هفتمین همایش سالانه بانکداری الکترونیک و نظام‌های پرداخت
نوآوری، بازیگران جدید و کارآیی در کسب وکار مالی
تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲و۳ بهمن ۱۳۹۶
7th Annual Conference on Electronic Banking and Payment Systems

ارزیابی سطح بلوغ فناوری بلاک‌چین جهت استفاده در صنعت پرداخت ایران

Maturity Assessment of Blockchain Technology to be adopted in Payment System

حسین یعقوبی، کارشناس ارشد تحقیقات فناوری‌های بانکی، شرکت خدمات انفورماتیک
H_Yaghoubi@isc.co.ir

بلاک‌چین[1] (زنجیره بلوک) یکی از عمده‌ترین روندهای فن‌آوری در دنیای Post-Nexus است که اخیرا بسیار مورد توجه قرار گرفته است. این فناوری مبتنی بر دفاتر ثبت توزیع شده[2] (DLT) بوده و مکانیزمی برای ایجاد اعتماد بین اعضای یک شبکه در غیاب نهاد ثالث در نظر گرفته می‌شود. صاحبنظران معتقدند بلاک‌چین در حال حاضر معادل اینترنت در هنگامه‌ی ظهورش در دهه ۹۰ میلادیست و انتظار می‌رود در آینده نزدیک، تحولات شگرف و انقلاب‌گونه‌ای در بسیاری از حوزه‌های کسب و کار از جمله بانکداری ایجاد نماید.

در حال حاضر مهمترین کاربرد فراگیر و اثبات‌شده‌ی زنجیره بلوک در بحث‌های مالی، استفاده از آن بعنوان زیرساخت توسعه پول‌های مجازی و رمز ارزها[3] همانند بیت‌کوین است اما توانایی بالقوه آن در سرعت بخشیدن به فرآیندهای تسویه بین بانکی و کاهش هزینه مربوط به سامانه‌های Back-office، علاقه بسیاری از بانک‌ها را به خود جلب کرده است. در همین راستا تعداد بسیار زیادی پروژه تحقیقاتی در سطح Proof of Concept در سرتاسر دنیا در حال انجام است.

با در نظر گرفتن ریسک‌های احتمالی بکارگیری هر تکنولوژی جدید و نیز حساسیت‌ها و ملاحظات ویژه‌ای که نسبت به توسعه و نوسازی سامانه‌های بانکی و پرداخت وجود دارد، در این مقاله به بررسی دقیق میزان بلوغ فن‌آوری بلاک‌چین جهت استفاده از آن در سامانه‌های زیرساخت پرداخت (از جمله سامانه‌های تسویه بین بانکی همچون ACH و RTGS) پرداخته شده است. نتایجی که در این مقاله بیان می‌شود نشان می‌دهد علی رغم منافع قابل توجهی که بلاک‌چین به ارمغان می‌آورد، هنوز راهی طولانی در پیش روست تا این فناوری به حدی از بلوغ برسد که بتوان با اطمینان خاطر، معماری سامانه‌های حیاتی پرداخت را بر اساس آن بازطراحی کرد. در انتهای مقاله حوزه‌هایی از عرصه‌ی پرداخت در ایران که نیاز کمتری به بلوغ فناوری دارند و از این بابت آماده‌ی پذیرش و بکارگیری فناوری بلاک‌چین می باشند پیشنهاد شده است.

واژگان کلیدی:

بلاک چین، زنجیره بلوک، پول مجازی، رمز ارز، مدل بلوغ، ارزیابی سطح بلوغ، سیستم پرداخت

[1] - Blockchain
[2] - Distributed Ledger Technology
[3] - Cryptocurrency

Abstract

Nowadays, Blockchain is considered as a mega Trend in post-nexus world. Blockchain is characterized as a state-of-the-art method of Decentralization. The Technology experts believe that the Blockchain and relevant technologies will play a disruptive role, affecting all kind of businesses.

Since the emergence of Blockchain and distributed ledger technologies (DLTs), the question of how this technology can be deployed in payment systems has captivated the industry. The search for implementations and use cases is now a key focus of R&D and innovation teams in major financial institutions.

In this paper an assessment of the maturity level of Blockchain and capabilities of existing DLT platforms has been carried out. Although The results have confirmed that Blockchain has the potential to bring new opportunities and efficiencies to the financial industry with their key strengths (including the ability to create Trust in a disseminated system, to provide transparency and efficiency in broadcasting information, to simplify reconciliation and high resiliency), this paper demonstrates that existing Blockchain platforms are currently not mature enough to fulfil the requirements of the financial community. In this paper, key requirements that Blockchain needs to attain in order to be widely adopted by the financial industry are identified

Key Words:

Blockchain, Cryptocurrency, Maturity assessment, Maturity Model, Payment System

۱. مقدمه

زنجیره بلوک یا همان بلاک‌چین برای اولین بار در سال ۲۰۰۸ و با معرفی بیت‌کوین مطرح شد[1]. زنجیره بلوک یک تکنولوژی است که بیت‌کوین و بسیاری دیگر از انواع پول‌های رمزنگاری‌شده[۱] برآن بنا نهاده شده است و در واقع مفهومی فراتر از بیت‌کوین است و نباید این دو را یکسان در نظر گرفت. برای بیان اهمیت این فناوری زیرساختی، ابتدا لازم است نگاهی به روندهای فناوری در حال وآینده بندازیم.

آینده‌پژوهان و صاحبنظران عرصه مدیریت فناوری بر این باورند که دنیا در مسیر حرکت به سمت کسب و کار دیجیتال[۲]، از عصر Nexus of Forces که به معنای همگرایی چهار نیروی فناوری (Social, Mobile, Cloud, Big data) می‌باشد گذر کرده است و وارد عصر پسا نکسوس[۳] شده است. در واقع این چهار نیروی فناوری هر تغییری که ممکن بوده است را بر کسب و کارها از جمله کسب و کار بانکی گذاشته است. مشخصه‌ی عمده عصر پسا- نکسوس اینست که مشتریان کسب و کارها دیگر تنها انسان‌ها[۴] نیستند بلکه اشیاء[۵] نیز بعنوان مشتری بالقوه (و در برخی موارد بالفعل) آنها شناخته می‌شوند. اشیاء، موجودیت‌های هوشمندی خواهند بود که از طریق شبکه‌ای که آنها را بهم متصل می‌کند، با یکدیگر تعامل خواهند داشت. این تعاملات شامل مراودات مالی نیز خواهد شد. بر همین اساس است که در عصر پسا نکسوس، موارد سه گانه‌ای که در ادامه می‌آید، بعنوان کلان روندهای[۶] فناوری شناخته می‌شوند: اینترنت اشیاء[۷]، هوش مصنوعی[۸]، بلاک‌چین.

