شرکت خدمات انفورماتیک

برنا
بستر نوین اعتماد

سند تشریحی زیرساخت خدمات بانکی مبتنی بر بلاکچین


بسم الله الرحمن الرحيم

فهرست

خلاصه مدیریتی

در سالیان اخیر، بلاک‌چین به عنوان یک فناوری بنیادی که انقلابی مهم در کسب و کارهای مختلف از جمله صنعت بانکداری بوجود خواهد آورد، توجه همگان را به خود جلب نموده است. پیش‌بینی می‌شود حجم بازار فناوری بلاکچین در صنایع مختلف، تا سال ۲۰۳۰ میلادی، بیش از سه تریلیون دلار باشد که حداقل ۵۲۰ میلیارد دلار آن مرتبط با صنعت بانکی و بیمه خواهد بود. بلاکچین و چالش‌های پیش روی آن، به عنوان یک شمشیر دولبه، فرصت ها و تهدیداتی را متوجه بازیگران فعلی صنعت بانکداری خواهد کرد اما قطعا آن بازیگرانی که نقش جدی در این تغییر بازی بلاکچین بر عهده گیرند، از مزایا و کاربردهای بی‌شمار آن سود خواهند برد.

شرکت خدمات انفورماتیک به عنوان شرکت پیشرو در توسعه فناوری‌های نوین بانکی و هم‌راستا با سیاست‌های راهبردی خود، توسعه زیرساخت مناسب و ارائه خدمات مبتنی بر فناوری بلاک‌چین را در دستور کار خود قرار داده است. بدین منظور یک پلتفرم جامع مبتنی بر بلاک‌چین با نام برنا را برای توسعه خدمات بانکی، طراحی و پیاده سازی کرده است. برنا در حال حاضر خدمات احراز هویت و شناخت مشتریان بصورت بین بانکی، صدور و مدیریت توکن و رمزارز و همچنین حسابرسی را به‌عنوان خدمات پایه ارائه می‌دهد. برنا به شکل یک اکوسیستم باز در اختیار بانک‌ها، شرکت‌های فناور و فعالین صنعت بانکی قرار خواهد گرفت و این اعضا نه تنها قادر خواهند بود در تست و توسعه این پلتفرم مشارکت نموده بلکه می‌توانند هرگونه خدمت بانکی و مالی موردنظر خود را مبتنی بر آن و با استفاده از خدمات پایه پیاده‌سازی کرده و به مشتریان خود ارائه نمایند. با توجه به ماهیت غیرمتمرکز و توزیع‌شده راهکارهای بلاکچینی، موضوع مشارکت جمعی دیگر اعضای اکوسیستم بانکداری در توسعه و بکارگیری برنا، یک الزام فنی، کارکردی و استراتژیک است.

در این گزارش، خلاصه‌ای از چگونگی کارکرد برنا ارائه شده است. در بخش اول به توضیح مفاهیم پایه در حوزه بلاکچین پرداخته شده تا مخاطب با فناوری و مدل‌ذهنی این ساختار آشنا شود. بخش دوم، به معرفی و بررسی کلی برنا از منظر کاربردی و تجاری اختصاص یافته و در بخش نهایی نیز معماری فنی این سیستم تشریح شده است.

بلاکچین

پروتکل اعتماد

بخش ۱

۱-۱ بلاکچین چیست؟

اینترنت تغییرات مثبت زیادی را در شیوه انتقال اطلاعات و قابلیت‌های تجاری به وجود آورده است، اما همچنان نمی‌توان با اطمینان هویت افراد را بدون نیاز به هویت سنجی متمرکز تأیید کرد، پول یا سایر دارایی‌های دیجیتال را بدون به‌کارگیری واسطه‌ای قابل‌اطمینان از یک فرد به فرد دیگر منتقل کرد و یا قراردادها را به‌صورت کاملاً خودکار درآورد. برای حل این مشکل می‌بایست یک روش هویت سنجی غیرمتمرکز را با پروتکلی امن برای انتقال و اشتراک اطلاعات همراه کرد تا نسبت به صحت تراکنش‌های نظارت‌نشده و اطلاعات ثبت‌شده اطمینان حاصل شود.

در سیستم‌های تجاری فعلی، هر جزء پایگاه‌های داده مخصوص به خود را داشته و یا طرفین به نهادی ثالث برای ایجاد اعتماد و هماهنگی مراجعه می‌کنند. بلاکچین پاسخ به مسائل و چالش‌هایی در کسب‌وکار است که در آن شبکه ای از افراد و نهادها به زیرساختی جهت انتقال ارزش و اشتراک اطلاعات نیاز دارند به‌طوری‌که نهادهای مرکزی در نظارت، صحت‌سنجی، ایجاد امنیت و نگهداری اطلاعات آن حاکمیت مطلق نداشته باشند.

نهادهای مرکزی در موارد زیادی به دلیل لزوم وجود یک مرکزیت قانونی در ایجاد اعتماد میان اعضای یک شبکه تجاری شکل‌گرفته‌اند. به‌عنوان‌مثال یکی از نقش‌های بانک‌ها در اقتصاد، ایجاد اعتماد میان افراد و نهادها در انتقال پول است، به‌طوری‌که از مسئله دوپرداختی جلوگیری شده و امنیت دارایی‌ها نیز حفظ شود. بلاکچین، راهکاری فنّاورانه برای حل مسئله اعتماد است به‌طوری‌که اعتماد نه ناشی از اختیارات و مسئولیت‌های قانونی یک نهاد مرکزی، بلکه نتیجه ایجاد پروتکل‌های ارتباطی است که امکان و انگیزه خرابکاری را به حداقل می‌رساند. به عبارتی، بلاکچین پروتکل اعتماد است.

بلاکچین معماری جدیدی برای مدیریت پایگاه داده و انجام تراکنش‌های اطلاعاتی بر روی داده‌هایی است که مالکیت آن‌ها و یا اثبات صحت ثبت آن‌ها ارزش اقتصادی دارد. (مانند دارایی‌های دیجیتال و یا اسناد مختلف زنجیره تأمین یک کسب‌وکار).

بلاکچین راهکاری برای ثبت دائمی و غیرقابل تغییر اطلاعات به‌صورت توزیع‌شده، نگهداری غیرمتمرکز اطلاعات و انتقال بدون واسطه آن است.

بلاکچین از پیوند چند راهکار و نوآوری فناورانه دیگر به وجود آمده است:

- پروتکل‌های شبکه‌های همتا به همتا، معماری توزیع‌شده سیستم‌های اطلاعاتی و پایگاه‌های داده
- الگوریتم‌های اجماع جهت اصالت‌سنجی، پردازش و ثبت توزیع‌شده اطلاعات
- رمزنگاری نامتقارن (سیستم کلید عمومی و امضای دیجیتال)

برای آنکه بتوان بلاکچین را به‌عنوان راهکار احتمالی مناسبی برای حل مسائل کسب‌وکار در نظر گرفت، باید مجموعه‌ای از ویژگی‌ها و شرایط در مسئله وجود داشته باشد:

شبکه تجاری

بلاکچین زمانی به‌عنوان یک راهکار معنا پیدا می‌کند که مجموعه‌ای از افراد و سازمان‌ها بخواهند یک فرآیند تجاری مشترک را مدیریت کنند.

چالش اعتماد

اعتماد کامل میان همه اعضا وجود نداشته باشد. ممکن است در یک شبکه تجاری وضعیت نبود مطلق اطمینان حاکم باشد و یا سطحی از اعتماد (و نه اطمینان کامل) میان اعضا وجود داشته باشد

پایگاه داده مشترک

انجام فرآیندهای تجاری در این شبکه در شرایط عدم اطمینان کامل مستلزم وجود یک پایگاه داده مشترک و غیرانحصاری بین اعضا باشد.

ثبت دائمی و بدون تغییر اطلاعات

تغییرناپذیری و اطمینان از ثبت دائمی اطلاعات در پایگاه داده مشترک دغدغه اعضای شبکه تجاری باشد.

ارتباط مستقیم اعضا بدون واسطه

واسطه زدایی و ارتباط مستقیم اعضا از لحاظ تجاری خلق ارزش کرده و یا موجب صرفه‌جویی اقتصادی شود.

ارزش تجاری

اطلاعات به اشتراک گذاشته شده و منتقل شده ارزش تجاری و اقتصادی داشته باشند.

موارد کاربرد فناوری بلاکچین را می‌توان به سه گروه تقسیم کرد:

۱
ثبت و نگهداری اطلاعات ثابتی که معمولاً مالکیت آن‌ها معامله نمی‌شود

۲
ثبت و نگهداری اطلاعات قابل معامله.

۳
خودکارسازی فرآیندها و قراردادهای تجاری

ثبت و نگهداری اطلاعات ثابت

ثبت دائمی

پایگاه داده توزیع‌شده برای نگهداری اطلاعات مرجع

مثال

- ثبت پتنت و حق مالکیت معنوی
- ثبت مبدأ و اصل دارایی ها و کالا

هویت

پایگاه داده توزیع‌شده از اطلاعات هویتی

مثال

- شناخت مشتری
- رأی‌گیری
- هویت‌دیجیتال

ثبت و نگه‌داری اطلاعات قابل معامله

ثبت تغییرات اطلاعات

پایگاه داده توزیع شده برای ثبت تغییرات و انتقال مالکیت دارایی‌ها در بستر دیجیتال

مثال

- مدیریت زنجیره تأمین

زیرساخت پرداخت

پایگاه داده توزیع شده برای ثبت اطلاعات تراکنش های مالی و پرداخت‌های مبتنی بر رمزارز

مثال

- تسویه‌بین‌بانکی پرداخت‌های فرامرزی
- پیگیری

قراردادها

قراردادهای هوشمند

مجموعه‌ای از اصول و شرایط تجاری که در قالب یک برنامه در پایگاه داده توزیع‌شده ثبت شده و می‌تواند به عنوان راهکار خودکارسازی اجرای قراردادهای تجاری استفاده شود.

مثال

- جبران خسارت بیمه
- تسویه‌معاملات بورسی

ترکیبی

راهکارهایی که ثبت و نگهداری اطلاعات استاتیک، اطلاعات قابل معامله و قراردادهای هوشمند را در کنار هم دارد

مثال

- ارائه زیرساخت بلاکچینی
- عرضه اولیه توکن

۲-۱ انواع راهکارهای بلاکچینی

یکی از مفیدترین تقسیم‌بندی‌ها برای فهم و طراحی بهتر راهکارهای مبتنی بر بلاکچین، توجه به دو عامل حق مالکیت زیرساخت داده (یا همان حق عضویت در شبکه) و حق ثبت اطلاعات در بلاکچین است.

بر اساس حق مالکیت زیرساخت داده، راهکارهای بلاکچینی را به دو گروه عمومی و خصوصی تقسیم‌بندی می‌کنند. در بلاکچین‌های عمومی، سرورهای نگهداری اطلاعات عمومی است و درنتیجه هرکسی می‌تواند عضو شبکه شده و تأمین کننده زیرساخت شود و به اطلاعات بلاکچین دسترسی داشته باشد. در بلاکچین‌های خصوصی، اطلاعات بر روی سرورهای خصوصی نگهداری می‌شوند و دسترسی به اطلاعات بلاکچین منوط به داشتن صلاحیت عضویت در شبکه خصوصی آن بلاکچین است.

بر اساس حق ثبت اطلاعات در بلاکچین، راهکارهای بلاکچینی به دو گروه بدون نیاز به مجوز و نیازمند مجوز تقسیم می‌کنند. در بلاکچین‌های بدون نیاز به مجوز، هرکسی که در شبکه آن بلاکچین عضو باشد، حق پردازش و ثبت اطلاعات را دارد. در بلاکچین‌های نیازمند مجوز، حق ثبت اطلاعات محدود به اعضای دارای مجوز بوده و سایر اعضا تنها می‌توانند اطلاعات را مشاهده کنند.

	بدون نیاز به مجوز	نیازمندمجوز
عمومی	• هرکسی حق عضویت در شبکه را داشته و می‌تواند اطلاعات را از روی بلاکچین بخواند و یا اطلاعات جدید را بر روی بلاکچین ثبت کند • بر روی سرورهای عمومی نگهداری می‌شود. • اعضا به‌صورت ناشناس در شبکه حضور دارند.	• هرکسی حق عضویت در شبکه و خواندن اطلاعات را دارد. تنها اعضای شناخته‌شده و دارای صلاحیت می‌توانند اطلاعات جدید را بر روی بلاکچین ثبت کنند.
خصوصی	• تنها اعضای صلاحیت‌سنجی‌شده می‌توانند عضو شبکه شوند. • هر عضو شبکه حق دسترسی به اطلاعات و ثبت اطلاعات جدید را دارد. • اطلاعات بر روی سرورهای خصوصی نگهداری می‌شود.	• تنها اعضای صلاحیت‌سنجی‌شده حق میتوانند عضو شبکه شوند. • همه اعضای شبکه حق مشاهده اطلاعات بلاکچین را دارند، اما تنها اعضای خاصی با مجوز ویژه حق ثبت و پردازش اطلاعات را داشته و سطوح دسترسی مختلف تعریف میشود.

