نشریـه علمـی
دانش مالی تحلیل اوراق بهادار
سال چهاردهم، شماره پنجاه‌ام
تابستان ۱۴۰۰

# یک چارچوب مبتنی بر بلاکچین EOSIO برای ارز دیجیتال بانک مرکزی (CBDC)

**امیر یزدی نژاد**[۱]
**عبدالمجید دهقان**[۲]

تاریخ دریافت: ۱۳۹۹/۱۰/۲۹ تاریخ پذیرش: ۱۴۰۰/۰۳/۰۳

**چکیده**

در سال های اخیر شاهد پیشرفت قابل توجه فناوری بلاکچین[۱] و فراگیر شدن ارزهای رمزپایه[۲] به صورت همزمان بوده ایم. کریپتوکارنسی های غیرمتمرکز[۳] مانند بیت کوین[۴] و اتر (رمزارز پروژه اتریوم[۵]) هرچند نمی توانند جایگزین پول فیات[۶] شوند اما قدرت پول فعلی بانک های مرکزی را تهدید می کنند. انتشار ارز دیجیتال بانک مرکزی[۷] (CBDC) می تواند یک پاسخ احتمالی به موج ایجاد شده و در حمایت از پول ملی باشد. در همین راستا این پژوهش به تجزیه و تحلیل ویژگی ها و اندازه گیری پارامترهای مرتبط با یک بلاکچین مبتنی بر نرم افزار منبع باز EOSIO 2.0 با تمرکز بر امکان پیاده سازی آن با هدف ارائه و پشتیبانی از یک CBDC به صورت مقیاس پذیر[۸] و تراکنش های بدون کارمزد[۹] می پردازد، سپس یک مدل نظری برای اجرای CBDC توسط EOSIO 2.0 با مشخص کردن نقش بانک های تجاری، به طوری که اثرات منفی احتمالی صدور و عرضه CBDC بر آن ها به حداقل برسد، ارائه می کند.

**واژه‌های کلیدی:** بیت کوین؛ بلاکچین؛ کریپتوکارنسی؛ EOSIO؛ CBDC.

۱- دانشجوی مقطع کارشناسی ارشد مدیریت مالی، دانشکده مدیریت و حسابداری، دانشگاه آزاد اسلامی واحد یادگار امام خمینی (ره)-شهرری، تهران، ایران amir.yazdinejad88@gmail.com .

۲- استادیار گروه مدیریت بازرگانی، دانشکده مدیریت و حسابداری، دانشگاه آزاد اسلامی واحد یادگار امام خمینی (ره)؛ شهرری، تهران، ایران، نویسنده مسئول. mjd.dehghan@gmail.com

## ۱- مقدمه

اولین تلاش ها در راستای ساخت ارزهای دیجیتال نیازمند بانک به عنوان یک واحد مرکزی بود (چاوم، ۱۹۸۲) و (لا و همکاران، ۱۹۹۶). بعدها رویکردهایی مانند B-money (دای، ۱۹۹۸)، Karma (ویشنومورتی و همکاران، ۲۰۰۳)، RPOW (فینِی، ۲۰۰۴) و Bit Gold (سابو، ۲۰۰۵) ایده راه حل معمای رمزنگاری بر اساس روش اثبات کار[۱۰] (PoW) را معرفی کردند. با این روش همه می توانند تبدیل به یک "حفار طلای دیجیتال" شوند و به طور مستقل از یک بانک پول را استخراج کنند ولی هنوز هم برای حفظ سوابق مالکیت به یک مرجع مرکزی نیاز دارند. اما بیت کوین یک راه حل بسیار بلند پروازانه تر را هدف قرار داده است: راه حل خلاص شدن از مرکزیت بانکی (ناکاموتو، ۲۰۰۸). برای این منظور سازوکارهایی برای ایجاد سکه، ذخیره سازی و مدیریت دفتر کل به صورت توزیع شده مورد نیاز است. چالش اصلی، دستیابی به اجماع در مورد سکه های موجود و مالکیت آن ها بدون تأیید کننده مرکزی و بدون روابط اعتماد متقابل بین شرکت کنندگان است. بنابراین چگونه می توانیم مرکزیت بانکی را از بین ببریم؟ بیت کوین این کار را با یک روش بسیار عملی حل می کند، به یک معنا همه بانک هستند. یعنی هر شرکت کننده یک نسخه از سوابق را که به صورت کلاسیک در بانک ذخیره می شود، نگه می دارد. ما می توانیم آن را یک دفتر کل توزیع شده در نظر بگیریم که منعکس کننده همه تراکنش ها و مالکیت ها باشد. در بیت کوین زنجیره بلوکی یا همان بلاکچین نقش این دفتر کل توزیع شده را به عهده می گیرد (سورس و شوئِرمن، ۲۰۱۶).

