لذا حتماً باید در پیاده‌سازی دقت کافی به خرج داده شود و از سخت‌افزار قوی و ارتباطات شبکه سریع استفاده شود و تنظیمات اثرگذار بر کارایی بهینه‌سازی شوند.

بر اساس یک مطالعه پیش‌تر انجام شده [۴۵] پروتکل اجماع Raft مورد استفاده در راهکار پیشنهادی تأخیر قابل چشم‌پوشی در تایید تراکنش‌ها دارد و اکثر زمان تأخیر مربوط به پردازش تراکنش است که در هر شکلی از پیاده‌سازی غیرقابل صرف‌نظر است. در عوض، اندازه قالب اثر ملموسی بر تاخیر تراکنش‌ها دارد.

به عنوان جمع‌بندی به مطالعه شرکت IBM بر روی فبریک اشاره می‌شود[۴۶] که در آن یک سخت‌افزار اختصاصی با پردازنده Intel Xeon Silver 4210 CPU، 64GB RAM، SSD storage به عنوان گره پردازشی در نظر گرفته شده است و توانسته است به نرخ ۲۰ هزار تراکنش در ثانیه برسد. با توجه به گزارش شبکه شاپرک از تراکنش‌های پرداخت با کارت‌های بانکی، متوسط نرخ تراکنش این شبکه در سال ۱۴۰۲ معادل ۱۵۶۴ تراکنش در ثانیه است. [۴۷]. مقایسه این نرخ با نرخ فبریک نشان می‌دهد که راهکار پیشنهادی در صورت تنظیم مناسب می‌تواند حجم مناسبی از تراکنش‌ها را پردازش کند که بسیار بیشتر از نرخ کل تراکنش‌های کارت‌های بانکی در کشورمان است.

۴.۴ مقایسه با کارهای مرتبط

مقایسه با راهکارهای پیشنهادی [۷–۱۱، ۲۸، ۳۲، ۳۳] از جهت مشکلات شناسائی شده در صورت‌حساب الکترونیکی در جدول ۳ آمده است. شاخص‌ها همان‌هایی هستند که در بخش مقدمه ذکر شد. جهت مقایسه، مقاله‌هایی انتخاب شده‌اند که فقط به بیان کلیات بسنده نکرده باشند و در آن‌ها اجزای مدل نیز شرح داده شده باشد.

بر اساس جدول ۳، با تخصیص گره‌های پردازشی به سازمان امور

جدول ۳. تحلیل انتقادی مقاله های مرور شده

شاخص‌ها	شماره مقاله	راهکار مدل پیشنهادی
جلوگیری از جعل اطلاعات تراکنش و یا جعل یک تراکنش	[۷، ۹-۱۱]	دخالت بانک‌ها و سازمان امور مالیاتی در ثبت داده‌ها در زنجیره قالبی، اتصال داده‌های بانک‌ها و سازمان امور مالیاتی از طریق اوراکل به زنجیره قالبی
عدم پیچیدگی و طولانی‌بودن فرایند صدور صورت‌حساب الکترونیکی	[۷، ۸]	الکترونیکی شدن صورت‌حساب، تطبیق اطلاعات صورت‌حساب در زمان ثبت، استفاده از سازوکار اجماع Raft
پرهیز از ریسک بسیار بالای نگه‌داری داده در پایگاه‌داده مرکزی	[۲۸، ۳۲]	استفاده از زنجیره قالبی سازمانی برای ذخیره‌سازی توزیع شده نامتمرکز
کدگذاری دقیق کالا و خدمات	[۱۱]	حضور اتاق اصناف و نقش نظارتی در ایجاد پیشنهاد تراکنش
حفظ محرمانگی و حریم خصوصی در عین شفافیت	[۹، ۱۱، ۳۲]	تعریف کانال و مجموعه‌داده خصوصی و کنترل دسترسی مبتنی بر ویژگی در زنجیره قالبی سازمانی، احراز هویت و کنترل دسترسی با گواهی الکترونیکی و زیرساخت کلید عمومی

مالیاتی و بانک‌ها در شبکه زنجیره قالبی ، این نهادها در تأیید تراکنش‌ها و نظارت لحظه‌بلحظه بر سامانه دخالت داده شده‌اند. به‌عبارت‌دیگر، هیچ تراکنشی که سازمان امور مالیاتی و بانک‌ها تأیید نکنند، قابلیت ثبت در سامانه را ندارد. همچنین از سازوکار اوراکل برای متصل‌کردن بانک‌ها و سازمان امور مالیاتی به قرارداد هوشمند استفاده شد تا امکان تطابق داده‌ها با واقعیت وجود داشته باشد. بحث جلوگیری از جعل فقط در [۲۷] دیده شده است که در آن تأیید تراکنش‌ها توسط سازمان امور مالیاتی انجام می‌شود.