بلاکچین به معنای حذف کامل واسطه‌ها، ناشناخته بودن اعضا و نبود هرگونه اعتماد میان اعضا نیست. گرچه در بیت‌کوین به‌عنوان اولین مورد کاربرد بلاکچین و معروف‌ترین آن‌ها تمامی این شرایط وجود دارد، اما در بسیاری از موقعیت‌های تجاری و موارد کاربرد عملیاتی راهکارهای بلاکچینی، آنچه بیش از همه موردتوجه قرارگرفته، راهکارهای خصوصی و نیازمند مجوز است. در چنین راهکارهای به دلیل شناس بودن اعضای شبکه و مشخص بودن اعضای دارای حق ثبت اطلاعات، ضمن غیرمتمرکز بودن محل‌های ثبت و نگهداری اطلاعات، امنیت و اعتماد با مکانیسم‌های ساده‌تری به‌دست‌آمده و حریم شخصی نیز به دلیل وجود سطوح دسترسی حفظ خواهد شد.

۱-۳ رمزارز و توکن‌های رمزنگاری‌شده

فناوری بلاکچین با محصولی به نام بیت‌کوین به دنیا معرفی شد. رمزارزها، پول‌های دیجیتالی هستند که ایجاد، مالکیت و انتقال آن‌ها بر بستر بلاکچین بوده و ماهیت آن‌ها با راهکارهای رمزنگاری همراه شده است، به همین دلیل به آن‌ها رمزارز، به معنای ارزهای رمزنگاری‌شده می‌گویند. شیوه خاص مالکیت و تراکنش رمزارزها، آن‌ها را از سایر انواع پول دیجیتال متمایز می‌کند.

انواع مختلفی از رمزارزها وجود دارد که مهم‌ترین تفاوت آن‌ها در شیوه خلق پول و بستر کاربردی آن‌هاست. بیتکوین به عنوان یک رمزارز کاملاً غیرمتمرکز بر بستر بلاکچین بیت‌کوین خلق، نگهداری و منتقل می‌شود. خلق پول در بیتکوین بدون وجود یک نهاد مرکزی و تنها بر اساس مشارکت افراد مختلف در تأمین توان پردازشی شبکه صورت می‌گیرد که به آن عملیات استخراج[1] می‌گویند. سمت دیگر طیف رمزارزها، رمزارزهای بانک مرکزی هستند. رمزارزهای بانک مرکزی معادل پول قانونی (فیات) بوده و خلق آن توسط بانک مرکزی و مطابق با سیاستهای پولی کشور بوده و تنها بستر نگهداری و انتقال آن به زیرساختی بلاکچین تبدیل شده است.

علاوه بر موضوع پول، به‌طورکلی می‌توان هر دارایی را با ایجاد توکن رمزنگاری‌شده در قالب دیجیتال درآورده و آن را بر بستر بلاکچین، نگهداری و منتقل کرد. به عبارتی رمزارز، یک نوع از توکن‌های رمزنگاری‌شده است که با هدف کارکرد پولی ایجاد می‌شوند. به فرآیند ایجاد توکن و خلق دارایی دیجیتال در شبکه بلاکچینی، اصطلاحاً توکنیزه کردن[2] می‌گویند. ایجاد توکن در راهکارهای مختلف بلاکچینی کارکردهای متفاوتی دارد. دیجیتالی کردن دارایی‌ها، ایجاد سیستم پرداخت درون برنامه‌ای و تأمین مالی پروژه‌ها ازجمله مهم‌ترین دلایل ایجاد توکن رمزنگاری‌شده در پروژه‌های بلاکچینی هستند.

[1] Mining

[2] Tokenization

برنا

بستر نوین اعتماد

بخش ۲

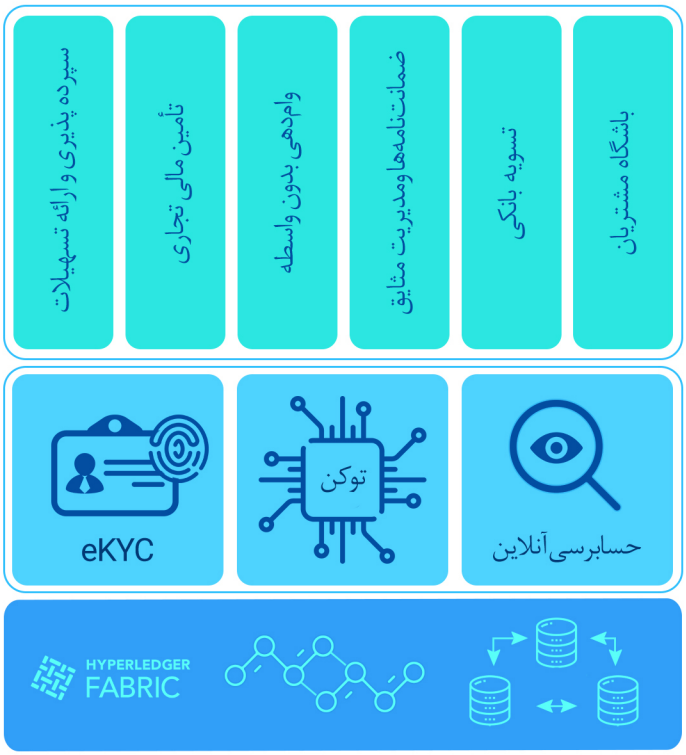
۲-۱ معرفی برنا

شرکت خدمات انفورماتیک در تابستان سال ۱۳۹۷ مدل مفهومی زیرساخت انتقال مالی ایران بر بستر بلاکچین موسوم به رمزارز بانک مرکزی را طراحی و آزمایش کرد. گام بعدی در این پروژه، همکاری با سایر بانک‌ها و نهادهای مالی در جهت گسترش خدمات مالی و بانکی است. نتیجه این تلاش‌ها ایجاد زیرساختی بلاکچینی برای یکپارچه‌سازی، استانداردسازی و کاهش هزینه‌های توسعه راهکارهای بلاکچینی در صنعت بانکداری ایران است که با عنوان برنا، بستر نوین اعتماد معرفی میشود.

طراحان اولیه برنا استفاده از راهکارهای توزیع اجماع را به‌عنوان بستری برای ایجاد شفافیت و کارآمدی در جهت بازآفرینی نظام اقتصادی و توسعه همه‌جانبه ایران دیجیتال حیاتی می‌بینند. بااین‌حال توسعه زیرساخت‌های مبتنی بر فناوری بلاکچین نیز چالش‌های بسیاری در خود دارد که می‌تواند انطباق نظام بانکی و سایر دستگاه‌های کشور را با این انقلاب فناوری به تأخیر بیندازد.

عدم وجود استانداردهای مشترک، هزینه‌های بالای توسعه سرویس‌ها از پایه، نبود نمونه‌های اجرایی موفق و قابل‌اتکا، چالش‌های مرتبط با رگولاتوری، عدم امکان حضور مؤثر فین‌تک‌ها و درنهایت رقابت غیر سازنده ازجمله چالش‌های شناسایی‌شده‌ای است که ضرورت توسعه راهکاری برای پوشش تمامی این چالش‌ها را ضروری می‌کند.

هدف اصلی برنا فراهم کردن زیرساخت بلاکچینی باز، مشترک، منصفانه و قابل توسعه برای بانک‌ها و دیگر نهادهای مالی کشور است تا بدون نیاز به صرف هزینه‌های هنگفت، جهت توسعه محصولات از ابتدا و بدون داشتن دغدغه در مورد استاندارد سرویس‌های بلاکچینی خود در ارتباط با دیگر نهادها، بتوانند سرویس‌های خود را توسعه دهند و با سایر شرکا در ارتباط باشند.



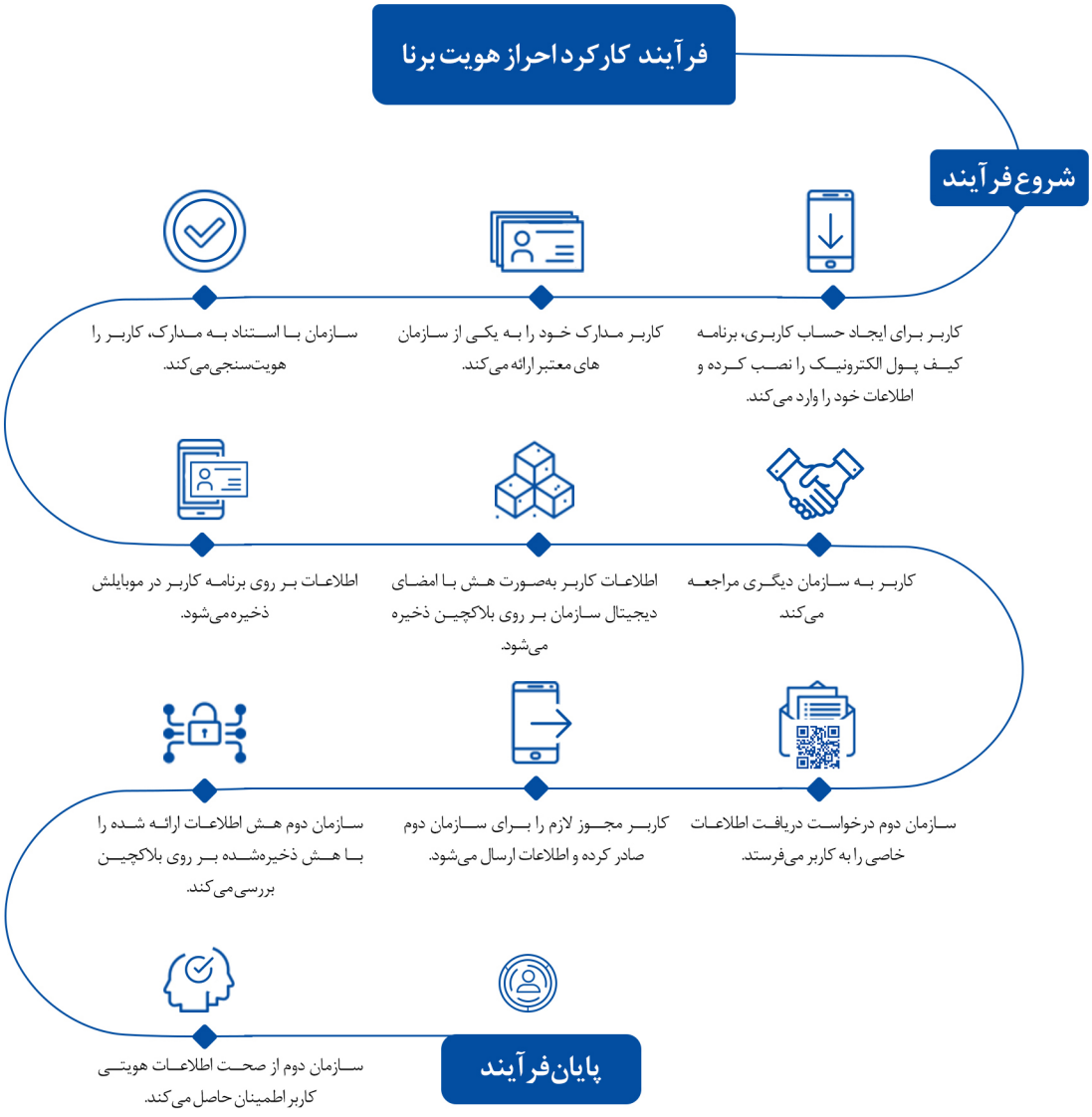
خدمات اختصاصی رقابتی

خدمات پایه مشترک مبتنی بر تعامل

زیرساخت

برنا از سه سطح اصلی تشکیل شده است. در پایین‌ترین سطح، زیرساختبلاکچین قرار دارد. این زیرساخت بر روی پلتفرم متن‌باز بلاکچینی هایپرلجر فبریک[1] که توسط بنیاد لینوکس و شرکت IBM معرفی شده است توسعه داده شده است. پایگاه‌های داده توزیع‌شده و گره‌های تأییدکننده اطلاعات در این سطح قرار دارند.