این کلان روندها بیان می‌کنند که جهان در آینده نه چندان دور، متشکل از اشیاء هوشمندی است که به یکدیگر متصل هستند و بلاک‌چین مکانیزمی برای ایجاد اعتماد بین این اعضا در این فضای بسیار پیچیده خواهد بود[2].

بلاک‌چین یک نوع پایگاه داده یا دفترکل[۹] از رکورد تراکنش‌ها است که در قالب بلوک‌هایی پشت سر هم قرار گرفته‌اند. در واقع هر بلوک مجموعه‌ای از چندین تراکنش است. هر بلوک یک تمبر زمانی[۱۰] دارد و به بلوک پیشین خود نیز مرتبط می‌شود. کلمه‌ی زنجیره در نام آن نیز به همین مفهوم ارتباط بین بلوک‌ها اشاره دارد. نسخه‌ای از این پایگاه داده در اختیار هر یک از اعضای یک شبکه گذاشته می‌شود و تنها زمانی یک رکورد (تراکنش) تایید و به انتهای بلوک‌ها اضافه می‌شود که بین اعضای گروه روی صحت آن رکورد اجماع[۱۱] صورت پذیرد. این بدین معناست که هیچ نیازی به یک نهاد مرکزی برای تایید رکورد نمی‌باشد.

---

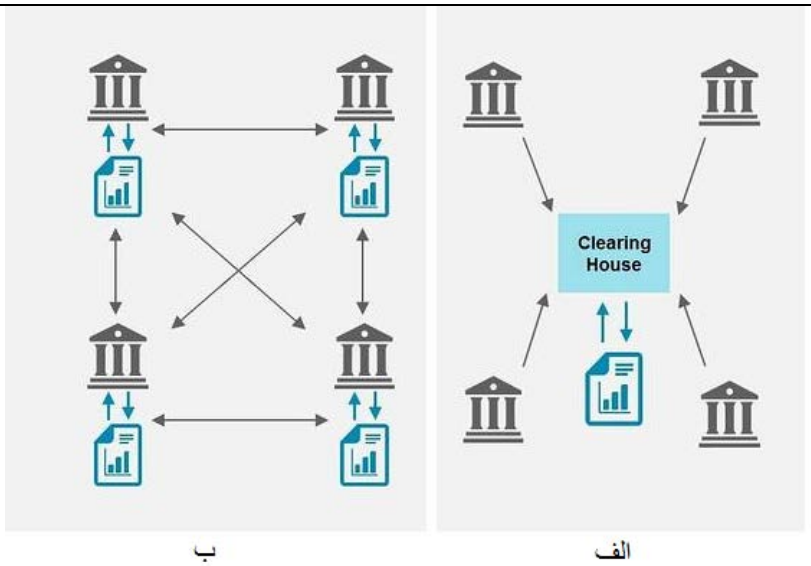
1 - Cryptocurrency
2 - Digital Business
3 - Post- Nexus
4 - Human
5 - Things
6 - Mega Trends
7 - Internet of Things
8 - Artificial Intelligence
9 -Ledger
10 -Time stamp
11 -Consensus

ناب بودن ایده‌ی بلاک‌چین به همین دلیل است که درغیاب یک نهاد مرکزی باز هم می‌تواند اعتماد[1] را بین اعضا و نیز نسبت به صحت تراکنش‌ها بوجود آورد. بعنوان مثال تراکنش‌های بانکی را در نظر بگیرید. در حالت معمولی اگر فرد الف قصد انتقال وجه به فرد ب را داشته باشد، این انتقال را بواسطه یک نهاد ثالث مورد اعتماد که همانا بانک است انجام می‌دهد. فناوری بلاک‌چین این فرآیند را دستخوش تحول بنیادین می‌کند بطوریکه الزام به وجود بانک را از بین می‌برد. در این حالت اگر فرد الف از طریق شبکه وجهی را به فرد ب منتقل کند، آنرا به تمامی اعضای شبکه اعلام می‌کند. سپس هر یک از اعضا، سابقه رکوردهای مربوط به فرد الف را در دفترکل خود (نسخه‌کپی شده از بلاک‌چین) که در اختیار دارد بررسی می‌کند. اگر تمام اعضا بر صحت این تراکنش طبق پروتکلی که در شبکه وضع شده است، به اجماع برسند، رکورد تراکنش وارد زنجیره بلوک شده و تمامی اعضا نسخه خود را بروز می‌کنند. بنابراین خلاء وجودی بانک بواسطه توزیع دفتر کل نزد تمامی اعضا و بالتبع بالارفتن شفافیت جبران می‌گردد.

بنابرآنچه بیان شد، زنجیره بلوک یک پایگاه داده باز[2] و غیر متمرکز[3] از تراکنش‌هاییست که یک ارزش[4] را انتقال می‌دهند. زنجیره بلوک در نوع کاربرد، عمومیت دارد بدین معناکه از ایده‌ی آن می‌توان برای هر نوع تراکنشی که ارزشی (value) را منتقل می‌کند استفاده کرد. ارزش انتقال داده شده می‌تواند پول، کالا، رای، مالکیت معنوی، ایمیل، بیمه و یا هر چیزی دیگری باشد. در واقع کاربردهای زنجیره بلوک نامحدود است.

بلاک‌چین اخیرا بسیارمورد توجه بانک‌ها قرار گرفته است. چرا که هم یک تهدید جدی برای بانک‌هاست و هم یک فرصت عالی. تهدید است چرا که فلسفه وجودی بانک را بعنوان یک واسط مورد اعتماد برای ثبت تراکنش‌ها از بین می‌برد. فرصت است چرا که کاربردهای بسیار زیادی را برای بانک به ارمغان خواهد آورد. در حال حاضر مهمترین کاربرد بلاک‌چین در بحث-های مالی، استفاده در پول‌های مجازی و همچنین تدوین قراردادهای هوشمند[5] است اما توانایی بالقوه زنجیره بلوک در در سرعت بخشیدن به فرآیندهای تسویه بین بانکی و کاهش هزینه مربوط به سامانه‌های Back-office، علاقه بسیاری از بانک-ها را به خود جلب کرده است. پیش‌بینی می‌شود تا سال ۲۰۲۱، بلاک‌چین تا ۳۰٪ از هزینه‌های بانک‌ها را بواسطه‌ی تحول در معماری سیستم‌های تسویه بین بانکی کاهش دهد[3]. شکل (۱) ساختار تسویه بین بانک‌ها را در حالت حضور اتاق پایاپای بعنوان یک نهاد واسط برای تسویه (الف) و در حالت استفاده از فناوری بلاک چین (ب) نشان می‌دهد.

