

ارائه چارچوبی جهت تدوین سند راهبردی توسعه فناوری زنجیره بلوک مبتنی بر تحلیل حوزه های کاربرد



معاونت فناوری اطلاعات و ارتباطات

گروه اقتصاد دیجیتال

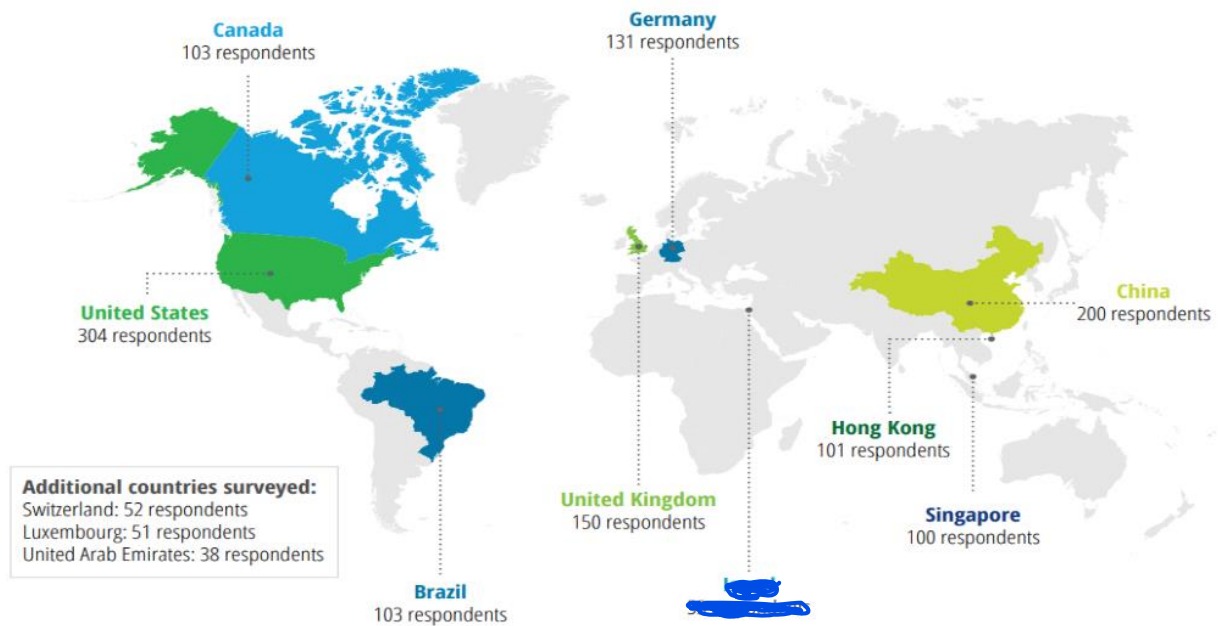
ورژن ۰،۰

خلاصه مدیریتی

فناوری زنجیره بلوک به عنوان یک فناوری نوظهور در حال تغییر زیرساخت‌های اجتماعی-اقتصادی (Socio-economic) کشورهاست. یکی از این تغییرات کلیدی، تحول در مفهوم اعتماد (Trust) است. این تحول فناورانه رویکرد جدیدی به اعتماد را بر مبنای رمزنگاری و انگیزه‌های نظری غیرمتمرکز پدید آورده است. همواره مفهوم اعتماد شکل‌دهنده فعالیت‌های اجتماعی-اقتصادی جوامع بوده است و تحول در این مفهوم اثری چشم‌گیر به همراه خواهد داشت. از این رو، پژوهش حاضر نظر به اهمیت این فناوری در راهبرد سیاست‌های کلان اقتصادی ج.ا.ا چارچوبی را برای تدوین سند راهبردی این فناوری در حوزه‌های کاربردی ارائه نموده است. در این پژوهش سعی شده تا با روش‌های تکنیکال تحلیل فناوری مانند علم‌سنجی و تحلیل پتنت و تحلیل‌های غیرتکنیکال مانند تحلیل حجم و روند بازار، میزان سرمایه‌گذاری‌ها و تحلیل مکان‌محور توسعه فناوری، تحلیلی جامع از جذابیت فناوری در حوزه‌های کاربرد مشخص گردد، حوزه‌های تحلیل بر اساس بخش‌بندی فناوری از روش‌ها و الگوریتم‌های کاربردی آن انتخاب گردیده است. در گام بعدی به منظور ارزیابی توانمندی فناوری در حوزه‌های کاربرد، تمرکز فعالیت‌های استارت‌آپی و شرکت‌های سرمایه‌گذاری بزرگ مانند موسسات مالی و بانک‌ها ارزیابی شده است، سپس به منظور انجام مطالعه‌ی تطبیقی رویکردها و برنامه‌های دولتی و خصوصی در کشورهای پیشرو در مقایسه با اقدامات ج.ا.ا مورد بررسی قرار گرفته است. در پایان بر اساس نتایج بدست آمده از دو بعد ارزیابی توانمندی و جذابیت فناوری، و همچنین مطالعه‌ی تطبیقی چارچوبی جهت تدوین سند راهبردی فناوری زنجیره بلوک در سه سطح حمایت از توسعه فناوری، حمایت از اکوسیستم و تعیین جایگاه دولت ارائه شده است.

امروزه مطالب زیادی در رابطه با فناوری زنجیره بلوک در اخبار مرتبط با فناوری منتشر شده است، در این اخبار و تحلیل‌ها از این فناوری به عنوان یک پدیده تحول‌آفرین حداقل در حوزه‌های پولی-مالی یاد می‌شود. چندی پیش از این فناوری به عنوان راهی برای دور زدن بانک‌ها و حفاظت از سوابق تراکنش‌ها در میان بوده است، اما در واقعیت یک تحول بسیار بزرگ‌تری در راه خواهد بود. به گفته موسسه‌ی تحقیقاتی Deloitte در سال ۲۰۱۹ نتایج نظرسنجی که از ۱،۳۸۶ سازمان در ۱۲ کشور و با ۱۱ زبان مختلف انجام گرفته ۵۳٪ از این سازمان‌ها فناوری زنجیره بلوک را به عنوان یکی از ۵ استراتژی کلیدی سازمان‌شان مطرح نموده‌اند. حدود ۴۱٪ از مدیران این سازمان‌ها بیان نمودند که شرکت‌های‌شان سرمایه‌گذاری بیش از ۵ میلیون دلار را در دست برنامه‌ریزی دارند. شکل (۱) نشان‌دهنده پراکندگی نظرسنجی فوق است (Delitte, 2019).

دلیل استفاده از فناوری زنجیره بلوک در شرکت‌های مطالعه شده توسط Deloitte شامل ایجاد کسب و کار جدید (۲۳٪)، افزایش امنیت و کاهش ریسک (۲۳٪)، افزایش سرعت سیستم‌ها (۱۷٪)، افزایش شفافیت (۱۱٪)، کاهش هزینه‌ها (۹٪)، بهبود شناسایی و کنترل (۹٪) و کاهش کلاهبرداری (۸٪) بوده است (Delitte, 2019). مطالعات مذکور و بسیاری از شرکت‌های تحقیقاتی مطرح دنیا مانند PWC، Gartner و همچنین میزان جذابیت سرمایه‌گذاری، جایگاه این فناوری را به عنوان یکی از فناوری‌های تحول‌آفرین آینده اثبات نموده است. بر همین اساس، سعی شده به منظور افزایش همراستایی بین اهداف توسعه‌ای، شفافیت در تقسیم و تنظیم وظایف در بخش‌های مختلف سیاست‌گذاری با این فناوری چارچوبی توصیه‌ای ارائه گردد. از آنجایی که نقطه‌ای اتکاء در توصیه‌های سیاستی بر تأثیرگذاری بر تصمیمات در سطوح مختلف جامعه می‌باشد، و پذیرش و مقبولیت فناوری‌های نوظهور به واسطه‌ی آگاهی و کسب دانش کافی ایجاد خواهد شد. سعی شده تا نیاز اطلاعاتی و تحلیلی در رابطه با روند تحول‌آفرین این فناوری تولید گردد. در همین راستا به منظور تحلیل فناوری مذکور از روش‌های مانند تحلیل متون انتشارات علمی و گواهی ثبت اختراع (پتنت) در حوزه‌های راهبردی این فناوری کمک گرفته شده است. در پایان نیز پس از بررسی سیاست‌های توسعه فناوری سایر کشورها و همچنین کشور ایران توصیه‌های به منظور دستیابی بهینه و بهنگام به این فناوری کلیدی ارائه گردیده است.



Source: Deloitte's 2019 Global Blockchain Survey.

شکل ۱. توزیع جغرافیایی نظرسنجی Deloitte (Delitte, 2019)

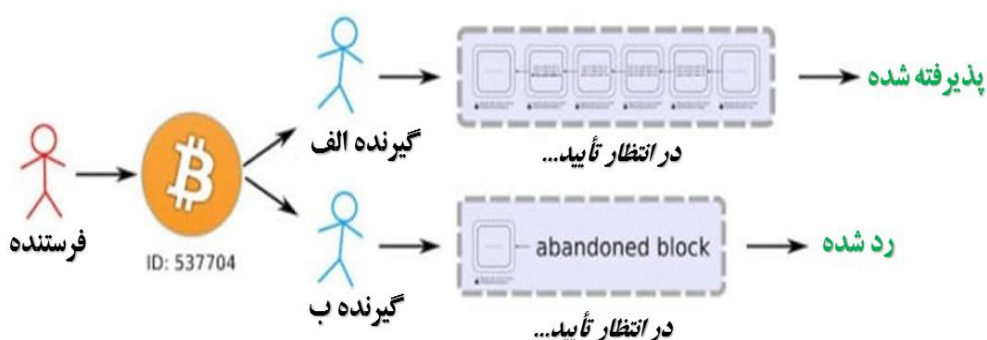
۲- مرور ادبیات

۲-۱- فناوری زنجیره بلوک چیست؟

فناوری زنجیره بلوک در حقیقت روشی برای نگهداری سوابق تراکنش‌ها، بسته‌ای از داده‌ها و سایر سوابق به صورت رمزنگاری شده است، به صورتی که هر کسی می‌تواند به این سوابق، داده‌ها و اطلاعات دسترسی داشته باشند، اما قادر به تغییر در آن نیست. به عبارتی، این فناوری یک دفتر کل عمومی است که امکان ذخیره‌سازی سوابق داده‌ها/ تراکنش‌ها را به جای ذخیره متمرکز بر روی یک سرور، آن را از طریق شبکه‌ای از گره‌ها و به صورت توزیع شده انجام می‌دهد، و امکان تغییر و دستکاری غیر مجاز اطلاعات برای گره‌ها به صورت انفرادی وجود ندارد. در این شبکه هر تبادل و یا تراکنش با اجماع^۱ اکثر مشارکت‌کنندگان در شبکه ثبت و به دفتر کل توزیع شده اضافه خواهد شد (Narayanan and et al., 2016). این ماهیت غیرمتمرکز بودن در فناوری زنجیره بلوک همان چیزی است که باعث ایجاد امنیت و عدم دستکاری غیر مجاز و یا هک در عین دسترسی کامل به داده‌ها خواهد شد.

