پژوهشکده پولی و بانکی
بانک مرکزی جمهوری اسلامی ایران

کاربرد پول دیجیتال بانک مرکزی در زنجیرهٔ تأمین‌مالی

گزارش سیاستی

زمستان ۱۴۰۰

www.mbri.ac.ir

پژوهشکده پولی و بانکی
بانک مرکزی جمهوری اسلامی ایران

شناسنامهٔ گزارش

شمارهٔ گزارش: MBRI-PR-1414

عنوان گزارش سیاستی: کاربرد پول دیجیتال بانک مرکزی در زنجیرهٔ تأمین‌مالی

نویسنده: زهرا لطیفی

ناظر داخلی: دکتر سیداحمدرضا جلالی نائینی

واژگان کلیدی: پول دیجیتال بانک مرکزی، پرداخت، زنجیرهٔ تأمین‌مالی

طبقه‌بندی JEL: D86, E42, E51, E42, E44, E51, L14, O33, O38, L86

تاریخ انتشار گزارش: آذر ۱۴۰۰

خلاصه مدیریتی

شکاف در زیرساخت‌های مالی پیامدهای طولانی‌مدت برای توسعهٔ اقتصادی و اجتماعی دارد. ابزارهای معمول تأمین‌مالی، به‌دلیل بهره‌وری پایین، هزینه‌های بالای معامله، و مدت‌زمان معاملهٔ طولانی، از عوامل اصلی در عدم تطابق بین توسعهٔ زیرساخت‌ها و تأمین‌مالی موجود محسوب می‌شوند (تیان[1] و همکاران، ۲۰۲۰). همچنین در تأمین‌مالی سنتی، اشکالاتی در مدیریت جریان اطلاعات، تدارکات، و جریان سرمایه وجود دارد که منجر به نابرابری و عدم تقارن اطلاعات می‌شود. کلاهبرداری و تقلب در نحوهٔ استفاده از تسهیلات نیز به‌وفور اتفاق می‌افتد. برای حل مشکلات مالی سنتی، در این گزارش نوع جدیدی از بستر مالی را معرفی می‌کنیم که از پول دیجیتال بانک مرکزی، توکن‌سازی بلاک‌چین، و قراردادهای هوشمند برای مدیریت کل فرایند بهره می‌برد. این بستر مشکل عدم اعتماد را بین دهنده و گیرندهٔ وام مرتفع می‌کند؛ کارایی جریان سرمایه و جریان اطلاعات را بهبود می‌بخشد؛ هزینه‌ها را کاهش می‌دهد و خدمات مالی بهتری را به طرف‌های مربوطه ارائه می‌دهد. پول دیجیتال بانک مرکزی ماهیت نظارت را تغییر داده و این نظارت متمرکز جمع‌آوری و تجزیه و تحلیل داده‌های عمدهٔ مالی کاربران را تسهیل می‌کند (دوو[2] و همکاران، ۲۰۲۰). برای نظارت بر تسهیلات در شبکهٔ پول دیجیتال بانک مرکزی، می‌توان فاکتورها را به توکن تبدیل کرد. توکن‌ها می‌توانند طیف وسیع‌تر و متنوعی از وام‌دهندگان را جذب کنند، زیرا وجوه می‌تواند از هر فردی که به شبکهٔ پول دیجیتال بانک مرکزی دسترسی دارد، تأمین شود. یک فاکتور توکنایزشده مجهز به ویژگی‌هایی مانند قابل ردیابی‌بودن، تقسیم‌پذیری و تغییرناپذیری است که می‌تواند توسط چندین وام‌دهنده تأمین شود، ضمن اینکه از تأمین‌مالی مضاعف جلوگیری می‌کند. علاوه‌براین، می‌توان مالکیت توکن‌های فاکتور را در شبکه منتقل کرد. در نهایت، فرایند توکنایزکردن این پتانسیل را دارد که به تحول در زنجیرهٔ تأمین‌مالی اعم از کاهش هزینهٔ تأمین اعتبار تأمین‌کنندگان، شفافیت، حذف واسطه، کاهش تقلب، کاهش زمان، و اطمینان از محل خرج تسهیلات کمک کند.

نتایج تحقیقات نشان می‌دهد نشانه‌گذاری (توکنایزکردن) می‌تواند مدیریت نقدینگی، بازده معاملات، و شفافیت را بین واسطه‌ها بهبود بخشد. از طرفی به‌دلیل زیرساخت‌های فنی محدود، عدم قطعیت مقررات، نوسانات بازار توکن و نبود بخش دولتی، پتانسیل آن هنوز به‌طور کامل درک نشده است (تیان و همکاران، ۲۰۲۰). پول دیجیتال بانک مرکزی اگرچه فرصت‌هایی را ارائه می‌دهند، بسته به هدف افرادی که به انبوه داده‌های تولیدشده دسترسی دارند، پتانسیل ایجاد تهدید را نیز دارند. میزان سود و تهدید بالقوه تا حد زیادی به نیت مسئولان طراحی و استقرار این فنّاوری بستگی دارد. از بُعد مثبت، پول دیجیتال بانک مرکزی می‌تواند با افزایش نظارت بر جامعه، توانایی مقامات را در درک چگونگی عملکرد اقتصاد و پاسخ‌گویی به مشکلات افزایش دهد و از جنبهٔ منفی، داده‌های جمع‌آوری‌شده می‌توانند توانایی نظارت بر جامعه را برای اقتدارگرایان جهت استفاده از قدرت سیاسی حتی در خارج از مرزهای جغرافیایی تقویت کنند (هافمن[3]، ۲۰۲۱). در میان حجم عظیمی از داده‌های شخصی که به‌عنوان ورودی برای فعالیت تجاری جمع‌آوری و پردازش می‌شوند، یک چالش مهم از اقتصاد دیجیتال مطرح می‌شود که شامل مسائل مربوط به حاکمیت داده‌ها، حمایت از مصرف‌کننده، و شیوه‌های ضد رقابتی ناشی از انبار داده است. نتیجهٔ نهایی این فرایند نه‌تنها به فنّاوری بلکه به ساختار اساسی بازار و چهارچوب حاکمیت داده‌ها بستگی دارد. بنابراین، تلاش اصلی بر ایجاد تعادل بین «ناشناس‌بودن و قابل کنترل‌بودن»[4] است.

برای برآوردن نیازهای درحال تحولِ بازارهای مالی و اطمینان از یک نظام مالی باثبات و سالم، تعدادی از بانک‌های مرکزی آزمایش‌هایی برای پول دیجیتال بانک مرکزی و فنّاوری زیربنایی مرتبط با آن (به‌ویژه فنّاوری دفترکل‌توزیع‌شده) انجام داده‌اند. بااین‌حال، آزمایش‌های اولیه مزایای قابلِ‌توجهی برای پرداخت کلان نشان نداده است. اگرچه در مورد بلوغ فنّاوری دفترکل توزیع‌شده تردیدهایی وجود دارد، فنّاوری‌ها و طرح‌های احتمالی مرتبط به‌سرعت درحال تکامل‌اند و بانک‌های مرکزی باید دائماً ارزیابی کنند که آیا پول دیجیتال بانک مرکزی با این فنّاوری می‌تواند مفید باشد یا خیر.

---

[1] Tian

[2] Du

[3] Hoffman

[4] Controllable Anonymity

فهرست مطالب

فهرست شکل‌ها

۱ مقدمه

پول دیجیتال بانک مرکزی[1] یک شکل دیجیتال از پول است که توسط یک بانک مرکزی صادر می‌شود. این نوع پول را مقام پولی یک کشور تنظیم می‌کند و بانک مرکزی، دولت، یا نهادهای مجازِ بخش خصوصی با استفاده از پایگاه داده‌ای کنترل و اجرا می‌کنند. در یک طبقه‌بندی کلی، پول دیجیتال بانک مرکزی به دو نوع خرد و کلان تقسیم می‌شود.