مشکل پیچیدگی و زمان‌بر بودن فرایند ثبت صورت‌حساب از یک‌سو اصولاً با پیاده‌سازی صورت‌حساب الکترونیکی در راهکار پیشنهادی تسهیل می‌شود. ثانیاً با اتصال اوراکل بانک‌ها و سازمان امور مالیاتی، قرارداد هوشمند می‌تواند یک‌سری کنترل‌های درستی را به‌صورت خودکار در لحظه و پیش از ثبت تراکنش انجام دهد. نهایتاً، سازوکار اجماع Raft که برای زنجیره قالبی انتخاب شده است، در عین قطعیت و بازگشت‌ناپذیر بودن، بسیار سریع است و در حد سرعت سامانه‌های متمرکز عمل می‌کند. این در حالی است که زنجیره‌های قالبی عمومی مبتنی بر اثبات کار یا سایر سازوکارهای اثبات، نیازمند پردازش‌های سنگین یا فرایندهای اجماع زمان‌بر هستند.

در راهکار پیشنهادی، اطلاعات اصلی و مهم تراکنش بر روی زنجیره قالبی نگهداری می‌شوند و فقط از طریق قرارداد هوشمند مربوطه و بر اساس مجوزهایی که تعریف شده است قابل‌دسترسی هستند. داده‌های زنجیره قالبی به‌صورت توزیع شده و مضاعف بر روی چندین گره محاسباتی که در اختیار سازمان‌های عضو شبکه زنجیره قالبی هستند نگهداری می‌شود. این راهکار نسبت به روش‌های سنتی که در آن اطلاعات فقط روی یک سرور مرکزی نگهداری می‌شد، قابلیت اطمینان بسیار بیشتری دارد و در صورت خرابی حتی دو گره محاسباتی، سامانه می‌تواند بدون هیچ خلل و قطعی به کار خود ادامه دهد؛ بنابراین دسترس‌پذیری بسیار بالایی نیز دارد. در این سازوکار چند سازمان (امور مالیاتی و بانک‌ها) گره‌های مختص خود را دارند و به همین دلیل، نامتمرکز است و در مقایسه با سامانه‌های ذخیره‌سازی توزیع شده متمرکز که در آن فقط یک نهاد متولی نگهداری همه اطلاعات است، از شفافیت و اطمینان بسیار بالاتری نسبت به عدم دست‌کاری برخوردار است. به‌غیراز موارد ذکر شده، مهم‌ترین چالش استفاده از زنجیره قالبی برای صورت‌حساب‌های مالیاتی حفظ محرمانگی و حریم خصوصی است. اگرچه در نگاه اول این نیازمندی با موضوع شفافیت در تقابل است، اما ازآنجاکه زنجیره قالبی سازمانی انتخاب شد، کنترل بسیار دقیقی بر دسترسی اطلاعات وجود دارد. با تعریف مجموعه‌داده خصوصی و استفاده از ویژگی کانال در فبریک، در مدل می‌توان صورت‌حساب الکترونیکی و محتویات تراکنش‌های آن را به‌صورت محرمانه درآورد. استفاده از گواهی‌های الکترونیکی، کلید عمومی و خصوصی و کنترل دسترسی مبتنی بر ویژگی تضمین می‌کند که فقط افراد و نهادهای مجاز می‌توانند به بخش‌هایی از اطلاعات که به‌واسطه الزامات قانونی نیاز دارند دسترسی پیدا کنند. در میان کارهای مرتبط فقط الخودره و همکاران [۲۳] که آن‌ها نیز از زنجیره قالبی خصوصی استفاده کرده‌اند موفق شده‌اند امنیت و حریم خصوصی را در عین شفافیت تأمین کنند.