¹ Consensus

فناوری زنجیره بلوک برای اولین بار در سال ۲۰۰۸ و با ظهور بیت‌کوین به دنیا معرفی شد. گفته می‌شود بیت‌کوین توسط ساتوشی ناکاموتو^۱ (یا گروهی تحت این نام) به عنوان یک کاربرد از دفتر کل عمومی ارائه شده است. این کاربرد در واقع اولین پول دیجیتالی را بدون نیاز به یک مرجع معتبر صادرکننده ایجاد نموده است و به صورت خلاصه این پروژه راهکاری فنی برای مسئله دوبار خرج کردن^۲ در سیستم‌های پولی دیجیتالی معرفی نموده است (شکل ۲). در گذشته برای سیستم‌های پولی دیجیتالی (برای مثال ارز دیجیتالی معرفی شده در سال ۱۹۹۸ به نام Bit Gold) مسئله کلیدی کپی کردن تراکنش‌ها و خرج کردن دوباره آن بوده است (Peck, 2012).



شکل ۲. ثبت تراکنش در زنجیره بلوک بیت‌کوین (Coinsutra, 2020)

در زنجیره بلوک عمومی مانند بیت‌کوین وقتی تراکنش‌ها برای تأیید به شبکه ارسال می‌شوند، کلیدی گره‌های تأییدکننده از آن آگاهی پیدا خواهند نمود، و هر یک از این تأییدکنندگان تعدادی از تراکنش‌های ارسالی را در داخل یک بلوک قرار خواهند داد و سعی می‌کنند تا مسئله‌ی ریاضی اثبات کار را حل نمایند. در صورت موفق شدن، بلوک حاوی تراکنش‌ها برای سایر تأییدکنندگان برای کنترل صحت آن ارسال خواهد شد، و برای ثبت قطعی یک تراکنش در زنجیره بلوک می‌بایست بیش از ۵۰٪ تأییدکنندگان آن را کنترل و به صحت آن رأی دهند. در این صورت است که کسی نمی‌تواند پولی را که یکبار خرج کرده، دوباره و دوباره خرج نماید (Coinsutra, 2020).

طبق منحنی اشتیاق فناوری^۳ ترسیم شده (شکل ۳) حاصل از درخواست^۴ گواهی ثبت می‌توان از Bank of America در سال ۲۰۱۳ و شرکت GoldmanSachs در سال ۲۰۱۴ را به عنوان پیشروهای اکتساب فناوری زنجیره بلوک نام

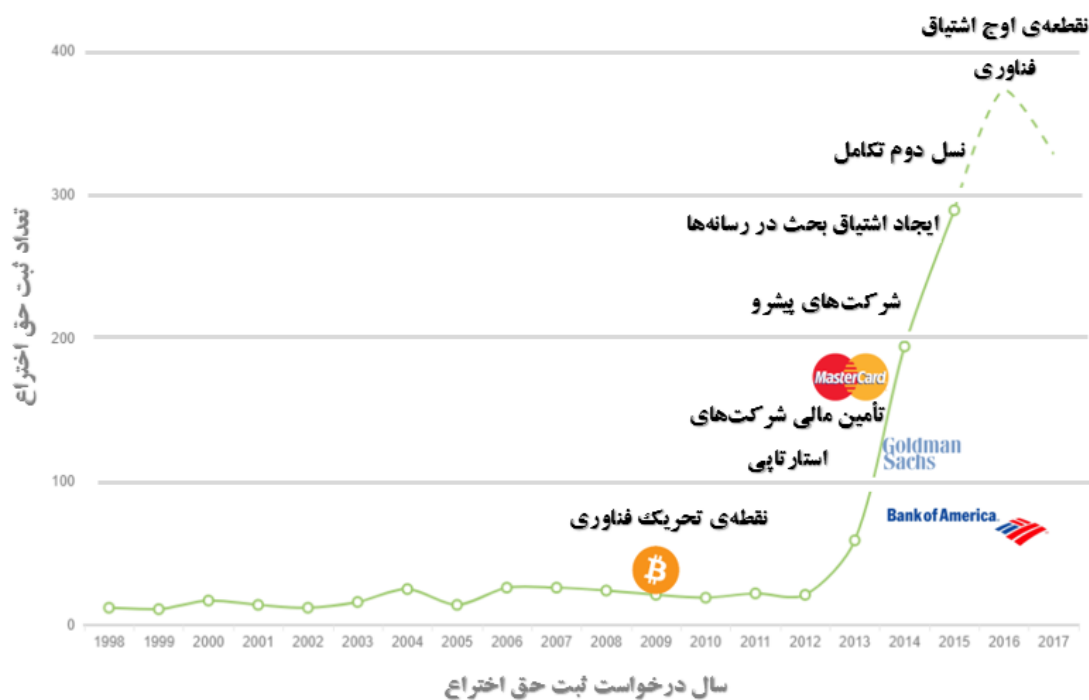
¹ Satoshi Nakamoto

² Double spending

³ Hype Cycle

⁴ Patent application / filing

برد(Patsnap, 2019). در حقیقت فناوری زنجیره بلوک و بلاخص ارز دیجیتالی مانند بیت‌کوین تحولی از عصر اینترنت اطلاعات را به سوی عصر اینترنت ارزش ۱ ایجاد نموده‌اند. در عصر اینترنت اطلاعات یک موجودیتی دیجیتالی است که در زمان ارسال کپی می‌شود و بعد از انتقال هر دو طرف (فرستنده و گیرنده)، اطلاعات را بدست می‌آورند، در حالی که در اینترنت ارزش در صورت انتقال موجودیت ارزش دیجیتالی حتماً فرستنده آن ارزش را از دست خواهد داد و گیرنده یک ارزش یکتا بدست خواهد آورد(Visconti, 2019).



شکل ۳. منحنی اشتیاق فناوری بر اساس تعداد گواهی حق اختراع (Coinsutra, 2020)

طبق نظر کارشناسان این فناوری پتانسیل ایجاد تغییراتی عمده در طیف وسیعی از محصولات و فرآیندهای تجاری را خواهد داشت، زیرا این فناوری توانمندی تعامل مستقیم و بدون نیاز به شخص ثالث مورد اعتماد^۲ (TTP) را ممکن ساخته است. همکاری‌ها در این فناوری نوید بهبود فرآیندهای تجاری بین شرکت‌ها را از طریق افزایش سرعت تسویه‌ها، کاهش کارمزد تراکنش، افزایش امنیت در مقابل جعل و شفافیت و قابلیت ردیابی تراکنش‌ها و همچنین بازدهی قابل توجه نسبت به سرمایه‌گذاری‌های صرف شده برای توسعه را خواهد داد. در سطح تئوریک فناوری زنجیره بلوک پتانسیل تبدیل شدن به یک عامل خودمختار و توزیع شده را برای صنایعی سنتی متکی بر اعتماد دارد. در این رویکرد نوین،

¹ Internet of Value

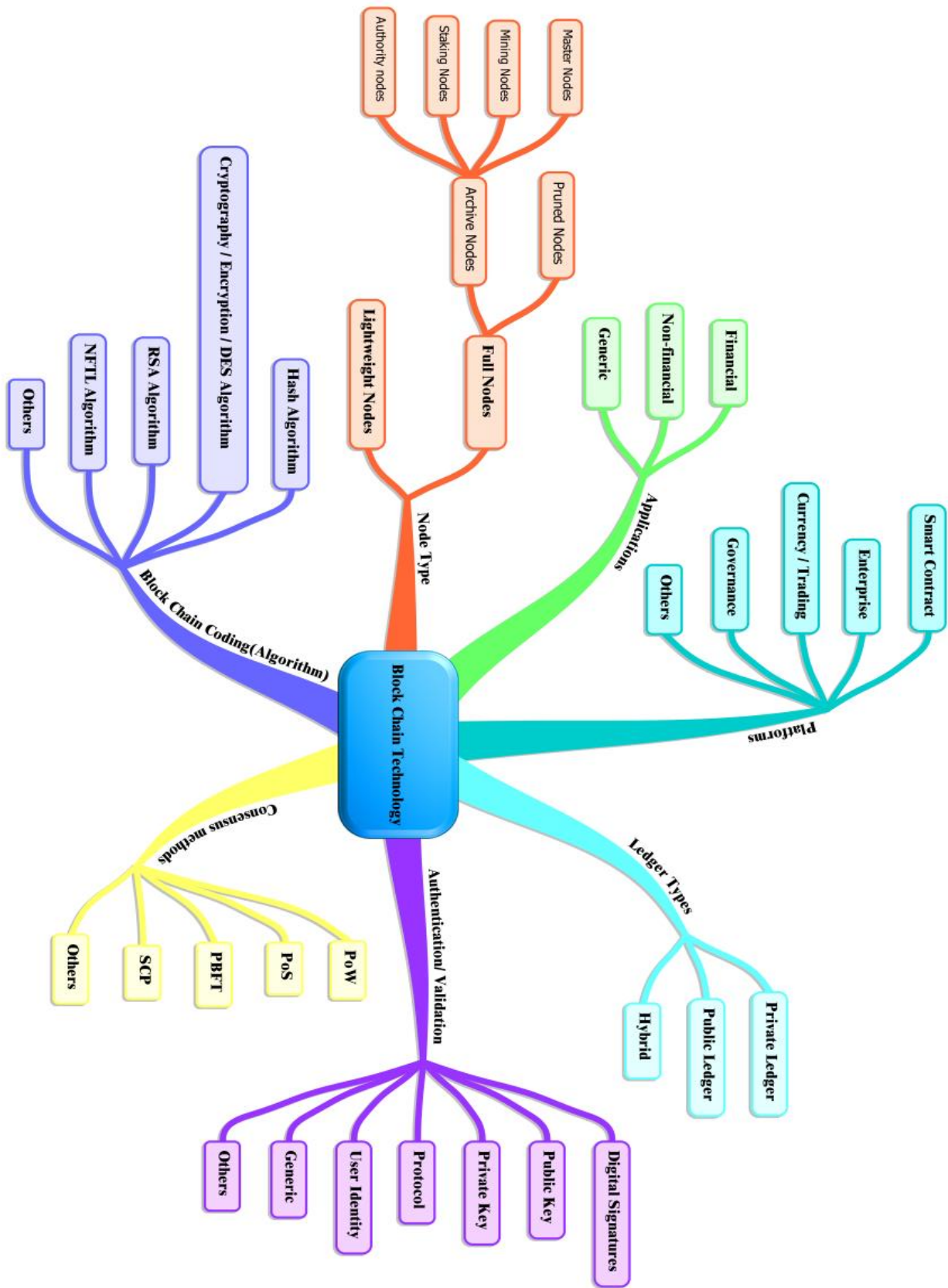
² Trusted third party

سیستم اعتماد از طریق رمزنگاری و انگیزه‌های نظری (تئوری بازی‌ها) به صورت غیرمتمرکز ایجاد می‌گردد، که تکیه‌گاه کلیدی برای توسعه کاربرد این فناوری است (Locher and Pignolet, 2018). این تغییر ماهیت نه تنها در معاملات دیجیتال پدیدار می‌شود، بلکه در زندگی روزمره نیز راه خواهد یافت. در ادامه سعی خواهد شد برخی از کاربردهای بالقوه و بالفعل این رویکرد جدید مورد واکاوی قرار گیرد.