۱-۱ پول دیجیتال بانک مرکزی در سیستم کلان

پول دیجیتال بانک مرکزی کلان[2] برای تسویهٔ نقل‌وانتقالات بین‌بانکی و معاملات عمده در نظر گرفته شده است و مانند ذخایر نگهداری‌شده در بانک مرکزی اما با قابلیت‌های اضافی عمل می‌کند. از لحاظ هزینه‌های عملیاتی و استفاده از وثیقه و نقدینگی، استفاده از پول‌های دیجیتال بانک مرکزی کلان از امنیت بیشتری برخوردار است. این نوع پول که قابلِ‌مقایسه با ذخایر سنتی بانک مرکزی در سیستم‌های پرداخت بین‌بانکی است، می‌تواند به‌طور بالقوه کارایی و مدیریت ریسک در تسویه را بهبود بخشد. یک مثال مشروط‌بودن پرداخت‌هاست که در آن پرداخت تنها در صورت برآورده‌شدن شرایط خاصی انجام می‌شود که می‌تواند طیف گسترده‌ای از دستورالعمل‌های پرداخت مشروط را شامل شود، که فراتر از مکانیسم «تحویل درمقابل پرداخت»[3] امروز در سیستم‌های تسویهٔ ناخالص آنی[4] است. در واقع، پول‌های دیجیتال بانک مرکزی کلان می‌توانند «پول قابلِ‌برنامه‌ریزی بانک مرکزی»[5] را برای خودکارسازی و کاهش ریسک پشتیبانی کنند. این رویکرد به سیستم اجازه می‌دهد تا استانداردهای بین‌المللی را برای حمایت از قابلیت همکاری طراحی کند (بانک تسویهٔ بین‌الملل، ۲۰۲۱).

علاوه‌براین، فنّاوری پول دیجیتال بانک مرکزی کلان امکان پیوند به سایر پلتفرم‌ها را مهیا می‌کند. پیوند مستقیم اوراق بهادار یا پلتفرم‌های تبدیل ارز[6] به پلتفرم‌های نقدی می‌تواند سرعت معاملات را افزایش دهد و ریسک تسویه را از بین ببرد. تسویه‌حساب در بازارهای فرابورس و همچنین اعطای وام‌های تجاری و تأمین‌مالی تجارت، در صورت پیوند مستقیم با یک سیستم پول دیجیتال بانک مرکزی کلان به‌طور قابلِ‌توجهی بهبود می‌یابد. پول‌های دیجیتال بانک مرکزی کلان همچنین می‌تواند زیرساخت پرداخت فرامرزی را ساده کند و تعداد واسطه‌های درگیر را به‌شدت کاهش دهد. این ویژگی در زنجیرهٔ تأمین‌مالی بین‌المللی می‌تواند کارایی و امنیت را بهبود بخشد، نقدینگی و ریسک طرف مقابل[7] را به حداقل برساند، و هزینه را کاهش دهد.

همچنین، استقرار فنّاوری دفترکل توزیع‌شده[8] اجازه می‌دهد تا ویژگی‌های هوشمند از قبیل اختصاص بودجه، محدودکردن استفاده از آن در زمان و مکان، اعمال نرخ بهرهٔ مشروط، و موارد دیگر فراهم شود. این ویژگی‌های هوشمند به بانک‌های مرکزی این امکان را می‌دهد تا ابزارهای جدید و قدرتمند سیاست‌های پولی عملیاتی مانند نرخ‌های بهره را بررسی کنند.

۱-۲ پول دیجیتال بانک مرکزی در سیستم خرد

پول‌های دیجیتال بانک مرکزی خرد سیستم پولی دوطرفهٔ متعارف را تغییر می‌دهند، به این دلیل که پول دیجیتال بانک مرکزی در اختیار عموم قرار می‌گیرد، همان‌طور که پول نقد برای عموم مردم به‌عنوان مطالبهٔ مستقیم از بانک مرکزی در دسترس است. مسئلهٔ مهم برای نظام پرداخت این است که پول‌های دیجیتال بانک مرکزی خرد چگونه در مدیریت داده‌ها، چشم‌انداز رقابتی شرکت‌های ارائه‌دهندهٔ خدمات پرداخت، و کل صنعت پرداخت تأثیر می‌گذارد. بانک‌های مرکزی می‌توانند با تسهیل ورود بازیگران جدید و پرورش نوآوری در خدمات پرداخت، عملکرد سیستم پولی را تقویت کنند. این اهداف را می‌توان با ایجاد بسترهای پرداخت باز[9] که رقابت و نوآوری را ترویج می‌کنند، تضمین کرد؛ در این‌صورت تأثیرات شبکه به‌سمت رقابت بیشتر و خدمات بهتر هدایت می‌شود (بانک تسویهٔ بین‌الملل، ۲۰۲۱).

---

[1] Central Bank Digital Currency (CBDC)

[2] Wholesale CBDCs

[3] Delivery Versus Payment (DVP)

[4] Real-Time Gross Settlement (RTGS)

[5] Programmable Money CBDC

[6] Foreign Exchange (FX)

[7] Counterparty Risk

[8] Distributed Ledger Technology (DLT)

[9] Open Payment Platforms

پول‌های دیجیتال بانک مرکزی خرد به دو شکل در دسترس‌اند:

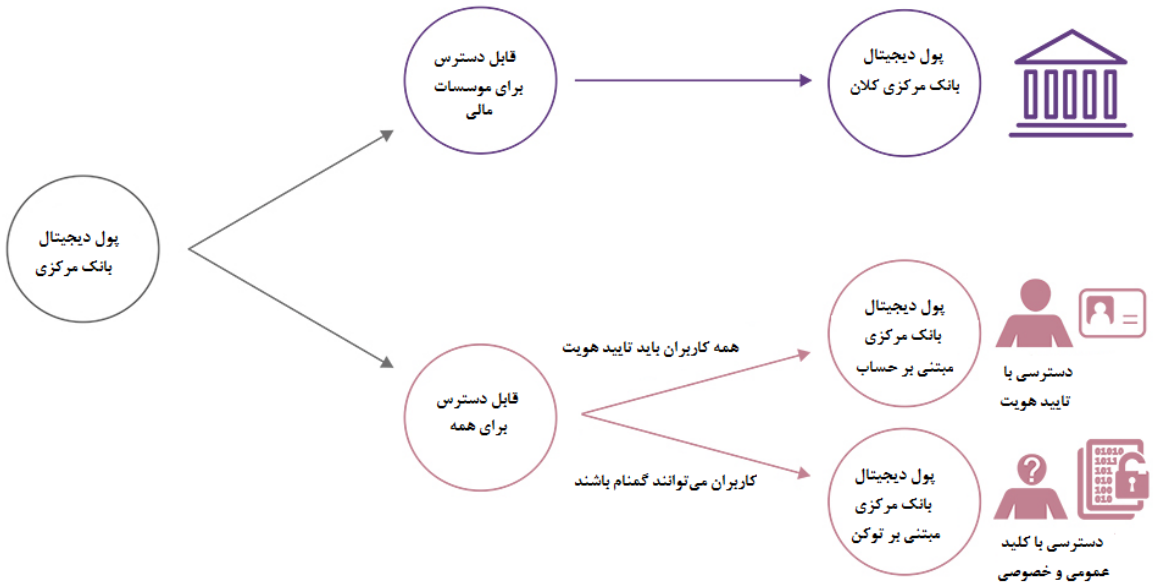
۱ـ۲ـ۱ مبتنی بر حساب

این رویکرد مبتنی بر تأیید هویت کاربران (دسترسی مبتنی بر حساب) است. پول‌های دیجیتال بانک مرکزی مبتنی بر حساب[1]، که قبلاً به‌عنوان پول الکترونیکی بانک مرکزی توصیف می‌شدند، درست مانند حساب‌های سپردهٔ معمولی عمل می‌کنند. کاربر ملزم به ایجاد حسابی است که می‌تواند با آن تراکنش انجام دهد و همچنین پول دیجیتال را ارسال و دریافت کند. یک معامله به دسترسی به اطلاعات کاربران برای تأیید شناسهٔ فرستنده و گیرنده نیاز دارد. در نوع سپرده‌محور، معاملات ناشناس امکان‌پذیر نیست.

۱ـ۲ـ۲ مبتنی بر توکن‌های دیجیتال

توکن دیجیتال[2] مشابه پول نقد است که امکان دسترسی به توکن و ناشناس‌بودن در پرداخت‌ها را فراهم می‌کند. این گزینه به کاربران شخصی اجازه می‌دهد تا براساس یک امضای دیجیتال با استفاده از رمزنگاری کلید خصوصی‌ـعمومی، بدون نیاز به شناسایی شخصی، به پول دسترسی داشته باشند.

سیستم‌های مبتنی بر توکن شامل انتقال ارزش از یک کیف پول به کیف پول دیگر است. در نظام‌های مالی سنتی، یک توکن می‌تواند یک اسکناس یا یک سکه باشد. بیت‌کوین نمونهٔ ارزهای رمزنگاری‌شدهٔ مبتنی بر توکن است. سیستم‌های مبتنی بر توکن دیجیتال نیازی به تأیید هویت کاربر برای ارسال یا دریافت پرداخت ندارند؛ اما معامله براساس کلیدهای عمومی و خصوصی و امضای دیجیتال بین فرستنده و گیرنده تأیید می‌شود. توکن دیجیتال امکان دسترسی به رمز و ناشناس‌بودن در پرداخت‌ها را فراهم می‌کند. این گزینه به کاربران شخصی اجازه می‌دهد تا براساس یک امضای دیجیتال رمز عبور با استفاده از رمزنگاری کلید خصوصی و عمومی، بدون نیاز به شناسایی شخصی، به پول دسترسی داشته باشند (بانک تسویهٔ بین‌الملل، ۲۰۲۱).