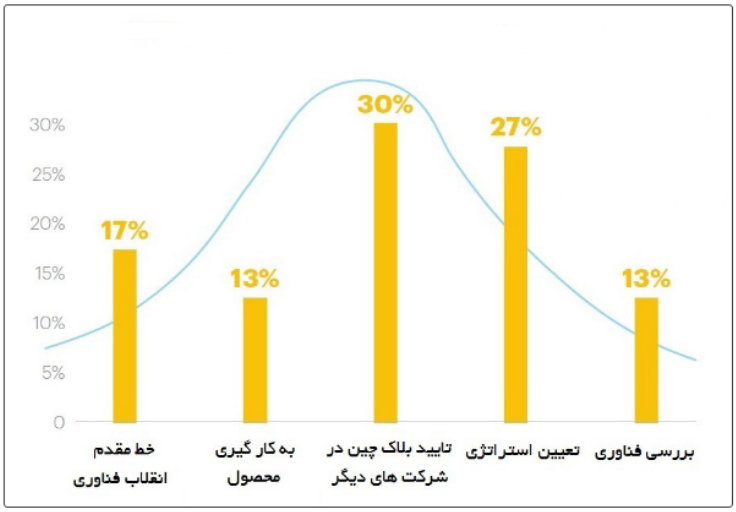
[1]- Trust
[2]- Open
[3] - Distributed
[4] - Value
[5] - Smart Contract



شکل۱) الف- تسویه بین بانکی در حالت حضور یک نهاد مرکزی (اتاق پایاپای)

ب- تسویه بین بانکی در حالت استفاده از فناوری بلاک چین(اشتراک گذاری دفتر کل)

بررسی‌ها نشان می‌دهد عمده بانک‌های اروپایی و آمریکای شمالی نه تنها از مرحله‌ی بررسی و شناخت این تکنولوژی گذر کرده‌اند بلکه با تعیین استراتژی خود در قبال آن، به توسعه یک محصول یا سرویس مبتنی بر آن اقدام کرده اند (شکل ۲).



شکل۲) بانک‌های اروپا و آمریکای شمالی در چه مرحله‌ای از تطبیق با فناوری زنجیره بلوک هستند؟ (منبع: سایت عصربانک به ترجمه از Accenture)

علی‌رغم موج روزافزونی که در بکارگیری بلاک‌چین ایجاد شده است، اما بانک‌ها کماکان در این مسیر با چالش‌های عمده‌ای روبرو خواهند بود. اولین چالش، پیدا کردن یک مورد- کاربرد[1] مناسب برای پیاده سازی روی بلاک‌چین است. گارتنر معتقد است تا سال ۲۰۱۸، در ۸۰٪ موارد توسعه داده شده، بانک‌ها به این نتیجه می‌رسند که کاربرد مناسبی را انتخاب نکرده بودند.[4] به بیان دیگر به این نتیجه می‌رسند که بلاک‌چین (توسعه توزیع شده) کمکی به بهبود کارایی یا کاهش هزینه آن محصول یا سرویس نکرده است. چالش بعدی، عدم وجود یک استاندارد مشخص برای پیاده‌سازی زنجیره بلوک است. عدم وجود استاندارد در تمام جنبه‌های بلاک‌چین از جمله فرآیند اجماع، پروتکل ارتباطی و شبکه مورد استفاده و نیز حاکمیت آن (دسترسی آزاد[2] و دسترسی نیازمند مجوز[3]) وجود دارد. از دیگر چالش‌ها، دغدغه‌هاییست که کماکان روی دو موضوع صحت-سنجی تراکنش‌ها و نیز حفظ حریم شخصی وجود دارد. این دو مساله در بیت‌کوین به کمک الگوریتم‌های رمزنگاری کلید نامتقارن حل شده. هر کاربردی که بخواهد از زنجیره بلوک استفاده نماید لازم است که فرآیندهای مطمئنی برای این موضوع ارائه دهد.

چالش مهم دیگر که موضوع بحث این مقاله نیز می‌باشد و در بخش‌های بعدی به تفصیل بررسی می‌شود این است که این تکنولوژی بسیار نوظهور است و بلوغ آن مورد تردید است. چرخه بلوغ فناوری[4] مربوط به تکنولوژی‌های بلاک‌چین، تراکم سنگین فناوری‌ها در مرحله رشد و مرحله انتظارات غیرواقعی را نشان می‌دهد[5] که نشان دهنده میزان بلوغ نه چندان بالای آنست.

با توجه به اهمیت موضوع بلاک‌چین در دنیا و در نظر گرفتن این موضوع که بانک‌های ایران نیز نباید از این تکنولوژی تحول‌زا[5] غافل باشند، در این مقاله سعی شده است تا میزان بلوغ فن‌آوری بلاک‌چین جهت استفاده از آن در سامانه‌های زیرساخت پرداخت (از جمله سامانه‌های تسویه بین بانکی همچون ACH و RTGS) به دقت مورد بررسی قرار گیرد و بر اساس آن پیشنهادات واقع‌بینانه‌ای برای ارائه سرویس‌های مبتنی بر بلاک‌چین در ایران ارائه گردد.

در ادامه‌ی این مقاله و در بخش بعد مروری بر ادبیات موضوع می‌شود و پس از اشاره به روش تحقیق، در بخش چهارم به تفصیل بلوغ بلاک‌چین مورد واکاوی قرار می‌گیرد. در بخش پنجم یافته‌های مهم این مقاله در قالب جمع‌بندی بیان می‌گردد و چند سرویس پیشنهادی برای استفاده از بلاک‌چین در فضای بانکی و پرداخت ایران ارائه می‌گردد.

[1] - Usecase
[2] - Permissionless Blockchain
[3] - permissioned Blockchain
[4] - Hype Cycle
[5] - Disruptive Technology

۲. ادبیات موضوع

بلاک‌چین برای اولین بار توسط ساتوشی ناکاماتو در سال ۲۰۰۸ و با معرفی بیت‌کوین مطرح شد[1]. در این مقاله، بیت‌کوین بعنوان یک پلتفرم انتقال پول نظیر به نظیر (p2p) معرفی شد که مبتنی بر بلاک‌چین بعنوان یک دفتر کل توزیع‌شده توسعه داده می‌شود. تا سال‌ها پس از این تاریخ، مفهوم بلاک‌چین همیشه همراه بیت‌کوین مطرح میشد.