۲-۲- بخش‌بندی فناوری زنجیره بلوک

هم اکنون، جدا از مباحث داغ رمزارزها که در حال حاضر به ظرفیت بازاری (MC)^۱ بیش از ۲۱۴ میلیارد دلار رسیده (Coinmarketcap, 2020)، کاربردهای این فناوری از صنعت حمل و نقل گرفته تا ارتباطات، از داده‌های مالکیت دارایی گرفته تا صنایع تولیدی خواهد بود. در این پژوهش به منظور بررسی دقیق‌تر حوزه‌های فناورانه و کاربردهای زنجیره بلوک بخش‌بندی از زیرحوزه‌های آن به صورت شکل (۴) ارائه شده است.

¹ Market capacity: Supply * Value



شکل ۴. بخش بندی فناوری زنجیره بلوک

به منظور بخش‌بندی فناوری زنجیره بلوک روش‌ها و الگوریتم‌های کاربردی آن شناسایی شده است: بخش اول، مربوط به سطح کاربرد فناوری زنجیره بلوک است، این بخش با عنوان پلتفرم در شکل فوق نشان داده شده است، و شامل سطح بکارگیری فناوری در تجارت/ارزهای رمزنگاری شده، قراردادهای هوشمند، درون شرکتی و حاکمیتی است. بخش دوم، مربوط به روش‌های اجماع در این فناوری‌ست، مفهوم اجماع در این فناوری مترادف تصمیم‌گیری برای صحت یک تراکنش، انتخاب، حذف و یا اضافه شدن گره‌های مشارکت‌کننده در شبکه و همچنین رأی‌گیری برای بکارگیری قوانین و روال‌های جدید در شبکه در نظر گرفته می‌شود. این بخش نیز به پروتکل اجماع گواه اثبات کار^۱ (PoW)، پروتکل گواه سهام^۲ (PoS)، پروتکل تحمل خطای بی‌زانس^۳ (PBFT) و پروتکل اجماع استلار^۴ (SCP). بخش سوم، مربوط به ساختار شبکه زنجیره بلوک است، به صورت کلی سه دسته برای ساختاردهی گره‌ها در شبکه وجود دارد، که بسته به نوع پذیرش در شبکه به زنجیره بلوک عمومی^۵، زنجیره بلوک خصوصی^۶ و شبکه هیبرید تقسیم‌بندی می‌شوند. در زنجیره بلوک عمومی گره‌ها بدون محدودیت و بدون نیاز به تأیید می‌توانند به شبکه متصل شوند. مانند بیت‌کوین و اتریوم ولی در نقطه‌ای مقابل، زنجیره بلوک خصوصی منحصر به یک شبکه و دسترسی محدود و با تأیید می‌باشد، مانند هایپرلدر فبریک^۷. نوع سوم شبکه‌های هیبرید مانند دراگون‌چین^۸ است که ترکیبی از ویژگی‌های زنجیره عمومی و خصوصی را داراست. بخش چهارم، مربوط به احراز هویت و اعتبارسنجی^۹ است، مباحث مطرح در این بخش عبارتند از مفهوم کلید عمومی^{۱۰}، کلید خصوصی^{۱۱}، امضاء دیجیتال^{۱۲}، شناسایی کاربر (احراز هویت). این کلیدها معمولاً برای دریافت و ارسال رمز ارز در شبکه زنجیره بلوک مورد استفاده است. کلید عمومی یک رشته ترکیبی از حروف و اعداد است که با استفاده از توابع ریاضی رمزنگاری (تابع یک طرفه‌ی هشینگ) از کلید خصوصی بدست می‌آید، در واقع کلید عمومی همانند آدرس هویت‌ها (آدرس کیف پول الکترونیکی) در زنجیره بلوک در نظر گرفته

1 Proof of Work: این پروتکل برای حل پازل ریاضی به گره‌ها یا همان ماینرها با هدف تأیید تراکنش و ایجاد بلاک جایزه داده می‌شود برای مثال، شبکه بیت‌کوین.
2 Proof of Stake: این پروتکل به منظور اجماع در یک سیستم پولی مبتنی بر زنجیره بلوک مورد کاربرد بوده و هر چه گره‌ها پول بیشتری در شبکه داشته باشند، شانس بیشتری برای ایجاد بلاک خواهند داشت. برای مثال، شبکه ویوز (WAVES).
3 Practical Byzantine Fault Tolerance: این پروتکل به منظور کنترل سوء رفتار گره‌ها در مسئله خطای بی‌زانس (اثر گره‌های معیوب بر شبکه) ایجاد شده است برای مثال شبکه ریپل (Ripple).
4 Stellar Consensus Protocol: این پروتکل مانند پروتکل تحمل خطای بی‌زانی ایجاد شده با این تفاوت که برای اجماع از رأی‌گیری فدرالی و توان گروه‌هایی از گره‌ها موسوم به گروه (Quorum) استفاده می‌نمایند.

5 Public Ledger

6 Private Ledger

7 Hyperledger Fabric

8 Dragonchain

9 Authentication / Validation

10 Public Key

11 Private Key

12 Digital Signatures

می‌شود، و کلید خصوصی یک رشته ترکیبی از کارکترها و اعداد است که همانند سپرد دسترسی کاربران را به رمز ارزها میسر می‌سازد. مفهوم امضاء دیجیتال به جهت تبادل بین موجودیت‌های الکترونیکی و با هدف احراز هویت، عدم انکار پیام ارسالی و حفظ اصالت پیام ایجاد شده است. بخش پنجم، مربوط به تکنیک‌های کدنویسی و الگوریتم‌های بکار رفته در زنجیره بلوک است، این بخش شامل الگوریتم هشینگ^۱، الگوریتم‌های رمزنگاری^۲، رمزگذاری^۳، استاندارد رمزنگاری داده‌ها^۴(DES)، الگوریتم RSA^۵ و الگوریتم NFTL^۶. بخش ششم، مربوط به انواع گره‌ها است، به طور کلی گره‌ها در زنجیره بلوک به دو دسته گره کامل^۷ و گره سبک^۸ تقسیم می‌شود. گره‌های کامل در شبکه به عنوان سرور عمل کرده و وظایف اجماع بین گره‌ها و تأیید تراکنش‌ها را بر عهده دارند، این گره‌ها نسخه‌ی کپی شده‌ای از زنجیره‌های تأیید شده را نیز دارا هستند. گره‌های سبک در واقع به واسطه‌ی گره‌های کامل به شبکه زنجیره بلوک متصل خواهند شد و وظیفه جستجو و انتقال آخرین تراکنش را به آخرین بلاک زنجیره خواهند داشت، این گره‌ها نسخه‌ی کامل از زنجیره بلوک را ندارند و هدف آنان افزایش سرعت و سهولت در فرآیندهای روزانه رمزارزهاست. بخش هفتم، مربوط به کاربردهای بالفعل و بالقوه فناوری زنجیره بلوک است، به طور کلی این کاربردها را به سه دسته کاربردهای مالی، کاربردهای غیر مالی (کاربرد در سایر صنایع) و کاربردهای عمومی تقسیم‌بندی می‌نمایند. از کاربردهای مالی این فناوری می‌توان به حوزه‌های فناوری مالی (فین‌تک) اشاره نمود، که شامل پرداخت مبتنی بر رمزارزها، صرافی‌های رمزارز، پرداخت برون‌مرزی (رمیتنس)^۹، تجارت سهام، فناوری‌های بیمه، فناوری‌های قانون‌گذاری^{۱۰}، تأمین مالی جمعی و غیره هستند، کاربردهای این فناوری نیز در حوزه‌های بانکداری نیز قابل توجه است. مانند، سیستم‌های اتاق تسویه بین بانکی. دسته کاربردهای بعدی مربوط به سایر صنایع خواهد بود. برای مثال، صنعت بهداشت و سلامت شامل کاربردهایی مانند امنیت و اشتراک‌گذاری داده‌های پزشکی، ساده‌سازی روند مطالبات درمانی، صنعت لجستیک مانند گواهی اصالت کالاها، صنعت غذا و زنجیره تأمین مانند کاهش تقلب، ردیابی کالا و حذف واسطه‌ها، صنعت بازی‌سازی، صنعت خرده‌فروشی، صنعت ساخت و تولید هوشمند(نسل ۴،۰) و اینترنت اشیاء صنعتی مانند امنیت داده‌ها و حریم خصوصی و غیره اشاره نمود. در پایان کاربردهای عمومی زنجیره بلوک می‌توان به

Hash Algorithm^۱: الگوریتمی است که برای افزایش امنیت و یکپارچگی داده‌ها از روش‌های درهم‌سازی استفاده می‌نماید.

² Cryptography

³ Encryption

^۴ Data Encryption Standard: این حوزه مربوط به استاندارد کدگذاری در سیستم زنجیره بلوک است.

^۵ Rivest-Shamir-Adleman: شیوه‌ای برای رمزنگاری به روش کلید عمومی (PKC) است که کاربردهای گسترده‌ای در تبادلات الکترونیکی دارد.

^۶ Nand flash translation layer: این الگوریتم مربوط به ذخیره‌سازی امن، سریع و کم مصرف در کارت‌های حافظه است.