شکل ۱ . انواع پول دیجیتال بانک مرکزی

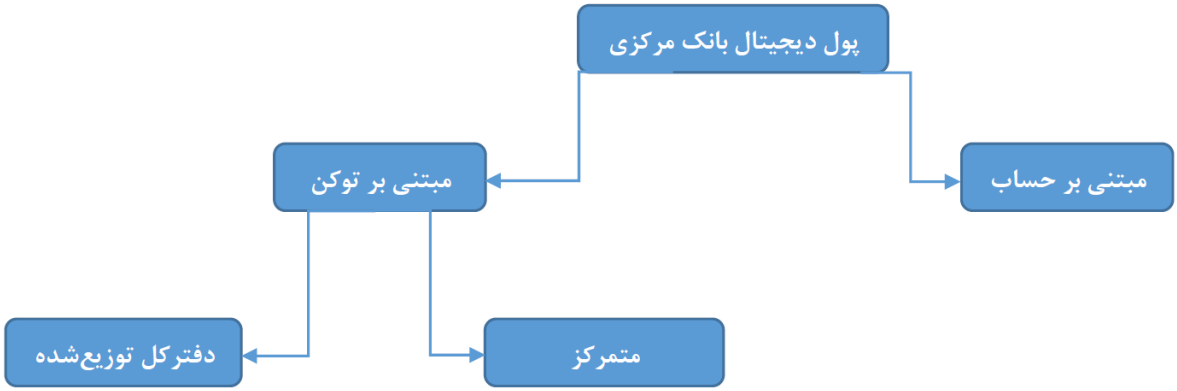
منبع: بانک تسویهٔ بین‌الملل، ۲۰۲۱

پول دیجیتال بانک مرکزی مبتنی بر توکن‌های دیجیتال، خود به دو نوع متمرکز و غیرمتمرکز (مبتنی بر دفترکل توزیع‌شده) تقسیم می‌شود. با دفترکل توزیع‌شده پس از اجماع و توافق، ثبت معاملات بین شرکت‌کنندگان هم‌زمان می‌شود. بدون دفترکل توزیع‌شده، اعتبار هر معامله توسط یک داور خاص تعیین می‌شود. شکل ۲ طبقه‌بندی پول دیجیتال مبتنی بر توکن بانک مرکزی را نشان می‌دهد.

---

[1] Account-Based

[2] Figital Token



شکل ۲ . تاکسونومی پول دیجیتال مبتنی بر توکن بانک مرکزی

منبع: گودل و همکاران، ۲۰۲۱

براساس بررسی که بانک تسویهٔ بین‌الملل انجام داده است، حدود ۸۰ درصد از بانک‌های مرکزی درحال کار روی جنبه‌ای از پول دیجیتال بانک مرکزی اعم از تحقیق، طراحی، یا اجرای آزمایشی هستند. در سال ۲۰۲۰، باهاما «سند دالر»[1] را به‌عنوان پول دیجیتال بانک مرکزی خرد راه‌اندازی کرد. بعضی کشورها درحال برنامه‌ریزی پول دیجیتال بانک مرکزی خرد به‌عنوان جایگزین پول نقد هستند. به‌طور خاص، چین و سوئد درحال پیشرفت خوب و انجام اجرای آزمایشی‌اند. در سوئد، تصمیم برای راه‌اندازی «ای‌کرونا»[2] از اوایل سال ۲۰۲۲ جدی است. بانک مرکزی اروپا درحال کار روی پیکربندی یورو دیجیتال است. بااین‌حال، معرفی یورو دیجیتال پیش از سال ۲۰۲۵ پیش‌بینی نمی‌شود.

فعالیت پیرامون پول دیجیتال بانک مرکزی کلان نیز زیاد است. بانک تایلند با پروژهٔ اینتانون[3] درحال حاضر در مرحلهٔ پیشرفته قرار دارد. سازمان پول هنگ‌کنگ، قصد دارد یک پلتفرم با چند پول دیجیتال بانک مرکزی را معرفی کند که می‌تواند معاملات چندارزی را بسیار سریع‌تر و مقرون‌به‌صرفه پردازش کند. همچنین، سنگاپور در شرف راه‌اندازی پول دیجیتال بانک مرکزی کلان است. درحال حاضر، فقط منتظر تصمیم مقامات برای اجرای پروژهٔ یوبین[4] است. در ایالات متحده، انجمن دیِم[5] درحال کار با بانک سیلورگیت[6] برای صدور یک پول دیجیتال پایدار[7] با پشتوانهٔ دلار است. یک مثال دیگر Sygnum's DCHF است: توکن دیجیتال که یک به یک به فرانک سوئیس متصل و کاملاً توسط فرانک پشتیبانی می‌شود. سوئیس در میان کشورهایی است که امکانات پول دیجیتال بانک مرکزی کلان را بررسی می‌کند. SNB، SIX، و BIS Innovation Hub (BIH) در دسامبر سال ۲۰۲۰ گزارش کردند که به‌عنوان بخشی از پروژهٔ هلوتیا[8]، دو مطالعهٔ امکان‌سنجی در زمینهٔ تسویهٔ دارایی‌های توکنایزشده با پول بانک مرکزی روی یک دفترکل توزیع‌شده انجام شده است. SNB، SIX، و BIS Innovation Hub پروژهٔ هلوتیا را در سال ۲۰۲۱ ادامه می‌دهند. هدف این است که اطمینان حاصل شود مزایای دفترکل توزیع‌شده بیش از هزینه‌های آن است (بانک مرکزی سوئیس، ۲۰۲۱). SNB با موفقیت دو مطالعهٔ امکان‌سنجی را به‌همراه SIX و BIS Innovation Hub در سال ۲۰۲۰ انجام داد. از یک طرف، امکانات قانونی صدور پول دیجیتال بانک مرکزی کلان برای بازار بین‌بانکی (اثبات مفهوم یک[9]) مورد بررسی قرار گرفت. از طرف دیگر، سیستم پرداخت موجود برای پردازش دارایی‌های توکنایزشده (اثبات مفهوم[10] ۲) به یک سیستم عامل دفترکل توزیع‌شده مرتبط شد. طرفین درگیر هر دو مورد را ارزیابی و مقایسه کردند.

بانک مرکزی چین نیز با رنمینبی دیجیتال[11] یک گام اساسی برای تغییر برداشته است. در سه‌ماههٔ نخست ۲۰۲۱، اولین معاملهٔ کسب‌وکار به

---

[1] Sand Dollar
[2] E- krona
[3] Inthanon
[4] Ubin
[5] Diem
[6] Silvergate
[7] Stablecoin
[8] Helvetia
[9] PoC1
[10] Proof of Concept
[11] Renminbi (e-RMB)

کسب‌وکار[1] از طریق رنمینبی دیجیتال انجام شد. رنمینبی دیجیتال چیزی فراتر از یک وسیله برای مبادله است. بانک مرکزی چین نیز می‌تواند همهٔ جریان‌های مالی را کنترل کند و کنترل بیشتری بر نظام مالی و حساب‌های سرمایهٔ چین اعمال کند (هافمن، ۲۰۲۰). یایا فانوزی و امیلی جین[2] در گزارشی که برای مرکز امنیت امریکا نوشتند ادعا کرده‌اند که رنمینبی دیجیتال احتمالاً باعث نظارت در اقتصاد و دخالت دولت در زندگی شهروندان چینی خواهد بود. آن‌ها ادعا کردند استقرار یوان الکترونیکی[3] یا رنمینبی دیجیتال باعث می‌شود بانک مرکزی اطلاعات عظیمی از فعالیت اقتصادی شهروندان خود را استخراج کند. هافمن[4] در ASPI، که سال گذشته یکی از اولین گزارش‌ها در مورد رنمینبی دیجیتال را منتشر کرد، می‌گوید یوان الکترونیکی توانایی نظارت را به میزان قابلِ‌توجهی گسترش می‌دهد. پول دیجیتال بانک مرکزی چین هم توسط بانک مرکزی چین و هم از طریق عموم مردم استفاده می‌شود و قرار است به‌جای پول نقد در گردش[5] جایگزین شود. این پول دیجیتال یک طرح عملیاتی دولایه خواهد داشت. ردیف اول بانک خلق چین است که صدور آن را کنترل می‌کند. ردیف دوم شامل بانک‌های تجاری مانند علی‌پی[6] است که توزیع را کنترل می‌کند. اگرچه این پول دیجیتال با مشخصهٔ «ناشناس‌بودن کنترل‌شده» درحال ساخت است، گمنامی واقعی را ارائه نمی‌کند، زیرا بانک مرکزی چین بر جریان معاملات پایان به پایان و همچنین ثبت‌نام کاربران و مؤسسات نظارت دارد.