از اوایل سال ۲۰۱۵ مفهوم بلاک‌چین بطور مجزا مورد توجه بسیار قرار گرفت و از آن بعنوان یک فناوری نوظهور که نه تنها در پول‌های رمزی بلکه قادر است در بسیاری از صنایع و کسب و کارها تحول شگرفی ایجاد نماید نام برده شد. توانایی بالقوه بلاک‌چین در تحول کسب و کارها را با ظهور اینترنت در دهه‌ی ۹۰ میلادی و تحولی که ایجاد نمود مقایسه می‌شود[4][5][6][7]. این مقالات علاوه بر مفهوم کلان بلاک‌چین، ارکان اساسی آن از جمله انواع فرآیند اجماع، استانداردها، رگولاتوری و اعمال حاکمیت در آن را معرفی می‌کردند و به صورت موردی، کاربردهای آن در صنایع مختلف از جمله بانک، بورس سهام، سلامت، کشاورزی و مدیریت زنجیره ارزش[1] بررسی می‌کردند. با توجه به گستردگی مطالب و مقالاتی که در این زمینه منتشر شده است، در این بخش از بیان مفاهیم کلی آن صرف‌نظر شده است و در ادامه تنها به مقالاتی اشاره می‌شود که در زمینه بررسی میزان بلوغ بلاک‌چین منتشر شده‌اند و یا به بیان تجربه از پیاده‌سازی سامانه‌های زیرساخت پرداخت مبتنی بر آن پرداخته‌اند.

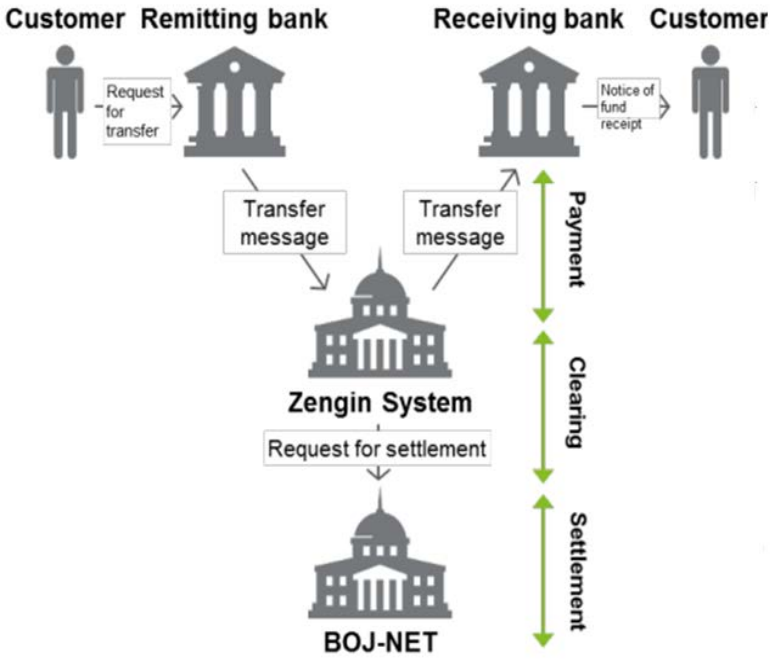
گارتنر در [5]، هایپ سایکل مربوط به تکنولوژی‌های بلاک‌چین را ارائه می‌دهد که نشان از تراکم بالای فناوری‌ها در مرحله رشد[2] و مرحله انتظارات غیرواقعی[3] دارد (شکل ۳). این شکل نشان‌دهنده‌ی میزان بلوغ نه چندان بالای این تکنولوژی‌هاست.

در مقاله‌ی "انتقال پیام‌های پرداخت بین بانکی بر بستر بلاک‌چین"[8] که توسط مرکز مطالعات بلاک‌چین ژاپن[4] در سال ۲۰۱۶ منتشر شد، تجربه پیاده‌سازی یک پروژه مقدماتی برای انتقال پیام‌های تسویه بین بانکی مبتنی بر بلاک‌چین به اشتراک گذاشته شده است. در این مقاله جریان‌کاری[5] مدل سنتی انتقال پیام که بواسطه‌ی سامانه‌های متمرکز واسط بنام BOJ-NET و Zengin (معادل ACH و RTGS در ژاپن) اتفاق می‌افتد، با مدل پیشنهادی که از مفهوم بلاک‌چین استفاده می‌کند و نهاد واسط را حذف می‌کند مقایسه شده است. دو شکل (۴) و (۵) این دو مدل را نشان می‌دهند. نتایج این مقاله نشان می‌دهد در حالیکه ظرفیت پردازش سامانه Zengin در حالت پیک، ۱۳۸۰ تراکنش در ثانیه است، در محیط آزمایشی مبتنی بر بلاک چین، ظرفیت بالاتر از ۱۵۰۰ تراکنش در ثانیه بدست آمده است.

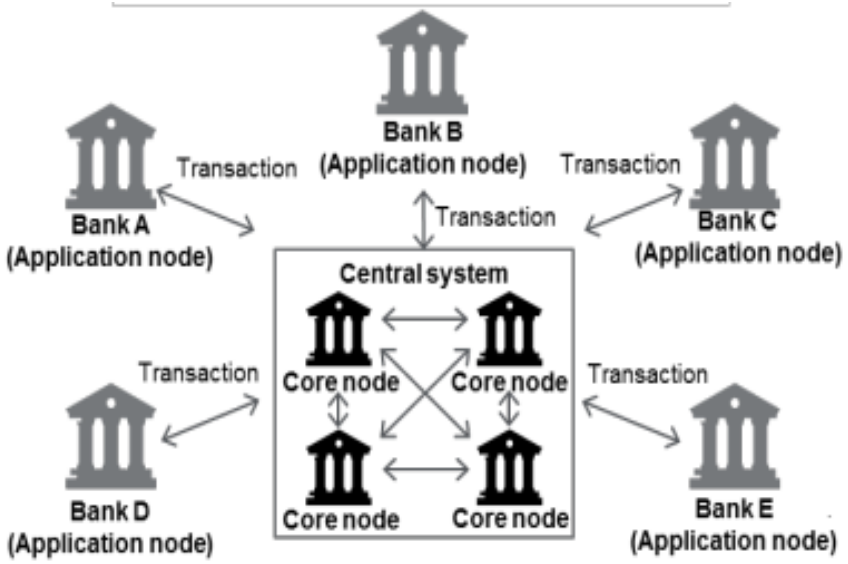
---

[1] - Supply Chain Management
[2] - Technology Trigger
[3] - peak of inflated expectations
[4] - Blockchain Study Group: این موسسه در سال ۲۰۱۵ با همکاری ۴ بانک ژاپن و باهدف کشف فرصت های بلاک چین در صنعت مالی و بانک تاسیس شده است.
[5] - WorkFlow

شکل۳) هایپ سایکل مربوط به فناوری‌های مربوط به زنجیره بلوک. قریب به اتفاق آنها در مراحل ابتدایی خود هستند.



شکل۴) معماری فعلی انتقال پیام‌های پرداخت بین بانکی در ژاپن بواسطه سامانه های Zengin , BOJ-NET



شکل۵) معماری جدید انتقال پیام‌های پرداخت بین بانکی

در این معماری، نهاد واسط تبادل پیام (Zengin)با یک معماری مبتنی بر بلاک چین جایگزین شده است.