۵ نتیجه‌گیری و پیشنهادها

ویژگی‌های تمرکززدایی، مقاومت در برابر دست‌کاری، شفافیت و خودکارسازی زنجیره قالبی در مدل پیشنهادی باعث می‌گردد که بتواند بر برخی از مشکلات صورت‌حساب الکترونیکی فائق آید. همچنین مشخص شد که زنجیرة قالبی مناسب سامانه مالیاتی باتوجه‌به بحث محرمانگی اطلاعات، زنجیره قالبی سازمانی است. به‌منظور پیاده‌سازی از میان سکوهای زنجیره قالبی سازمانی، فبریک انتخاب گردید.

بر مبنای معماری پیشنهادی، لایه‌های مختلفی ارائه شد. لایه شبکه شامل سازمان امور مالیاتی، بانک‌ها در داخل شبکه، مودیان، اتاق اصناف جامع حسابداران رسمی خارج از شبکه هستند. لایه پروتکل از تراکنش فروش، زنجیره قالبی و وضعیت سراسری تشکیل شده است. در لایه کنترل داده به‌منظور حفظ محرمانگی از کانال و مجموعه‌داده خصوصی بهره گرفته شد. در لایه حاکمیتی مرکز صدور گواهی الکترونیکی میانی دولتی عام کشور معرفی شد که مرجعی برای صدور گواهی الکترونیکی برای هر یک از کاربران است. البته دسترسی هر یک از کاربران بر اساس خط‌مشی کنترل دسترسی تعیین شده است. در لایه یکپارچه‌سازی رویداد و اوراکل ارتباط با شبکه خارج از زنجیره قالبی را فراهم می‌کنند و در

لایه برنامه، برنامه کاربردی مشتری نحوه ارتباط با شبکه زنجیره قالبی را مشخص می‌کند. ارزیابی امنیتی، کارایی، و مقایسه با کارهای پیشین نیز نشان دهنده مطلوبیت راهکار پیشنهادی است.

به‌عنوان کارهای آتی پیشنهادی می‌توان اشاره کرد که باتوجه‌به کار گیری سکوی فبریک و ارائه معماری صورت‌حساب الکترونیکی مبتنی بر فبریک، نحوه فرایند اجرای تراکنش برای مطالعه‌های آتی پیشنهاد می‌گردد. همچنین باتوجه‌به ارتباط تنگاتنگ صورت‌حساب الکترونیکی با سامانه مالیات بر ارزش‌افزوده، مطالعه در این حوزه شایان توجه هست.

مراجع

[1] Cai, Cynthia Weiyi. Triple-entry accounting with blockchain: How far have we come? *Accounting & Finance*, 61(1):71–93, 2021.

[2] Gökten, Soner and Özdoğan, Burak. The doors are opening for the new pedigree: a futuristic view for the effects of blockchain technology on accounting applications. in *Digital Business Strategies in Blockchain Ecosystems: Transformational Design and Future of Global Business*, pp. 425–438. 2020.

[3] Dai, Jun and Vasarhelyi, Miklos A. Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3):5–21, 2017.

[4] Baisalbayeva, K, van der Enden, E, Ion, V, Tsavdaris, H, Deputy, D, van der Vlist, F, and Aygun, C. Blockchain for tax compliance. tech. rep., Microsoft, PwC, and Vertex, 2019.

[5] Faccia, Alessio and Mosteanu, Narcisa Roxana. Tax evasion, information systems and blockchain. *Journal of Information Systems & Operations Management*, 13(1):65–74, 2019.

[6] Wijaya, Dimaz Ankaa, Liu, Joseph K, Suwarsono, Dony Ariadi, and Zhang, Peng. A new blockchain-based value-added tax system. in *Proceedings of the 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25, 2017*, pp. 471–486. Springer International Publishing, 2017.

[7] Ibañez, Juan Ignacio, Bayer, Chris N, Tasca, Paolo, and Xu, Jiahua. Triple-entry accounting, blockchain and next of kin: Towards a standardization of ledger terminology. *arXiv preprint arXiv:2101.02632*, 2021.

[8] Fatz, Filip, Hake, Philip, and Fettke, Peter. Towards tax compliance by design: a decentralized validation of tax processes using blockchain technology. in *2019 IEEE 21st conference on business informatics (CBI)*, vol. 1, pp. 559–568. IEEE, 2019.