۲ استفاده از پول دیجیتال بانک مرکزی در زنجیرهٔ تأمین‌مالی

برای کاهش تقلب در پرداخت و استفاده از تسهیلات می‌توان از یک پلتفرم «کسب‌وکار به شخص»[7] که به شبکهٔ پول دیجیتال بانک مرکزی متصل شود، استفاده کرد. خریداران، فروشندگان (تأمین کنندگان)، و بانک‌ها، اسناد تجاری را از طریق پلتفرم مبادله کنند و پرداخت‌ها از طریق پول دیجیتال بانک مرکزی، حتی در ساعات غیرکاری و تعطیلات انجام شود. همچنین، ازآنجاکه پول دیجیتال بانک مرکزی در داخل شبکه قابلِ‌دسترسی است، امکان ردیابی وضعیت معاملات را فراهم می‌کند و نیازی به مدیریت چندین قالب دستورالعمل پرداخت را از بین می‌برد و شفافیت، هرگونه تقلب را کاهش می‌دهد. اگرچه انتظار نمی‌رود پرداخت‌های پول دیجیتال بانک مرکزی به‌طور کامل جایگزین خدمات پرداخت موجود بانک‌ها شود، پرداخت‌های پول دیجیتال بانک مرکزی می‌توانند در کنار سپرده‌های بانکی و خدمات پرداخت نقش داشته باشند.

گردش کار پرداخت کسب‌وکارها در بستر «کسب‌وکار به شخص» می‌تواند مانند شکل ۳ باشد:

شکل ۳. گردش کار پرداخت کسب‌وکارها در پلتفرم

منبع: ستادوم و همکاران[8]، ۲۰۲۰

---

[1] B2B
[2] Yaya Fanusie and Emily Jin
[3] E-Yuan
[4] Hoffman
[5] M0
[6] Alipay
[7] Business To Person (B2P)
[8] Sethaudom and Supapongse

۱ــ خریدار سفارش خرید کالا از شرکت فروشنده (تأمین‌کننده) را می‌دهد.
۲ــ فروشنده کالا را به خریدار تحویل می‌دهد.
۳ــ فروشنده از طریق بستر کسب‌وکار به شخص فاکتور را برای خریدار ارسال می‌کند.
۴ــ بستر کسب‌وکار به شخص اسناد تجاری را تأیید می‌کند و خریدار پرداخت را تأیید می‌کند.
۵ــ از طریق فراخوانیِ رابط برنامه‌نویسی کاربردی[1]، انتقال در شبکهٔ پرداخت پول دیجیتال بانک مرکزی آغاز می‌شود.

۳ گردش کار توکنایزکردن فاکتور در زنجیرهٔ تأمین‌مالی

پلتفرم‌های «کسب‌وکار به شخص» با استفاده از فنّاوری بلاک‌چین، راهکارهای خرید خودکار مانند تطبیق و تأیید سفارش‌های خرید، رسید کالاها و فاکتورها را در اختیار اعضای شبکه قرار می‌دهد. تأمین‌کنندگان می‌توانند فاکتورها را به‌عنوان وثیقه برای درخواست تأمین‌مالی از وام‌دهندگان در همین بستر ارسال کنند. البته، اگر پلتفرم در دسترس تعداد محدودی از وام‌دهندگان باشد، تأمین‌کنندگان نمی‌توانند با نرخ رقابتی به بودجه دسترسی پیدا کنند. توکنایزاسیون فاکتور و گردش کار تأمین‌مالی به شرح شکل ۴ است.

شکل ۴ . توکنایزکردن فاکتور و گردش کار تأمین‌مالی

منبع: ستادوم و همکاران، ۲۰۲۰

۱ــ پس از اینکه خریدار فاکتور را به یک تأمین‌کننده ارسال کرد، تأمین‌کننده می‌تواند فاکتور را برای درخواست تأمین‌مالی از بستر کسب‌وکار به شخص انتخاب کند.

- اطلاعات فاکتور به‌عنوان مثال شمارهٔ فاکتور، خریدار، و اطلاعات تأمین‌کننده، میزان پول، و تاریخ سررسید برای توکنایزکردن به برنامهٔ غیرمتمرکزِ تأمین‌مالی در شبکهٔ پول دیجیتال بانک مرکزی ارسال می‌شود.
- قرارداد هوشمند توکن‌های فاکتور را در شبکهٔ پول دیجیتال بانک مرکزی تولید می‌کند. فاکتور با تعداد مشخصی از توکن‌ها نشان داده می‌شود.
- این اطلاعات فاکتور در پلتفرم در دسترس افراد مجاز قرار می‌گیرد.

۲ــ هر وام‌دهنده (بانک‌ها) می‌تواند اطلاعات فاکتور را در برنامه مشاهده و انتخاب کند که توکن‌ها را با نرخ بهره خریداری کند.

- وام‌دهنده می‌تواند همه یا بخشی از فاکتور را به‌صورت توکن خریداری کند.
- هنگامی‌که وام‌دهنده توکن‌های فاکتور را خریداری می‌کند، کیف پول وام‌دهنده به برنامه متصل می‌شود و یک معامله برای مبادلهٔ پول دیجیتال بانک مرکزیِ وام‌دهنده با توکن‌های فاکتور انجام می‌شود.

۳ــ تأمین‌کنندگان می‌توانند پول دیجیتال بانک مرکزی را که مبلغی است که وام‌دهنده از توکن‌های فاکتور خریداری کرده است، از طریق قرارداد هوشمند دریافت کنند.

۴ــ در تاریخ سررسید فاکتور، خریدار به تأمین‌کننده پول پرداخت می‌کند.

۵ــ وام‌دهنده پس از موعد مقرر، توکن‌ها را از تأمین‌کننده بازخرید و بهرهٔ آن را دریافت می‌کند.

[1] Application Programming Interface (API)

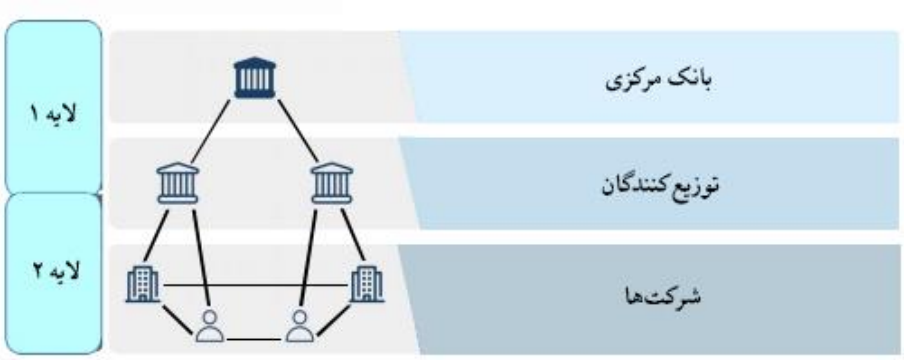
۴ نظارت بر تسهیلات با استفاده از قرارداد هوشمند

قرارداد هوشمند می‌تواند برای نظارت بر استفادهٔ درست از تسهیلات و یا مدیریت وام‌دهی استفاده شود. وام‌ها همراه با اطلاعات مالکیت وثیقه می‌توانند به‌عنوان قراردادهای هوشمند در بلاک‌چین ذخیره شوند. اگر وام‌گیرنده به تعهدات خود عمل نکند، قرارداد هوشمند می‌تواند به‌طور خودکار کلیدهای دیجیتال را که دسترسی وی به وثیقه را تضمین می‌کند، لغو کند. نکتهٔ حائز اهمیت این است که قراردادهای هوشمند تحول در سیستم حقوقی است و جایگزین سیستم حقوقی نخواهد بود. نقش وکلا ممکن است از داوری قراردادهای فردی به تولید الگوهای قرارداد هوشمند در بازار رقابتی تغییر یابد. امتیاز فروش قرارداد می‌تواند کیفیت، میزان قابل تنظیم‌بودن و سهولت استفاده از آن‌ها باشد. در درازمدت، می‌توان شاهد افزایش بازارهای سازمان‌یافتهٔ قراردادهای هوشمند بود که کاملاً از طریق قراردادهای هوشمند مدیریت می‌شوند (توستا و همکاران، ۲۰۱۹).