نکته‌ی مهمی که در این مقاله به آن اشاره شده است اینست که کل فرآیند تسویه بین بانکی به سه مرحله‌ی انتقال پیام، تهاتر و نهایتا تسویه تقسیم بندی شده است و در این آزمایش صرفا مرحله ی اول فرآیند مبتنی بر معماری جدید شده است. بدین معناکه دو مرحله تهاتر و تسویه کمافی السابق به روش غیر بلاک‌چینی صورت می‌پذیرد.

گارتنر در مقاله‌ی ارزشمندی که در این زمینه در اواخر سال ۲۰۱۶ منتشر نمود [9] اعتقاد دارد تکنولوژی بلاک‌چین هنوز به آن میزان از بلوغ نرسیده است که بتوان با بکارگیری آن، سیستم‌های زیرساختی و حیاتی پرداخت[1] را تغییر داد و بعنوان جمع‌بندی توصیه می‌کند حداقل باید ۵ سال صبر کرد (تا سال ۲۰۲۱) تا این تکنولوژی به بلوغ کافی برسد. پیش بینی گارتنر اینست که در کوتاه مدت و تا زمان رسیدن به بلوغ، بیشترین کاربردهای واقعی بلاک‌چین در دیگر صنایع (خارج از فضای بانک و پرداخت) خواهد بود. همچون "سیستم های ثبت و مدیریت رکوردها همچون ثبت اسناد رسمی، ثبت دارایی ها و سهام، ثبت احوال و تولد و وفات و همچنین ثبت مالکیت های فکری "

۳. روش تحقیق

با توجه به اهمیت مفهوم بلاک‌چین و اقبال زیاد بانک‌های دنیا به آن، در این مقاله سعی شده است مطالب مرتبط با بررسی سطح بلوغ آن که در سطح جهانی بصورت پراکنده و درقالب استانداردها، گزارشات و مقالات فنی در این‌باره منتشر شده‌اند، جمع‌آوری و تجمیع شده و براساس آن یک ارزیابی جامع از سطح بلوغ فعلی آن ارائه گردد بطوری که عاری از تناقض بوده و شفافیت لازم را جهت استفاده بانک‌های ایران و شرکت‌های فعال در حوزه فناوری‌های پرداخت کشور دارا باشد. برای ارائه پیشنهادات مناسب جهت بکارگیری بلاک‌چین در زیرساخت ایران، مستندات معماری نظام‌های پرداخت ایران (سامانه‌های

[1] - Back-end Bulk Payment system

شتاب، ساتنا و پایا) نیز مورد بررسی قرار گرفته است تا درحد امکان پیشنهادات ارائه‌شده واقع بینانه باشند.

۴. ارزیابی سطح بلوغ فناوری بلاک‌چین

با توجه به حساسیت‌ها و ملاحظات ویژه‌ای که بانک‌ها در رابطه با مسائل مالی مشتریان و افراد جامعه دارند، بسیار مهم است که هر فناوری جدید در این صنعت بصورت کنترل شده و پس از اطمینان کامل از کارایی و بلوغش بکار گرفته شود. به بیان مشخص، هر تکنولوژی جدید برای بکارگیری وسیع در صنعت بانکی مستلزم آنست که سطح قابل قبولی از هر کدام از نیازمندی‌های زیر را تامین نماید (شکل ۶).

- مدل حاکمیت قوی[۱] : مدل حاکمیت تعیین‌کننده‌ی نقش‌ها و مسئولیت‌های بازیگران مختلف بعلاوه‌ی قوانین فنی و کسب و کاری هر تکنولوژی (سرویس ارائه‌شده) است.
- کنترل کامل روی داده‌ها[۲] : به معنای کنترل بانک روی دسترسی به داده‌ها و حفظ محرمانگی آنهاست.
- انطباق با رگولاتوری[۳] : قابلیت تکنولوژی برای تطبیق با قوانین وضع‌شده توسط رگولاتور همانند قواعد ضد پولشویی و شناخت مشتری (KYC).
- استاندارد سازی[۴] : لزوم استاندارد شدن تکنولوژی در تمامی سطوح و واسط‌هایش[۵] به منظور اینکه بتواند در یک اکوسیستم بانکی، با دیگر سامانه‌ها تعامل[۶] و ارتباط داشته باشد.
- هویت سنجی دقیق[۷] : چارچوب هویت سنجی به منظور تشخیص مسئولیت هر تراکنش و تقویت انکارناپذیری
- امنیت در قبال تقلب[۸] : قابلیت جلوگیری، کشف و مقاومت در برابر حملاتی که هر روزه بیشتر و پیچیده تر می‌شوند.
- قابلیت اتکا[۹] : توانایی ارائه‌ی مستمر و قابل قبول سرویس‌های مالی (بعنوان مثال آمار در دسترس بودن بالای ۹۹,۹۹۹ درصد)
- مقیاس پذیری[۱۰] : توانایی ارائه سرویس در مقیاس بالا (بعنوان مثال قابلیت پردازش تعداد بالای تراکنش در هر

[1] - Strong Governance
[2] - Data Control
[3] - regulatory compliance
[4] - Standardization
[5] - Interface
[6] - Interoperability
[7] - identity Framework
[8] - Security and fraud management
[9] - Reliability
[10] - Scalability

شکل ۶) نیازمندی‌هایی که هر تکنولوژی جدید باید سطح قابل قبولی از آنان را تامین نماید تا بتواند بصورت وسیع در صنعت بانک و پرداخت بکارگرفته شود

در ادامه‌ی این بخش، میزان بلوغ فعلی بلاک‌چین در هر یک از این ابعاد و نیازمندی‌ها بررسی می‌شود.

- **مدل حاکمیت**: در حالیکه صنعت بانک و پرداخت نیازمند اعمال حاکمیت قویست بطوریکه تمامی نقش‌ها و مسئولیت‌های بازیگران هر سرویس یا سامانه‌ی آن باید بصورت شفاف مشخص گردد، اما بلوغ بلاک‌چین در این زمینه با نقصان‌ها و دغدغه‌های جدی روبروست. بلاک‌چین از یک مدل خود- حاکمیتی جمعی[1] بهره می‌برد. ممکن است این خاصیت بلاک‌چین در فضای پول‌های مجازی که مدل کسب و کاری آن c2c است، خاصیت جذاب و کارایی باشد، اما در فضای سرویس‌های بانکی نمی‌تواند آن سطح لازم از اعتماد و مسئولیت‌پذیری را حاصل نماید. مهمترین دغدغه، باز (open) بودن بلاک‌چین است. به این معنا که هرکسی قادر است به آن ملحق شده و تراکنش‌ها را مشاهده نمانید (بلاک‌چین با دسترسی آزاد[2]). بلاک‌چین‌های نیازمند مجوز[3] یک گام مثبت در این زمینه برداشته‌اند اما کماکان در تعریف دقیق نقش‌ها و سطح دسترسی افراد درگیر یک تراکنش فاصله‌ی زیادی با نقطه مطلوب فضای بانکی دارند و صرفا به تعیین حق خواندن/ نوشتن[4] برای اعضا و مکانیزهای محدودی برای اعتبارسنجی اکتفا کرده‌اند.
- **کنترل داده‌ها:** غالبا تبادل داده‌ها در تراکنش‌های مالی محرمانه است. چرا که این تراکنش‌ها شامل اطلاعات شخصی