پس از معرفی بیت کوین در سال ۲۰۰۸، ارزهای جایگزین رمزنگاری دیگری پدید آمده اند که به آن ها (گزینه های جایگزین بیت کوین یا آلتکوین[۱۱]) گفته می شود (گاتفرت، ۲۰۱۹). مهمترین آن ها یعنی پلتفرم اتریوم در سال ۲۰۱۳ با بهره گیری بیشتری از بلاکچین و قابلیت پشتیبانی از قراردادهای هوشمند معرفی و در سال ۲۰۱۵ عرضه شد (بوتِرین، ۲۰۱۳). بسیاری از مطالعات نشان داده اند که بلاکچین ها برای برنامه های مختلف ظهور کرده اند اما به علت برخی مشکلات مثل مقیاس پذیری، اندازه بلوک، افزایش اندازه زنجیره، امضاهای الکترونیکی و ...، محدودیت هایی در استفاده عملی از آن ها وجود دارد (جف، ۲۰۱۵)، (جانسون، ۲۰۱۶)، (اریک، ۲۰۱۵)، (پیتر، ۲۰۱۴)، (اشنور، ۱۹۹۱)، (پون و درایژا، ۲۰۱۶)، (لرنر، ۲۰۱۸)، (بَک و همکاران، ۲۰۱۴) و (پون و بوترین، ۲۰۱۷). برای مثال پردازش تراکنش در سیستم های متمرکز می تواند به هزاران سفارش در ثانیه برسد، در حالی که بلاکچین بیت کوین حدود ۷ و اتریوم حدود ۱۵ تراکنش در ثانیه را پردازش می کنند (این مقادیر در زمان های مختلف بسته به وضعیت شبکه متغیر می باشند). متفاوت از بیت کوین و اتریوم که سیستم های سنتی بلاکچین مبتنی بر PoW هستند، EOSIO سعی دارد با طراحی یک معماری جدید و روش اثبات سهام محول شده[۱۲] (DPoS) توان عملیاتی بالایی را ارائه دهد (لریمر، ۲۰۱۷) و (ژِنگ و همکاران، ۲۰۲۰). تاکنون بلاکچین های EOS، Telos (هورن، ۲۰۱۸)، BOS (بنیاد BOS، ۲۰۱۸)، MEETONE (تیم MEET.ONE، ۲۰۱۸)، WAX (کویگلی، ۲۰۱۹)، LYNX (کروگر، ۲۰۱۹) و ULTRA (تیم Ultra.io، ۲۰۱۹) مبتنی بر نرم افزار EOSIO ساخته شده اند. این پژوهش برای اولین بار طراحی CBDC را بر روی یک بلاکچین مبتنی بر EOSIO پیشنهاد می دهد.

## ۲- مبانی نظری

### ۲-۱- CBDC

CBDC نوعی پول است که به صورت دیجیتالی توسط بانک مرکزی صادر می شود. انتشار ارز دیجیتال بانک مرکزی در بسیاری از بانک های مرکزی در سراسر جهان در حال آزمایش است. تقاضا برای CBDC تا حدی از عوامل مختلفی ناشی می شود، از جمله علاقه شدید به ادغام فناوری در بخش مالی، ظهور روش ها و خدمات جدید پرداخت، توجه روز

افزون به کریپتوکارنسی ها و همچنین ناپدید شدن تدریجی پول نقد فیزیکی (CPMI، ۲۰۱۸). یک نظرسنجی از ۶۳ کشور در سال ۲۰۱۹، که توسط بانک تسویه حساب های بین المللی[۱۳] (BIS) منتشر شد، نشان داد که ۷۰ درصد از پاسخ دهندگان مشغول کار به روی CBDC بودند. پاسخ دهندگان حدود ۸۰ درصد از جمعیت جهان و تقریبا ۹۰ درصد از کل اقتصاد دنیا را تشکیل می دادند. شرکت کنندگان در این نظرسنجی از پیش زمینه های اقتصادی متنوعی با ۴۱ کشور در حال توسعه و ۲۲ اقتصاد پیشرفته برخوردار بودند (بارونیتی و هولدن، ۲۰۱۹)

CBDC می تواند به صورت ۲۴/۷ در دسترس باشد و یا بانک مرکزی می تواند تصمیم بگیرد که ساعات عملیاتی خاصی را مشخص کند. CBDC یک بدهی بانک مرکزی محسوب می شود و پرداخت بهره توسط آن از لحاظ فنی امکان پذیر است. بانک مرکزی این نرخ بهره را تعیین می کند و می تواند همانند نرخ سود بانکی باشد یا در سطحی تنظیم شود که بسته به اهداف بانک مرکزی تقاضای CBDC را افزایش یا کاهش دهد و یا می تواند یک مقدار اسمی ثابت داشته باشد. طراحی CBDC به صورت کاملاً ناشناس و یا کاملاً قابل ردیابی امکان پذیر است. هرچند CBDC شکل جدیدی از پول است و با تحولات تکنولوژی، در آینده نیز احتمالا با شکل های جدیدی از پول مواجه خواهیم بود، اما همه اشکال مختلف بایستی سه وظیفه زیر را عهده دار شوند:

- پول به عنوان وسیله یا واسطه مبادله؛ می بایست برای هر دو طرف معامله قابل پذیرش باشد.
- پول به عنوان واحد حساب یا سنجش ارزش؛ به عنوان واحد پولی استاندارد برای اندازه گیری ارزش کالاها، خدمات و دارایی ها استفاده می شود. برای نتیجه گیری این عملکرد، یک ارز باید بدون کاهش ارزش در واحدهای کوچکتر تقسیم گردد.
- پول به عنوان وسیله حفظ یا ذخیره ارزش (پس انداز)؛ باید با گذشت زمان پایدار بماند. این بدان معناست که می توان با اطمینان خاطر پول را با گذشت زمان ذخیره و بازیابی کرد (گارتز و لیندربرت، ۲۰۱۷).

### EOSIO -۲-۲

نرم افزار منبع باز EOSIO با هدف فراهم ساختن تراکنش های بدون هزینه، پشتیبانی از برنامه های غیرمتمرکز، اجرای قراردادهای هوشمند پیچیده و امکان انجام هزاران تراکنش در ثانیه در ماه ژوئن سال ۲۰۱۸ منتشر شد و در سال ۲۰۲۰ به نسخه EOSIO 2.0 ارتقاء پیدا کرد. اگر شبکه بیت کوین را بلاکچین نسل یک و شبکه اتریوم را (در اینجا مقصود اتریوم ۱ می باشد) نسل دو بدانیم، EOSIO یک بلاکچین نسل سومی است. هرچند برخی EOSIO را به همراه Cosmos (تیم Core پروژه Cosmos، ۲۰۱۶) و PolkaDot (وود، ۲۰۱۹) در گروه نسل چهارم بلاکچین قرار داده اند (دورُو، ۲۰۱۸). EOSIO به جای استفاده از روش PoW به عنوان یک روش پر هزینه، از پروتکل PoS که به تدریج جایگزین روش PoW خواهد شد، استفاده می کند. در روش PoS هر بلوک جدید به صورت تصادفی توسط داوطلبان منتخب تولید می شود اما شانس کسی که سهام بیشتری دارد بالاتر است. تاکنون نسخه های مختلفی از روش PoS ارائه شده اند که یکی آن ها توسط EOSIO با عنوان DPoS به عنوان یک پیاده سازی مبتنی بر دموکراسی معرفی شده است.