[9] Fatz, Filip, Hake, Philip, and Fettke, Peter. Confidentiality-preserving validation of tax documents on the blockchain. in *Wirtschaftsinformatik (Zentrale Tracks)*, pp. 1262–1277, 2020.

[10] Kim, Young Ran. Blockchain initiatives for tax administration. *UCLA Law Review*, 69:240, 2022.

[11] Setyowati, Milla Sepliana, Utami, Niken Desila, Saragih, Arfah Habib, and Hendrawan, Adang. Blockchain technology application for value-added tax systems. *Journal of open innovation: technology, market, and complexity*, 6(4):156, 2020.

[12] Ricci, Piergiorgio and Mammanco, Valentina. Blockchain technology to support italian tax process. *European Journal of Engineering Science and Technology*, 2(3):1–10, 2014.

[۱۳] میرزایی، فرزام، محمدحسین، سید، و سرمدی، بیات. ارائه مدل عملی حفظ حریم خصوصی در قراردادهای هوشمند مبتنی بر زنجیره بلوکی با کاهش سربار. دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، ۱۰(۱):۳۴–۴۲، ۱۴۰۰.

[14] Luc, Desrosiers and Ricardo, Olivieri. Oracles: Common architectural patterns for hyperledger fabric. Unpublished.

[15] Olaleye, Sunday Adewale, Sanusi, Ismaila Temitayo, Dada, Oluwaseun Alexander, and Agbo, Friday Joseph. A bibliometric review of global visibility, impact and adoption of electronic invoicing: The past and the future. *Heliyon*, 9(3), 2023.

[16] Van Brederode, Robert F. Introduction: Why ethics matter in taxation. *Ethics and Taxation*, pp. 1–19, 2020.

[17] Wang, Juan. Application of blockchain technology in tax collection and management. in *Cyber Security Intelligence and Analytics: Proceedings of the 2020 International Conference on Cyber Security Intelligence and Analytics (CSIA 2020), Volume 2*, pp. 50–58. Springer, 2020.

[18] Konstantinidis, Ioannis, Siaminos, Georgios, Timplalexis, Christos, Zervas, Panagiotis, Peristeras, Vassilios, and Decker, Stefan. Blockchain for business applications: A systematic literature review. in *Business Information Systems: 21st International Conference, BIS 2018, Berlin,*

Germany, July 18-20, 2018, Proceedings 21, pp. 384–399. Springer, 2018.

[۱۹] عرب نوری، آرین، عیسی زاده، سهیل، و نژاد، شفیعی. سامانه لاگ حسابرسی پذیر امن مبتنی بر زنجیره قالب. دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، ۱۳(۲):۷۵-۸۶، ۱۴۰۳.

[20] Hevner, Alan R. A three cycle view of design science research. *Scandinavian journal of information systems*, 19(2):4, 2007.

[21] Hevner, Alan R, March, Salvatore T, Park, Jinsoo, and Ram, Sudha. Design science in information systems research. *MIS quarterly*, pp. 75–105, 2004.

[22] Peffers, Ken, Tuunanen, Tuure, Rothenberger, Marcus A, and Chatterjee, Samir. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[23] Alkhodre, Ahmad, Ali, Toqeer, Jan, Salman, Alsaawy, Yazed, Khusro, Shah, and Yasar, Muhammad. A blockchain-based value added tax (vat) system: Saudi arabia as a use-case. *International Journal of Advanced Computer Science and Applications*, 10(5):708–716, 2019.

[24] Merkx, Madeleine. Vat and blockchain: Challenges and opportunities ahead. *EC Tax Rev.*, 28:83, 2019.

[25] Hoffman, Michał R. Can blockchains and linked data advance taxation. in *Companion Proceedings of the the Web Conference 2018*, pp. 1179–1182, 2018.

[۲۶] قانونی شیشوان، وحیده، الهی، شعبان، دری نوگورانی، صادق، و یزدیان ورجانی، علی. سیستم مالیات بر ارزش افزوده مبتنی بر بلاکچین: مرور نظام‌مند. تحقیقات مالی، ۲۶(۲):۲۲۶-۲۴۷، ۱۴۰۳.

[27] Liu, Xidong. Research and application of electronic invoice based on blockchain. 232:04012, 2018.

[28] Nguyen, Van-Cam, Hoai-Luan, PHAM, Thi-Hong, TRAN, Huynh, Huu-Thuan, and Nakashima, Yasuhiko. Digitizing invoice and managing vat payment using blockchain smart contract. in *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*, pp. 74–77. IEEE, 2019.