[1] - Community Self-Governing
[2] - Permissionless Blockchain
[3] - Permissioned Blockchain
[4] - Read / Write

فرستنده/گیرنده و همچنین داده‌های حساس مالی آنهاست. بنابراین حفظ محرمانگی داده‌ها و دسترسی کنترل‌شده به آن، از مهمترین نیازمندی‌های صنعت بانکی برای راه‌اندازی هرگونه سرویس و یا راهکاریست. این درحالیست که داده‌هایی که روی دفتر کل بلاک‌چین ذخیره می‌شوند، بین تمام اعضا علام همگانی[1] می‌گردد. البته بصورت تئوری هویت طرفین یک تراکنش به کمک آدرس‌های بی نام، مخفی است، اما همین بی‌نام بودن در فضای کسب و کارهای B2B ممکن است دغدغه‌های بالقوه‌ای را بوجود آورد. چرا که در این فضا یک کمپانی باید از آدرس تمام کمپانی‌هایی که با آنها تعامل دارد آگاه باشد و در واقع بی نام بودن نقض می‌شود. البته برخی از پلتفرهایی که اخیرا مبتنی بر بلاک‌چین توسعه داده شده‌اند همانند Corda، این مشکل را با رمزنگاری محتوای تراکنش، تا حدی برطرف کرده اند[10]. اما همین رمزنگاری محتوا باعث میشود اعتبارسنجی تراکنش با محدودیت‌هایی روبرو باشد که برای بانک قابل قبول نباشد.

- **انطباق با رگولاتوری:** صنعت بانکداری بشدت رگوله است و با درنظر گرفتن تهدیدات جدید در این فضا، این وضعیت هر روز سخت‌گیرانه‌تر نیز شده و قوانین جدیدی وضع می‌شود. همانند قوانین ضد پولشویی. در همین راستا، هر راهکار فنی که بانک عرضه می‌کند باید در قبال اعمال قوانین و انطباق با آنها منعطف باشد. بررسی‌ها نشان می‌دهند وضعیت رگولاتوری بلاک‌چین بسیار مبهم است و هیچ بانک مرکزی یا نهاد دیگری در دنیا پیدا نمی‌شود که بطور شفاف این قوانین را وضع کرده و اعلام کرده باشد. در حال حاضر سوال‌ها و دغدغه‌های جدی در این زمینه وجود دارد از جمله اینکه اصلا چه کسی باید بلاک‌چین را رگوله کند و آیا اینکه قوانینی که قبلا برای بانک‌ها وضع شده بوده کماکان در صورت استفاده از بلاک‌چین هم معتبر است؟ با در نظر گرفتن ماهیت فرا- مرزی[2] بودن بلاک چین، این سوالات اهمیت بیشتری می یابند.

- **استاندارد سازی:** این مقوله به معنای همگون‌سازی سامانه‌های مبتنی بر بلاک‌چین با دیگر سامانه‌های بانک است بطوریکه بتوانند با هم تعامل داشته و داده ردوبدل کنند. امروزه در فضای بانکی استانداردهای متعددی همچون ISO، ISDA و FPL تعریف شده و استفاده می‌شوند. این درحالیست که مطابق با آنچه در مقدمه‌ی این مقاله بیان شده است، تکنولوژی بلاک‌چین فاقد هرگونه استاندارد در هر سطحی است. از فرمت پیام‌ها گرفته تا همبندی[3] شبکه، تا فرمت دفتر کل و یا محتوای قراردادهای هوشمند. حتی هیچ استانداردی روی فرآیند اجماع که یکی از ارکان بلاک‌چین است وضع نشده است.

- **هویت سنجی:** یک چارچوب دقیق برای هویت سنجی طرفین یک سرویس بانکی، از مهمترین نیازمندی‌های سامانه‌های بانکی بحساب می‌آید. قابلیت انکارناپذیری یک تراکنش منبع ایجاد اعتماد بوده و فرآیندهای لازم برای پیگیری دعاوی که ممکن است بوجود آید را تسهیل میکند. هویت سنجی همچنین پیش نیاز هر فرآیند شناخت مشتری (KYC) است که امروزه بسیار مورد تاکید بانک‌ها و نهادهای رگولاتور می‌باشد. بلوغ فعلی پلتفرم‌های بلاک‌چین در این زمینه تا چه حد است؟ برای پاسخ به این سوال باید این مورد را در نظر بگیریم که کاربران یک بلاک‌چین عمومی این قابلیت را دارند که بی‌نام بمانند. هویت‌ها در بلاک‌چین به کمک جفت‌کلیدهای نامتقارن تعریف می‌شوند که هیچ مکانیزمی قابل

[1] - Broadcast
[2] - Cross-Border
[3] - Topology

توجیهی برای بازیابی آنها وجود ندارد. در واقع هیچ نهاد واسطی وجود ندارد که تضمین دهد یک آدرس مشخص به چه هویتی متعلق است.