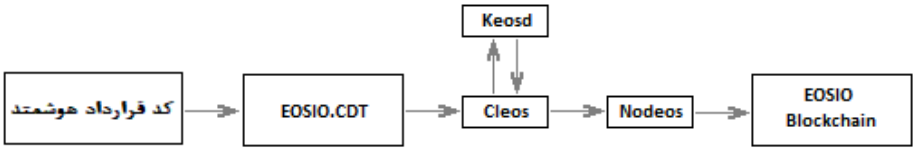
شمای کلی EOSIO در شکل ۱ نمایش داده شده است:

**شکل (۱) لایه های مختلف بلاکچین مبتنی بر EOSIO**

در لایه تولید کنندگان بلوک، داوطلبان به رأی گیری گذاشته می شوند و تمام عضوهای شبکه به صورت پویا ۲۱ تولید کننده بلوک[۱۴] (BP) فعال را انتخاب می کنند. تولید کنندگان بلوک امنیت شبکه را تأمین کرده و از محل تورم سالانه پاداش خود را دریافت می کنند و به این ترتیب برای تراکنش ها کارمزدی دریافت نمی شود (لریمر، ۲۰۱۷). طبق الگوریتم اجماع EOSIO در لایه بلاکچین زمانی یک تراکنش انجام می شود که حداقل دو سوم BPها (۱۴ = ۲/۳ * ۲۱) آن را تأیید کنند، به این ترتیب تراکنش ها در بلاکچین ثبت می گردند (ژِنگ و همکاران، ۲۰۲۰). لایه بعدی مربوط به قراردادهای هوشمند است. قراداد هوشمند سال ها قبل از بلاکچین پیشنهاد شد (سابو، ۱۹۹۷) اما تا زمان ظهور اتریوم به خوبی توسعه نیافته بود. این قراردادها، کدهای رایانه ای هستند که اجرای قوانین و ضوابط از پیش تعریف شده را به صورت خودکار در می آورند. قراردادهای هوشمند EOSIO به صورت Turing-complete بر روی ماشین مجازی وب اسمبلی به نام EOSVM اجرا می شوند. در EOSIO منابع محدود به RAM، CPU و NET می شوند. کاربران می توانند با Stake کردن توکن ها که بخشی از این CPU و NET را رهن کرده و با پرداخت توکن مقداری از RAM را خریداری کنند. این توکن ها که در لایه توکن ساخته می شوند همچنین می توانند برای انتقال همتا به همتا (P2P) استفاده شوند.

### ۲-۳- مولفه ها و ابزارهای پلت فرم EOSIO

- nodeos (node + EOSIO): هسته اصلی نود EOSIOکه می تواند با افزونه ها برای اجرای یک نود پیکربندی شود (لریمر، ۲۰۱۷). هرکسی که از Nodeos استفاده می کند می تواند به شبکه بپیوندد. Nodeos یک رابط کاربری استاندارد JSON-RPC را از طریق eosio::http_plugin و eosio::chain_plugin برای تعامل کاربران فراهم می کند (ژِنگ و همکاران، ۲۰۲۰).
- cleos (CLI + EOSIO): رابط خط فرمان[۱۵] برای تعامل با Nodeos، بلاکچین و مدیریت کیف پول[۱۶].
- keosd (Key + EOSIO): مؤلفه ای که از کلیدهای EOS.IO در کیف پول ها استفاده می کند.
- EOSIO.CDT: مجموعه ابزاری برای WebAssociation (Wasm) و تسهیل نوشتن قرارداد هوشمند.




**شکل (۲) نحوه ارتباط مؤلفه های EOSIO**

### ۲-۴- منابع سیستم

- RAM، در یک بلاکچین مبتنی بر EOSIO، یکی از منابع مهم سیستم است که توسط حساب های زنجیره بلوکی و قراردادهای هوشمند مصرف می شود. RAM به عنوان یک حافظه دائمی عمل می کند و از آن برای ذخیره اسامی، حساب ها، مجوزها، موجودی توکن ها و سایر داده ها استفاده می شود.
- CPU، در یک بلاکچین مبتنی بر EOS.IO، زمان پردازش یک عمل را نشان می دهد و با میکروثانیه (µs) اندازه گیری می شود. CPU که در cleos با عنوان cpu bandwidth مشخص می شود، نشان دهنده مقدار زمان پردازشی است که یک حساب برای انجام اقدامات در یک قرارداد در اختیاردارد.
- Network (NET) پهنای باند شبکه است که با بایت اندازه گیری می شود و به عنوان net bandwidth در cleos مشخص می گردد.