سطح میانی سطحی مشترک است که خدمات ارائه شده در آن مبتنی بر مشارکت بدون رقابت است. در این سطح، خدمات پایه‌ای ارائه می‌شود که مبنای توسعه سایر محصولات بلاکچینی خواهند بود. این خدمات دو ویژگی مهم دارند، اول آنکه تقریباً در تمامی کاربردهای بلاکچینی به نوعی به این خدمات نیاز است. ثانیاً، کارآمدی این خدمات نیازمند تعامل در بین بازیگران است و نه رقابت بین آن‌ها. این سطح مانند یک سیستم‌عامل بلاکچینی برای بازیگران بانکی است که می‌توانند با استفاده از ابزارهای پایه‌ای محصولات اختصاصی خودشان را به‌سادگی و بدون داشتن دغدغه در مورد ارتباط‌پذیری محصولشان با دیگر محصولات بلاکچینی توسعه دهند. عملیات شناخت مشتری، انتشار توکن و حسابرسی ازجمله این سرویس‌هاست.



[1]Hyperledger Fabric

در بالاترین سطح فضای ارائه خدمات کاملاً رقابتی است و تمام بازیگران بانکی، دیگر صنایع و حتی فینتک‌ها می‌توانند سرویس‌های اختصاصی خود را به‌سادگی با استفاده از امکانات و خدمات دو سطح دیگر توسعه داده و مجموعه خدمات یکپارچه‌ای را به برنا اضافه کنند. این سطح مانند یک پلتفرم توسعه و عرضه برای سرویس‌های مالی بلاکچینی خواهد بود که بانک‌ها می‌توانند از محصولات و سرویس‌های بلاکچینی عرضه‌شده توسط بازیگران مختلف و حتی استارت‌آپ‌ها در قالب اپلیکیشن‌ها استفاده کنند.

بدین ترتیب برنا توازنی مؤثر میان همکاری و رقابت را ایجاد کرده است و استفاده‌کنندگان برنا خود توسعه‌دهندگان آن نیز هستند.

نظام مالی برنا بر اساس پرداخت در ازای خدمت طراحی شده است. هر بازیگری برای آنچه فراهم می‌کند (سرویس، داده، زیرساخت و ...) از بازیگرانی که از آن استفاده می‌کنند کارمزد دریافت خواهند کرد. هیچ محدودیت خاصی برای توسعه سرویس‌های جدید و یا مشارکت در تأمین زیرساخت برای بازیگران وجود نخواهد داشت. تمام آنچه باید رعایت شود استانداردهای مشترک و قوانین بانک مرکزی و دیگر نهادهای رگولاتور است.

برنا شفافیتی مثال‌زدنی را در اختیار نهادهای ناظر و رگولاتورها قرار می‌دهد. در حال حاضر بخش مهمی از نظارت‌ها به صورت آفلاین است. به این معنی که اگر بانک یا موسسه‌ای تخطی از قوانین داشته باشد ممکن است مدت‌ها طول بکشد تا بانک مرکزی متوجه این نقض قانون شود و واکنش نشان دهد. در برنا نظارت آفلاین جای خود را به حکمرانی آنلاین داده است.

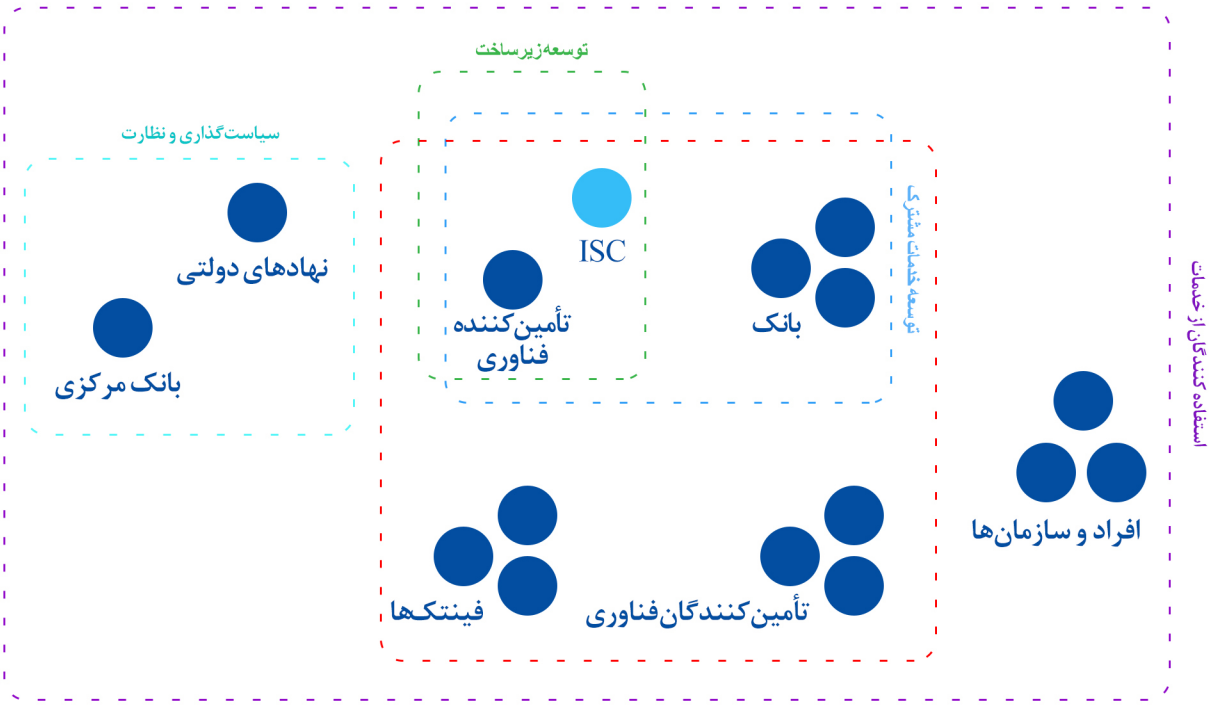
برنا رگولاتور را مجهز به قابلیت بخش‌نامه‌های هوشمند می‌کند. قواعد و دستورالعمل‌های بانک مرکزی به‌جای انتشار از طریق بخش‌نامه‌ها در قالب کد و به‌عنوان سیاست‌های شبکه برنا وارد آن می‌شود و با استفاده از مفهوم قراردادهای هوشمند در تمام شبکه جاری شده و اجازه انجام رفتارهای خارج از ضوابط را نمی‌دهد. در آینده نزدیک، نهادهای دیگر همچون سازمان امور مالیاتی، بازرسی کل کشور و دیگر نهادهای ناظر هم می‌توانند از قابلیت‌های این بستر استفاده کنند.

توسعه مالی کشور بدون حضور پرقدرت فینتک‌ها ممکن نیست؛ اما راهکارهای سازمانی بلاکچینی عموماً به‌قدری وسیع هستند که امکان توسعه آن توسط شرکت‌های کوچک ممکن نیست. برنا زیرساختی قدرتمند برای ورود فین‌تک‌ها به این بازار ایجاد کرده است. فین‌تک‌ها می‌توانند بدون محدودیت از ابزارهای شناسایی مشتریان استفاده کنند. هیچ‌یک از بازیگران بزرگ نمی‌توانند حتی یک استارت‌آپ نوپا را از دسترسی به اطلاعاتی منع کند که مشتری به‌عنوان مالک اطلاعات تمایل به اشتراک آن اطلاعات دارد. برنا آغاز تحقق استانداردهای PSD۲ در ایران خواهد بود. دسترسی به این قابلیت‌ها هیچ هزینه خاصی نخواهد داشت و یک فین‌تک مانند سایر اعضا تنها بر اساس خدماتی که دریافت می‌کند پرداخت خواهد داشت تا شروع تجارت برای آن‌ها ساده، سریع و کم‌هزینه باشد.

برنا بستر نوین اعتماد در نظام مالی ایران است. نظامی که شفاف‌تر، سالم‌تر، کارآمدتر و در خدمت توده‌های مردم خواهد بود.

۲-۲ بازیگران کلیدی: برنا، اکوسیستمی شامل همه و برای همه

برنا پلتفرمی باز است که به بازیگران مختلف اجازه توسعه کاربردها و استفاده از زیرساخت‌ها را می‌دهد. گروه‌های مختلف بازیگران هر یک نقش‌های متعددی در برنا بر عهده دارند تا اکوسیستم آن بتواند با در نظر گرفتن ملاحظات قانونی و امنیتی بالاترین بازدهی و بهترین تجربه کاربری را در اختیار قرار دهد.



بازیگر	نقش
بانک مرکزی	• خلق نقدینگی مرتبط با ریال • مجوزدهی و تعریف چارچوب‌ها و مدیریت انتشار دارایی‌های دیگر مرتبط با بانک مرکزی همچون اوراق مشارکت • تعریف سیاست‌های مربوط به چارچوب‌های قانونی بر روی شبکه
برنا	• ترویج برنا بین بازیگران مختلف • توسعه و نگهداری زیرساخت‌های پلتفرم • توسعه سرویس‌های پایه و عمومی • مجوزدهی، تأیید و مدیریت بازیگران اصلی به‌خصوص دارندگان دفاتر اطلاعاتی و تأییدکنندگان تراکنش‌ها • تعریف سیاست‌های مربوط به زیرساخت بر روی شبکه

بازیگر	نقش
نهادهای دولتی	• دریافت گزارش‌های موردنظر در چارچوب قانون و رعایت حریم شخصی در مورد تراکنش‌ها
بانک‌ها و مؤسسات مالی	• ثبت‌نام و احراز هویت استفاده‌کنندگان • تأمین سرویس احراز هویت برای دیگر بازیگران • متولی و نگهبان دفتر توزیع‌شده • خدمت‌رسانی به‌عنوان تأییدکننده تراکنش‌ها و دریافت کارمزد • تعریف و ارائه خدمات بانکی و دیگر خدمات ارزش‌افزوده بر روی پلتفرم مانند سپرده بانکی
تأمین‌کنندگان فناوری	• توسعه سرویس‌های موردنظر بانک‌ها و شرکت‌ها بر روی برنا • ارائه خدمات زیرساختی و به‌عنوان خدمت به بازیگران
فینتک‌ها	• تعریف و ارائه سرویس‌های فین‌تک بر روی پلتفرم به استفاده‌کنندگان • همکاری در تأمین داده‌های مشترک برای دیگر بازیگران
استفاده‌کنندگان (مردم و شرکت ها)	• احراز هویت و دریافت کلید عمومی و خصوصی خود از بانک • استفاده از خدمات مختلف بازیگران برنا در چارچوب قوانین

۲-۳ مزایا و چالش‌های برنا برای بازیگران

	مزایا	چالش ها
بانک مرکزی	**پیشتازی:** استفاده بهنگام از قابلیت‌های فناوری بلاکچین در پلتفرم واکنشی مناسب به تحول انقلابی این فناوری در صنعت مالی است و اجازه می‌دهد تا بانک مرکزی در توسعه‌های آتی این فناوری در کشور و یا در همکاری‌های بین‌المللی نقش راهبردی داشته باشد. **اعمال حاکمیت:** استفاده از قراردادهای هوشمند و کد کردن روال‌ها و مقررات کمک می‌کند تا حرکت از نظارت آفلاین به اعمال حاکمیت آنلاین عملی شود و بانک مرکزی بتواند راهکار گزارش‌گیری مؤثری را در اختیار داشته باشد.	**استانداردسازی:** راهکارهای مبتنی بر بلاکچین و سرویس‌های قابل تعریف بر پلتفرم برنا نیازمند تعریف استانداردها و چارچوب‌های جدیدی هستند. بانک مرکزی باید روال و حدود تعاملات، همکاری‌ها و همچنین چارچوب‌های مربوط به حفاظت از حریم شخصی و مشروعیت قراردادهای هوشمند را برای بانک‌ها تعریف کند.