⁷ Full nodes

⁸ Lightweight nodes

⁹ Cross-border remittances

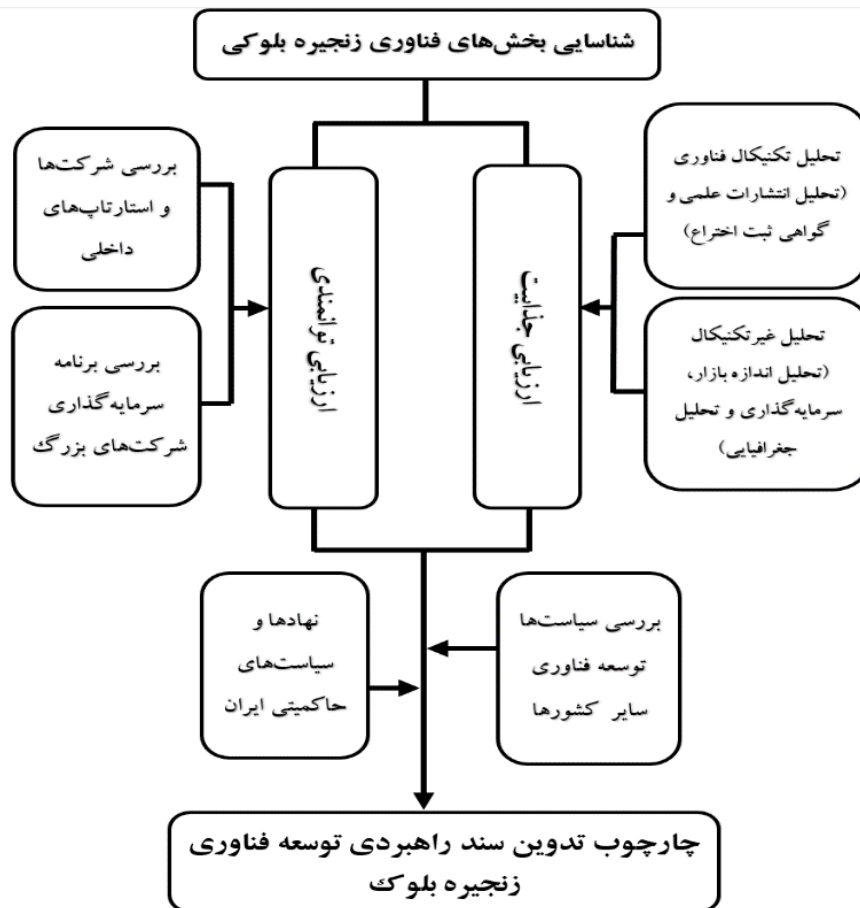
¹⁰ RegTech

مواردی چون نظرسنجی و رأی‌گیری، ثبت و ذخیره‌سازی امن داده‌ها و اطلاعات، تضمین کیفیت و مدیریت زنجیره تأمین و حفاظت از مالکیت معنوی اشاره نمود.

۳- روش‌شناسی پژوهش

تمرکز این پژوهش بر توسعه فناوری زنجیره بلوک در کشور ایران است. از این رو، می‌توان آن را از نظر نتیجه، پژوهشی کاربردی و از بعد هدف دارای ماهیتی توصیفی و تجویزی دانست، داده‌های استفاده شده در این پژوهش به دلیل ماهیت بین رشته‌ای و نوظهور آن ترکیبی از داده‌ها کمی و کیفی است و سعی شده در طی مراحل انجام پژوهش از متخصصان و صاحب نظران حوزه مذکور نظرخواهی صورت گیرد. در ابتدا به منظور شناسایی حوزه‌های فناوری هدف^۱ (TTA) روش‌ها، الگوریتم‌ها و حوزه‌های کاربرد در صنایع مختلف مورد مطالعه و تبادل نظر با متخصصان فنی این حوزه قرار گرفته است، خروجی این بخش تدوین بخش‌بندی فناوری به عنوان یک نقشه جامع از حوزه‌های اصلی این فناوری است. در مرحله بعدی پژوهش به منظور ارزیابی جذابیت فناوری سعی شده تا با بهره‌گیری از تحلیل انتشارات علمی و گواهی ثبت اختراع روند حوزه‌های فناوری مورد بررسی قرار گیرد، اصطلاحاً به این بخش تحلیل تکنیکال فناوری گفته شده است، و در ادامه در بخش غیرتکنیکال به مسائل اندازه بازار، حجم سرمایه‌گذاری و تحلیل‌های مکان محور حوزه‌های مختلف فناوری توجه گردیده است، در پایان بخش اول تحلیل‌های تکنیکال و غیر تکنیکال بدست آمده و نتایج در اختیار صاحب‌نظران فنی به منظور تدقیق تحلیل‌ها قرار گرفته است. در بخش دوم به منظور شناسایی توانمندی و آشنایی با پیشرفت‌های کاربردی این فناوری در شرکت‌های استارت‌آپی فعال در این حوزه مورد بررسی قرار گرفته است و در بُعد دوم به منظور شناسایی سطح توجه صنعت به این بخش سعی شده تا مروری از برنامه‌های اعلامی شرکت‌های فعال و سرمایه‌گذاری‌های آن‌ها مورد بررسی قرار گیرد. در بخش بعدی سعی شده تا سیاست‌های توسعه فناوری منتشر شده در کشورهای پیشرو و همچنین طریقه‌ی برخورد و همراهی حاکمیت ج.ا.ا با این فناوری با هدف مطالعه‌ی تطبیقی مورد واکاوی قرار گیرد. در پایان با توجه نتایج حاصل چارچوبی سه سطحی برای تدوین سند راهبردی توسعه فناوری زنجیره بلوک در ایران ارائه گردیده است.

¹ Technology Target Area



شکل ۵. روش‌شناسی پژوهش

۴- تجزیه و تحلیل یافته‌ها

۴-۱- بازار فناوری زنجیره بلوک: اندازه، پیش‌بینی و تحلیل حوزه‌های کاربرد

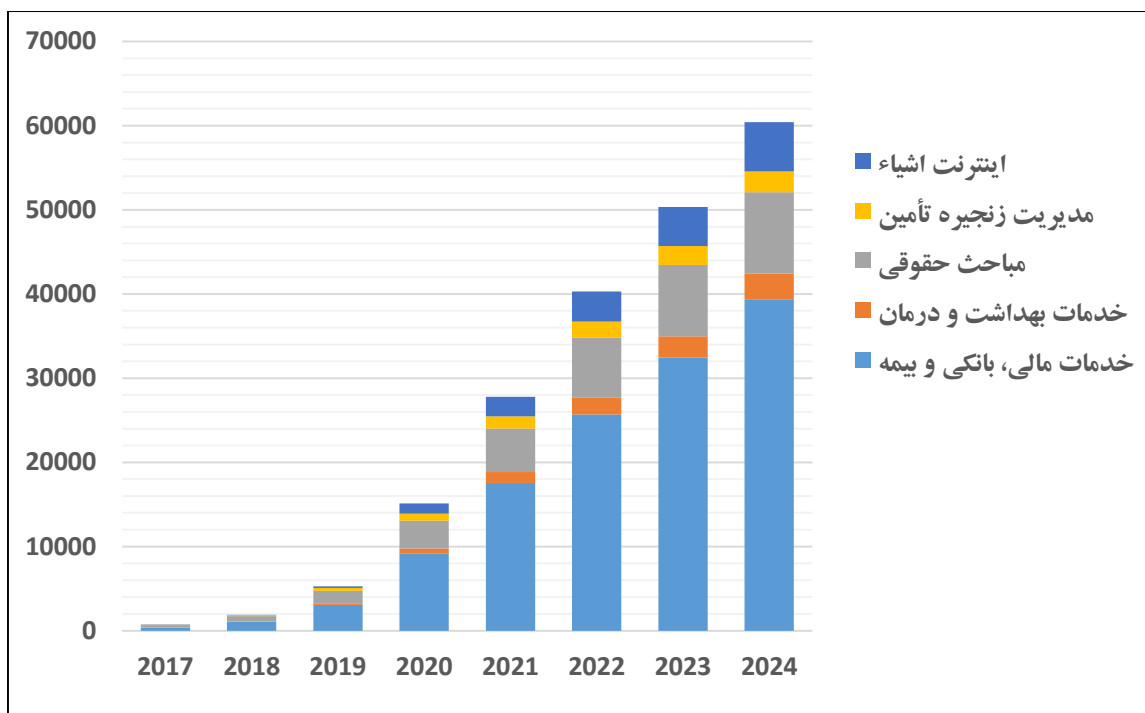
فناوری زنجیره بلوک برای سال‌های زیادی از زمان معرفی دستخوش نوسانات زیادی بوده است، تا اینکه در سال ۲۰۱۷ به یک بازار ۷۰۶ میلیون دلاری در سرتاسر دنیا رسیده است. پس از این شروع ناخوشایند و کاربردهای جنایتکارانه و تروریستی با هدف مخفی‌سازی، امروز این فناوری شاهد رشد قابل قبولی است، و در حال آماده‌سازی برای ایجاد زیرساخت‌های اقتصادی دیجیتال نوین در دنیاست. بازار این فناوری در سال ۲۰۱۷ در حوزه‌های جغرافیایی عبارتند از؛ آمریکا حجم بازار حدود ۵۳۶٫۶ میلیون دلار و سهم ۷۶٪، اروپا حجم بازار حدود ۱۰۵٫۹ میلیون دلار و سهم ۱۵٪، چین و هند حجم بازار حدود ۳۵٫۵ میلیون دلار و سهم ۵٪، ژاپن و آسیا-اقیانوسیه حجم بازار حدود ۲۱٫۲ میلیون دلار و سهمی برابر با ۳٪ و ۱٪ باقیماند متعلق به سایر کشورها است. پیش‌بینی می‌شود که این فناوری تا سال ۲۰۲۴ بازاری حدود ۶۰ میلیارد دلار دست یابد (WinterGreen, 2018).

با حرکت بانک‌ها و صنعت مالی به سوی عصری مدرن در پردازش تراکنش‌های تسویه بلادرنگ^۱ فناوری زنجیره بلوک توانمندی بیشتری می‌یابد. این بخش بزرگ از بازار فناوری زنجیره بلوک در سال‌های پیشین به واسطه‌ی حضور فناوری‌های محاسباتی ابر رایانه‌ها^۲ مانند IBM، Microsoft و Accenture تحت تسلط بوده است. به گزارش شرکت تحقیقات بازار وینترگرین^۳ از بازار ۷۰۶ میلیون دلاری در سال ۲۰۱۷ حدود ۳۲٪ سهم بازار IBM، ۱۹٪ سهم بازار مایکروسافت و سهم بازار Accenture حدود ۱۷٪ بوده است. برای مثال، در بین کاربران بزرگ ظرفیت محاسبات ابری IBM برای ۶۰ مرکز داده، تقاضا برای فناوری زنجیره بلوک آن هم با هدف استفاده در مدیریت زنجیره تأمین خود در صدر درخواست‌ها بوده است. مثالی دیگر، فروشگاه زنجیره‌ای Wal-Mart و شرکت شبکه پرداخت کار بانکی Visa فناوری زنجیره بلوک را به منظور ساده‌سازی زنجیره تأمین، سرعت بخشیدن به پرداخت و ذخیره سوابق تراکنش‌ها بکارگیری خواهند کرد. پیش‌بینی‌ها حاکی از این است که تا ۵ سال آینده ۵۵٪ شرکت‌های بزرگ (بیش از ۱۰،۰۰۰ نفر کارمند) به فضاهایی ابری با خدمات بلاکچین نیازمند خواهند بود (WinterGreen, 2018). بر اساس آمار شرکت وینترگرین در سال ۲۰۱۷ سرمایه‌گذاری‌های خصوصی در شرکت‌های زنجیره بلوک به ۴،۵ میلیارد دلار رسیده است که از مدت مشابه خود در سال ۲۰۱۶ این عدد ۸ برابر شده، و حدود ۱۵،۲ میلیون نفر از جمعیت سرتاسر جهان جزو کاربران این فناوری محسوب می‌شوند (WinterGreen, 2018). با توجه به نمودار (۶) می‌توان روند پیش‌بینی بخش‌های بازار را مشاهده نمود در سال ۲۰۱۷ اندازه بخش بازار برای خدمات مالی، بانکی و بیمه ۳۸۱،۲ میلیون دلار، برای خدمات بهداشت و درمان ۱۴،۱ میلیون دلار، برای مباحث حقوقی ۲۵۵،۶ میلیون دلار، برای مدیریت زنجیره تأمین ۴۸ میلیون دلار و برای اینترنت اشیا ۷،۱ میلیون دلار بوده است (WinterGreen, 2018).