### ۲-۵- پیشینه پژوهش

مطالعات کمی در مورد EOSIO وجود دارد. کوان و همکاران (۲۰۱۹) تشخیص آسیب پذیری های جعلی انتقال قراردادهای هوشمند[۱۷] در EOSIO را بررسی کرده اند. هوآنگ و همکاران (۲۰۲۰) به توصیف فعالیت ها در EOSIO پرداخته اند. ژِنگ و همکاران (۲۰۲۰) یک چارچوب مجموعه داده های EOSIO را معرفی نموده و آمار این اطلاعات پردازش شده را ارائه می دهند. در رابطه با CBDC تا کنون پژوهشی در مورد طراحی آن توسط EOSIO منتشر نشده است. اولین بار دانشگاه لندن یک چارچوب برای CBDC به نام RSCoin ارائه کرده است (دنزیس و مایکل جان، ۲۰۱۵). تحقیق دیگری یک مدل برای CBDC به نام MBDC معرفی می کند که در آن به منظور پردازش سریع تر از معماری چندزنجیره ای استفاده شده است (سان، ۲۰۱۷). در این مدل بانک های مرکزی و بانک های تجاری و سایر آژانس ها بلاکچین را ایجاد و نگهداری می کنند. در آخرین مطالعه منتشر شده در این حوزه تفاوت های عملکردی بین ارزهای دیجیتال غیرمتمرکز و CBDC مورد تجزیه و تحلیل قرار گرفته و سپس امنیت و الزامات عملکردی مورد نیاز CBDC بحث می شود. سپس یک چارچوب مبتنی بر بلاکچین برای CBDC با سه لایه از جمله لایه نظارت، لایه شبکه و لایه کاربر پیشنهاد می گردد (تسای و همکاران، ۲۰۱۸). از سال ۲۰۱۵ به بعد، بانک های مرکزی کشورهای مختلف اقدام به تحقیق و بررسی و در مواردی آزمایش های عملی در مورد CBDC کرده اند که جزئیات آن در جدول ۱ نشان داده شده است (اوپاری و کیم، ۲۰۲۰).

**جدول (۱) پروژه های کشورهای مختلف در رابطه با CBDC از سال ۲۰۱۵ الی ۲۰۱۹**

| سال | نام بانک یا سازمان | عنوان یا موضوع پروژه یا تحقیق |
|---|---|---|
| 2015 | بانک انگلستان | RSCoin |
| 2016 | بانک خلق چین | شروع آزمایش CBDC |
| | بانک کانادا | Project Jasper |
| | بانک فدرال آلمان | Project BLOCKBASTER |
| | بانک فرانسه | Project MADRE |
| | بانک مرکزی برزیل | Project SALT |
| | سازمان پولی سنگاپور | Project Ubin |
| | بانک مرکزی اروپا و بانک ژاپن | Project Stella |
| 2017 | سازمان پولی هنگ کنگ | Project LionRock |
| | بانک فنلاند | تحقیق درباره G-CBDC |

| سال | نام بانک یا سازمان | عنوان یا موضوع پروژه یا تحقیق |
|---|---|---|
| | بانک مرکزی سوئد | e-Krona |
| | بانک مرکزی اروگوئه | e-Peso |
| | بانک ملی دانمارک | ارزیابی پیامدهای CBDC بر زیرساخت های بازار مالی دانمارک |
| 2018 | بانک رزرو آفریقای جنوبی | Project Khokha |
| | دولت ونزوئلا | Project Petro |
| | بانک لیتوانی | LBChain |
| | بانک ملی سوئیس | بررسی استفاده از DLT در خدمات مالی سوئیس |
| | بانک نروژ | تحقیقات در مورد فاز اول اجرای CBDC |
| | بانک تایلند | Project Inthanon |
| 2019 | بانک کره جنوبی | تحقیق درباره GA-CBDC |
| | بانک کانادا و سازمان پولی سنگاپور | Project Jasper-Ubin |
| | بانک مرکزی اروپا | ارائه یک تعریف استاندارد برای دارایی های رمزارزی |

## ۳- روش پژوهش

روش تحقیق حاضر از این جهت که نتایج مورد انتظار آن را می توان در راستای پیاده سازی و اجرای ارز رمزپایه با پشتیبانی دولت و بانک مرکزی به خدمت گرفت از حیث هدف از نوع کاربردی می باشد. همچنین از آنجا که روابط بین متغیرها به صورت همزمان بررسی می شود، از نوع همبستگی است.

در این تحقیق به منظور بررسی ویژگی ها و توانایی های EOSIO، شاخص های آن را با بلاکچین چند کریپتوکارنسی مطرح در این حوزه مقایسه می کنیم. پارامترهای مهم و تعیین کننده در عملکرد ارزهای دیجیتال توسط بلاک اکسپلوررهای جدول ۲ بررسی و اندازه گیری شده اند.

**جدول (۲) بلاکچین اکسپلوررهای مورد استفاده برای اندازه گیری پارامترهای بلاکچین های مختلف**

| ارز رمزپایه | بلاکچین اکسپلورر | | | |
|---|---|---|---|---|
| | ۱ | ۲ | ۳ | ۴ |
| بیت کوین | Blockchain.info | Live.blockcypher | Blockchair | Viawallet |
| اتر | Etherscan | Ethplorer | Blockchair | Eth.tokenview |
| بیت کوین کش | Oklink | Viawallet | Blockchair | Bch.tokenview |
| لایت کوین | explorer.litecoin | chainz.cryptoid | Blockchair | Ltc.tokenview |
| توکن مبتنی بر EOSIO | Bloks.io | Eospark | Eosflare | Eosx.io |

## ۵- متغیرهای و مدل های پژوهش

- مقیاس پذیری؛ که با تعداد تراکنش بر ثانیه (TPS) و برای هر ارز دیجیتال توسط بلاک اکسپلورر یا جستجوگر بلاکچین مربوط به همان زنجیره بلوکی اندازه گیری می شود.
- نسل بلاکچین؛ که برای رمزارزهای فاقد قابلیت اجرای قرادادهای هوشمند نسل یک، دارا بودن توانایی اجرای قراردادهای هوشمند ساده نسل دو و داشتن قابلیت اجرای قراردادهای هوشمند پیچیده نسل سه تعریف می گردد.
- الگوریتم اجماع؛ که در اینجا دو نوع کلی مبتنی بر اثبات کار (PoW) و مبتنی بر اثبات سهام (PoS) مورد توجه است.