	مزایا	چالش ها
نهادهای دولتی	**سهولت در بازرسی و کشف جرم:** شفافیت و قابل رشد بودن تراکنش‌ها و تعاملات در پلتفرم، نظارت بر رفتارها، کشف و پیگیری جرائم را ساده تر می‌کند. **یکپارچگی:** ثبت اطلاعات در یک دفتر مشترک و عدم امکان بروز مغایرت و ایجاد یکپارچگی کاملی از داده‌ها را در اختیار قرار می‌دهد. به‌علاوه پلتفرم ضمانت حاصل می‌کند تا روال‌ها در مورد تمامی افراد حقیقی و حقوقی به‌طور یکسان طی شوند و از بدخوانی مقررات و یا تبعیض جلوگیری می‌کند.	**آموزش:** بدنه بزرگ سازمان‌های مختلف باید برای استفاده از قابلیت‌های نظارتی زیرساخت های جدید آموزش ببینند. **تطبیق:** سیستم‌های نرم‌افزاری مختلف فعلی سازمان‌ها برای استفاده حداکثری از راهکارهای گزارش‌گیری برنا باید به‌روزرسانی شوند.
بانک‌ها و مؤسسات مالی	**مدل‌های جدید درآمدی:** سرویس‌های جدیدی که به‌واسطه زیرساخت‌های مبتنی بر بلاکچین عملی و با به‌صرفه می‌شوند جریان‌های جدید درآمدی برای بانک‌ها به همراه خواهد داشت. **صرفه‌جویی:** صرفه‌جویی ناشی از همکاری‌های بین‌بانکی و همچنین کاهش هزینه‌های زیرساختی نسبت به راهکارهای فعلی هزینه‌های بانک‌ها را به‌طور قابل‌ملاحظه‌ای کاهش خواهد داد. **کاهش تخلفات:** مزایایی همچون شفافیت و عدم امکان دست‌کاری اطلاعات موجب کاهش هزینه های تحمیلی ناشی از تخلفات نظیر جعل می شود.	**توسعه زیرساخت‌ها:** استفاده از قابلیت‌های فناوری بلاکچین نیازمند توسعه زیرساخت‌ها و محصولات جدیدی است که هزینه‌های نرم افزاری بانک‌ها را در کوتاه‌مدت افزایش خواهد داد.
شرکت‌های نرم‌افزاری بانکی	**بازار جدید:** محصولات و سرویس‌های متنوع و جدیدی که بانک‌ها و مؤسسات مالی بر روی پلتفرم تعریف خواهند کرد بازار کار جدید و گسترده‌ای را برای شرکت‌های بزرگ نرم‌افزاری پدید خواهد آورد.	**عدم بلوغ:** عدم وجود نمونه‌های موفق و همچنین سرویس‌های با طول عمر بالا و پایدار شده در جهان، توسعه سرویس‌ها را برای شرکت های نرم‌افزاری پرهزینه‌تر و مدیریت ریسک را سخت‌تر می‌کند. **کمبود نیروی انسانی:** کمبود زیاد نیروی انسانی مجرب و آشنا با پلتفرم‌های بلاکچینی توسعه سرویس‌های مبتنی بر برنا را برای شرکت‌ها سخت‌تر خواهد کرد.

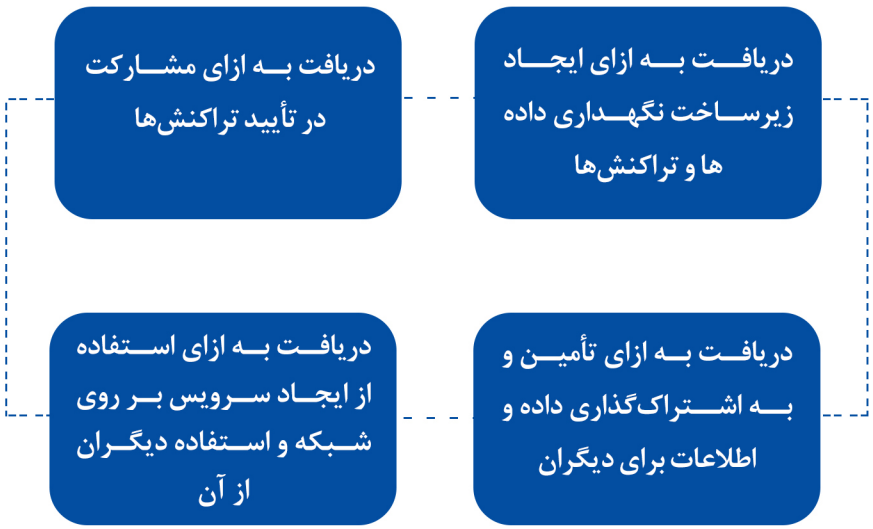
	مزایا	چالش ها
استارت‌آپ‌ها	**افزایش سرمایه‌گذاری:** وجود پلتفرم امن و تحت مقررات کشور جهت توسعه کاربردهای مالی، موجب افزایش تمایل سرمایه‌گذاری در فناوری بلاکچین و کاربردهای مرتبط با آن خواهد شد. **رقابت منصفانه:** استانداردهای کد شده در پلتفرم مانع از ایجاد انحصار و امتیاز غیرمنصفانه علیه استارت‌آپ‌ها و شرکت‌های نوپا می‌شود.	**کمبود نیروی انسانی:** کمبود زیاد نیروی انسانی مجرب و آشنا با پلتفرم‌های بلاکچینی توسعه سرویس‌های مبتنی بر برنا را برای استارت‌آپ‌ها سخت‌تر خواهد کرد.
استفاده‌کنندگان (مردم و شرکت‌ها)	**گستره وسیع خدمات:** تعداد زیادی خدمات جدید و متنوع بر بستر این پلتفرم در اختیار گروه‌های مختلف از شرکت‌ها و شهروندان قرار خواهد گرفت **کاهش کلاه‌برداری:** ذات شفاف و قابل ردگیری بودن فناوری بلاکچین و همچنین دسترسی به اطلاعات هویتی با کیفیت بالاتر، باعث ایجاد بستر امن پرداختی می‌شود.	**سرقت‌های سایبری:** در اوایل ارائه راهکارهای مبتنی بر بلاکچین و وجود ناآشنایی نسبی مردم و شرکت‌ها با نحوه تأمین امنیت و حریم شخصی در زیرساخت‌های بلاکچینی از طریق نگهداری کلیدهای خصوصی، امکان سرقت‌های سایبری را افزایش می‌دهد.

۲-۴ مدل تجاری برنا: پرداخت به ازای خدمات، دریافت به ازای خدمت

تأمین هزینه‌های توسعه و نگهداری برنا نیازمند تعریف مدل‌های درآمدی متنوع برای نقش‌آفرینان است. باز بودن زیرساخت برنا این امکان را فراهم می‌کند تا تمامی بازیگران در اکوسیستم مالی و بانکی و حتی در آینده، شرکت‌های غیرمالی نیز بتوانند با فراهم کردن زیرساخت، سرویس، داده، خدمات و ... از نگهداری و توسعه این زیرساخت مدل درآمدی پایداری داشته باشند.

در برنا بازیگران امتیاز ویژه‌ای در درآمدزایی نخواهند داشت و در این شبکه اشتراکی هر بازیگر برای استفاده از خدمات دیگران هزینه پرداخت خواهد کرد و در قبال خدماتی که ارائه می‌کند درآمد خواهد داشت؛ بنابراین این‌که چه کسی یا کسانی آغازگر شبکه باشند، در درآمدزایی آینده ایشان امتیاز اصلی نیست و قدرت اصلی در میزان تأمین زیرساخت و خدمات خواهد بود.

درآمدهای بازیگران می‌تواند از طرق زیر حاصل شود:



بازیگران می‌توانند برحسب نیاز خود و یا تقاضای بازار سرویس‌های مختلفی را بر روی برنا توسعه دهند. این سرویسها حتی می‌تواند مشابه باشد (جز چند سرویس عمومی و مشترک که سیاست برنا همکاری همه در توسعه و استفاده از آن است) و عملاً چند بازیگر برای ارائه یک سرویس مبتنی بر بلاکچین بر روی برنا با یکدیگر رقابت داشته باشند؛ بنابراین قیمت خدمات به‌صورت رقابتی مشخص خواهد شد که باعث بهینه شدن هزینه‌های پرداختی میشود.

۵-۲ اصول و اهداف برنا

ردیف	هدف	توضیحات	برنا چه می‌کند؟
۱	**افزایش کارآمدی**	سرویس‌های ارائه‌شده مبتنی بر بلاکچین باید بتواند چالش‌های تکنیکی و تجاری در راهکارهای پیشین را با هزینه‌ای معقول بهبود بخشند	برنا برخی سرویس‌هایی را ارائه می‌کند که تاکنون عملیاتی نشده‌اند و می‌توانند کارآمدی سازمان‌ها را افزایش دهند. در مورد دیگر سرویس‌ها که نمونه مشابه فعلی دارند اراده بازیگران و بررسی توجیه‌پذیری آتی توسط خودشان باعث شکل‌گیری و تجاری شدنشان خواهد بود.

ردیف	هدف	توضیحات	برنا چه می‌کند؟
۱	**افزایش کارآمدی**	سرویس‌های ارائه‌شده مبتنی بر بلاکچین باید بتواند چالش‌های تکنیکی و تجاری در راهکارهای پیشین را با هزینه‌ای معقول بهبود بخشد.	برنا برخی سرویس‌هایی را ارائه می‌کند که تاکنون عملیاتی نشده‌اند و می‌توانند کارآمدی سازمان‌ها را افزایش دهند. در مورد دیگر سرویس‌ها که نمونه مشابه فعلی دارند اراده بازیگران و بررسی توجیه‌پذیری آتی توسط خودشان باعث شکل‌گیری و تجاری شدنشان خواهد بود.
۲	**انطباق‌پذیری**	پلتفرم باید به‌گونه‌ای باشد که استفاده از هر بخش آن نیازمند اعمال کمترین تغییرات در ساختارها و سیستم‌های جاری باشد.	مدل معماری ماژولار برنا این امکان را فراهم می‌کند تا هر بازیگر سرویس موردنظر خود را به زیرساخت‌های فعلی خود بدون نیاز به تغییر خاصی اضافه کند.
۳	**پایداری تجاری**	پلتفرم باید به‌گونه‌ای باشد که تأمین هزینه‌های نگهداری آن از طریق راهکاری پایدار که به پرداخت‌های حاکمیتی و یا قانونی وابستگی نداشته باشد و بتواند در دوران مختلف با راهکاری عملیاتی و البته منصفانه و قابل دفاع هزینه های جاری خود را تأمین کند.	در برنا درآمدها بر اساس سرویس‌دهندگی است. هر بازیگر به میزان زیرساخت، سرویس، داده و ... که برای بازیگران دیگر فراهم می‌کند می‌تواند از آن‌ها کارمزد دریافت کند. اگر کارمزدی منصفانه نباشد همواره امکان توسعه سرویس‌های موازی توسط دیگر بازیگران وجود خواهد داشت.
۴	**هماهنگی با رگولاتور**	پلتفرم باید بتواند قدرت کامل و قابل‌انعطافی برای اعمال نظارت و حاکمیت را در اختیار رگولاتور قرار دهد.	بانک مرکزی گره اصلی در برنا است و می تواند اصول و چارچوب‌ها را برای توسعه سرویس‌ها در قالب کد به شبکه اعمال کند. بانک مرکزی به تمام داده‌هایی که نقض حریم شخصی نباشد به‌صورت برخط دسترسی کامل دارد و می‌تواند ابزارهای گزارش‌گیری اختصاصی خود را برای انواع کاربردها داشته باشد.

ردیف	هدف	توضیحات	برنا چه می‌کند؟
۵	**حداکثرسازی شاخص شفافیت**	پلتفرم باید زمینه را برای گزارش گیری برخط از تمام آنچه منافاتی با حریم شخصی ندارد را در اختیار نهادهای ناظر قرار دهد.	برنا تضمین یکپارچگی و سلامت حداکثری داده را می‌دهد. هر اطلاعاتی که منافاتی با حریم شخصی نداشته باشد برای تمامی سازمان‌های ناظر قابل مشاهده و دسترسی خواهد بود.
۶	**حریم شخصی**	پلتفرم باید به‌گونه‌ای توسعه یابد که در عین توسعه همکاری میان شرکتی داده‌های مصرف‌کنندگان و حریم شخصی آن‌ها کاملاً محفوظ باشد.	مدل معقلب پلتفرم برنا راهکار مدیریت هویت شخصی است. هیچ نهادی نمی‌تواند به داده های مصرف‌کننده جز با دریافت مجوز از خود او و یا دریافت و ثبت مجوز قانونی دریافت شده از محاکم قضایی بر روی شبکه دسترسی داشته باشد. تمام دسترسی‌ها، مجوزها، درخواست‌ها و ... در شبکه برای همیشه ثبت و قابل ارجاع خواهد بود.
۷	**مشتریان در صدر توجه**	سرویس‌های طراحی شده باید مشتریان و افزایش کیفیت زندگی تجاری آن‌ها را بر اساس شاخص های مختلفی همچون هزینه، سرعت و امنیت در اولویت قرار دهد.	در برنا هر بانکی می‌تواند بنا به درکی که از تقاضای مشتری دارد سرویس‌های ویژه خود را توسعه دهد. درعین‌حال تمامی سرویس‌ها ارتباط مناسبی با یکدیگر دارند و مشتری میان سرویس‌های جزیره‌ای گم نخواهد شد. انتقال از هر سرویس به سرویس دیگر و تعامل آن‌ها با یکدیگر سطح جدیدی از خدمت‌دهی را برای مشتریان خلق خواهد کرد.
۸	**حمایت از ثبات اقتصادی**	قابلیت‌ها و سرویس‌های پلتفرم باید شرایط را برای بهبود شاخص هایی که موجب ثبات اقتصادی می‌شود فراهم کنند.	برنا در مورد خلق یا توکنی کردن هر نوع ارزش، استانداردها و چارچوب‌های شفافی دارد که از اقدامات کلاهبردارانه و خارج از چارچوب قانون ممانعت می‌کند.