حساب‌های Escrow (مفهومی حقوقی که یک ابزار مالی را توصیف می‌کند که به‌موجب آن، دارایی توسط شخص ثالثی به نمایندگی از دو طرف دیگر که درحال انجام یک معامله هستند، نگهداری می‌شود): قراردادهای هوشمند می‌توانند به‌عنوان حساب‌های Escrow تنظیم شوند که مبادله بین دو طرف را کنترل می‌کند. این قرارداد، خدمات خارجی را کنترل می‌کند (به‌عنوان مثال ردیابی GPS) و وقتی مالکیت از فروشنده به خریدار منتقل می‌شود، قرارداد به‌طور خودکار وجوه را به فروشنده آزاد می‌کند. البته، پیاده‌سازی قراردادهای هوشمند کار ساده‌ای نیست و چالش‌هایی دارد که یکی از آن‌ها انعطاف‌پذیری است. قراردادهای هوشمند فرض می‌کنند که طرفین می‌توانند تمام جنبه‌های مذاکرات را در آغاز معاملهٔ خود تعیین کنند. اما در دنیای واقعی، قراردادها غالباً مبهم‌اند، زیرا آنچه پس از توافق طرفین اتفاق می‌افتد اغلب غیرقابل پیش‌بینی است. قراردادهای هوشمند باید دارای سازوکارهایی باشند که به طرفین اجازه دهد در صورت تمایل طرفین، توافق‌نامه‌های خود را اصلاح کنند.

۵ سیستم و نقش‌های دولایه در شبکهٔ پول دیجیتال بانک مرکزی

یک سؤال اساسی در طراحی پول دیجیتال بانک مرکزی، نقش‌های مربوط به بانک مرکزی و بخش خصوصی، و دسترسی آن است. در یک سیستم پول دیجیتال بانک مرکزی یک‌لایه، بانک مرکزی مسئول کل فرایند پایان به پایان ازجمله پردازش مشتری، صدور پول دیجیتال بانک مرکزی، نگهداری حساب و تأیید معامله است؛ اما سیستم دولایه از واسطه‌ها برای توزیع پول دیجیتال بانک مرکزی و انجام کلیهٔ فعالیت‌ها و خدمات رو به مشتری استفاده می‌کند.



شکل ۵. سیستم دولایهٔ واسطه‌ها برای توزیع پول دیجیتال بانک مرکزی

منبع: ستادوم و همکاران، ۲۰۲۰

سطح بانک مرکزی: بانک مرکزی به‌عنوان تنها صادرکنندهٔ پول دیجیتال بانک مرکزی، مسئول صدور، امحا، و کنترل پول دیجیتال در گردش است.

سطح توزیع کننده: تحت یک سیستم دولایه، توزیع‌کنندگان مانند بانک‌های تجاری و ارائه‌دهندگان خدمات پرداخت مسئولیت رسیدگی به عملکردهای مربوط به کاربر و توزیع، مانند فرایندهای شناسایی مشتری[1] و مبادلهٔ پول دیجیتال بانک مرکزی و سپرده‌ها را دارند. ازاین‌رو،

[1] Know Your Customer (KYC)

واسطه‌ها ضروری‌اند، حتی اگر مسئولیتی در قبال تسویه‌حساب و تأمین نهایی معامله نداشته باشند. قابلیت همکاری یکپارچه با پلتفرم توزیع‌کننده برای مدیریت چنین عملیاتی بسیار مهم است.

سطح شرکت: برای به‌دست‌آوردن کیف پولِ پول دیجیتال بانک مرکزی، همهٔ کاربران باید هویت خود را به تأیید توزیع‌کنندگان برسانند. زمانی‌که کاربران کیف پول خود را دارند و پول دیجیتال بانک مرکزی را از توزیع‌کنندگان دریافت می‌کنند، می‌توانند انتقال را به‌صورت همتا به همتا[1] و آنی[2] انجام دهند.

۶ معماری کلی پول دیجیتال بانک مرکزی

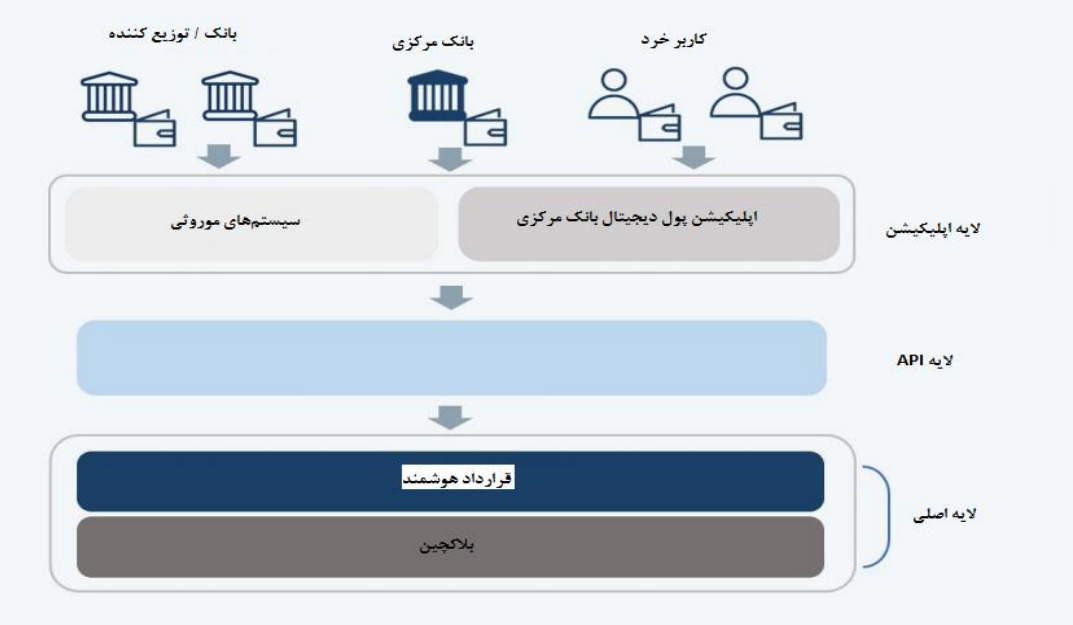
شناخت کلی از یک سطح ساده از معماری پول دیجیتال بانک مرکزی در زنجیرهٔ تأمین‌مالی به درک بهتر فرایند کمک می‌کند. در این معماری، لایهٔ اصلی جایی است که عملیات داده انجام می‌شود. داده‌ها از طریق رابط برنامه‌نویسی از کاربران دریافت می‌شود و به‌صورت همتا به همتا مدیریت می‌شود. در لایهٔ اصلی، دو زیرلایه وجود دارد که لایه‌های بلاک‌چین و قرارداد هوشمند هستند.

۶-۱ لایهٔ بلاک‌چین: شبکه‌ای از رایانه‌هاست که معاملات را به‌صورت منظم ارسال، اجرا، و ذخیره می‌کند. بلاک‌چین یک پایگاه دادهٔ توزیع‌شده است که تمام داده‌ها، معاملات، و سایر اطلاعات مربوطه را ثبت می‌کند. به هر رایانه در شبکه یک گره گفته می‌شود. گره‌ها در مورد اعتبارسنجی تراکنش‌ها، ساختار آن‌ها در بلاک‌ها و پخش آن‌ها به شبکهٔ بلاک‌چین پاسخ‌گو هستند. وقتی توافق حاصل شد، یک بلاک جدید به شبکهٔ بلاک‌چین اضافه می‌شود و هر گره نسخهٔ محلی خود را با آخرین داده‌ها به‌روز می‌کند.

۶-۲ لایهٔ قراردادهای هوشمند: لایه‌ای برای قراردادهای هوشمند و قوانین اساسی است. این لایه شامل کدها و قوانین اجراست. صدور، امحا و کنترل دسترسی توکن‌ها با یک برنامهٔ رایانه‌ای اعمال می‌شود. به چنین برنامه‌هایی قرارداد هوشمند گفته می‌شود و در صورت تحقق شرایط از پیش تعیین‌شده، اجرا می‌شود.

۶-۳ لایهٔ رابط برنامه‌نویسی: این لایه برنامه‌ها را قادر می‌سازد تا با بلاک‌چین ارتباط برقرار کنند؛ به‌عنوان مثال، یک برنامه می‌تواند با گره‌های بلاک‌چین و قراردادهای هوشمند از طریق رابط‌های برنامه‌نویسی تعامل کند.

۶-۴ لایهٔ اپلیکیشن: شامل برنامه‌ها و سیستم‌های موروثی[3] است که کاربران نهایی از آن‌ها برای تعامل با شبکهٔ بلاک‌چین استفاده می‌کنند. رابط‌های کاربر، فریم‌ورک‌ها، و اسکریپت‌ها در این لایه قرار دارند. شکل ۶ ترتیب لایه‌ها را نشان می‌دهد.