[29] Ainsworth, Richard Thompson and Alwohaibi, Musaad. Blockchain, bitcoin, and vat in the gcc: the missing trader example. 2017.

[30] Ainsworth, Richard Thompson, Alwohaibi, Musaad, and Cheetham, Mike. Vatcoin: the gcc's cryptotaxcurrency. *Law and Economics Research Paper*, 2016.

[31] Ainsworth, Richard Thompson and Shact, Andrew. Blockchain (distributed ledger technology) solves vat fraud. *Tax Notes*, 83:1165, 2016.

[32] Setyowati, Milla Sepliana, Utami, Niken Desila, Saragih, Arfah Habib, and Hendrawan, Adang. Strategic factors in implementing blockchain technology in indonesia's value-added tax system. *Technology in Society*, 72:102169, 2023.

[33] Søgaard, Jonas Sveistrup. A blockchain-enabled platform for vat settlement. *International Journal of Accounting Information Systems*, 40:100502, 2021.

[34] Bashir, Imran. *Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3*. Packt Publishing Ltd, 2023.

[35] Büyüközkan, Gülçin and Tüfekci, Gizem. A decision-making framework for evaluating appropriate business blockchain platforms using multiple preference formats and vikor. *Information Sciences*, 571:337–357, 2021.

[36] Nanayakkara, Samudaya, Rodrigo, MNN, Perera, Srinath, Weerasuriya, Geeganage Thilini, and Hijazi, Amer A. A methodology for selection of a blockchain platform to develop an enterprise system. *Journal of Industrial Information Integration*, 23:100215, 2021.

[37] Polge, Julien, Robert, Jérémy, and Le Traon, Yves. Permissioned blockchain frameworks in the industry: A comparison. *Ict Express*, 7(2):229–233, 2021.

[38] hyperledger, Team. Hyperledger fabric. 2.5. 2023.

[39] Zand, Matt, Wu, Xun Brian, and Morris, Mark Anthony. *Hands-On Smart Contract Development with Hyperledger Fabric V2*. O'Reilly Media, Inc., 2021.

[40] Baker, Jeff. The technology–organization–environment framework. *Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1*, pp. 231–245, 2011.

[۴۱] آیین‌نامه اجرائی ماده ۳۲ قانون تجارت الکترونیک. ۱۳۸۶.

[42] Rouhani, Sara, Belchior, Rafael, Cruz, Rui S, and Deters, Ralph. Distributed attribute-based access control system using permissioned blockchain. *World Wide Web*, pp. 1–28, 2021.

[43] Robinson, Oliver C. Sampling in interview-based qualitative research: A theoretical and practical guide. *Qual-*

itative research in psychology, 11(1):25–41, 2014.

[44] Mohammadzadeh, Nasibeh, Nogoorani, Sadegh Dorri, and Muñoz-Tapia, José Luis. Decentralized factoring for self-sovereign identities. *Electronics*, 10(12):1467, 2021.

[45] Piao, Xuefeng, Li, Mingxin, Meng, Fanchao, and Song, Huihui. Latency analysis for raft consensus on hyper-ledger fabric. in *International Conference on Blockchain and Trustworthy Systems*, pp. 165–176. Springer, 2022.

[46] Ferris, C. Answering your questions on hyper-ledger fabric performance and scale. *Retrieved from ibm. com/blogs/blockchain/2019/01/answering-your-questions-on-hyperledger-fabric-perf ormance-and-scale*, 2019.

[۴۷] شبکه الکترونیکی پرداخت‌کارت (شاپرک)، گزارش اقتصادی، شاپرک، ۱۴۰۳.

پیوست

ویژگی‌های خبرگان به شرح جدول ۴ است.

جدول ۴. گروه‌بندی خبرگان

	توصیف
خبرگان زنجیره‌بلوکی (۵ نفر)	استاد دانشگاه و پژوهشگر و مشاور در حوزه زنجیره‌بلوکی
	توسعه‌دهنده زنجیره‌بلوکی
	توسعه‌دهنده زنجیره‌بلوکی، متخصص هایپرلجر فبریک
	توسعه‌دهنده زنجیره‌بلوکی
	مدیر نوآوری در حوزه فناوری زنجیره‌بلوکی

پرسش‌های زنجیره قالبی بر مبنای الزامات پیاده‌سازی یک فناوری مبتنی بر چارچوب TOE که به تحلیل فرایند پذیرش و استفاده از نوآوری‌های فناورانه در سازمان‌ها در سه جنبه سازمان، فناوری و محیط می‌پردازد.