- قابلیت پشتیبانی از زنجیره های چندگانه[18] و ارتباطات میان بلاکچینی[19] (IBC) که مربوط به ویژگی های هر بلاکچین است.
- میزان متمرکز یا غیر متمرکز بودن بلاکچین؛ که بستگی به تعداد نودها و نحوه توزیع کوین یا توکن ها بین نودهای شبکه دارد.
- زمان بلوک؛ مدت زمانی که لازم است تا یک بلوک در بلاکچین تولید شود، توسط بلاک اکسپلورر اندازه گیری می شود و بر حسب ثانیه است.
- اندازه بلوک؛ حجم بلوک بر حسب بایت (معمولاً مگابایت یا MB) است که می تواند ثابت یا متغیر باشد.
- زمان تأیید یک تراکنش؛ که بر حسب دقیقه ارائه شده است.
- هزینه تراکنش؛ بر حسب واحد دلار و توسط بلاک اکسپلوررها به صورت میانگین به دست آمده است.

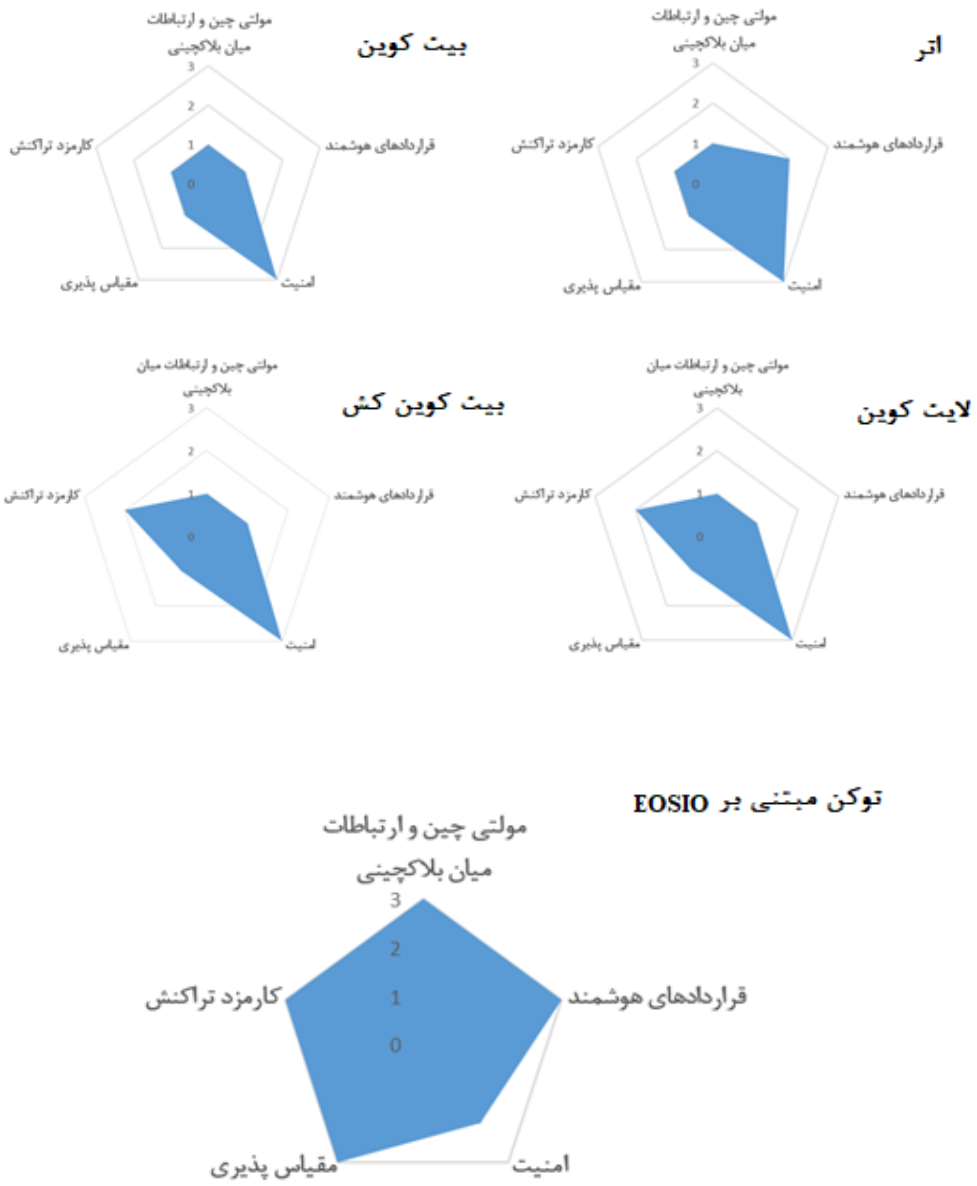
تعداد عملیات یا Operation؛ که در طی ۲۴ ساعت برای بلاکچین های با بیشترین تعداد عملیات ارائه شده است، می تواند انتقال سکه یا توکن باشد و یا سایر اقدامات در بلاکچین مانند به روزرسانی یا ایجاد دارایی، رأی گیری، اظهار نظر ، ارسال یک پست و ... .

## ۶- یافته های پژوهش

همانطور که در جدول ۳ مشهود است، تعداد عملیات های بلاک چین EOSIO به تنهایی بیش از ۴ برابر تمام بلاکچین های فعال دیگر می باشد. رمزارز مبتنی بر EOSIO به هزاران TPS می رسد که برای عملکرد به عنوان یک CBDC ضروری است. این تراکنش ها رایگان و بدون کارمزد هستند و بلافاصله تأیید می شوند. تنها مواردی که بلاکچین EOSIO در آن نسبت به رقبا ضعیف تر ظاهر می شود امنیت کمتر و نیمه غیرمتمرکز بودن آن است. اما باید به این نکته توجه داشت که هرچند این تمرکززدایی کمتر در بلاکچین های غیرمتمرکز مانند بیت کوین ها یک ایراد اساسی در نظر گرفته می شود اما از آنجا که CBDC ذاتاً متمرکز است این مورد از یک نقطه ضعف در حوزه کریپتوکارنسی ها به یک مزیت در CBDC تبدیل می گردد. همچنین مقدار امنیت با وجود پایین تر بودن از بلاکچین های رقیب، از سیستم های متمرکز فعلی بالاتر است. ارزیابی بلاکچین های تحت آزمون در پنج حوزه مهم مورد بحث به شکل راداری (نمودار ۱) نشان داده شده است.