ردیف	هدف	توضیحات	برنا چه می‌کند؟
۹	**توسعه‌پذیری آتی**	امکان تغییرات و توسعه سریع و کم‌هزینه آتی و اضافه شدن دیگر سرویس‌ها و دیگر نیازمندی‌های احتمالی از اهمیت کلیدی برخوردار است.	برنا یک شبکه باز است که به تمامی بازیگران اجازه می‌دهد تا هر سرویسی که مدنظر دارند را به‌راحتی بر روی سرویس‌های پایه توسعه دهند و تجاری کنند.
۱۰	**توسعه‌منصفانه و رقابت‌پذیری**	پلتفرم باید به‌گونه‌ای باشد که بازیگران در توسعه، به‌کارگیری و درآمدزایی از سرویس‌ها امتیاز انحصاری و غیرمتعارفی نسبت به دیگران نداشته باشند.	هر بانک و در آینده هر استارت‌آپ و شرکتی می‌تواند سرویس موردنظر خود را بدون هیچ محدودیت خاصی بر روی برنا توسعه دهد. سرویس بابت منابع، داده‌ها و یا خدماتی که از سرویس‌های دیگر دریافت می‌کند هزینه می‌پردازد و بابت خدماتی که ارائه می‌دهد درآمد خواهد داشت. مدل‌های قیمت‌گذاری کاملاً رقابتی است و امکان وجود چندین سرویس مشابه با ویژگی‌ها و قیمت‌های متفاوت توسط توسعه‌دهندگان مختلف بر روی برنا وجود دارد.
۱۱	**افزایش امنیت**	پلتفرم باید امنیت تمامی بازیگران و مصرف‌کنندگان را در حدی بسیار بالا تضمین کند.	زیرساخت برنا با توزیع‌شدگی مناسب داده‌ها امنیت داده‌ها را در حد بالایی تضمین می‌کند.
۱۲	**مصالحه اهداف مختلف سازمان‌ها**	پلتفرم باید به شکلی باشد تا برای به حداکثر رساندن اثربخشی تعادل مناسبی بین همکاری و رقابت میان بازیگرانی که به لحاظ تجاری تضاد منافع دارند برقرار کند.	اکوسیستم و معماری برنا به شکلی است که در موارد محدودی که سرویس‌ها کاملاً مشترک و همگانی هستند توسعه به‌صورت همکاری است اما بر روی این سرویس‌های مشترک همگانی هر بازیگری امکان توسعه محصولات اختصاصی و رقابت با دیگر بازیگران را دارد. به‌این‌ترتیب هزینه چندباره برای سرویس‌های مشترک انجام نمی‌شود و درعین‌حال رقابتی فشرده در سطح خدمات به مشتری وجود خواهد داشت.

ردیف	هدف	توضیحات	برنا چه می‌کند؟
۱۳	**تقویت سیاست‌ها و اهداف کلی حاکمیت**	پلتفرم و ویژگی‌ها و قابلیت‌های آن باید بیشترین هماهنگی را با چشم اندازهای حاکمیت در توسعه و شفافیت اقتصادی داشته باشد.	برنا به واسطه زیرساختی قابل ره‌گیری می تواند مسیر جریان‌های مالی را مشخص و با تعریف چارچوب‌هایی منابع حمایتی ویژه، دولت را در مسیر مورد انتظار در جهت افزایش تولید هدایت کند.
۱۴	**هزینه توسعه پایین**	توسعه ابتدایی و آتی پلتفرم باید با به‌صرفه‌ترین روش‌ها انجام شود.	برنا از پلتفرم منبع‌باز هایپرلجر به‌عنوان زیربنای توسعه خود استفاده کرده است که با توجه به اینکه این پلتفرم توسط هزاران نفر در جهان در حال ارتقا هست بسیاری از هزینه های توسعه برنا کم خواهد شد.
۱۵	**انطباق بین‌المللی**	امکان ارتباطات آتی با نهادهای مالی دیگر کشورها باید در پلتفرم وجود داشته باشد.	برنا از معتبرترین پلتفرم توسعه راهکارهای سازمانی مبتنی بر بلاکچین با نام هایپرلجر به عنوان زیرساخت استفاده کرده است. این زیرساخت برای نهادهای مالی در سراسر جهان آشنا و معتبر است. به‌علاوه معماری آن به گونه‌ای است که بیشترین توانایی را برای ارتباط با دیگر پلتفرم‌های بلاکچینی و غیر بلاکچینی در اختیار دارد.

۲-۶ چالش‌ها و فرصت‌های مرتبط با رگولاتوری در برنا

۲-۶-۱ فرصت‌های جدید در مدیریت سیاست‌ها و رگولاتوری

به همان اندازه که بلاکچین‌های عمومی و رمزارزهایی همچون بیت‌کوین برای قانون‌گذاران چالش‌های حقوقی جدید ایجاد کرده‌اند راهبردهای مبتنی بر بلاکچین‌های سازمانی با شفافیتی که ایجاد می‌کنند به‌عنوان یک ابزار قدرتمند در دست رگولاتورها عمل می‌کنند.

بخشی مهمی از طراحی برنا به این موضوع پرداخته است که چگونه این زیرساخت می‌تواند نیازمندی‌های رگولاتور را بهتر پوشش داده و ابزارهای کارآمدتری را نسبت به راهکارهای فعلی برای نظارت و اعمال حاکمیت در اختیار قرار دهد. برخی از مزایای برنا برای رگولاتور عبارت‌اند از:

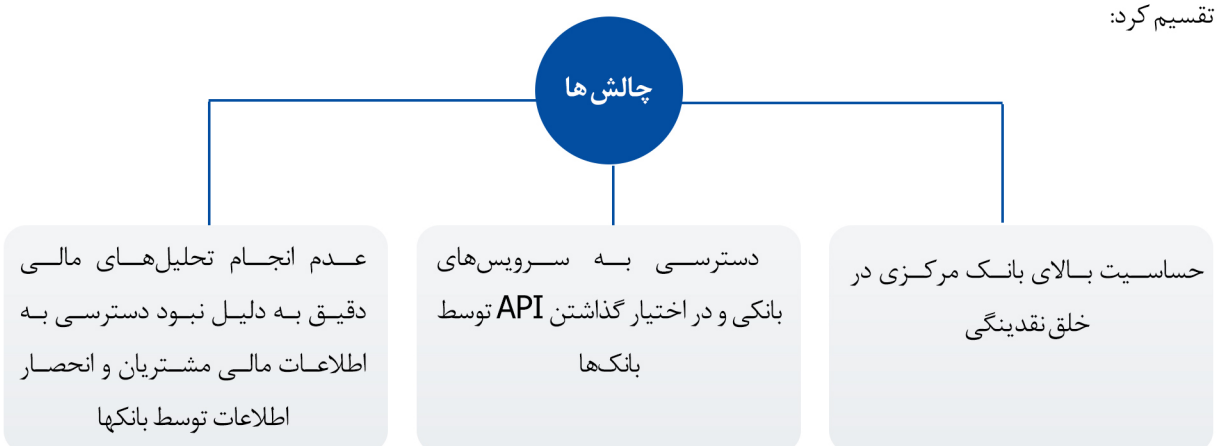
۱. تغییرناپذیری و غیرقابل خدشه بودن اطلاعات: با ثبت اطلاعات توسط بازیگران بر روی برنا، رگولاتور اطمینان پیدا می‌کند که این داده‌ها تحت هیچ شرایطی قابل‌تغییر و دست‌کاری نیستند. این ویژگی ممتاز می‌تواند کیفیت فرایندهای حسابرسی را به طرز چشمگیری افزایش دهد.

۲.ره‌گیری بدون خطا: در برنا سابقه کلیه رویدادها ثبت و ذخیره می‌شوند و بنابراین ره‌گیری یک رویداد و فرایندهای انجام گرفته در آن بسیار ساده است. به‌عنوان‌مثال می‌توان کلیه فرایندهای منجر به صادر شدن یک اعتبار اسنادی را بررسی کرد. رگولاتور به تمامی این اطلاعات (جز مواردی که برای دسترسی به آن نیاز به حکم قضایی باشد) به‌صورت آنلاین دسترسی دارد و در مورد سایر داده‌ها نیز اطمینان دارد که امکان از بین رفتن مسیر فرایند ممکن نیست. این قابلیت فرایند شناسایی خاطی در فرایند کشف تقلب را به مراتب ساده‌تر خواهد کرد.

۳. اعمال حاکمیت آنلاین: تعیین پروتکل‌ها و سیاست‌های شبکه و استفاده از قراردادهای هوشمند می‌توانند به‌عنوان ابزارهای اعمال حاکمیت استفاده شوند. بر این اساس الزامات بانک مرکزی لازم نیست که از طریق بخشنامه به بانک‌ها ارسال شود و به‌جای آن کافی است تغییراتی در پارامترهای یکی از قراردادهای هوشمند ایجاد شود. با این تغییر عملاً بخشنامه به حالت اجرا درمی‌آید و انجام رفتاری خارج از قاعده جدید در شبکه ممکن نیست.

۲-۶-۲ PSD2 و سطح جدید خدمات برای فینتک‌ها

در اکوسیستم استارت‌آپی ایران، در بسیاری از شاخه‌ها، نمونه‌های داخلی شرکت‌های موفق جهان دیده می‌شود که بعضاً توانسته‌اند به موفقیت‌های بزرگی نیز در بازار کشور برسند؛ اما در حوزه فینتک‌ها این آمار چندان مطلوب نیست. به‌غیراز استارت‌آپ‌های حوزه پرداخت، کمتر اپلیکیشن و سرویس مالی توانسته در بازار ایران عرض‌اندام کند. این موضوع بیانگر چالش‌های زیاد در توسعه فین‌تک‌هاست. به‌طورکلی می‌توان این چالش‌ها را به چند دسته تقسیم کرد:



زیرساخت شفاف و قابل نظارت برنا این امکان را فراهم می‌کند تا فینتک‌ها بتوانند بدون مسائل قبلی دسترسی وسیعی به امکانات داشته باشند. برخی از مزایای برنا عبارت‌اند از:

عدم وجود چالش خلق نقدینگی: در صورت تصمیم بر انتشار رمزارز بانک مرکزی بر روی برنا تمامی بازیگران می‌توانند بدون هیچ محدودیتی نسبت به راه‌اندازی کیف پول اقدام کنند. ازآنجاکه دارایی مشتری همواره بر روی بستر برنا قرار دارد امکان خلق نقدینگی مضاعف وجود ندارد و بانک مرکزی به تمامی تراکنش‌ها نظارت خواهد داشت.

عدم وجود چالش شناخت مشتری: استفاده از اطلاعات سیستم بانکی برای شناخت مشتری بدون درخطر افتادن حریم شخصی کاربر یکی از چالش‌های مهمی است که به‌واسطه زیرساخت شناخت مشتری برنا کاملاً حل می‌شود و فینتک ها می‌توانند از سرویس شناخت مشتری کل نظام بانکی بدون از بین رفتن حریم شخصی افراد استفاده کنند.

دریافت داده‌های مشتریان: داده‌های مشتریان تاکنون جزو دارایی‌ها و منبع مزیت رقابتی بانک‌ها محسوب می‌شدند؛ اما مقررات جدید اتحادیه اروپا موسوم به PSD۲ که از ابتدای ۲۰۱۸ اجرایی شده است به اشتراک‌گذاری داده ها را باز می‌کند و اجازه می‌دهد بانک‌ها و فینتک‌ها بهترین و کارآمدترین روش را برای پرداخت‌ها و سایر تراکنش‌های مشتریان برگزینند. این بدان معنی است که بانک‌ها می‌بایست اطلاعات مشتریان خود را به درخواست آنان با دیگر بازیگران دارای مجوز به اشتراک بگذارند. این کاملاً قابل‌درک است که بانک‌ها چندان تمایلی به اشتراک‌گذاری این داده ها با فینتک‌ها نداشته باشند اما این قانون با استناد به اینکه این داده‌ها در حقیقت برای مشتری است و به‌منظور رعایت حقوق مصرف‌کنندگان لازم‌الاجراست. بر بستر برنا فینتک‌ها دارای مجوز می‌توانند به اطلاعات مشتریان با دریافت مجوز از خودشان دسترسی داشته باشند و در صورت عدم امکان دسترسی خسارت دریافت کنند.

توسعه ساده: برنا بسیاری از زیرساخت‌های لازم برای توسعه اپلیکیشن‌ها را در اختیار استارت‌آپ‌ها قرار می‌دهد؛ بنابراین فینتک‌ها می‌توانند صرفاً به طراحی سرویس فکر کنند و در مورد سرویس‌هایی که برای خدمت‌رسانی نیاز دارند نگرانی نداشته باشند.