نظرسنجی خبرگان زنجیره قالبی

نتایج مصاحبه با متخصصان در حوزه زنجیره قالبی به شرح جدول ۵ می‌باشد. در جدول ابعاد مصاحبه باتوجه‌به پرسش‌ها به سه بخش فنی، سازمانی و محیطی تقسیم‌بندی گردیده است.

از جنبه فنی بهره‌گیری از استانداردهای طراحی فرایندها در قرارداد هوشمند و خط‌مشی از دو جنبه از سوی خبرگان پاسخ داده شد. چون پیاده‌سازی با بهره‌گیری از استانداردهای BPMN می‌باشد دو نفر از خبرگان باتوجه‌به عدم آشنائی کامل با استاندارد مدنظر، اظهارنظری نکردند اما دو نفر دیگر مطابقت با استاندارد طراحی را تأیید نمودند.

مکانیزم اجماع چون از پروتکل‌های پیشنهادی خود فبریک می‌باشد می‌تواند امنیت را تأمین کند. مجموعه‌داده خصوصی و الگوریتم هش در مدل می‌تواند امنیت و صحت را تأمین کند. البته از نظر یکی از خبرگان چون در خود فبریک الگوریتم هش و رمزنگاری پیشنهاد شده است برای جلوگیری از دوباره‌کاری، رمزنگاری مجدد پیشنهاد نمی‌گردد اما تبادل بین مقیاس‌پذیری و درعین‌حال مقاوم نسبت به فناوری‌های کوانتوم در بحث رمزنگاری می‌بایست موردتوجه قرارگیرد. وضعیت نهائی تراکنش و اینکه معتبر یا غیرمعتبر است شناخته می‌شود، مورد تأیید می‌باشد.

داده‌های حساس در شبکه به‌درستی ذخیره می‌شوند اما اینکه این داده‌های حساس کدام‌ها هستند از نظر یکی از خبرگان به مباحث مالیاتی بر می‌گردد. طبق نظر یکی از خبرگان «بررسی این که داده‌های وارد شده با داده‌های دنیای واقعی تطابق دارند نیاز به یك نهاد ناظر یا یك توکن و یا NFT دارد که احراز حقیقت و صحه‌گذاری بر اطلاعات را انجام دهد.»

از جنبه سازمانی می‌توان گفت مدل توانسته است بر الزامات فائق بیاید. در خصوص سازگاری با سیستم‌های سنتی می‌توان گفت از نظر خبرگان از یک سو می‌توان گفت مدل می‌تواند در بستر نرم‌افزارها و سخت‌افزارهای موجود به‌درستی عمل کند و از سوی دیگر لزومی هم برای سازگاری وجود ندارد. طبق دیدگاه یکی از خبرگان «موضوعات حاکمیتی همچون مالیات بحث اسناد و مدارک همچنان نقش اساسی را ایفا می‌کند. باید بین اسناد و مدارک دیجیتال و کاغذی همبستگی ایجاد شود تا آن را انکارناپذیر کند، برای مثال تصویری از اسناد و مدارک کد شود و در دفتر ذخیره شود.» چون از زنجیره قالبی در مدل بهره گرفته شده است ذخیره داده به‌صورت امن تضمین می‌شود. ذخیره‌کردن داده‌ها در دو بخش داده‌های داغ که به آن‌ها مراجعه می‌شود و داده‌های بیات شده که آرشیو می‌شوند باید انجام گیرد و بهره‌گیری راهکارهای لایه دو مانند زنجیره‌های جانبی که تراکنش‌ها خارج از زنجیره‌بلوکی تأیید می‌شوند و رول‌آپ‌ها که تراکنش‌ها را جمع کرده و تبدیل به یک تراکنش جدید می‌کنند، توصیه می‌شود. جلوگیری از دسترسی غیرمجاز از طریق گواهی الکترونیکی و مجوزدار بودن زنجیره قالبی تأمین می‌شود و گره پردازشی وجود ندارد که دسترسی کامل داشته باشد. پیشنهاد می‌گردد در مدل از گره پردازشی که حتی خارج از سازمان‌های ذی‌نفع باشد، انتخاب گردد که نقش نظارتی در شبکه داشته باشد.