¹ Real -Time settlement

² Mainframe

³ WinterGreen Research, Inc.



نمودار ۶. روند پیش‌بینی بخش‌های بازار فناوری زنجیره بلوک (WinterGreen, 2018)

تحلیل‌های منتج از سرمایه‌گذاری و پیش‌بینی جذابیت این بخش‌ها، وضعیت بازار رو به پیشرفت را نشان می‌دهد. برای مثال، بیشترین جهش مربوط به حوزه خدمات مالی، بانکی و بیمه‌ای است، و پیش‌بینی می‌شود تا سال ۲۰۲۴ اندازه این بازار به ۳۹,۳ میلیارد دلار برسد. بر اساس تئوری انتشار نوآوری ارائه شده توسط Accenture فناوری بلاکچین در سال ۲۰۱۶ در مرحله‌ی ابتدای چرخه عمر فناوری قرار داشته و ظرفیت بکارگیری آن توسط موسسات مالی به ۱۳,۵٪ بوده است (Accenture, 2016). محرک این رشد بالا در آن سال‌ها عامل همگام‌سازی^۱ دفاتر داخلی موسسات مالی و اعتباری با یکدیگر بوده است، که معمولاً این عملیات طولانی و با افزایش سرمایه درگیری ریسک آن نیز افزایش پیدا خواهد کرد. فناوری زنجیره بلوک به بانک‌ها این امکان را می‌دهد تا راحت‌تر و بدون مرز با یکدیگر تجارت نمایند، با ایجاد اعتماد بانک مرکزی کشورها نیز این تجارت منعطف‌تر و قابل کنترل‌تر خواهد شد. این عامل برای کشورها با عنوان فرآیند نوسازی و اجرای اقتصاد دیجیتال ایجاد خواهد شد. Santander اولین بانک بریتانیاست که از فناوری زنجیره بلوک برای انتقال مستقیم پرداخت‌های بین‌المللی خود استفاده کرده است، با بهره‌گیری از این سیستم به صورت شبانه روزی می‌توان مبلغی بین ۱۰ تا ۱۰ هزار پوند را پرداخت نمود، و وجه به صورت بلادرنگ در حساب

¹ synchronizing

مقصد دریافت خواهد شد. اخیراً نیز شرکت American Express و Santander با همکاری شرکت Ripple سیستم‌های پرداخت برون‌مرزی خود بین آمریکا و انگلستان را بر پایه فناوری زنجیره بلوک ایجاد نموده‌اند. اولویت دوم، مربوط به حوزه مدیریت زنجیره تأمین است، این بخش در سال ۲۰۱۷ بازاری حدود ۴۸ میلیون دلار داشته و پیش‌بینی می‌شود تا سال ۲۰۲۴ به بازار حدود ۲,۵ میلیارد دلار برسد. فناوری زنجیره بلوک به دلیل مزیت‌هایش در رهگیری کالا و صدور گواهی و یا صورتحساب بین تولیدکننده، حمل‌کننده و خریدار برای حوزه زنجیره تأمین که نگرانی امنیت و دستکاری را دارند، بسیار جذاب خواهد بود. از این رو، شرکت IBM به عنوان یک شرکت ارائه‌دهنده فناوری با هفت بانک بزرگ اروپایی برای ساخت و میزبانی زنجیره تجاری-مالی دیجیتال بر بستر زنجیره بلوک توافق نموده است، این بستر با هدف ساده‌سازی و تسهیل تجارت داخلی و برون‌مرزی برای شرکت‌های کوچک و متوسط طراحی شده است. از سوی دیگر این شرکت با ۱۰ تولیدکننده مواد غذایی از جمله Nestlé, Tyson Foods, Wal-Mart, Kroger و Unilever به منظور ایجاد سیستمی برای ردگیری محصول از مزرعه تا قفسه‌های فروشگاه به منظور کنترل و ایمنی مواد غذایی طراحی را شروع نموده است (IBM, 2018). اولویت سوم، مربوط به مباحث حقوقی است، این بخش در سال ۲۰۱۷ بازاری حدود ۲۵۵,۶ میلیون دلار داشته و پیش‌بینی می‌شود تا سال ۲۰۲۴ به میزان بازار حدود ۹,۷ میلیارد دلار ایجاد گردد. به صورت کلی موسسات حقوقی بخشی از بازار فناوری زنجیره بلوک در حوزه ارزشهای مجازی هستند، و با توجه به قابلیت خودمختاری و خطاناپذیری قراردادهای هوشمند به عنوان جایگزین‌های خوبی برای قراردادهای سنتی تلقی می‌شوند. در سال ۲۰۱۷ حدود ۱۰ شرکت حقوقی و ۴ موسسه حقوقی به اتحاد شرکتی اتریوم^۱ (EEA) پیوستند، اگرچه که قراردادهای هوشمند در حوزه مباحث قراردادهای سنتی توجهات را به خود جلب کرده است ولی با ترکیب توسعه‌دهندگان قرارداد هوشمند و وکلا و همکاری آنان می‌توان راهکارهای متری‌تری را برای این صنعت پیش‌بینی نمود (WinterGreen, 2018). اولویت چهارم، مربوط به خدمات بهداشت و درمان است، که در سال ۲۰۱۷ بازار حدود ۱۴ میلیون دلار داشته و پیش‌بینی‌ها حاکی از افزایش آن به ۳,۱ میلیارد دلار تا سال ۲۰۲۴ است. در حقیقت فناوری زنجیره بلوک پتانسیل تغییر اکوسیستم خدمات درمانی را دارد و این تغییر از طریق قرارداد بیماران بر محور برنامه‌های توسعه با افزایش امنیت، حفظ حریم خصوصی و قابلیت اشتراک‌گذاری داده‌ها در کل اکوسیستم بهداشت و درمان قابل اجرا خواهد بود. این فناوری می‌تواند با ایجاد سوابق پزشکی الکترونیک کارآمد، متمایز و ایمن الگویی جدید را برای تبادل اطلاعات سلامت ارائه دهد. برای مثال، یکی از زیرساخت‌های اجرا شده توسط مایکروسافت سامانه‌ی آژور^۲ است، این سامانه خدمات زنجیره بلوک را بر بستر فضای

¹ Ethereum Enterprise Alliance

² AZURE

ابری ارائه می‌دهد. یکی از کاربردهای ارائه شده در این زیرساخت استارت‌آپ اسپریچس^۱ است، در حقیقت این راهکار به منظور ردگیری و کنترل وسایل پزشکی در کل چرخه‌ی عمرش از تولید تا اسقاط ایجاد شده است. این راهکار موجب شده تا روند تعمیر و نگهداری این وسایل بهبود یافته و منتج به افزایش ایمنی بیمار، کاهش هزینه‌ها و بهبود کیفیت درمان شود (Houlding, 2019). اولویت پنجم، مربوط به فناوری اینترنت اشیا (IoT) است، این حوزه کاربرد در سال ۲۰۱۷ بازاری حدود ۷,۱ میلیون دلار داشته و پیش‌بینی می‌شود تا سال ۲۰۲۰ این بازار به حجمی حدود ۵,۸ میلیارد دلار دست یابد. از کاربردهای کلیدی فناوری زنجیره بلوک در اینترنت اشیا می‌توان به امنیت داده و تاب‌آوری سیستم^۲ اشاره نمود. نمونه کاربردی ایجاد شده این فناوری برای این حوزه می‌توان به آیوتا^۳ اشاره نمود، که یک حلقه تراکنشی برای تسویه و انتقال داده برای اینترنت اشیا است، در حقیقت این کاربرد به منظور دستیابی به اجماع در یک شبکه‌ی فرد به فرد توزیع شده^۴ ایجاد شده است. مزیت این زنجیره بلوک مقیاس پذیری بالا، معامله بدون هزینه و معامله آفلاین است (WinterGreen, 2018). بر این اساس، حوزه‌های اولویت‌دار توسعه فناوری زنجیره بلوک شامل (۱) خدمات مالی، بانکی و بیمه‌ای، (۲) مدیریت زنجیره تأمین، (۳) مباحث حقوقی (قراردادهای هوشمند)، (۴) خدمات بهداشت و درمان و (۵) حوزه اینترنت اشیا است.

۴-۲- تحلیل تکنیکال روند فناوری زنجیره بلوک

۴-۲-۱- تحلیل انتشارات علمی

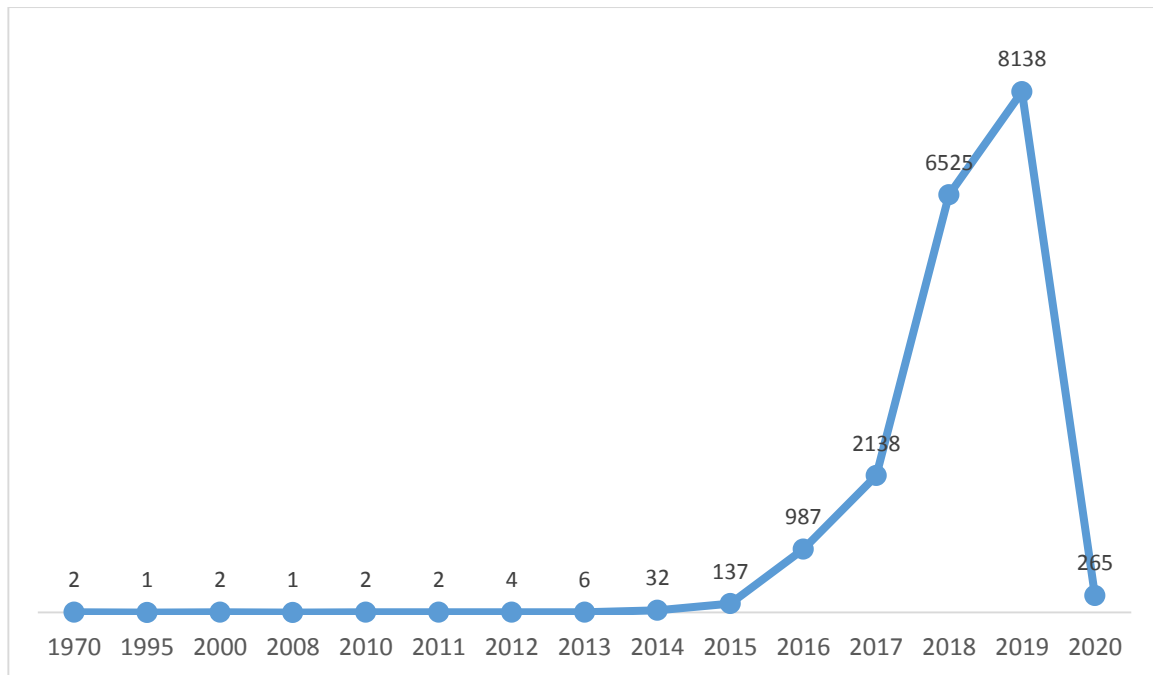
بر اساس اطلاعات مستخرج از پایگاه تحلیلی Lens تعداد انتشارات علمی تا اوایل سال ۲۰۲۰ حدود ۱۷,۴۴۲ عدد بوده است. ۱۴٪ از این انتشارات متعلق به کتاب‌هاست و ۵۵٪ آن مربوط به مقالات علمی بوده است. با توجه به نمودار (۸) نشان‌دهنده روند انتشارات علمی بین سال‌های ۱۹۷۰ تا کنون است، همانطور که نمایان است بیشترین جهش در تولید انتشارات علمی مربوط به سال‌های بعد از ۲۰۱۷ بوده است. یکی از مطالب تأثیرگذار در آن سال، یادداشت هاروارد بیزینس رویو با عنوان "حقایق زنجیره بلوک" بوده است (HBR, 2017).