**جدول (۳) مقایسه بلاک چین مبتنی بر EOSIO با بلاکچین های دیگر بلاکچین های مورد آزمون**

| | EOSIO 2.0 | Bitcoin | Ethereum | Fork of Bitcoin (BCH) | Litecoin |
|---|---|---|---|---|---|
| سال عرضه | 2020 | 2009 | 2015 | 2017 | 2011 |
| الگوریتم اجماع | PoS (DPoS) | PoW | PoW (Ethash) | PoW | PoW (Scrypt) |
| پشتیبانی از قرارداد هوشمند | Yes | No | Yes | No | No |
| پشتیبانی از زنجیره های چندگانه | Multi | Single | Single | Single | Single |
| تمرکززدایی | Semi-Decentralized | Decentralized | Decentralized | Decentralized | Decentralized |
| مدت زمان تشکیل هر بلوک (ثانیه) | 0.5 | 600 | 15 | 600 | 150 |
| حداکثر سایز هر بلوک (MB) | 1 | 1 | 0.025 (Variable) | 8 | 1 |
| نرخ تراکنش بر ثانیه | 10,000 | 7 | 15 | 24 | 56 |
| میانگین هزینه تراکنش (دلار) | Free | Variable (1 - 6 During May - June 2020) | Variable (0.2 - 0.6 During May - June 2020) | 0.0011 | 0.0011 |
| درصد عملیات به مجموع عملیات تمام بلاکچین ها | 82% | 1% | 1% | <1% | <1% |




**نمودار (۱) ارزیابی بلاکچین های مورد مطالعه در حوزه های مختلف**

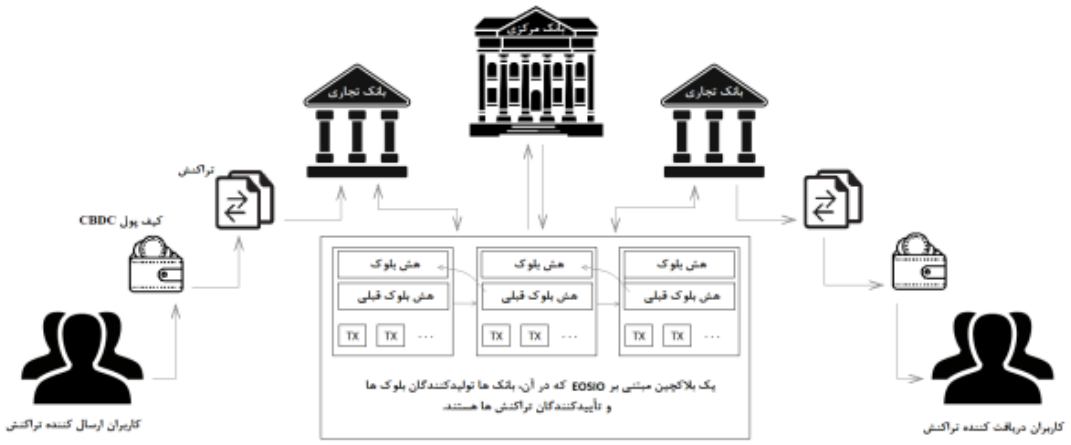
### ۷- یک چارچوب مبتنی بر EOSIO برای CBDC

در این بخش یک چارچوب CBDC مبتنی به روی یک بلاکچین EOSIO با تعیین کردن نقش بانک ها به عنوان BP ارائه و همچنین تغییرات مورد نیاز برای تطبیق بلاکچین EOSIO برای عملیاتی کردن CBDC توضیح داده می شود. در نهایت مراحل یک تراکنش از زمان ارسال توسط یک ارسال کننده تا زمان دریافت توسط یک دریافت کننده تشریح می گردد.

**۷-۱- بانک ها به عنوان BP**

برای مشاهده تأثیرات CBDC بر بانک های تجاری توجه به تغییرات احتمالی بانک ها برای رقابت با این شکل جدید ارز لازم است. در این بخش CBDC دارای بهره به حساب می آید زیرا این امر بیشترین تأثیر را روی بانک ها خواهد داشت. طراحی CBDC همراه با بهره باعث تقاضای بیشتر آن می شود و حجم بیشتری از آن در اقتصاد به گردش در می آید. با این حال از آنجا که سپرده های بانکی نیز بهره را ارائه می دهند، اثرات احتمالی به نرخ تعیین شده توسط بانک مرکزی بستگی دارد. بانک های تجاری بخش بزرگی از بودجه خود را از سپرده گذاران دریافت می کنند. اگر CBDC دارای بهره باشد، با توجه به اینکه نگهداری آن نسبت به سپرده امن تر است، ممکن است پول ورودی به بانک ها از محل سپرده با کاهش قابل توجهی مواجه شود. در این حالت ممکن است بانک ها با اجرای نرخ بالاتر سود وام، اقدامات کاهش هزینه، استفاده از راه حل های نوآورانه در حوزه فین تک و افزایش ریسک در سرمایه گذاری به مقابله با این وضعیت بپردازند. بانک های تجاری می توانند آن هایی باشند که تراکنش های CBDC را تأیید می کنند. می توان سیستم مشابهی را با کریپتوکارنسی ها اتخاذ کرد که در آن تولیدکنندگان بلوک یا تأیید کنندگان تراکنش، بانک های تجاری باشند و مقداری از مبلغ تراکنش را به عنوان پاداش دریافت کنند. این هزینه می تواند جریان دیگری از درآمد باشد و می تواند در جبران کاهش تأمین بودجه از سپرده ها مفید باشد.