از جنبه محیطی بحث قوانین و منطق تراکنش نیاز به اشراف به قوانین و فرایندهای مالیاتی دارد بنابراین غالب خبرگان در این بخش اظهارنظر ننمودند. از نظر یکی از خبرگان «قراردادهای هوشمند شکل دیجیتالي شده قوانین و مقررات نمی‌باشند و در برخی موارد حتی پیاده‌سازی قراردادهای هوشمند مبتنی بر قوانین و مقررات امکان‌پذیر نیست و می‌بایست در قوانین تغییراتي اعمال شود.»

زنجیره قالبی در کل مقیاس‌پذیر نمی‌باشد اما چون مدل تعداد گره پردازشی کمی دارد و سازمان خصوصی است بهتر از زنجیره قالبی‌های عمومی عمل می‌کند. از طرفی چون تعداد تراکنش در هر ثانیه مشخص نمی‌باشد نمی‌توان تصمیم‌گیری نهائی انجام داد. در بحث مقیاس‌پذیری از دیدگاه یکی از خبرگان «باید مشخص گردد که به لحاظ زمانی یك پیام تا چه اندازه روی زنجیره‌بلوکي می‌ماند تا تأیید شود. درصورتی‌که هم‌زمانی

جدول ۵. نظرسنجی خبرگان زنجیره قالبی

در مدل پیشنهادی ————————		گزینه استخراجی از MAXQDA	درصد هر گزینه
فنی	قراردادهای هوشمند و خط‌مشی‌ها از استاندارد طراحی فرایندها بهره می‌گیرند.	تأیید می‌شود	۴۰
		تأیید نمی‌شود اما ضرورت دارد	۲۰
		عدم اظهارنظر	۴۰
	مکانیزم اجماع با نیازهای امنیت و عملکرد هماهنگ است	تأیید می‌شود	۸۰
		تأیید نمی‌شود اما ضرورت دارد	۲۰
	رمزنگاری و الگوریتم درهم‌سازی به امنیت و صحت کمک می‌کند.	تأیید می‌شود	۱۰۰
	وضعیت نهائی تراکنش مشخص می‌گردد.	تأیید می‌شود	۸۰
		تأیید نمی‌شود اما ضرورت دارد	۲۰
	داده‌های حساس در شبکه به‌درستی پردازش و ذخیره می‌شوند.	تأیید می‌شود	۱۰۰
سازمانی	سازگاری با سیستم‌های سنتی وجود دارد.	تأیید می‌شود	۲۰
		تأیید نمی‌شود اما ضرورت ندارد	۸۰
	مدیریت و ذخیره داده به طور امن تضمین می‌شود.	تأیید می‌شود	۱۰۰
	مکانیزم‌های مدیریت هویت و کنترل دسترسی از دسترسی غیرمجاز به شبکه جلوگیری می‌کنند.	تأیید می‌شود	۱۰۰
محیطی	قوانین به‌درستی نمایش داده می‌شوند.	تأیید می‌شود	۴۰
		عدم اظهارنظر	۶۰
	منطق تراکنش به‌درستی قوانین تعریف شده را اجرا می‌کند.	تأیید می‌شود	۴۰
		عدم اظهارنظر	۶۰
	افزایش حجم تراکنش‌ها مقیاس‌پذیر است.	تأیید می‌شود	۴۰
		تأیید نمی‌شود اما ضرورت ندارد	۲۰
		تأیید نمی‌شود اما ضرورت دارد	۴۰

تراکنش‌ها رخ دهد فرایند تأیید به چه شکل می‌باشد. در مقیاس‌پذیری علاوه بر تعداد فاکتور زمان نیز حائز اهمیت می‌باشد.»