¹ Spiritus

² Data Assurance and Resilience

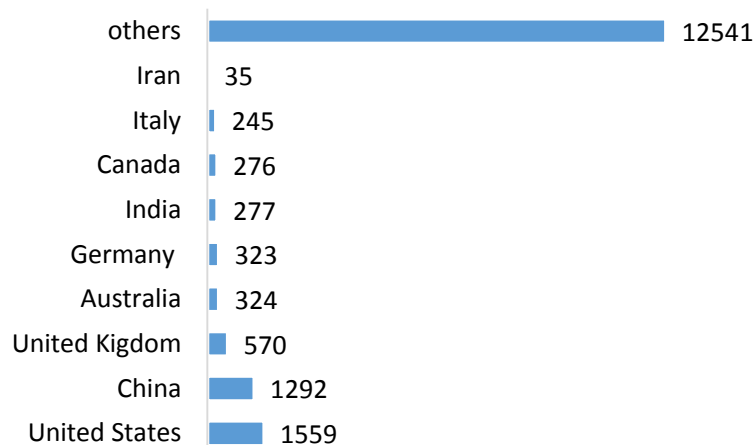
³ IOTA

⁴ Decentralized peer-to-peer



نمودار ۸. روند انتشارات علمی بین سال ۱۹۷۰ تا ۲۰۲۰

بر اساس متن کاوی انجام شده از متون علمی منتشر شده در بازه زمانی ۲۰۱۶ تا کنون حوزه‌های مهم و پرکاربرد در پژوهش عبارتند از امنیت شبکه، رمزارزها، مدیریت تراکنش در پایگاه داده، محاسبات توزیع شده^۱ و مقیاس‌پذیری^۲. بر اساس بخش‌بندی فناوری اولویت حوزه‌های پژوهش بر بخش‌های الگوریتم‌های رمزنگاری (مباحث امنیتی) و اجماع (مقیاس‌پذیری و زمان‌بر بودن)، بخش سخت‌افزاری (مقیاس‌پذیری گره‌ها) و بخش پلتفرم‌های تجاری (رمزارزها) است.



نمودار ۹. توزیع جغرافیایی انتشارات علمی ۱۹۷۰ تا ۲۰۲۰

¹ Distributed computing

² Scalability

بر اساس نمودار (۹) بیشترین تعداد انتشارات علمی متعلق به آمریکا (۰.۹٪)، چین (۰.۷٪) و انگلستان (۰.۳٪) است، و ایران نیز در این رابطه ۱۳ سند علمی منتشر کرده است. بر اساس تحلیل متن کاوی انتشارات شرکت IBM تمرکز فعالیت‌های پژوهشی این شرکت بر مباحثی چون زنجیره بلوک مجاز مانند فابریک لجر، پروتکل‌های ارتباطی بین زنجیره بلوک‌های متفاوت و درگاه‌های داده دنیای واقعی برای زنجیره بلوک (اوراکل‌ها)^۱، مباحث مقیاس‌پذیری زنجیره بلوک، تحمل خطای بیزانس در برنامه‌های اینترنتی (MAFTIA^۲)، ذخیره‌سازی و اشتراک‌گذاری امن داده‌ها می‌باشد. دومین موسسه با بیشترین انتشارات آکادمی علوم چین^۳ است. پژوهش‌های این موسسه عمدتاً توسط NSFC^۴ تأمین مالی شده است، و تمرکز پژوهش در این آکادمی بر حوزه‌های کاربرد این فناوری در حمل و نقل هوشمند، هوشمندسازی بر پایه داده‌ها^۵ و امنیت ملی، ایجاد سیستم زنجیره بلوک موازی سیستم بهداشت درمان، کاربرد زنجیره بلوک در شبکه‌های اجتماعی، رمزارزها، ایجاد اعتبار بر پایه زنجیره بلوک، قراردادهای هوشمند در مدیریت رفتار اجتماعی (SBM)^۶ و مباحث استخراج بیت‌کوین اهم از استخراج به روش پرداخت PPLNS^۷ بوده است. برای ایران عمده پژوهش‌های انجام شده در دانشگاه‌های پلی‌تکنیک امیرکبیر، دانشگاه آزاد اسلامی و دانشگاه تهران بوده و مباحث بیشتر حول محور موضوعات ترکیبی بین زنجیره بلوک و اینترنت اشیا و هوش مصنوعی است. حوزه‌های کاربرد مورد مطالعه این فناوری در بازاریابی، بهداشت و درمان، بیمه و زنجیره تأمین مورد توجه بوده است.

۲-۲-۴- تحلیل گواهی ثبت اختراع

براساس پایگاه تحلیلی Patent inspiration در رابطه با موضوع زنجیره بلوک در پایگاه‌های داده ثبت اختراع در سطح دنیا ۵،۱۲۰ گواهی منتشر شده است.

¹ Oracles

² Malicious and Accidental Fault Tolerance for Internet Applications

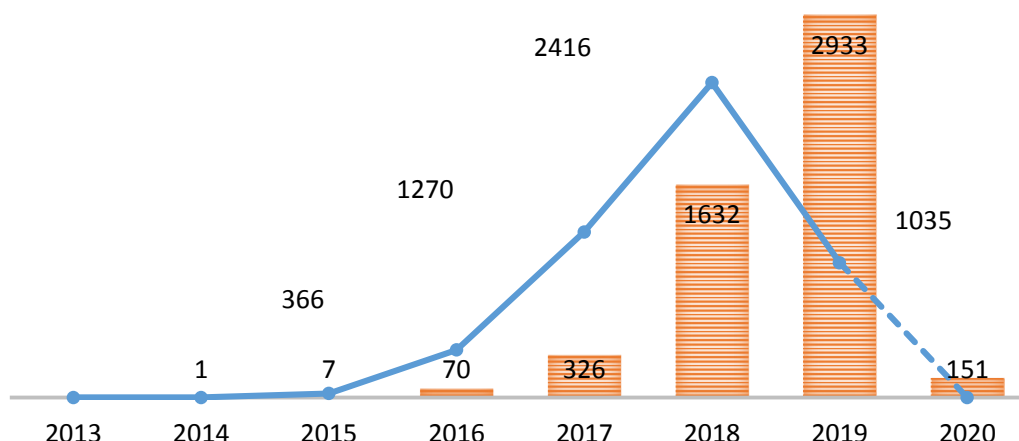
³ Chinese academy of science

⁴ Natural Science Foundation of China

⁵ Data-driven intelligence

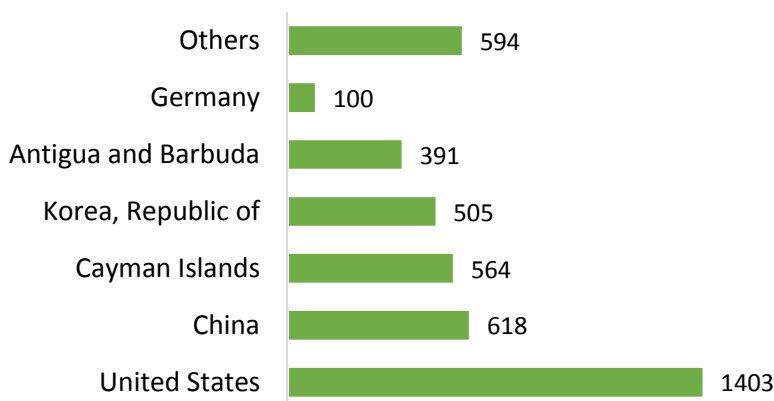
⁶ Social behavior management

^۷ استخراج (Mining pool) به منظور اشتراک‌گذاری توان پردازشی ماینرها ایجاد شده تا بتوانند بر اساس آن بلوک‌های بیت‌کوین را در زنجیره بلوک ایجاد نمایند. روش PPLNS یکی از روش‌های پرداخت به ماینرهای شریک در استخراج است که بر اساس یک میزان ثابت به آن‌ها سهم پرداخت خواهد شد.



نمودار ۱۰. روند درخواست ثبت اختراع از سال ۲۰۱۴ تا ۲۰۲۰

در نمودار (۱۱) خط آبی نشان‌دهنده روند درخواست‌ها و ستون‌ها نشان‌دهنده تعداد انتشار است. بیشترین شیب افزایش درخواست برای ثبت اختراع از سال ۲۰۱۶ شروع گردیده است، بین سال ۲۰۱۶ تا ۲۰۱۹ اختراعات منتشر شده حدوداً ۴۲ برابر شده است.