EOSIO با هدف غیرمتمرکز کردن شبکه، BPهای داوطلب را به رأی گیری می گذارد تا ۲۱ BP فعال انتخاب شوند. هرچه تعداد BPها بیشتر شوند، شبکه غیر متمرکزتر و سرعت انجام تراکنش ها کندتر می شود. در مدلی که در این پژوهش ارائه می دهیم با توجه به ذات متمرکز CBDC نیازی به رأی گیری برای انتخاب BPها نداریم. همچنین با کاهش تعداد BPها سرعت شبکه را افزایش خواهیم داد. اما چگونه همه بانک ها را در فرایند تولید بلوک دخیل کنیم در حالی که تعداد BPها را کاهش داده ایم. در اینجا یک راه حل ارائه می گردد: تعداد ثابتی از BPهای مشخص و تعیین شده توسط بانک مرکزی (که در مدل پیشنهادی همان بانک های تجاری هستند) در ۳ گروه تقسیم بندی می شوند و هر گروه در بازه های زمانی ۱۲ ساعته نقش تولید بلوک ها، تأیید تراکنش ها و تأمین امنیت شبکه را به عهده می گیرند. در هر ۱۲ ساعت یکی از این ۳ گروه و به نوبت به عنوان BP فعالیت می کنند و دو گروه دیگر در حالت رزرو هستند. فرض می کنیم ۳۰ بانک تجاری به عنوان BP زیر نظر بانک مرکزی فعالیت می کنند. این ۳۰ بانک به ۳ گروه ۱۰ تایی تقسیم می شوند. گروه اول به مدت ۱۲ ساعت BP فعال می باشد، در ۱۲ ساعت بعدی گروه دوم و در ۱۲ ساعت آخر گروه سوم. به این ترتیب این چرخه هر ۳۶ ساعت یکبار از سر گرفته می شود. نحوه فعالیت هر بانک در شبکه مثل تعداد بلوک های از دست رفته توسط بلاک اکسپلورر شبکه رصد می شود و BPها بر اساس کیفیت عملکرد خود پاداش گرفته و یا جریمه می شوند. BPها با توجه به تأمین منابع شبکه که موجب انجام رایگان تراکنش ها می شوند، از محل تورم سالانه CBDC که توسط بانک مرکزی تعیین می شود پاداش دریافت می کنند. این موضوع به آن ها کمک می کند تا هزینه های نگهداری شبکه را پوشش دهند و نیز بتوانند ریسک ناشی از خروج نقدینگی از آن ها را که به دلیل صدور CBDC ایجاد می شود و پیشتر در مورد آن بحث کردیم تا حدی پوشش دهند. در شکل ۳ جایگاه بانک به عنوان BP در این مدل نشان داده شده است.




**شکل (۳) مدل گردش CBDC مبتنی بر یک بلاکچین EOSIO**

### ۷-۲- انجام تراکنش

تراکنش های کاربران می تواند در داخل شبکه و یا به صورت بین مرزی صورت پذیرد. هر کابر در شبکه یک حساب دارد که در واقع همان کیف پول الکترونیکی است. این کیف پول به صورت یک نرم افزار در رایانه ها و دستگاه های هوشمند نصب می شود و در صورت عدم دسترسی صاحب حساب به آن، او قادر به بازیابی آن خواهد بود. کاربر می تواند CBDC را در داخل این کیف پول نگهداری کند، آن را به حساب دیگری انتقال دهد و یا با آن عملیات پرداخت انجام دهد. همچنین با توجه به قابلیت های بلاکچین نسل سومی EOSIO در پشتیبانی از قراردادهای هوشمند، کاربر قادر است CBDC را در پروژه های نیازمند نقدینگی Stake کند و پاداش بگیرد و نیز امکان وام دهی و یا دریافت وام توسط کاربران از یکدیگر فراهم می شود.

برای انجام تراکنش، کاربر درخواستی را به شبکه برای انتقال CBDC از کیف پول خود به حساب دیگری ارسال می کند. BPها پس از انجام عملیات ضد پولشویی[۲۰] (AML) وظیفه تأیید تراکنش ها و ثبت آن ها در بلاکچین را دارند. با توجه به اینکه در مدل ما ۱۰ BP فعال وجود دارد پس از دریافت ۷ تأیید از BPها (۷ > ۲/۳ * ۱۰) که بیش از دو سوم آن ها را شامل می شود، تراکنش انجام می گیرد و CBDCها از کیف پول ارسال کننده به کیف پول دریافت کننده منتقل می شوند. نظارت بر تمام حساب ها و نیز عملکرد بانک ها به عنوان BP بر عهده بانک مرکزی می باشد. این فرآیند در شکل ۳ نمایش داده شده است.

### ۸- نتیجه گیری

در این پژوهش ما تفاوت های بین CBDC و کریپتو کارنسی ها را تشریح کردیم و نیز به مقایسه پارامترهای یک بلاکچین مبتنی بر EOSIO 2.0 با دیگر بلاکچین های مطرح در این حوزه پرداختیم. سپس اثرات احتمالی صدور CBDC به روی بانک های تجاری را مورد بررسی قرار دادیم و سرانجام یک چارچوب مبتنی بر بلاکچین نسل سومی EOSIO 2.0 برای صدور و گردش CBDC با مشخص کردن نقش بانک های تجاری به طوری که اثرات منفی عرضه CBDC بر آن ها به حداقل برسد ارائه دادیم. همانطور که پیشتر مشاهده کردیم تعداد عملیات های بلاک چین EOSIO به تنهایی بیش از ۴ برابر تمام بلاکچین های فعال دیگر می باشد در حالی که امکان انجام تراکنش های بدون کارمزد را نیز فراهم می سازد. با توجه به تمرکززدایی بسیار کم EOSIO و ذات متمرکز CBDC، یک بلاکچین مبتنی بر EOSIO می تواند برای صدور و عرضه CBDC مورد استفاده قرار بگیرد.