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2025, Volume 23, Number 1 (pp. 45–63)
https://monadi.isc.org.ir

A secure and privacy-preserving electronic invoice based on blockchain technology

Vahideh Ghanooni Shishavan [1], Shaban Elahi [2,*], Sadegh Dorri Nogoorani [3] and Ali Yazdian Varjani [4]

[1] *Department of Information Technology Management, Faculty of Management and Economics, Tarbiat Modares University, Tehran, Iran*
[2] *Department of Management, Faculty of Administrative Science and Economics, Vali-e-Asr University, Kerman, Iran*
[3] *Department of Computer System Architecture, Faculty of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran*
[4] *Department of Power, Faculty of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: March 02, 2024
Accepted: April 30, 2025
Published Online: May 31, 2025

Keywords:
Electronic invoice, Blockchain technology, Hyperledger fabric

Type: Research paper

The issuance of electronic invoices in the tax system, although a new topic, has not yet been able to fully provide an optimized tax system. Some of the challenges in the tax system include transaction data forgery, the complexity of the invoicing process, and the risks associated with storing data in centralized databases. Blockchain technology, with features such as transparency, resistance to tampering, and decentralization, can be a suitable solution. Ensuring the privacy and security of tax data and maintaining a balance between transparency and confidentiality in tax systems is of utmost importance.

In this paper, a tax system model has been proposed base on a permissioned private blockchain. In this type of blockchain, only validating nodes have access to the information, and data access is restricted. This approach prevents the exposure of confidential information. Our proposed model consists of several processing nodes that are part of the blockchain network. These nodes are responsible for validating transactions and verifying information. In this model, various organizations, including the tax administration, banks, and other entities, connect to the blockchain network via nodes, but the network is not organizationally part of any single entity. Each organization interacts with the network through its own specific processing nodes.

The model includes six layers, explained as follows:

1) **Network Layer:** This layer consists of processing nodes that represent various organizations (e.g., the tax administration, banks, tax payers, chambers of commerce, and official accountants). These nodes are responsible for validating transactions and maintaining the distributed ledger. The network generally includes organizations, processing nodes, and users.
2) **Protocol Layer:** This layer manages transaction processes, consensus, and data storage. Here, sales transactions are recorded, and the global state is maintained in the distributed ledger. Consensus in this model is achieved through the Raft algorithm, which is resistant to potential failures.

* Corresponding author
Email addresses: vahideh.ghanooni@modares.ac.ir (Vahideh Ghanooni Shishavan), elahi@vru.ac.ir (Shaban Elahi), dorri@modares.ac.ir (Sadegh Dorri Nogoorani), yazdian@modares.ac.ir (Ali Yazdian Varjani)
© 2025 ISC. All rights reserved.

3) **Privacy Layer:** Private data is isolated and stored in different channels to prevent unauthorized access. For each transaction, data related to goods and services, exemptions, and liabilities are stored in private datasets. These data are only accessible by authorized processing nodes.
4) **Governance Layer:** This layer is responsible for managing electronic certificates and network security. Security is ensured through a certificate authority, public and private keys, and access control mechanisms. Additionally, identity management and member access control within the network are handled in this layer.
5) **Integration Layer:** This layer uses tools like gRPC and Oracles to communicate with external systems. Events are recorded and sent to other network members, and the necessary data for completing transactions is supplied through Oracles.
6) **Application Layer:** This layer consists of applications that provide a user interface for interacting with the blockchain. These applications connect to smart contracts and other blockchain components through a Software Development Kit (SDK).

The model has been evaluated from four perspectives:

(1) Qualitative Evaluation: Experts in various fields have reviewed the model.
(2) Technical perspective: the model ensures data security through consensus protocols and digital certificates. It also offers better scalability due to the use of a private blockchain.
(3) Organizational Perspective: The model is compatible with traditional systems and can be easily implemented on existing infrastructures.
(4) Environmental Perspective: Some challenges, such as coordination with tax laws and processes, require attention.

From a security perspective, three main aspects have been examined:

(1) Confidentiality: This is ensured by storing data in the private blockchain, identity verification through digital certificates, and appropriate access control.
(2) Data Integrity: This is guaranteed through the consensus protocol and the recording of transactions via smart contracts.
(3) Availability: This is maintained by designing a distributed network that is resilient to node failures. Regarding the efficiency of the proposed model, it is suitable for large-scale and national implementations.

The system continuously records transactions and, compared to traditional systems, places less strain on the infrastructure. Tests have shown that the Raft consensus protocol has low latency and good performance.

Our comparison with previous systems that use public or centralized blockchains shows that our proposed model has more advantages. The most significant benefits are its transparency, security, and scalability. In comparison to other models, this system has successfully addressed challenges related to data forgery and the complexity of the invoicing process.