نمودار ۱۱. تحلیل جغرافیایی ثبت درخواست گواهی ثبت اختراع

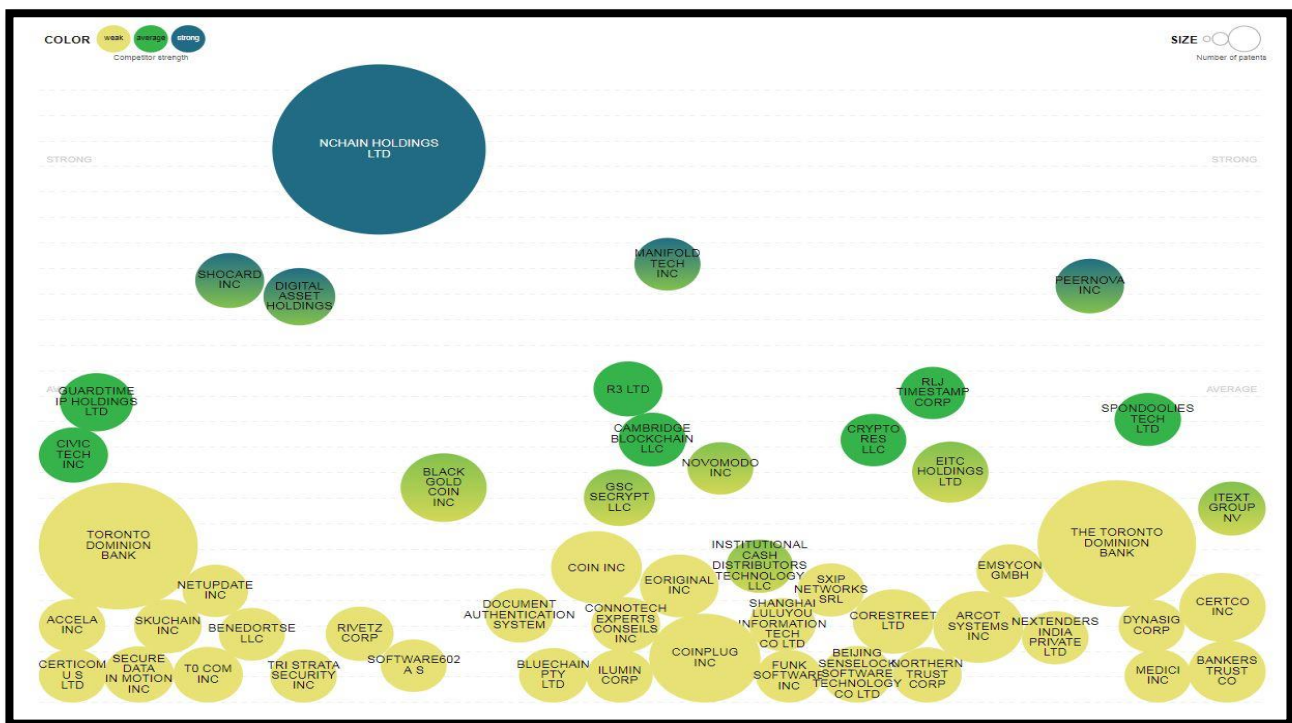
با توجه به نمودار (۱۱) بیش‌ترین ثبت اختراع برای کشورهای آمریکا (۳۴٪) و چین (۱۵٪) هستند. با بررسی اختراعات ثبت شده برای این دو کشور می‌توان اینگونه بیان نمود که فعالان بخش خصوصی (شرکت‌های بزرگ مانند Bank of America, Visa, MasterCard, IBM, ...) در آمریکا بیشتر به دنبال ثبت اختراع بوده‌اند ولی در کشور

چین عمده درخواست‌های ثبت اختراع توسط دانشگاه‌های این کشور بوده است. برخی از دانشگاه‌های فعال در این کشور با حوزه‌های تمرکزشان به شرح زیر هستند:

- دانشگاه پکینگ (مدرسه عالی شنزن)^۱ - کاربرد زنجیره بلوک در مدیریت دامین وب^۲
- دانشگاه فناوری گاندونگ^۳ - کاربردهای زنجیره بلوک در صنعت ساخت و تولید
- دانشگاه ژئی‌یانگ^۴ - فضای ابر بر پایه زنجیره بلوک^۵ و پرداخت‌های برون مرزی با رمزارزها

نکته جالب دیگر در ثبت اختراعات وجود دو کشور جزیر کایمن و کشور آنتیگوآ و باربودا می‌باشد، با نام این دو کشور جمعاً ۹۵۵ گواهی اختراع صادر شده است. این حجم ثبت اختراعات به نظر به دلیل سهولت فعالیت شرکت‌های فعال در حوزه زنجیره بلوک و رمزارزها در این مناطق می‌باشد.

شکل (۱۲) نشان دهنده رقابت شرکت‌ها در انتشار گواهی حق اختراع است، این شکل بر اساس تعداد و ارجاعات در گواهی‌ها رقابت را بین شرکت‌های فعال نشان می‌دهد.



شکل ۱۲. تحلیل بازیگران کلیدی ثبت گواهی اختراع

¹ Peking University (Shenzhen Graduate School)

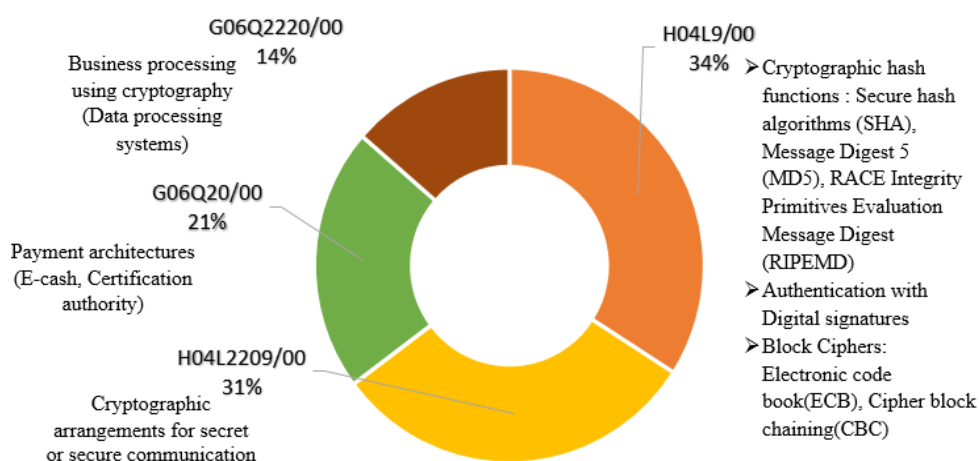
² Web Domain Management

³ University Guangdong technology

⁴ Zhejiang University

⁵ Cloud-based Blockchain

با توجه به آمار شرکت‌های درخواست‌کننده‌ی ثبت اختراع، فعال‌ترین و پر ارجاع‌ترین ثبت اختراع متعلق به شرکت هلدینگ Nchain است، مرکز اصلی این شرکت در لندن است و عمده فعالیت این شرکت تحقیق و توسعه روی پلتفرم زنجیره بلوک عمومی مانند بیت‌کوین با تمرکز بر مباحث تراکنش پرداخت و مباحث رمزنگاری و امنیت بوده است. پرتعدادترین شرکت دارای اختراع هلدینگ گروه Alibaba است، این شرکت دارای ۵۳۹ گواهی ثبت اختراع است، و بیشترین موضوعات مورد توجه این شرکت عبارتند از الگوریتم‌های اجماع، تبادل داده بین زنجیره بلوک‌های مختلف، افزایش سرعت تراکنش‌ها در زنجیره بلوک، ذخیره‌سازی، پردازش، حفاظت از داده‌ها در زنجیره بلوک (روش رمزنگاری هم‌ریختی^۱)، کاربردهای قرارداد هوشمند(رای گیری)، روش‌های احراز هویت در زنجیره بلوک، تراکنش محرمانه در زنجیره بلوک (مانند روش رمزنگاری اثبات دانایی صفر^۲) و محاسبات ابری بر بستر زنجیره بلوک (به روش FaaS^۳). نمودار (۱۳) نشان دهنده دسته‌بندی CPC برای کل اختراعات ثبت شده است، این دسته‌بندی نشان‌دهنده حوزه‌های مهم و پرتکرار در گواهی ثبت اختراعات است و به صورت نیابتی می‌توان از آن به عنوان حوزه‌های داغ فناوری یاد نمود:



نمودار ۱۳. دسته‌بندی CPC گواهی ثبت اختراع

دسته اول، که ۳۸٪ گواهی ثبت اختراعات را شامل می‌شود، مربوط به مکانیزم‌های رمزنگاری برای تولید هش، تأیید اعتبار با استفاده از امضاء دیجیتال و رمزگذاری قطعه‌ای^۴ می‌باشد. دسته دوم، با سهمی به میزان ۳۱٪ از گواهی ثبت اختراعات در رابطه به کاربردهای رمزنگاری در ایجاد ارتباطات ایمن و محرمانه است. دسته سوم، با داشتن ۲۱٪ از

¹ Homomorphic encryption

² Zero-knowledge proof

³ Function as a service

⁴ Block cipher

گواهی ثبت اختراعات، مربوط به کاربردهای طراحی فرآیندهای پرداخت بر اساس پورتکل‌های پول الکترونیکی (E-cash) و مرجع صدور گواهی (CA) ۱ می‌باشد. دسته چهارم، با ۱۴٪ از گواهی ثبت اختراعات شامل کاربرد رمزنگاری در فرآیند پردازش داده‌های سازمانی و مالی می‌باشد. با توجه به دسته‌بندی حاصل از تحلیل اختراعات بخش‌های فناوری مهم رامی‌توان به الگوریتم‌های رمزنگاری و کاربرد فناوری زنجیره بلوک در مباحث مالی (پرداخت) جمع‌بندی نمود.

۴-۳- تحلیل سیاست‌های توسعه فناوری زنجیره بلوک

۴-۳-۱- سیاست‌های توسعه فناوری زنجیره بلوک کشورها

به طور کلی سیاست‌های توسعه فناوری و کاربرد فناوری زنجیره بلوک در کشورها توسط بخش خصوصی و یا دانشگاه‌ها دنبال می‌شود. اتحادیه اروپا در رابطه با این فناوری گزارشی را تحت عنوان "بلاکچین برای دولت دیجیتال: ارزیابی عملکردهای پیشگام در خدمات عمومی" منتشر کرده است و در آن ضمن بررسی حوزه‌های کاربرد بالقوه این فناوری در حوزه‌های کاهش بروکراسی، افزایش راندمان اداری و افزایش اعتماد عمومی عنوان شده است و بیان شده که هنوز این فناوری جنبه‌ی مختل‌کننده و تحول‌آفرینی را برای دولت‌ها نداشته و پیشنهاد نموده تا کشورهای سیاستگذار در این حوزه تلاش خود را جهت برطرف‌سازی موانع غیر فناورانه مانند ناسازگاری بین راهکارهای مبتنی بر زنجیره بلوک، ایجاد چارچوب قانونی برای فعالیت کسب و کارهای مربوطه انجام دهند (Fintechnews, 2019). بانک خلق چین^۲ (PBoC) به منظور نظارت و کنترل کسب و کارهای مرتبط با بلاکچین گواهینامه‌ی محصول فین‌تک (CFP۳) را برای ۱۱ حوزه صادر می‌نماید، این حوزه‌ها و گواهینامه‌های مرتبط با پرداخت‌های دیجیتال هر سه سال یکبار مورد بازبینی قرار خواهد گرفت. فرآیند اعطای گواهینامه شامل بررسی محل فیزیکی، بازرسی کدهای فنی، الگوریتم‌ها، عملکرد شبکه بلاکچین^۴ و غیر خواهد بود. برای گواهینامه‌های صادر شده برنامه‌های بازدید تصادفی برای کنترل و پیگیری بیشتر در نظر گرفته شده است. یکی از فعالیت‌های که موجب تسهیل سرمایه‌گذاری در این حوزه گردیده است، معرفی RMB^۵ است (Fintechnews, 2019). از طرفی دیگر، کشور استرالیا برنامه خود را در گزارشی تحت عنوان "نقشه‌راه برای استاندارد زنجیره بلوک" منتشر کرده است، در این گزارش ابعاد فنی برای توسعه، مدیریت و