## فهرست منابع


* D. Chaum, “Blind signatures for untraceable payments,” in Proc. 2nd Conf. Adv. Cryptol., Aug. 1982, pp. 199–203.
* L. Law, S. Sabett, and J. Solinas, “How to make a mint: The cryptography of anonymous electronic cash,” Amer. Univ. Law Rev., vol. 46, no.4, 1996.
* W. Dai. (1998). B-Money [Online]. URL: http://www.weidai.com/bmoney.txt
* V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, “KARMA: A secure economic framework for peer-to-peer resource sharing,” in Proc. 1st Workshop Econ. Peer Peer Syst. (P2PEcon’03), 2003.
* H. Finney, “Rpow [Online],” URL: http://cryptome.org/rpow.html, 2004.
* N. Szabo, “Bit Gold [Online],” URL: http://unenumerated.blogspot.de/2005/12/bit-gold.html, 2005.
* Nakamoto. S, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
* Florian Tschorsch and Björn Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, 2016.
* Joline Göttfert, “A cointegration analysis of Bitcoin, Bitcoin Cash, EOS, Ethereum, Litecoin and Ripple,” UMEA Universities, 2019.
* V. Buterin, “Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform,” URL: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_ smart_contract_and_decentralized_application_platform-vitalikbuterin.pdf, 2013.
* G.Jeff, “Block size increase to 2MB,” URL: https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki, Github Repository, 2015.
* L .Johnson, “Merkelized Abstract Syntax Tree,” URL: https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki, Github Repository, 2016.
* L. Eric, L. Johnson, and W.Pieter, “Segregated Witness,” URL:https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki, Github Repository, 2015.
* W. Pieter, “Dealing with malleability,” URL:https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki, Github Repository, 2014.
* C.P.Schnorr, “Efficient signature generation by smart cards,” Journal of cryptology 4.3: 161-174, 1991.
* J.Poon, and T.Dryja, “The bitcoin lightning network: Scalable offchain instant payments,” 2016.
* S. D. Lerner, “Raiden Network, cheap, scalable token transfers for Ethereum,” 2018.
* A. Back et al., “Enabling Blockchain Innovations with Pegged Sidechains,” URL: http://www.opensciencereview.com/papers/123/enablingblockchaininnovations-with-pegged-sidechains, 2014.
* J.Poon, and V.Buterin, “Plasma: Scalable Autonomous Smart Contracts,” White paper, 2017.
* D. Larimer, “EOS.IO technical white paper,” URL: https://github.com/EOSIO/Documentation, 2017.
* W. Zheng et al., “XBlock-EOS: Extracting and Exploring Blockchain Data From EOSIO,” 2020.
* D. Horn, “Telos Whitepaper: A sustainably decentralized EOSIOnetwork,” URL: https://resources.telosfoundation.io/telos_white_paper_7_17.pdf, 2018.
* BOS FOUNDATION LTD, “BOSCore technical white paper,” URL: https://osshkbk01.oss-cn-hongkong.aliyuncs.com/bos/res/BOSCoreTechnicalWhitePaper.pdf, 2018.
* MEET.ONE Team, “MEET.ONE: The Portal to EOS white paper,” URL: https://meet.one/MEETONE_EN.pdf, 2018.
* W. Quigley et al., “WAX Protocol Whitepaper,” URL: https://github.com/worldwide-asset-exchange/whitepaper, 2019.
* F. Krueger, “LynxChain Whitepaper 1.0,” URL: https://medium.com/lynxwallet/lynx-chain-whitepaper-1-0-6869fd9582c3, 2019.
* ULTRA Team, “ULTRA: The Future of Digital Games Distribution Whitepaper,” URL: https://ultra.io/whitepaper, 2019.
* W. Tsai et al., “A Multi-Chain Model for CBDC,” 5th International Conference on Dependable Systems and Their Applications (DSA), 2018.
* E. A. Opare and K. Kim., “A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures,” IEEE Access: Special

Section On Blockchain Technology: Principles and Applications, 2020.

* Committee on Payments and Market Infrastructures (CPMI), "Central Bank Digital Currencies," Bank for International Settlements, 2018.
* C. Barontini, H. Holden, "Proceeding with caution - a survey on central bank digital currency," Bank for International Settlements, URL: https://www.bis.org/publ/bppdf/bispap101.pdf, 2019.
* Madelein Gartz, Ida Linderbrandt, "Are Cryptocurrencies the Future of Money, Whether a Transition to Cryptocurrency, as National Currency of Sweden, Would be Possible and What it Would Imply for the Swedish Society," DEGREE PROJECT IN TECHNOLOGY. STOCKHOLM, SWEDEN, 2017.
* COSMOS CR team, "CosmosCR: A new internet build in a virtual reality metaverse," PolkaDot Whitepaper, 2016.
* G. Wood, "POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK," Cosmos CR Whitepaper V 1.2, 2019.
* N. Durov, "Telegram Open Network," TON Whitepaper Ver.3, 2018.
* N. Szabo, "The idea of smart contracts," 1997.
* Y. Huang, H. Wang, L. Wu, G. Tyson, X. Luo, R. Zhang, X. Liu, G. Huang, and X. Jiang, "Characterizing eosio blockchain," 2020.
* L. Quan, L.Wu, and H.Wang, "EVulHunter: Detecting Fake Transfer Vulnerabilities for EOSIO's Smart Contracts at Webassemblylevel," 2019.
* G. Danezis, S. Meiklejohn, "Centrally banked cryptocurrencies," URL: https://arxiv.org/abs/1505.06895, 2015.
* H. Sun et al., "Multi-Blockchain Model For Central Bank Digital Currency," 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2017

## یادداشت ها

[1] Blockchain
[2] Cryptocurrencies
[3] Decentralized
[4] Bitcoin
[5] Ethereum
[6] Fiat Currency
[7] Central Bank Digital Currency
[8] Scalabe
[9] Feesless
[10] Proof of Work
[11] Alternatives to Bitcoin
[12] Delegated Proof of Stake
[13] Bank for International Settlements
[14] Block Producer
[15] Command Line Interface
[16] Wallet
[17] Smart Contracts
[18] Multi Chain
[19] Inter Blockchain Communication
[20] Anti-Money Laundering