شکل ۶. معماری کلی پول دیجیتال بانک مرکزی

منبع: ستادوم و همکاران، ۲۰۲۰

[1] Peer-Peer (P2P)

[2] Real-Time

[3] Legacy Systems

اگر یک طرح پول دیجیتال بانک مرکزی دولایه انتخاب شود، این سیستم نقش مؤسسات مالی را در سازوکارهای انتقال سیاست پولی حفظ می‌کند؛ از منابع و زیرساخت‌های موجود استفاده می‌کند؛ از نوآوری پشتیبانی و از طریق توسعهٔ بازارمحور، رقابت را تقویت می‌کند. مؤسسات مالی، مانند بانک‌های تجاری و ارائه‌دهندگان خدمات پرداخت[1]، باید دارای برنامه‌های کاملاً توسعه‌یافته، زیرساخت‌های فنّاوری اطلاعات، و سیستم‌های خدماتی همراه با کانال‌های توزیع قوی، قابلیت‌های پردازش مشتری، و توانایی ارائهٔ خدمات مالی پیشرفته باشند. علاوه‌براین، چون مردم به خدمات مالی ارائه‌شده توسط مؤسسات تجاری عادت کرده‌اند، یک سیستم دولایه می‌تواند به تقویت پذیرش عمومی پول دیجیتال بانک مرکزی کمک کند.

۷ عملیات اصلی و فرعی در پول دیجیتال بانک مرکزی برای زنجیرهٔ تأمین‌مالی

چهار نیاز عملیاتی شامل ۱ـ مدیریت چرخهٔ حیات پول دیجیتال بانک مرکزی: صدور، توزیع، امحا، و انتقال پرداخت، ۲ـ یکپارچگی پلتفرم، ۳ـ توکنایزکردن فاکتور، و ۴ـ پول قابلِ‌برنامه‌ریزی است.

علاوه‌براین، شش مورد غیرکاربردی یعنی ۱ـ نهایی‌بودن، ۲ـ قابلیت همکاری، ۳ـ حریم خصوصی، ۴ـ انعطاف‌پذیری، ۵ـ مقیاس‌پذیری، و ۶ـ امنیت به‌عنوان ملاحظات اصلی در طول طراحی و توسعهٔ راه‌حل لازم است.

۷-۱ نهایی‌بودن

برای نهایی‌بودن معامله، می‌توان از سازوکار اجماع اثبات اختیار[2] با الگوریتم تحمل خطای بیزانس ۲/۰[3] استفاده کرد که روشی اجماعی است که تعداد کمی از بازیگران بلاک‌چین را به‌عنوان اعتبارسنج برای اعتبارسنجی معاملات یا تعاملات با شبکه اختصاص می‌دهد. پروتکل اثبات اختیار برای شبکه‌های خصوصی کاربرد دارد که شرکت‌کنندگان یکدیگر را می‌شناسند و میزان اطمینان بین آن‌ها وجود داشته باشد. الگوریتم تحمل خطای بیزانس ۲/۰ نهایی‌بودن را قطعی می‌کند. هنگامی‌که یک معامله توسط شبکهٔ بلاک‌چین اعتبار یابد، دیگر این معامله بازگشت‌پذیر نیست.

۷-۲ انعطاف‌پذیری

انعطاف‌پذیری سیستم‌ها برای اطمینان از تداوم تجارت از اهمیت بیشتری برخوردار است، زیرا شرکت‌های بیشتری دیجیتالی می‌شوند و عملیات به‌طور فزاینده‌ای در بستر دیجیتال انجام می‌شود. ثابت شده است که بلاک‌چین به‌دلیل استقرار چندین گره اعتبارسنجی، به افزایش انعطاف‌پذیری داده‌ها کمک می‌کند. بنابراین، هنگامی‌که یک گره خراب است، کل سیستم تحت‌تأثیر قرار نخواهد گرفت. در الگوریتم تحمل خطای بیزانس ۲/۰، گره‌های اعتبارسنجی برای تأیید تراکنش‌ها و بلاک‌ها وجود دارند. اعتبارسنج‌ها به‌نوبت برای ایجاد بلوک بعدی فعالیت می‌کنند. پیش از قراردادن بلوک روی زنجیره، اکثریت (بیشتر از ۶۶٪) اعتبارسنج‌ها ابتدا باید بلوک را امضا کنند. الگوریتم تحمل خطای بیزانس ۲/۰ برای تحمل خطا در بیزانس به حداقل چهار اعتبارسنج نیاز دارد. تحمل خطای بیزانس توانایی شبکهٔ بلاک‌چین برای عملکرد صحیح و اجماع، به‌رغم خرابی گره‌ها یا انتشار اطلاعات نادرست به همسالان است.

۷-۳ قابلیت همکاری

قابلیت همکاری به برقراری ارتباط بین دو یا چند سیستم دفترکل توزیع‌شده یا بلاک‌چین اشاره دارد که می‌تواند شامل شناسایی رویدادها، جابه‌جایی/مبادلهٔ دارایی، انتقال داده یا منطق پیچیدهٔ معامله باشد که شامل چندین دفترکل است.

تضمین قابلیت همکاری پلتفرم پول دیجیتال بانک مرکزی در سطوح مختلف لازم است:

- **سطح دارایی:** توکن پول دیجیتال بانک مرکزی باید براساس استاندارد توکن جهانی[4] ساخته شود و با سایر استانداردهای ERC[5] سازگار باشد.
- **سطح شبکه:** شبکه باید با شبکه‌های جهانی دیگر قابلِ‌همکاری باشد؛ به‌عنوان مثال، شبکه‌ای که براساس پروتکل اتریوم با استفاده از هایپرلجر بسو[6] ساخته شده است، می‌تواند با هر شبکهٔ خصوصی اتریوم و همچنین با شبکهٔ اصلی اتریوم قابلیت همکاری داشته باشد.

---

[1] Payment Service Providers (PSP)

[2] Proof -of -Authority (PoA)

[3] Istanbul Byzantine Fault Tolerance 2.0 (IBFT 2.0)

[4] Universal Token

[5] Ethereum Request for Comments (ERC)

[6] هایپرلجر بسو (Hyperledger Besu) نرم‌افزاری متن‌باز است که به‌منظور استفاده در شبکه‌های عمومی و خصوصی مبتنی بر پروتکل اتریوم است. این نرم‌افزار بخشی از مجموعهٔ ابزار و راهکارهای ارائه‌شدهٔ پروژهٔ معظم هایپرلجر است.

● **سطح کاربرد:** برای اینکه پلتفرم پول دیجیتال بانک مرکزی با سایر برنامه‌ها تطبیق‌پذیر باشد، لایهٔ رابط برنامه‌نویسی کاربردیِ باز[1] باید استاندارد باشد و به‌خوبی طراحی شده باشد تا از قابلیت همکاری یکپارچه اطمینان حاصل کند.

۷-۴ امنیت

برای امنیت در بلاک‌چین، دو مؤلفهٔ اصلی باید در نظر گرفته شود: امنیت شبکه و امنیت داده‌ها.

۷ـ۴ـ۱ امنیت شبکه

● **اجازهٔ دسترسی:** در شبکه‌های خصوصی و بامجوز، فقط گره‌های تأییدشده اجازه دارند با سطوح دسترسی به شبکه متصل شوند و اقدامات مجاز را انجام دهند (به‌عنوان مثال، پردازش یا شرایط هویتی).

● **فایروال[2]:** برای محدودکردن اتصالات شبکه، باید فایروال پیکربندی و دسترسی برای شرکت‌کنندگان مجاز تعریف شود.

۷ـ۴ـ۲ امنیت داده‌ها

● رمزگذاری رِست[3] با اطمینان از رمزگذاری کامل پایگاه داده، از بازیگران مخربی که به یک گره در یک شبکهٔ خصوصی دسترسی پیدا می‌کنند، جلوگیری می‌کند.

● مدیریت کلید به ذخیره‌سازی، مدیریت کلیدها، و امضای معاملات بلاک‌چین اشاره دارد. در بلاک‌چین، کلیدهای خصوصی برای دسترسی کاربران به حساب‌ها، امضا، و ارسال معاملات ضروری است.

علاوه بر این موارد، باید برای پیکربندی‌های امنیتی بیشتر و بهبود امنیت گره‌ها و نقاط ادغام، موارد ذیل را درنظر گرفت:

- ✓ کنترل دسترسی مبتنی بر نقش و امتیازاتی که برای تعریف دسترسی محدود برای شرکت‌کنندگان مجاز تعریف می‌شود.
- ✓ مدیریت لاگ[4]، که سوابق معاملات را میان شرکت‌کنندگان حفظ می‌کند.
- ✓ ابزار مانیتورینگ که امکان نظارت بر فعالیت‌های جاری و رویدادهای نامناسب را فراهم می‌کند.