ورود ساده به بازار: امکان اعمال دستورات و بخش‌نامه‌های بانک مرکزی در قالب سیاست‌های شبکه در برنا، شرایطی را فراهم می‌کند تا فین‌تک‌هایی که بر بستر برنا فعالیت می‌کنند به‌صورت خودکار در چارچوب این مقررات قرار بگیرند. در نسخه کامل‌تر انجام فعالیت بر بستر برنا به‌منزله داشتن مجوز سطح اول فعالیت فین‌تک می‌تواند قلمداد شود.

معماری
و ساختار فنی برنا

بخش ۳

برنا به‌عنوان زیرساخت سیستم مالی مبتنی بر بلاکچین در شبکه‌ای شامل ذی‌نفعان مختلف، یک سامانه فوق کلان مقیاس[1] محسوب می‌شود؛ چراکه فاکتورهای طراحی، کنترل و نظارت همه‌جانبه در این سیستم، در تمام سطوح و در بین تمام بازیگران شبکه به تحلیل دقیق‌تر و آینده‌نگرانه‌تری نسبت به سیستم‌های معمول نیاز دارد. در این بخش ابتدا به معرفی پلتفرم و ابزارهای مورداستفاده در برنا پرداخته شده، پس‌ازآن معماری کلی این سیستم تشریح می‌شود.

۳-۱ معرفی هایپرلجر فبریک

هایپرلجر فَبریک چارچوبی ماژولار و عمومی برای توسعه محصول، راه‌حل و یا نرم‌افزارهایی بر بستر بلاکچین است که در راه‌اندازی زیرساخت‌های بلاکچین سازمانی می‌تواند نقش مهمی ایفا کند. مشخصات اصلی این محصول از ابتدا به نحوی تعیین‌شده‌اند که پاسخگوی نیازمندی‌های استفاده در سازمان‌ها باشد. این نیازمندی‌ها عبارت‌اند از:

شناسایی و تأیید هویت تمامی اعضای شبکه

تأخیر کم در تائید تراکنش‌ها

امنیت بالای شبکه

خصوصی بودن شبکه

بازدهی بالای شبکه در پردازش تراکنش‌ها

حفظ حریم خصوصی کاربران و محرمانه بودن تراکنش‌ها و قراردادهای حساس

ساختار ماژولار

ماژولار بودن فبریک را می‌توان در قابلیت استفاده از الگوریتم‌های مختلف که هریک اهداف متفاوتی را دنبال می کنند، خلاصه کرد. به‌عنوان‌مثال الگوریتم‌های مخصوص پروتکل مدیریت هویت، اجماع و رمزنگاری داده‌ها می‌توانند بنا بر معیارهای طراحی بلاکچین، به شبکه متصل شده و تنظیمات انتخابی آن را شکل دهند. این ویژگی، فبریک را به شبکه‌ای قابل تنظیم، با انطباق‌پذیری بالا با دامنه وسیعی از انتخاب‌های کاربردی برای توسعه‌دهندگان آن تبدیل می‌کند.

[1] Ultra Large Scale System

۳-۱-۱ قابلیت‌های کلیدی طراحی هایپرلجر فبریک

دارایی‌ها: دارایی‌های تعریف‌شده در شبکه می‌توانند شامل هر چیزی باشند که در شبکه تجاری دارای ارزش هستند. این دارایی‌ها در شبکه فبریک به‌صورت مجموعه‌ای از جفت‌های key-value تعریف می‌شوند. این ساختار داده روشی بنیادی برای ارائه اطلاعات در سیستم‌های محاسباتی و نرم‌افزارها است که تغییرات آن در قالب تراکنش در دفتر اعضای شبکه ثبت می‌شود.

قرارداد هوشمند: استفاده از قراردادهای هوشمند در بسیاری از بخش‌های فبریک با اهداف متفاوت به چشم می‌خورد. پارامترهای اصلی شبکه فبریک توسط قراردادهای هوشمند تعریف و تعیین می‌شوند. این قراردادها را «قراردادهای سیستمی» می‌نامند. قراردادهای سیستمی به دو نوع تقسیم می‌شوند: نوع اول «قراردادهای چرخه حیات و پیکربندی» هستند که قوانین شبکه و کانال‌ها را مشخص می‌کنند. نوع دوم «قرارداد تأیید و اعتبارسنجی» است که الزامات تأیید اعتبار تراکنش‌ها را تعریف می‌کند. تعریف دارایی‌ها و ثبت جابجایی آن‌ها هم با استفاده از قرارداد هوشمند انجام می شود. به‌عبارت‌دیگر، توانایی ایجاد هرگونه تغییر در ساختار داده جفت key-value، در اختیار قرارداد هوشمند است. این تغییرات در صورت اضافه کردن دارایی جدید، شامل تعریف جفت key-value جدید شده و در صورت جابجایی دارایی، منجر به تغییر و به‌روزرسانی این ساختار می‌شود.

قابلیت‌های دفتر کل: سابقه کامل تراکنش‌های اعضای شبکه به‌صورت تغییرناپذیر در دفتر کل مشترک آن‌ها ذخیره می‌شود. در ساختار فبریک علاوه بر دفتر کل مشترک شبکه، هریک از کانال‌های ایجادشده نیز دفتر کل مخصوص خود را دارند. تغییرناپذیری سوابق این دفاتر به‌وسیله رمزنگاری و ثبت تراکنش‌ها در قالب بلوک‌های متوالی امکان‌پذیر است. اطلاعات ذخیره‌شده در دفتر کل مشترک اعضای شبکه، به‌جز تاریخچه تراکنش‌ها، حاوی پایگاه داده‌ای است که وضعیت فعلی فبریک در آن ذخیره می‌شود.

حفظ حریم خصوصی: قابلیت همزیستی کسب‌وکارهای رقیب در یک شبکه، از اهداف مهم فبریک است که تنها در صورت حفظ حریم خصوصی امکان‌پذیر است. برای حفظ محرمانگی تراکنش‌های شخصی در این شبکه، کاربران می توانند هم از «کانال‌های خصوصی» و هم از «مجموعه داده‌های خصوصی» استفاده کنند.

نیاز شبکه به این دو قابلیت، در شرایط همکاری کسب‌وکارهای رقابتی و حضور نهادهای نظارتی در کنار یکدیگر بیش از هر موقعیت دیگری احساس می‌شود.

کانال‌ها، مسیرهای خصوصی تبادل پیام هستند که اطلاعات آن‌ها تنها در دسترس اعضای عضو کانال بوده و خارج از دسترس اعضای دیگر شبکه است.

مجموعه داده‌های خصوصی زمانی استفاده می‌شوند که یک سازمان و زیرمجموعه‌هایش که در یک کانال حضور دارند، بخواهند اطلاعات تراکنش ها را از اعضای دیگر کانال مخفی کنند.

خدمات امنیتی: حفظ امنیت، حریم خصوصی و محرمانگی در شبکه فبریک، از نگرانی‌های اصلی معماری بلاکچین محسوب می‌شوند. برای این منظور، شناسایی و تأیید هویت اعضای شبکه، از بدو ورود صورت می‌گیرد. همچنین، زیرساخت امنیتی کلید عمومی[1] که در این شبکه استفاده شده، همراه با ایجاد گواهی رمزنگاری‌شده، به صورت کامل هویت سازمان‌ها، اجزای شبکه و تمامی کاربران آن را در هر تعامل تأیید می‌کند. از نتایج مهم این ویژگی، قابلیت شناسایی و ردیابی تمامی تراکنش‌ها توسط نهادهای قانون‌گذار و نظارت‌کننده است.

از ویژگی‌های دیگر فبریک در زمینه امنیت و مدیریت هویت، استفاده از «فهرست‌های کنترل دسترسی» است. همان‌طور که از نامش پیداست، این لیست توانایی‌های هریک از اعضای شبکه را مشخص کرده و ایجاد سطوح مختلف دسترسی را در شبکه ممکن می‌سازد. به‌عنوان‌مثال، بانکی که از اعضای عادی شبکه به‌حساب می‌آید قابلیت اجرا و استفاده از قرارداد های هوشمند تعریف‌شده را دارد، اما نمی‌تواند قرارداد جدید تعریف کند و نیازمند اخذ دسترسی از نهادهای مربوطه است.

اجماع: اجماع به‌طور خلاصه، چرخه کامل تأیید صحت مجموعه‌ای از تراکنش‌ها و ثبت آن‌ها در قالب یک بلوک است. «سیاست‌های تأیید[2] » شامل تمامی شاخص‌ها و معیارهای مشخص‌شده در شبکه و قراردادهای هوشمند است که برای تأیید تراکنش‌ها موردتوافق اعضا قرارگرفته‌اند. در چرخه زندگی یک تراکنش، این سیاست‌ها تعیین می‌کنند تراکنش باید توسط کدام اعضای شبکه تأیید شود و پس‌ازآن به ثبت برسد. لازم به ذکر است تأیید تراکنش تنها توسط این گروه از اعضای مشخص‌شده انجام نمی‌شود، بلکه تعدادی دیگر از اعضای شبکه نیز برای اطمینان از اعمال صحیح سیاست‌های تأیید، پیش از ثبت نهایی در دفتر کل، قرارداد هوشمند تأیید و اعتبارسنجی را مجدداً اجرا کرده و تراکنش را در صورت تأیید، ثبت می‌کنند.

الگوریتم‌های اجماع متفاوتی را می‌توان به‌صورت ماژولار در چارچوب هایپرلجر فبریک به کار برد. انتخاب نوع الگوریتم اجماع، بر اساس سیاست‌های تأیید انجام می‌شود.

۳-۱-۲ انواع تراکنش‌ها در هایپرلجر فبریک

دو نوع تراکنش در شبکه بلاکچین هایپرلجر فبریک وجود دارد:

تراکنش‌های تنظیمی

این تراکنش‌ها فقط توسط گره‌های اصلی شبکه قابل انجام بوده و همان‌گونه که از اسمشان پیداست منجر به تنظیم و تغییر در شبکه بلاکچین می‌شوند.

تراکنش‌های تبادلی

این تراکنش‌ها توسط همه گره‌های شبکه قابل انجام هستند و منجر به انجام یک عملیات و ثبت نتیجه آن در شبکه بلاکچین می‌شوند.

[1] Public Key Infrastructure

[2] Endorsement policy

۳-۱-۳ انواع همتا در شبکه هایپرلجر فبریک

گره‌ها در شبکه فبریک همتا[1] نامیده شده و می‌توانند با توجه به پیکربندی شبکه نقش و وظایف متعددی را بر عهده بگیرند. انواع همتا به دو دسته کلی تقسیم می‌شوند:

همتای تأییدکننده: این نوع همتا شامل اعضایی است که قرارداد هوشمند تأیید و اعتبارسنجی را اجرا کرده و از آن برای تأیید تراکنش‌ها استفاده می‌کنند. تأیید تراکنش توسط هر همتا، با یک امضای دیجیتال مشخص می‌شود. سیاست‌های تأیید شبکه، میزان اهمیت تأیید تراکنش توسط هر همتا را مشخص می‌کنند.

همتای ثبت‌کننده: این نوع همتا شامل تمامی اعضای حاضر در کانال‌های شبکه است که بلوک‌های حاوی تراکنش‌ها را دریافت و ثبت می‌کنند. ثبت این تراکنش‌ها در دفتر کل مشترک همتایان ثبت‌کننده، پس از تأیید شدن آن‌ها اتفاق می‌افتد.

۴-۱-۳ مراحل پردازش تراکنش در هایپرلجر فبریک

جریان پردازش تراکنش‌ها در فبریک به سه مرحله تقسیم می‌شود. این جداسازی مزایای متعددی را به همراه می‌آورد، ازجمله این مزایا می‌توان به بهبود مقیاس‌پذیری شبکه، کاهش سطوح اضافی اعتماد و بازبینی و بهبود عملکرد کلی آن اشاره کرد.

مرحله اول

تأیید تراکنش‌ها توسط همتایان تأییدکننده است. این مرحله با استفاده از اجراشدن قرارداد هوشمند توسط این همتایان صورت می‌گیرد که آن را به علت عدم تمرکز در پردازش اطلاعات، پردازش توزیع‌شده می‌نامیم.

مرحله دوم

مرتب‌سازی تراکنش‌ها است. این مرحله در ساختار فبریک از انعطاف بالایی برخوردار بوده و نحوه انجام آن بر اساس معیارهای شبکه مشخص می‌شود.

مرحله سوم

شامل اعتبار سنجی مجدد و نهایی تراکنش‌ها است که درنهایت به ثبت تراکنش‌ها در دفتر کل اعضای شبکه منجر می‌شود.