- **امنیت:** حملات سایبری یک تهدید بسیار جدی و روزافزون برای سامانه‌های بانکی است. تعداد و پیچیدگی این حملات هر روز بیشتر می‌شود. هر راهکار مبتنی بر بلاک‌چین باید با این فرض توسعه داده شود که مورد حملات متعدد قرار خواهد گرفت. بنابراین باید در مقابل چنین حملاتی مقاوم بوده و آنها را کشف نماید. بلاک‌چین بعنوان یک سیستم توزیع‌شده، اصالتا طوری طراحی شده است که در مقابل حملات خرابکارانه مقاوم باشد. در واقع بواسطه توزیع آخرین نسخه‌ی همسان از دفتر کل بین تمام اعضا و همچنین الگوریتمهای رمزنگاری، سطح خوبی از امنیت در بلاک‌چین فراهم شده است و عملا سامانه‌های میتنی بر آن از ریسک نقطه‌ی واحد شکست[1] مبرا هستند. با این وجود این امنیت در ازای یک هزینه هنگفت بدست می‌آید. این هزینه در قالب قدرت پردازشی صرف شده برای فرآیند اجماع بیان می‌شود. ممکن است در برخی موارد، این هزینه آنچنان بالا رود که از منافعی که بدست می‌آید بیشتر نیز شود. به همین دلیل است که پلتفرم‌های جدیدی که توسعه داده می‌شوند از رویکرد بلاک‌چین‌های غیر عمومی و نیازمند مجوز هستند تا بتوان روی تک تک اعضا کنترل دسترسی‌هایی را تعریف نمود.
- **قابلیت اتکا:** تضمین پایداری سامانه‌ها وسرویس‌های بانکی، همتراز با بحث امنیت، در بالاترین سطح حساسیت مدیران و مشتریان بانک است. راهبری سامانه‌ها و در دسترس بودن سرویس آن در بالاترین سطح ممکن برای سامانه‌ای همچون شتاب و ساتنا (RTGS) از اهمیت حیاتی برخوردار است تا حدی که تمهیدات فراوانی برای بازیابی از بحران (بعنوان مثال فاجعه‌های طبیعی همچون زلزله یا جنگ) برای آنها اندیشیده می‌شود. یکی از نقاط قوت فناوری بلاک‌چین، توانایی ذاتی آن در بازیابی و ساختار مقاوم آنست. با این وجود باید در نظر داشت که سامانه‌های مهم بانکی که امروزه مبتنی بر معماری متمرکز هستند، سطح دسترسی بالای ۹۹٪ را فراهم ساخته‌اند. در بلاک‌چین، در دسترس بودن سامانه‌های بلاک‌چینی کاملا به در دسترس بودن زیرساخت اعضای آن وابسته است و توسط یک نهاد مرکزی کنترل نمی‌شود. بنابراین اگر اکثریت اعضای یک شبکه بلاک‌چینی در دسترس نباشند یا عامدا با یکدگیر تبانی کرده و اقدام به انتشار داده‌های غیر معتبر نمایند، می توانند دفتر کل توزیع شده را مخدوش نموده و سرویس آنرا مختل نمایند.
- **مقیاس پذیری:** این یک مساله پذیرفته شده است که سامانه‌های بانکی باید قادر باشند نرخ بسیار بالایی از تراکنشات را (حتی در حد چندین هزار تراکنش در ثانیه) پردازش کنند. طبق آمار موجود در سایت شبکه‌ی شاپرک، رکورد پردازش بیش از ۱۰۰ میلیون تراکنش در یک روز نیز ثبت شده است که با در نظر گرفتن ساعات اوج فعالیت آن، آمار نزدیک به ۲۵۰۰ تراکنش در ثانیه درحالت پیک بدست می‌آید[11]. بر همین اساس، هر راهکار بلاک‌چینی باید قادر باشد این مقیاس سرویس را انجام دهد. اما عملا پروتکل‌های رایجی که برای اجماع در شبکه‌های بلاک‌چینی استفاده می‌شوند،

[1] - Single Point of Failure

همانند همانند روش اثبات کار[1]، در صورتی که اعضای شبکه بسیار زیاد شوند، این مقیاس را به تعداد نسبتا کمی محدود می‌کند

۵. جمع بندی : نتیجه ارزیابی بلوغ بلاک چین و ارائه پیشنهاد برای بکارگیری آن در فضای بانک و پرداخت ایران

در این مقاله به ارزیابی دقیق میزان بلوغ فناوری بلاک‌چین پرداخته شد که این بخش به بیان جمع‌بندی آن می‌پردازد. این مقاله تایید می‌کند که فناوری بلاک‌چین و بطور کلی تکنولوژی دفتر کل توزیع‌شده (DLT[2])، بواسطه نقاط قوت کلیدی خود، زمینه‌ساز تحول در بانکداری خواهد بود و فرصت‌های جدیدی برای افزایش بهره‌وری، کاهش هزینه و ایجاد مدل‌های جدید کسب و کار در بانک‌ها فراهم خواهد کرد. نقاط قوت کلیدی این فناوری شامل موارد "ایجاد اعتماد در یک محیط بدون نهاد واسط"، "کارآمد بودن در پخش همگانی اطلاعات"، "شفافیت در بالاترین سطح"، "تسهیل رفع مغایرت بین بانکی" و "مقاومت در برابر از بین رفتن اطلاعات" می‌شود.

اما نتایج ارزیابی این مقاله بیان می‌کند علی‌رغم فرصت‌های بوجود آمده و توسعه‌های قابل توجهی نیز که در این زمینه رخ داده است، کماکان حجم بالایی از تحقیق و توسعه نیاز است تا این فناوری و پلتفرم‌هایی که بر اسان آن تولید می‌شوند به بلوغ کافی، در حدی که پیش نیازهای صنعت بانکی را تامین نماید، برسند. شکل ۷، خلاصه‌ی ارزیابی بلوغ بلاک‌چین را بر اساس معیارهای صنعت بانک و پرداخت نشان می‌دهد. بر اساس این نتایج، بلاک‌چین در هیچ یک از این حوزه‌ها به بلوغ لازم نرسیده است. در واقع این فناوری در مراحل اولیه توسعه‌ی خود است و به همین علت است که تا کنون هیچ پلتفرمی در بازار ارائه نشده است که این نیازها را بطور کامل تامین نماید تا بتوان از آن در مقیاس بزرگ بانک استفاده کرد. بر اساس شکل ۷، عدم وجود استانداردهای مشخص برای تعامل بلاک‌چین با سامانه‌های قدیمی[3] بانک، عدم وجود یک رگولیشن واحد و شفاف و همچنین نبود یک مدل حاکمیت قوی، از مهمترین کاستی‌های فعلی فناوری بلاک چین است.

با در نظر گرفتن این کاستی‌ها و عدم بلوغ کافی بلاک‌چین، بکارگیری آن در سامانه‌های حیاتی و زیرساختی پرداخت همچون سامانه‌های ملی پرداخت در ایران (همچون شتاب، پایا[4] و ساتنا[5]) بسیار دشوار، غیر قابل توجیه و پر ریسک خواهد بود. ارزیابی این مقاله نشان می‌دهد راهی طولانی در پیش روست تا این فناوری به حدی از بلوغ برسد که بتوان با اطمینان خاطر، معماری سامانه‌های حیاتی پرداخت را بر اساس آن بازطراحی کرد. برآوردهای جهانی نشان می‌دهد این مسیر حداقل به ۵ سال زمان نیاز دارد.