۷-۵ مقیاس‌پذیری

مقیاس‌پذیری به اندازهٔ شبکه (تعداد شرکت‌کنندگان) و حجم معاملات (تعداد معاملات) قابلِ‌مدیریت در شبکه اشاره دارد.

۷ـ۵ـ۱ اندازهٔ شبکه

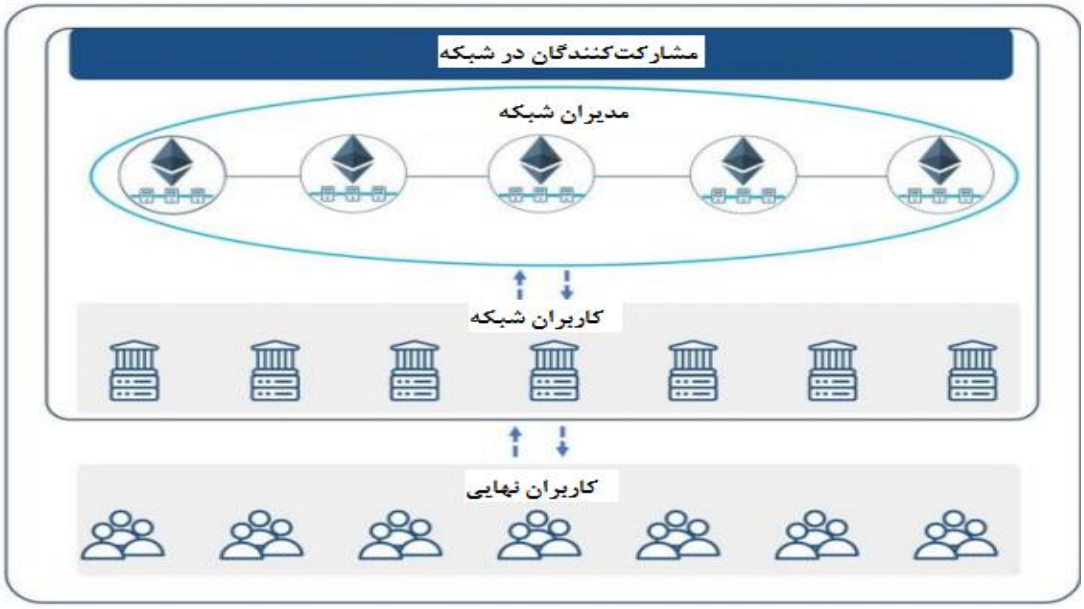
شرکت‌کنندگان شبکه دو نوع‌اند: کاربران شبکه و مدیران شبکه. کاربران در سازوکار اجماع بلاک‌چین مشارکت نمی‌کنند. تعداد کاربران شبکه محدودیتی ندارند، زیرا می‌توان به تعداد لازم، گره اعتباردهی‌نشده اضافه کرد. از طرف دیگر، مدیران شبکه و مالک گره‌های اعتبارسنجی‌شده در سازوکار بلاک‌چین شرکت می‌کنند. ذکر این نکته ضروری است که کاربران نهایی پول دیجیتال بانک مرکزی (به‌عنوان مثال، شرکت‌ها و خانوارها) شرکت‌کنندهٔ شبکه نیستند.

۷ـ۵ـ۲ حجم معامله

حجم معامله توسط شبکه محدود نمی‌شود، اما عملکرد کلی شبکه (با تعداد تراکنش‌ها در ثانیه اندازه‌گیری می‌شود[5]) به زمان لازم برای پردازش و تأیید تراکنش‌ها بستگی دارد. برای افزایش مقیاس‌پذیری و عملکرد، از راه‌حل رول‌آپ[6] می‌توان استفاده کرد. رول‌آپ یک رویکرد کلی برای مقیاس‌گذاری قراردادهای باز است؛ یعنی قراردادهایی که همه می‌توانند آن را ببینند و با آن‌ها تعامل داشته باشند. در یک رول‌آپ، تراکنش در خارج از زنجیرهٔ اصلی اتریوم (لایهٔ ۱) انجام می‌شود، اما داده‌های معامله روی لایهٔ ۱ ارسال می‌شود. یک قرارداد هوشمند رول‌آپ در لایهٔ ۱ می‌تواند با استفاده از داده‌های معامله در لایهٔ ۱، اجرای صحیح معامله را در لایهٔ ۲ اعمال کند. سازوکار رول‌آپ می‌تواند تعداد تراکنش‌ها در ثانیه را به میزان قابلِ‌توجهی افزایش دهد.

---

[1] Open API
[2] Firewall
[3] Encryption at Rest
[4] Log Management
[5] Transactions Per Second
[6] Rollup



شکل ۷. شمای کلی مشارکت‌کنندگان در شبکه

منبع: ستادوم و تین‌جم، ۲۰۲۰

۷-۶ حریم خصوصی

سطح مطلوب حریم خصوصی در پول دیجیتال بانک مرکزی هنوز قابلِ‌بحث است، زیرا تعادل بین ترجیح کاربر و جلوگیری از معاملات تقلبی باید بادقت محاسبه شود. سیستم پول دیجیتال بانک مرکزی متشکل از دارایی‌ها و معاملات است که دارای مالک (O) و موجودی (B) و معامله است که معامله نیز خود شامل پرداخت‌کننده (Pr)، گیرنده (Pe)، و مبلغ (A) است. حریم خصوصی، میزان پنهان‌بودن داده‌های دارایی‌ها و معاملات از نهادهای شرکت‌کننده است. نهادها (بانک پرداخت‌کننده یا مؤسسات ارائه‌دهندهٔ خدمات مالی[1]، دریافت‌کننده، مؤسسات دولتی، ارائه‌دهندگان خدمات پرداخت، و عموم مردم) هریک دارای درجهٔ قابلِ‌توجهی از دید نسبت به دارایی‌ها و معاملات هستند. درک مدل تجاری پول دیجیتال بانک مرکزی، ویژگی‌ها، و بستر فنّاوری برای انتخاب سازه‌های مناسب و ترکیب مناسب آن‌ها ضروری است؛ به‌عنوان مثال، در سیستمی که معاملات خصوصی توسط MSB تأیید می‌شود، اگر مدل کسب‌وکار بیان می‌کند که مؤسسات ارائه‌دهندهٔ خدمات مالی بسیار مورداعتمادند، پروتکل‌های حریم خصوصی را می‌توان با فرض صادق‌بودن تأییدکنندگان ساده کرد. در غیر این‌صورت، پروتکل‌های انتخاب‌شده باید از تأییدکنندگان غیرمعتمد محافظت کنند، که پیچیدگی بالاتری را به‌دنبال دارد. اگر مبالغ پنهان است، طرح‌های انتخاب‌شده باید از محاسبات رمزگذاری‌شدهٔ پرداختِ سود پشتیبانی کنند. علاوه‌براین، انتخاب تکنیک‌های حفظ حریم خصوصی به بستر انتخاب‌شده نیز بستگی دارد (داربها و آرورا[2]، ۲۰۲۰). ازآنجاکه فنّاوری‌های افزایش حریم خصوصی به هوشیاری نیاز دارند (زیمرمن[3]، ۱۹۹۱)، مؤسسات ارائه‌دهندهٔ خدمات مالی و جامعه باید متعهد شوند پیوسته فنّاوری زیربنای ویژگی‌های حریم خصوصی این طرح را حفظ و ممیزی کنند و بهبود بخشند (گودل و همکاران، ۲۰۱۹).

کیف پول‌ها برای اطمینان از اینکه طرف‌های معامله فاش نمی‌شوند، باید بر فنّاوری افزایش حریم خصوصی، مانند امضای کور[4] یا اثبات دانش صفر متکی باشند (گودل و همکاران، ۲۰۲۱). برای پول دیجیتال بانک مرکزی می‌توان از پروتکل‌های حریم خصوصی استفاده کرد که فقط شرکت‌کنندگان بتوانند موجودی توکن قبل و بعد و مقادیر انتقال را ببینند، اما اعتبارسنج‌ها بتوانند یکپارچگی انتقال را تأیید کنند و رگولاتور بتواند به‌طور بالقوه بر همه نوع معاملات نظارت کند. شایان ذکر است که سطح بالاتری از حریم خصوصی تأثیر منفی در عملکرد کلی سیستم دارد. بدین‌ترتیب، اعمال تنظیمات حریم خصوصی در کل سیستم باید با دقت بیشتری بررسی شود.