[1] Peer

۳-۲ معرفی مرورگر هایپرلجر

مرورگر هایپرلجر یا هایپرلجر اکسپلورر[1]، ابزاری است برای به تصویر درآوردن اطلاعات عملیات انجام‌شده در بلاکچین هایپرلجر. عملکرد این ابزار به این صورت است که با ایجاد رابط‌های کاربری مفید و مؤثر، اطلاعات ضروری شبکه را به مخاطبان فنی و غیر فنی، نمایش می‌دهد. این اطلاعات شامل نام، حالت و لیست کامل گره‌های شبکه است. همچنین، از نمونه‌های دیگر این اطلاعات می‌توان به جزئیات بلوک‌ها، تراکنش‌ها، اطلاعات مربوط به آن‌ها، قراردادهای هوشمند و هرگونه اطلاعات مرتبط دیگر که در دفتر کل بلاکچین ذخیره می‌شود اشاره کرد. این‌گونه از داده های خام عموماً در قالبی عرضه می‌شوند که خواندن و درک آن‌ها برای انسان دشوار است، لذا با استفاده از مرورگر، علاوه بر ایجاد ابزار جست‌وجو و نظارت معمول، تجسم آسانی از این اطلاعات در قالب نمودارها، تصاویر، جداول و الگوهای متفاوت برای مخاطبان فراهم آورده شده است.

در این پروژه، ساختار ابزار اکسپلورر شامل یک وب‌سرویس است که در پشت‌صحنه به اجرا در آورده شده است. مسئولیت این سرویس حفظ پاسخگویی سرور بلاکچین و تعامل با تمام اجزای این ابزار است. همچنین در این ابزار از وب سوکت‌هایی برای ارتباط بین سرور و اجزای مختلف سمت کاربر استفاده شده است.

دستیابی به تجسمی یکپارچه از اطلاعات در سطح سازمانی، از دلایل تیم توسعه‌دهنده برای استفاده از ابزار اکسپلورر است که در بخش‌های متفاوتی لازم و ضروری واقع می‌شود. همچنین تیم توسعه‌دهنده و فنی از این اطلاعات به منظور توسعه ویژگی‌ها و اجزا مختلف این زیرساخت استفاده می‌کنند. همچنین، از این اطلاعات برای گردآوری گزارش ها و مطالعه تحولات تاریخی سیستم و اطلاعات مربوط به آن توسط پژوهشگران سازمان استفاده می‌شود. علاوه بر این اپراتورهای شبکه بلاکچین نیز برای مدیریت شبکه از این ساختار اطلاعاتی استفاده می‌کنند. مثال‌های استفاده مؤثر از این اطلاعات ساختاربندی شده در شبکه بلاکچین، محدود به این موارد نیستند.

۳-۳ تحلیل معماری نرم‌افزار

۳-۳-۱ لایه بلاکچین

لایه بلاکچین، تشکیل‌دهنده زیرساخت سیستم بانکی است و شرکت خدمات انفورماتیک به‌عنوان توسعه‌دهنده زیرساخت شبکه، آن را بنا می‌کند. با دور هم قرار گرفتن بازیگران مختلف شبکه مثل بانک‌ها و فینتک‌ها در این لایه، انواع کنسرسیوم‌های برای ایجاد و دریافت خدمات مختلف تشکیل می‌شود.

[1] Hyperledger Explorer

لایه بلاکچین دارای سه هسته مرکزی با سرویس‌های مختلف است که به تمام نیازمندی‌های اعضای شبکه پاسخ داده و هرکدام از اعضای شبکه قابلیت این را خواهند داشت که بتوانند از این هسته‌ها استفاده کرده و سرویس‌های موردنیاز و شخصی خود را تعریف و تنظیم کنند.

۳-۳-۱-۱ هسته شناخت مشتری

این هسته شامل سرویس‌های ثبت‌نام کاربران و احراز هویت است.

- **ثبت نام**

بانک‌ها یا نهادهای ذی‌ربط دیگر از این هسته برای ثبت‌نام کاربران در سیستم خود استفاده می‌کنند. اطلاعات کاربران در این فاز شامل نام، نام خانوادگی، کد ملی، عکس، شماره تلفن همراه و تاریخ تولد به همراه اطلاعات نهاد ثبت‌کننده اطلاعات است. نهاد تأییدکننده اطلاعات، با تأیید هویت کاربران اطلاعات کاربران را به‌صورت هش شده طی یک تراکنش در بلاکچین ثبت می‌کند.

- **احراز هویت**

در این سیستم، مالکیت اطلاعات کاربران با خودشان بوده و بانک‌ها در مرحله ثبت‌نام فقط ثبت‌کننده هش این اطلاعات در بلاکچین هستند و اصل اطلاعات نزد کاربر است. کاربران می‌توانند اطلاعات خود را به سازمان‌های ثالث در این شبکه با توجه به میزان اطلاعات درخواستی سازمان ارائه دهند و دیگر نیاز نیست کاربر مجدداً در این سازمان ثالث فرایند ثبت نام را طی کند. لذا سازمان ثالث پس از گرفتن اطلاعات موردنیازش از کاربر، طی یک تراکنش احراز هویت هش این اطلاعات ارائه‌شده را با مقادیر هش شده‌ای که در هنگام ثبت‌نام در بلاکچین ذخیره‌شده بود مقایسه می‌کند و درصورتی که مغایرتی وجود نداشت، کاربر احراز هویت موفقیت‌آمیزی خواهد داشت.

۳-۳-۱-۲ هسته شناخت مشتری

این هسته شامل سرویس‌های ایجاد، توزیع و انتقال توکن است.

- **ایجاد توکن**

در این هسته می‌توان انواع توکن‌های مورداستفاده برای مسائل مختلف را تعریف و ارزش‌گذاری کرد. همچنین می‌توان نظام استفاده از توکن ایجادشده را متناسب با نیازمندی مسائل مختلف تعیین و شخصی‌سازی نمود. اطلاعات توکن ایجادشده طی یک تراکنش تنظیمی روی بلاکچین ذخیره می‌شود. از ویژگی‌های اصلی این زیرساخت این است که می‌توان از این بستر جهت تولید و توزیع انواع توکن‌ها زیر نظر نهادهای مربوطه استفاده کرد. (برای مثال: وزارت نفت جهت تولید و توزیع توکن سوخت و انرژی، دولت جهت تولید و توزیع توکن یارانه)

- **توزیع توکن**

پس از ایجاد توکن، نهاد ذی‌ربطی که پس از ایجاد توکن وظیفه توزیع توکن را دارد می‌تواند از این سرویس استفاده کرده و با مشخص کردن آدرس‌های مقصد موردنظر خود اقدام به توزیع این توکن‌ها کند. اطلاعات مربوط به توکن‌های توزیع‌شده طی یک تراکنش تبادلی روی بلاکچین ذخیره می‌شود.

- **انتقال توکن**

کاربران سیستم و بازیگران شبکه می‌توانند توکن‌هایی که در دست دارند را طی تراکنش‌های تبادلی بین خود منتقل کنند. اطلاعات مربوط به توکن‌های منتقل‌شده طی یک تراکنش تبادلی روی بلاکچین ذخیره می‌شود.

۳-۱-۳-۳ هسته ثبت رکورد

این هسته شامل یک سرویس، ثبت رکوردهای تراکنش‌های بلاکچین است.

- **ثبت رکورد**

همان‌گونه که از اسم این سرویس پیداست وظیفه آن ثبت تمام رخدادهایی است که در چرخه حیات یک جزء (تراکنش، دارایی و ...) ممکن است رخ دهد. بررسی تمام تغییرات اجزای موجود در شبکه یکی از ویژگی‌های این سرویس است. اطلاعات مربوط به تغییرات یک وسیله طی یک تراکنش تنظیمی روی بلاکچین ذخیره می‌شود.

۳-۳-۲ لایه پنل کنترلی بازیگران سیستم

این لایه که در سمت کاربران نهایی سیستم است، به‌وسیله وب‌سرویسی با بلاکچین ارتباط برقرار می‌کند که فقط نقش ارتباط رست‌فول بین بلاکچین و کلاینت را دارد.

۳-۳-۲-۱ پنل بانک

لایه بلاکچین، تشکیل‌دهنده زیرساخت سیستم بانکی است و شرکت خدمات انفورماتیک به‌عنوان توسعه‌دهنده زیرساخت شبکه، آن را بنا می‌کند. با دور هم قرار گرفتن بازیگران مختلف شبکه مثل بانک‌ها و فینتک‌ها در این لایه، انواع کنسرسیوم‌های برای ایجاد و دریافت خدمات مختلف تشکیل می‌شود.

۳-۲-۳-۲ ثبت‌نام کاربران

کاربر برای اینکه بتواند برای اولین بار در این شبکه ثبت‌نام کند، باید به یکی از دو سازمان یک یا دو مراجعه کند. کارمند سازمان با مراجعه به پنل ثبت‌نام کاربران یک کد کیو آر جدید جهت ثبت‌نام کاربر درخواست می‌کند و این کد را جهت اسکن کردن با اپلیکیشن گوشی همراه در اختیار کاربر قرار می‌دهد. کاربر کیو آر کد را با اپلیکیشن اسکن می‌کند. سپس رمز کد محفوظ در کیو آر ارائه‌شده را با کلید خصوصی خود امضا کرده و به همراه اطلاعات کاربری خود به سازمان ثبت‌نام کننده می‌فرستد. سازمان ثبت‌نام کننده ابتدا رمز کد امضاشده را با کلید عمومی کاربر تائید می کند و در صورت صحت داشتن، کارمند سازمان اطلاعات این کاربر را در پنل خود مشاهده می‌کند. اکنون کارمند سازمان اطلاعات کاربر را با اطلاعات هویتی کاربر (کارت ملی وی) مقایسه و اعتبارسنجی می‌کند و در صورت معتبر بودن، ثبت‌نام کاربر را تائید می‌کند و هش اطلاعات کاربر طی یک تراکنش تنظیمی رو بلاکچین ذخیره می‌شود.

۳-۲-۳-۳ کنترل کاربران

سازمان‌ها باید بتوانند تعاملات کاربران خود را با سیستم‌های بانکی خود، کنترل کنند. لذا در این پنل کارمند بانک می‌تواند لیست کاربرانی که در این سازمان ثبت‌نام کرده‌اند را مشاهده و در بین آن‌ها جستجو کند. همچنین در صورت نیاز می‌تواند وضعیت فعالیت یک کاربر را متوقف یا آزاد کنند. در هنگام ثبت‌نام وضعیت فعالیت یک کاربر به‌صورت پیش‌فرض آزاد است. درصورتی‌که وضعیت فعالیت یک کاربر متوقف شود، آن کاربر دیگر نمی‌تواند از سرویس‌های مربوط به این سازمان استفاده کند.

۳-۲-۳-۴ گزارش سپرده‌گذاری کاربران

یکی از سرویس‌های رایج در نظام‌های بانکی، عملیات سپرده‌گذاری است. در این پنل ادمین‌های هر سازمان می‌توانند تمام سپرده‌های موجود در سازمان خود را ببینند و در بین آن‌ها جستجو کنند.

۳-۲-۳-۵ پنل احراز هویت

در این پنل، سازمان سومی که قرار است کاربر ثبت‌نام کرده را احراز هویت کند شبیه‌سازی شده است. ادمین پنل احراز هویت، اطلاعاتی را که نیاز است از کاربر بگیرد مشخص کرده و یک کد کیو آر تولید می‌کند.

در این پنل، سازمان سومی که قرار است کاربر ثبت‌نام کرده را احراز هویت کند شبیه‌سازی شده است. ادمین پنل احراز هویت، اطلاعاتی را که نیاز است از کاربر بگیرد مشخص کرده و یک کد کیو آر تولید می‌کند. درون این کد کیو آر اطلاعات درخواستی سازمان ثالث و اطلاعات سازمان ثالث و یک رمز کد است. در مرحله بعد، کاربر ثبت‌نام کرده باید این کیو آر را با اپلیکیشن گوشی همراه خود اسکن کرده تا در فرمی در اپلیکیشن اطلاعات درخواستی سازمان ثالث را ببیند و در صورت موافقت، ابتدا کد رمز را با کلید خصوصی خود امضا کند و به همراه اطلاعات خود به سازمان ثالث ارائه کرده و سپس این سازمان ابتدا رمز کد امضاشده را با کلید عمومی کاربر تائید می‌کند و در صورت صحت داشتن رمز کد امضاشده، اطلاعات ارائه‌شده توسط کاربر را با هش اطلاعات ثبت‌شده این کاربر در بلاکچین مقایسه می‌کند و در صورت صحت داشتن، کاربر را احراز هویت می‌کند.