---

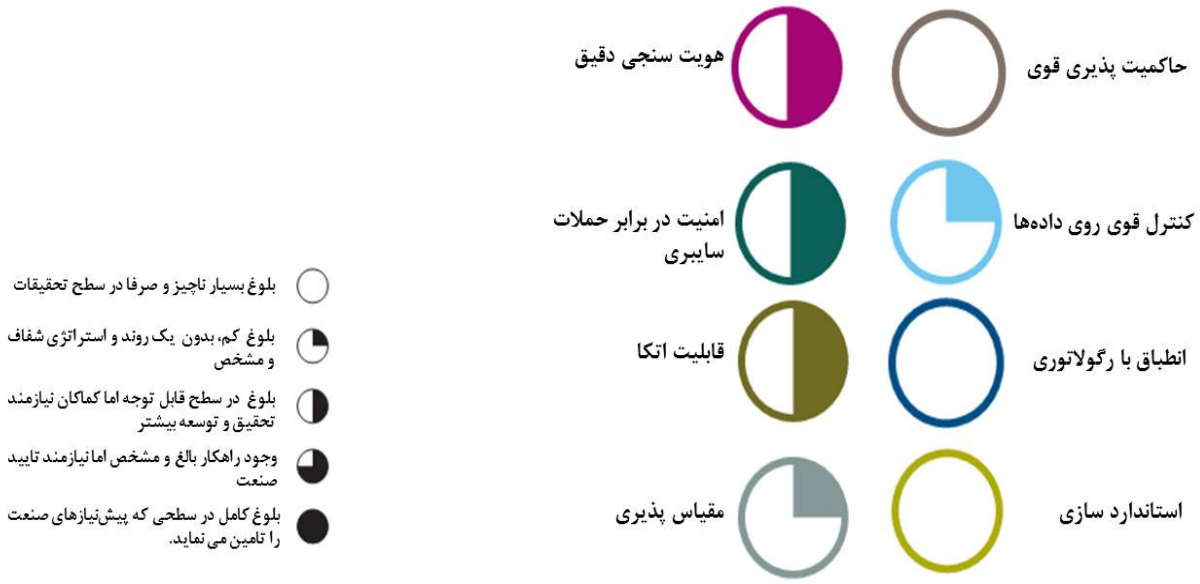
[1] - Proof of Work

[2] - Distributed Ledger Technology

[3] - legacy systems

[4] - سامانه‌ی اتاق پایاپای الکترونیک- معادل ACH

[5] - سامانه تسویه ناخالص آنی ° معادل RTGS



شکل۷) نتایج ارزیابی بلوغ بلاک‌چین

به بانک‌ها و شرکت‌های فعال در عرصه پرداخت ایران پیشنهاد می‌شود تا زمان رسیدن به بلوغ کافی، با انجام پروژه‌های proof of Concept (با دامنه‌ی محدود و در محیط پایلوت) و همچنین پیاده‌سازی سرویس‌هایی که از ریسک سیستمی کمتری برخوردار هستند، دانش سازمانی خود را در مورد بلاک‌چین توسعه داده و آمادگی لازم برای بکارگیری آن در آینده بدست آورند. از جمله مواردی که ریسک کمتری دارند و در حال حاضر مناسب توسعه مبتنی بر بلاک‌چین در فضای بانکی ایران می باشند موارد زیر پیشنهاد می‌شود:

- توسعه‌ی سرویس "ثبت و انتقال چک الکترونیک" مبتنی بر بلاک‌چین. در این اکوسیستم، مشتریان بانک، اعضای این شبکه بلاک‌چین خواهند بود. ثبت یک چک الکترونیک توسط مشتری و انتقالش به مشتری دیگر، در قالب یک تراکنش در بلاک‌چین مربوطه ذخیره می‌شود و بدین روش از انتقال مجدد چک به فرد دیگر و یا مخدوش کردن اطلاعات چک برای تقلب در مبلغ و تاریخ، جلوگیری می‌شود. بانک‌ها نیز در این اکوسیستم نقش اعتبارسنجی تراکنش‌ها(همانند نقش ماینرها[1] در بیت کوین) را بر عهده خواهند داشت. مرحله‌ی نقد شدن چک که حساسیت بالایی دارد، کماکان به روش فعلی و توسط سامانه ی چکاوک انجام خواهد پذیرفت.
- توسعه یک رمزارز جدید با کاربری محدود برای اعضای یک اکوسیستم مشخص (بعنوان مثال باشگاه مشتریان بانک)
- توسعه سیستم اعتبارسنجی مشتریان یک بانک بر اساس تاریخچه رفتار مالی آنان. این تاریخچه در قالب رکوردهای بلاک‌چین می تواند ذخیره گردد و اعتبار هر فرد، برآیند اجماع اعضای شبکه بر اساس پروتکل و قواعدی باشد که خود بانک مشخص می‌کند. (خرد جمعی)

[1] -Miner

- سامانه‌ی تامین مالی جمعی (Crowdfunding) مبتنی بر بلاک چین. در این اکوسیستم، هم متقاضیان تامین مالی و هم سرمایه گذاران، اعضای یک شبکه بلاک‌چین خواهند بود و سابقه و میزان مشارکت هر سرمایه گذار در هر پروژه، بعنوان یک رکورد تراکنش در دفتر کل توزیع شده ذخیره می‌گردد.
- سرویس انتقال وجه خرد آفلاین P2P با سقف محدود روی کیف پول موبایلی (و یا شبکه اجتماعی خاص بانک) مبتنی بر بلاک‌چین

۶. منابع

[1] Nakamato, S. "*Bitcoin: a Peer-to-Peer Electronic Cash System*", white paper (2008) Available at https:// bitcoin.org/bitcoin.pdf

[2] Walker, J.Mike. "*Hype cycle for Emerging Technologies for 2017*", July 2017, Available at www.gartner.com, ID: G00314560.

[3] Business Insider document, "*Here's how banks can save big with blockchain*", (Jan 2017) A discussion Paper available at http://www.businessinsider.com

[4] Care, J. Anthony D. "*Innovation Insight for Blockchain Security*", Aug 2016, Available at www.gartner.com, ID: G00308535.

[5] Furlonger, D. Valdes, R. " *Hype Cycle for Blockchain Technologies and the Programmable Economy, 2016*", July 2016, Available at www.gartner.com, ID: G00308190

[6] Farahmand, H. "*Blockchain: The Dawn of Decentralized Identity*", Sept. 2016, Available at www.gartner.com, ID: G00303143.

[7] Heudecker, N. Judah, S. "*Experiment With Blockchain for Data Management Innovation*", Aug 2016, Available at www.gartner.com, ID: G00314377

[8] Report on "*Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation*", Japan Blockchain Study Group, Nov. 2016, Available at http://www2.deloitte.com

[9] Newton, A. Uzureau, C. "*Blockchain Will Prove to Be a Risky Route for Payment Systems*", 2016, Available at www.gartner.com, ID: G00310735

[10] Brown, R Carlyle, J. Grigg, I. "*Corda: An Introduction* ", white paper (2016) , Available at https:// docs.corda.net

[11] مراجعه شود به آمار منتشر شده در سایت https://shaparak.ir/