---

[1] Money Services Business (Non-Bank Financial Institution)

[2] Darbha & Arora

[3] Zimmermann

[4] Blind Signatures

پروتکل اثبات دانش صفر[1] برای افزایش تنظیمات حریم خصوصی در بلاک‌چین معمولی معرفی شده است. Aztec یک پلتفرم جدید معرفی کرده است که از همان رمزنگاری پیشرفته برای بهبود مقیاس‌پذیری استفاده می‌کند. Aztec 2.0 یک نوع اثبات zk به نام zkSNARKs را به‌کار می‌گیرد تا بسیاری از معاملات را به یک رول‌آپ واحد منتقل کند که در زنجیرهٔ اصلی منتشر می‌شود؛ در نتیجه توان عملیاتی معاملات افزایش می‌یابد. این شبکه تا ۳۰۰ تراکنش در ثانیه کاملاً مقیاس‌پذیر است. ztec 2.0 از پروتکل اثبات دانش صفر برای دسته‌بندی معاملات خصوصی به‌صورت گسترده استفاده می‌کند. zkSNARKهای Aztec امکان حریم خصوصیِ قابل برنامه‌ریزی را فراهم می‌کنند. گروه‌های دیگری نیز درحال توسعهٔ فنّاوری‌های zk-rollup با هدف بهبود مقیاس‌پذیری اتریوم هستند. در قلب Aztec 2.0، یک استاندارد zkSNARK وجود دارد که تیم تحقیقاتی Aztec آن را توسعه داده است و PLONK نامیده می‌شود. برای ساخت یک سیستم دولایه برای پردازش معاملات از PLONK استفاده شد.

۷-۷ مدیریت و حاکمیت داده‌ها

داده‌ها در اقتصاد دیجیتال بسیار ارزشمندند. معامله با پول دیجیتال یا پول دیجیتال بانک مرکزی باعث تولید داده‌های ارزشمندی می‌شود. داده‌های ذخیره‌شده در بلاک‌چین به یک دارایی گرانبها تبدیل می‌شوند. به همین دلیل، چهارچوب‌های مناسبی برای مدیریت داده و حاکمیت داده باید تنظیم شود که داده‌ها به‌طور مؤثر و مداوم مدیریت شوند و حریم خصوصی و یکپارچگی داده‌ها تضمین شود. همچنین، ایجاد سیاست‌های صحیح در مورد استفاده از داده‌ها همراه با رویه‌هایی برای اجرای این سیاست‌ها و نظارت بر استفاده از داده‌ها لازم است.

۷-۸ مشارکت و دسترسی

برای موفقیت یک راهبرد کلی و شفاف از سیستم پول دیجیتال بانک مرکزی، ساختار حاکمیت قوی و دستورالعمل‌های کافی برای مشارکت اعضا لازم است. سلامت مالی شرکت‌ها، شهرت، شیوه‌های امنیت سایبری و سایر استانداردهای مربوطه باید به‌عنوان بخشی از این روند در نظر گرفته شود.

۸ جمع‌بندی

زنجیرهٔ تأمین‌مالی سنتی با مشکلاتی در مدیریت جریان اطلاعات، تدارکات، و جریان سرمایه مواجه است که منجر به نابرابری و عدم تقارن اطلاعات می‌شود. به همین دلیل، کلاهبرداری و تقلب در نحوهٔ استفاده از تسهیلات نیز به‌وفور اتفاق می‌افتد. در این گزارش، ما نوع جدیدی از بستر مالی را معرفی کردیم که از پول دیجیتال بانک مرکزی، توکن‌سازی بلاک‌چین، و قراردادهای هوشمند برای مدیریت کل فرایند بهره می‌برد. برای نظارت بر تسهیلات در شبکهٔ پول دیجیتال بانک مرکزی، می‌توان فاکتورها را به توکن تبدیل کرد. توکن‌های فاکتور می‌توانند طیف وسیع‌تر و متنوع‌تری از وام‌دهندگان را جذب کنند. وجوه می‌تواند از هر فردی که به شبکهٔ پول دیجیتال بانک مرکزی دسترسی دارد، تأمین شود. یک فاکتور توکنایزشده مجهز به ویژگی‌هایی مانند قابل‌ردیابی‌بودن، تقسیم‌پذیری، و تغییرناپذیری است که می‌تواند توسط چندین وام‌دهنده تأمین شود. علاوه‌براین، می‌توان مالکیت توکن‌های فاکتور را در شبکه منتقل کرد. هرچه تعداد مشارکت‌کنندگان در شبکه بیشتر شود، تأثیرات شبکه به‌سمت یک حلقهٔ ارزشمند از رقابت بیشتر و خدمات بهتر هدایت می‌شود. پول دیجیتال بانک مرکزی اگرچه فرصت‌هایی را ارائه می‌دهد، بسته به هدف افرادی که به انبوه داده‌های تولیدشده دسترسی دارند، پتانسیل ایجاد تهدید را نیز دارد. از بُعد مثبت، پول دیجیتال بانک مرکزی می‌تواند با افزایش نظارت بر جامعه، توانایی مقامات را در درک چگونگی عملکرد اقتصاد و پاسخ‌گویی به مشکلات افزایش دهد. اما در میان حجم عظیمی از داده‌های شخصی که به‌عنوان ورودی برای فعالیت تجاری جمع‌آوری و پردازش می‌شوند، یک چالش مهم از اقتصاد دیجیتال مطرح می‌شود که شامل مسائل مربوط به حاکمیت داده‌ها، حمایت از مصرف‌کننده، و شیوه‌های ضد رقابتی ناشی از انبار داده است. نتیجهٔ نهایی این فرایند نه‌تنها به فنّاوری بلکه به ساختار اساسی بازار و چهارچوب حاکمیت داده‌ها بستگی دارد. بنابراین، برای حرکت بر روی لبهٔ فنّاوری و استفاده از مزایای آن چالش‌ها نیز باید در نظر گرفته شوند و پیش از پیاده‌سازی، باید همهٔ ابعاد متأثر بررسی شود.

[1] Zero-Knowledge Proof

منابع و مآخذ

BIS Annual Economic Report (2021). CBDCs: An opportunity for the monetary system. Retrived from: https://www.bis.org/publ/arpdf/ar2021e3.htm.

Committee on Payments and Market Infrastructures, World Bank Group. (2020). Payment aspects of financial inclusion in the fintech era. Retrived from: https://www.bis.org/cpmi/publ/d191.pdf.

Darbha, S., & Arora, R. (2020). Privacy in CBDC technology (No. 2020-9). Bank of Canada. Retrived from: https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/.

Du, M., Chen, Q., Xiao, J., Yang, H., & Ma, X. (2020). Supply chain finance innovation using blockchain. *IEEE Transactions on Engineering Management,* 67(4), 1045-1058.

Goodell, G., Al-Nakib, H. D., & Tasca, P. (2021). A Digital currency architecture for privacy and owner-custodianship. *Future Internet*, 13(5), 130.

Goodell, G., & Aste, T. (2019). Can cryptocurrencies preserve privacy and comply with regulations? Front. Blockchain [CrossRef].

Hoffman, S. (2021). China's digital currency electronic payment and surveillance. Retrived from: https://www.uscc.gov/sites/default/files/2021-04/Samantha_Hoffman_Testimony.pdf.

Hoffman, S. (2020). The flipside of China's central bank digital currency. Retrived from: https://www.aspistrategist.org.au/the-flipside-of-chinas-central-bank-digital-currency/.

Sethaudom, S., Supapongse, M., & Thien-ngern, O., (2021). Central bank digital currency: The future of payments for corporates.

Swiss Bankers Association (2021). Discussion paper «New currencies for Switzerland?» Retrived from: https://www.swissbanking.ch/_Resources/Persistent/a/1/2/9/a1290092308e4ccb8d08841bfec49e97600cf1e9/SBA_Discussion_Paper_CDBC_EN.pdf.

Tian, Y., Lu, Z., Adriaens, P., Minchin, R. E., Caithness, A., & Woo, J. (2020). Finance infrastructure through blockchain-based tokenization. *Frontiers of Engineering Management*, 7(4), 485-499.

Tuesta, D., Alonso, J., & Ćamara, N. (2019). Smart contracts: The ultimate automation of trust. *Digital Economy Outlook.*

Zimmermann, P. (1991). *Why I wrote PGP. In PGP User's Guide*. Massachusetts Institute of Technology: Cambridge, MA, USA, Retrived from: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

پژوهشکده پولی و بانکی

بانک مرکزی جمهوری اسلامی ایران

تهران: میدان آرژانتین، ابتدای بزرگراه آفریقا، پلاک ۱۰

کدپستی: ۱۵۱۴۹۴۷۱۱۱ صندوق پستی: ۷۹۴۹-۱۵۸۷۵

www.mbri.ac.ir