۳-۳-۲-۶ پنل بانک مرکزی

بانک مرکزی به‌عنوان سازمان اصلی، دارای اختیارات کلان‌تری نسبت به سازمان‌های دیگر دارد. با حفظ حریم خصوصی کاربران و اختیارات بانک‌ها، بانک مرکزی به‌عنوان یکی از نهادهای حاضر در این کنسرسیوم می‌تواند عملیات زیر را انجام دهد:

- **تولید و توزیع توکن**

بانک مرکزی یا نهادهای ذی‌ربط دیگری که توسط بانک مرکزی اجازه تولید و توزیع توکن را دارند می‌توانند از این پنل استفاده کرده و با واردکردن آدرس‌های مقصد و میزان توکن‌های موردنظرشان اقدام به توزیع توکن‌ها کنند

- **گزارش تولید و توزیع توکن**

پس از تولید و توزیع توکن‌ها، بانک مرکزی یا نهادهای ذی‌ربطی که توسط بانک مرکزی اجازه تولید و توزیع توکن را دارند، می‌توانند از این پنل استفاده کرده و گزارش تولید و توزیع توکن‌های مربوط به خود را مشاهده کرده و در بین آن ها جستجو کنند.

- **گزارش تراکنش‌های کاربران**

در این شبکه، تراکنش‌های انتقال وجه بین کاربران دیگر مثل گذشته از یک بانک به بانک دیگر منتقل نمی‌شود، چراکه مالکیت حساب الکترونیکی کاربر با خود کاربر است، نه بانک. لذا تراکنش‌های انتقال وجه بین دو کاربر کاملاً به صورت همتا به همتا صورت می‌گیرد و بانک‌ها دیگر قادر به دیدن این تراکنش‌ها نیستند؛ اما بانک مرکزی به‌عنوان مهم‌ترین نهاد نظارت پولی و مالی کشور، باید حق مشاهده این تراکنش‌ها را داشته باشد. لذا در این پنل بانک مرکزی می‌تواند تمام تراکنش‌های انتقال توکن بین کاربران را مشاهده کرده و در بین آن‌ها جستجو کند.

- **کنترل نظرات کاربران**

این پنل تمام دیدگاه‌های ثبت‌شده کاربران را در اختیار کارمند بانک مرکزی قرار می‌دهد و وی می‌تواند در بین آن‌ها جستجو کند و در صورت نیاز دیدگاه‌های مغایر با اصول خود را گزارش و فیلتر کند. لازم به ذکر است در صورت گزارش شدن یک دیدگاه، همان‌گونه که انتظار می‌رود این دیدگاه از بلاکچین حذف نخواهد شد و فقط وضعیت آن از «در حال نمایش» به «مخفی و گزارش‌شده» تغییر می‌کند.

۳-۳-۳ لایه اپلیکیشن موبایل

این لایه که در سمت کاربران نهایی سیستم است، به‌وسیله وب‌سرویسی با بلاکچین ارتباط برقرار می‌کند که فقط نقش ارتباط رست‌فول بین بلاکچین و کلاینت را دارد. لذا در تمامی سناریوهای اپلیکیشن‌های گوشی همراه، دیگر نامی از وب‌سرویس برده نمی‌شود چراکه تنها وظیفه آن هدایت تراکنش از کلاینت به بلاکچین است.

۱-۳-۳-۳ شناخت مشتری

ثبت نام

کاربر به‌محض اینکه برای اولین بار وارد اپلیکیشن‌های گوشی همراه می‌شود، یک زوج کلید رمزنگاری‌شده در اپلیکیشن به وی اختصاص داده می‌شود که از این به بعد با کلید عمومی خود می‌تواند وجود خود را اثبات کند و در تمام ارتباطات خود (ثبت تراکنش یا جستجو بین تراکنش‌ها) از کلید خصوصی خود جهت امضا کردن و از کلید عمومی خود برای اثبات ادعای امضاشده خود استفاده کند. با این اوصاف، کاربر پس از مراجعه به بانک و اسکن کردن کد کیو آر مربوط به ثبت‌نام خود با اپلیکیشن گوشی همراهش، فرم ثبت‌نام را در مقابل خود می‌بیند و اطلاعات ثبت‌نامی خود را مطابق اطلاعات هویتی خود (کارت ملی) وارد می‌کند. در این کیو آر کد، یک کد رمز وجود دارد که اپلیکیشن پیش از ارسال تراکنش ثبت‌نام به شبکه بلاکچین این کد رمز را با کلید خصوصی خود امضا کرده و به همراه اطلاعات ثبت نامی خود و کلید عمومی خود به شبکه بلاکچین می‌فرستد. همان‌گونه که در بخش ثبت‌نام هسته شناخت مشتری گفته شد، صحت امضای این کد رمز توسط بلاکچین با کلید عمومی فرستاده‌شده توسط کاربر صورت می‌گیرد. اکنون کاربر باید منتظر تأیید کارمند سازمان ثبت‌نام کننده باشد. تا پیش از تأیید، کاربر نمی‌تواند هیچ عملیاتی را در اپلیکیشن گوشی همراه خود انجام دهد. پس از مشخص شدن وضعیت کاربر و در صورت تأیید شدن، این کاربر می‌تواند از قابلیت های تعبیه‌شده در اپلیکیشن گوشی همراه خود استفاده کند.

احراز هویت

کاربر ثبت‌نام کرده در این شبکه بلاکچین، ازاین‌پس دیگر نیاز نیست برای استفاده از دیگر سرویس‌های بانکی هر بار در آن‌ها ثبت‌نام کند. فقط کافی است اطلاعات خود را به بانک ثالثی که تقاضای ثبت‌نام وی را دارد، ارائه داده و آن بانک این اطلاعات ارائه‌شده را با اطلاعات ثبت‌نامی این کاربر در بلاکچین مقایسه کند و عملیات احراز هویت را انجام دهد. چرخه این عملیات بدین‌صورت است که کاربر با ورود به سازمان ثالث، یک کد کیو آر مربوط به احراز هویت در آن سازمان را با اپلیکیشن گوشی همراه خود اسکن کرده، سپس فرم اطلاعات درخواستی سازمان ثالث را در اپلیکیشن گوشی همراه خود مشاهده کرده، و در صورت موافقت این اطلاعات را بدون واردکردن مجدد اطلاعات، از اپلیکیشن خود به بانک ثالث ارائه دهد. (یک نسخه از اطلاعات کاربر پس از ثبت‌نام موفقیت‌آمیز در اپلیکیشن گوشی همراه وی و یک

نسخه هش شده آن در دفاتر توزیع‌شده بلاکچین ذخیره می‌شود، لذا کاربر دیگر نیاز نیست هر بار اطلاعات خود را وارد کرده، فقط کافی است آن را احراز کند.) همچنین در این کد کیو آر یک کد رمز محفوظ است که کاربر آن را با کلید خصوصی خود امضا کرده و به همراه اطلاعات و کلید عمومی خود به سازمان ثالث ارائه می‌دهد. این سازمان طی یک تراکنش تبادلی اطلاعات ارائه‌شده توسط کاربر را نسبت به اطلاعاتی که در زمان ثبت‌نام وی در شبکه بلاکچین ثبت‌شده بود، احراز می‌کند. در قرارداد هوشمند احراز هویت، پس از بررسی کردن صحت رمز کد امضاشده کاربر، اطلاعات ادعاشده کاربر را نیز نسبت به اطلاعات ثبت‌شده هنگام ثبت‌نام در بلاکچین بررسی و راستی آزمایی می‌کند و سپس نتیجه را به بانک ثالث اعلام می‌کند.

۳-۳-۳-۲ انتقال توکن

جابجایی توکن

هر کاربر ثبت‌نام کرده در این بخش از اپلیکیشن گوشی همراه خود می‌تواند با مشخص کردن آدرس مقصد و میزان مبلغ انتقال وجه طی یک تراکنش تبادلی عملیات انتقال وجه را انجام دهد. این تراکنش انتقال توکن پس از گذر از وب سرویس به قرارداد هوشمند مربوط به مدیریت توکن می‌رسد و تمام گره‌های تأییدکننده ابتدا این تراکنش را شبیه سازی کرده و سپس پاسخ خود را از طریق وب‌سرویس به اپلیکیشن ارسال می‌کنند و اپلیکیشن با جمع‌آوری همه پاسخ ها آن‌ها را به مرتب‌کننده می‌فرستد و مرتب‌کننده همان‌طور که از اسم آن پیداست طبق الگوریتم مشخص‌شده‌اش اقدام به مرتب کردن پاسخ‌های دریافتی می‌کند و آن‌ها را طبق الگوریتم اجماع تعریف‌شده بررسی می‌کند و اگر پاسخ های گره‌های تأییدکننده به اجماع رسیده بود این درخواست به‌عنوان یک درخواست موفقیت‌آمیز جهت ثبت شدن در تمام دفاتر توزیع‌شده به تمام گره‌های ثبت‌کننده داده می‌شود. در غیر این صورت، اگر پاسخ گره‌های تأییدکننده به اجماع نرسیده بود این درخواست به‌عنوان یک درخواست رد شده جهت ثبت شدن در تمامی دفاتر توزیع‌شده به تمام گره‌های ثبت‌کننده داده می‌شود.

گزارش جابجایی توکن

کاربران پس‌از انتقال یا دریافت توکن می‌توانند از طریق یک تراکنش جستار اقدام به گرفتن و مشاهده تمام تراکنش های مربوط به خود (تراکنش‌های ورودی و خروجی) کرده و در بین آن‌ها جستجو کنند.

۳-۳-۳-۳ سپرده‌گذاری

سپرده‌گذاری کردن

در این بخش، ابتدا طی یک تراکنش جستار، لیست تمام سپرده‌های بانکی ارائه‌شده از شبکه بلاکچین گرفته می‌شود. سپس کاربر با مشاهده انواع گوناگون سپرده‌گذاری و میزان و مدت هرکدام، یک نوع سپرده را انتخاب کرده و با مشخص کردن مبلغ سپرده، اقدام به سپرده‌گذاری در آن بانک می‌کند.

عملیات سپرده‌گذاری طی یک تراکنش تبادلی به شبکه بلاکچین فرستاده می‌شود و پس از تائید یا رد گره‌های تأیید کننده در دفاتر توزیع‌شده تمام گره‌ها ثبت می‌شود. لذا پس از سپرده‌گذاری، مسئولیت و مالکیت این توکن‌ها با قرارداد هوشمند بانک است.

گزارش سپرده‌های کاربر

پس از سپرده‌گذاری، طی یک تراکنش جستار، کاربران می‌توانند لیست تمام سپرده‌های باز خود را به همراه اطلاعات جزئی آن‌ها همانند تاریخ افتتاح حساب، تاریخ آخرین محاسبه سود و میزان موجودی و سود دریافتی این حساب خود را تا به آن لحظه ببینند.

بستن یک سپرده

همچنین کاربران می‌توانند در هرلحظه و طبق خط‌مشی مشخص‌شده توسط هر بانک، حساب سپرده خود را خالی کرده و موجودی نهایی خود را به همراه سود تخصیص‌یافته تا به آن لحظه را در کیف دیجیتالی خود ذخیره کنند. این عملیات طی یک تراکنش تبادلی به شبکه بلاکچین فرستاده می‌شود و در صورت تائید گره‌های تأییدکننده، عملیات انجام شده و نتیجه آن در دفاتر توزیع‌شده تمام گره‌ها ثبت می‌شود. لذا پس از بستن سپرده، مسئولیت و مالکیت این توکن‌ها مجدداً به خود کاربر بازمی‌گردد.

۴-۳-۳-۳ دیدگاه

ثبت دیدگاه

هر کاربر ثبت‌نام‌شده، در این بخش از اپلیکیشن گوشی همراه خود می‌تواند دیدگاهی به اسم خود، روی شبکه بلاکچین ذخیره کند. این اطلاعات طی یک تراکنش تبادلی به‌وسیله هسته مرکزی ثبت رکورد روی شبکه بلاکچین ذخیره می‌شود.

گزارش دیدگاه‌ها

در این بخش کاربران می‌توانند تمام دیدگاه‌های ثبت‌شده روی شبکه بلاکچین به‌وسیله هسته مرکزی ثبت رکورد را مشاهده کنند و پس از خواندن دیدگاه‌ها به‌وسیله دکمه تعبیه‌شده برای هر دیدگاه اقدام به ثبت علاقه‌مندی خود روی دیدگاه‌های دیگران کنند. لازم به ذکر است که هسته مرکزی ثبت رکورد مجزا از هسته مرکزی شناخت مشتری است لذا اطلاعات مربوط به نویسنده دیدگاه‌ها به‌صورت هش شده به کاربران نمایش داده می‌شود تا حریم خصوصی کاربران حفظ شود.