¹ Certificate authority

² People's Bank of China

³ Certification of Fintech Product

⁴ On-chain performance

⁵ Chinese renminbi digital currency

کاربری زنجیره بلوک مورد بررسی قرار گرفته است و راهبرد اساسی در این نقشه راه اولویت‌بندی فعالیت‌های مرتبط برای توسعه استانداردهای زنجیره بلوک «ISO/TC 307» عنوان شده است. توسعه استانداردهای مذکور در حوزه‌های حمایت از حریم خصوصی، امنیت، احراز هویت، قراردادهای هوشمند، حاکمیت زنجیره بلوک و سایر موضوعات با همکاری ذی‌نفعان صنعت، مصرف‌کنندگان و دانشگاه‌هایان در دست خواهد بود (Meguerditchian, 2018). کشور ترکیه به دلیل نیازهای ایجاد شده در فناوری زنجیره بلوک و توسعه تخصص‌های مورد نیاز برنامه‌ی را تحت عنوان ایجاد مرکز دانشگاهی زنجیره بلوک (تحت عنوان BlockchainIST^۱) در شهر استانبول در دانشگاه باغچه‌شهر^۲ (BAU) را در دستور کار قرار داده است، به طور کلی در ۶ دانشگاه دوره زنجیره بلوک در حال ارائه می‌باشد، دانشگاه نیکوزیا قبرس، دانشگاه پرینستون آمریکا، دانشگاه یونیورسیداد اروپای مادرید، دانشگاه دوک آمریکا، دانشگاه کالیفورنیا، برکلی، آمریکا و دانشگاه ترکیه [19]. کشور امارات متحده عربی نیز به منظور کاربرد این فناوری سندی را تحت عنوان "استراتژی زنجیره بلوک امارات متحده عربی برای افق ۲۰۲۱" منتشر نموده است، در این سند آمده است دولت امیدوار است که هر سال ۳ میلیارد دلار و ۷۷ میلیون ساعت کار صرفه‌جویی کند. مسئول پیگیری این راهبردها سازمان دولتی با عنوان دفتر دبی هوشمند^۳ (SDO) خواهد بود. یکی از مهم‌ترین فعالیت‌های صورت گرفته همکاری دو اپراتور تلکام برای ایجاد بستر بلاکچین است، این بستر قرار است به عنوان یک زیرساخت "پلتفرم به عنوان خدمات"^۴ (BPaaS) ارائه دهند. این پلتفرم معماری خود را به صورت هاستینگ ابر پایه با زنجیره بلوک خصوصی بر روی اتریوم و هایپرلجر فبریک^۵ ایجاد خواهد کرد. این دفتر برای اجراسازی آن راهبرد حوزه‌های عملکردی را به صورت سه بخش اصلی زیر در حال پیگیری دارد (UAE Government, 2018):

- ✓ بخش دولتی: بارگیری فناوری زنجیره بلوک در خدمات دولتی به منظور افزایش کارایی ارائه خدمات؛
- ✓ بخش ایجاد صنعت: حمایت و توانمندسازی شرکت‌ها و استارت‌آپ‌ها؛
- ✓ بخش رهبری افکار: هدایت افکار عمومی دنیا در رابطه با فناوری زنجیره بلوک برای ایجاد برند دبی به عنوان هاب اشتراک دانشی دنیا.

¹ BAU Blockchain and Innovation Center of Istanbul: <https://www.blockchainist.org>

² Bahcesehir University

³ Smart Dubai Office

⁴ Blockchain-Platform-as-a-Service

⁵ Hyper ledger fabric

۲-۳-۴- برنامه‌ها و اقدامات نهادهای حاکمیتی در ایران

تاکنون سیاست‌های توسعه فناوری زنجیره بلوک در ایران به دلیل تعدد سازمان‌های رگولاتوری با سردرگمی‌های روبه‌رو بوده است. این سردرگمی را در حوزه صنعت ماینینگ و دستوالعمل ارائه شده توسط بانک مرکزی می‌توان به وضوح مشاهده نمود. تاکنون ۲۰ استارت‌آپ در این حوزه در کشور ایجاد شده، که تقریباً ۱۴ درصد از استارت‌آپ‌های حوزه فناوری‌های مالی (فین‌تک) کشور را شامل می‌شوند. عمده این کسب و کارها در حوزه رمز ارز ۱ و استخراج بیت‌کوین فعال هستند و باید به این نکته توجه نمود که فرصت‌های در حال ظهور این فناوری در سایر کاربردهای آن قرار دارد. از فعالیت‌های امیدوارکننده در کشور می‌توان به ایجاد کنسرسیومی از بانک‌های ملی، ملت، پاسارگاد و پارسیان اشاره نمود، این کنسرسیوم به میزبانی بانک‌های مذکور به دنبال ایجاد توکن با پشتوانه طلا و املاک و اموال مازاد بانک‌ها، سازمان‌ها و سایر کاربردهای مبتنی بر زنجیره بلوک خواهد بود. از سوی دیگر، راه‌اندازی زیست بوم نوآوری باز بلاکچین توسط انجمن بلاکچین ایران با حمایت مرکز همکاری‌های تحول و پیشرفت ریاست جمهوری از جمله تلاش‌های کشور در جهت کاربردسازی برای این فناوری نوظهور بوده است. از زیرساخت‌های فنی راه‌اندازی شده در کشور می‌توان به آزمایشگاه بلاکچین دانشگاه صنعتی شریف^۱، آزمایشگاه بلاکچین دانشگاه خاتم^۲، آزمایشگاه بلاکچین دانشگاه امیرکبیر و آزمایشگاه بلاکچین پژوهشگاه فناوری اطلاعات اشاره نمود، عمده فعالیت‌های این آزمایشگاه به دلیل نوظهور بودن فناوری و شکل نگرفتن بازار متناسب و همچنین حمایت‌های اندک دولت متمرکز بر فعالیت‌های آموزشی و تربیت نیروی انسانی، فعالیت‌های پژوهشی و حمایت از پایان‌نامه‌های دانشگاهی، اجرای محدود آزمایشی برخی از پلتفرم‌های زنجیره بلوک و راه‌اندازی تعداد محدودی استارت‌آپ بوده است. ایجاد کمیته‌ی متناظر ISO/TC 307 در سازمان تنظیم مقررات و ارتباطات رادیویی وزارت ارتباطات و فناوری اطلاعات از جمله تلاش‌های کشور در اثرگذاری در سطح تدوین استانداردهای بین‌المللی است.

۵- نتیجه‌گیری و ارائه پیشنهاد‌های سیاستی

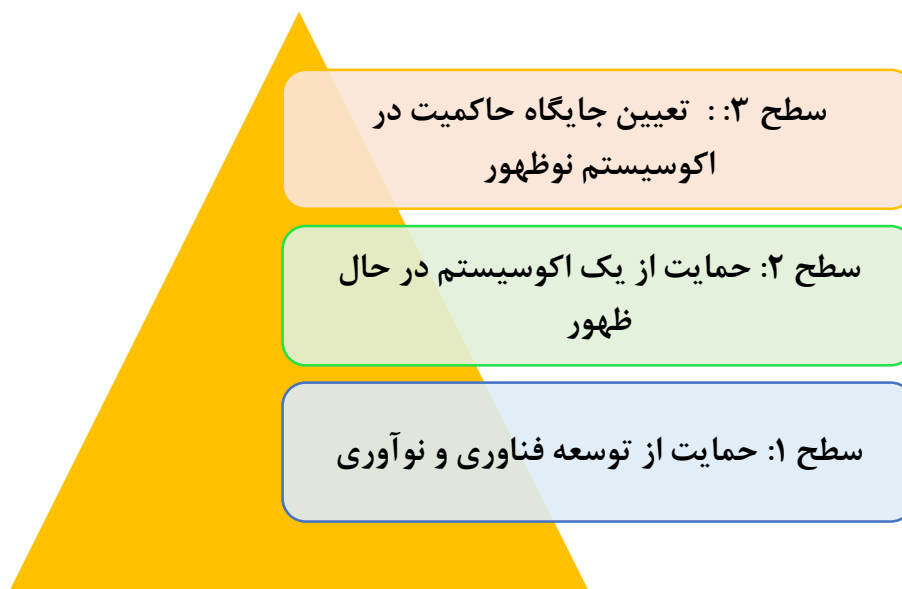
روند توسعه‌ی کاربردهای فناوری زنجیره بلوک با توجه به سرعت گسترش و تأثیرگذاری آن غیر قابل چشم‌پوشی است، و به رسمیت شناختن و استفاده از ظرفیت آن برای کشور فرصت‌های زیادی را ایجاد می‌نماید. آمارها و بررسی‌ها در این حوزه نشان داده که کشور از توانمندی فنی قابل قبولی برخوردار بوده و از سایر کشورها عقب‌نمانده است ولی در

¹ Cryptocurrency

² <https://decentralab.ir>

³ <http://blockchain.khatam.ac.ir>

حوزه توسعه اکوسیستم و سطح حاکمیت نیاز به توجه بیشتری خواهد بود. با توجه به مطالب بررسی شده در رابطه با روندهای فناوری زنجیره بلوک، برنامه سایر کشورها و همچنین تلاش‌های انجام گرفته در کشور می‌توان چارچوب پیشنهادی برای سند راهبردی را در سه سطح زیر ارائه نمود:



نمودار ۱۴. چارچوب پیشنهادی برای تنظیم سند راهبردی فناوری زنجیره بلوک

سطح ۱: حمایت از توسعه فناوری و نوآوری:

- جهت‌دهی سرمایه‌گذاری تحقیقاتی-کاربردی به منظور استفاده از توان آزمایشگاه‌های تخصصی ایجاد شده در کشور و با تمرکز بر حوزه‌های کلیدی مانند مقیاس‌پذیری، انواع روش‌های رمزنگاری و امنیت سایبری (توسعه الگوریتم)، افزایش سرعت تراکنش و عملیات (جلوگیری از تأخیر) و افزایش کارایی مصرف انرژی سیستم‌های مبتنی بر دفاتر توزیع شده با سرمایه‌گذاری بخش خصوصی و دولتی با مدل مشارکت حداقلی دولت مانند مدل کاتاپولت^۱ انگلستان؛
- ایجاد مراکز تخصصی دانشگاهی، و رشته‌های تخصصی در حوزه زنجیره بلوک با هدف تربیت نیروی انسانی متخصص و همچنین استفاده از فرصت جذب دانشجو در منطقه.

^۱ مدل Catapults: عبارتی از زیرساخت‌های فیزیکی که با همکاری دولت، صنعت و دانشگاه ایجاد و بهره‌برداری می‌گردد. بودجه این مدل به صورت $\frac{1}{3}$ توسط بودجه مصوب دولت، $\frac{1}{3}$ توسط بخش خصوصی و $\frac{1}{3}$ توسط متقاضی (دولت/عمومی/خصوصی) تأمین خواهد شد.

سطح ۲: حمایت از یک اکوسیستم در حال ظهور:

- حمایت از پژوهش‌های دانشگاهی به منظور بهبود عملکردهای تشخیص هویت مشتریان، مقابله با پولشویی، حل مشکل امنیت، حریم خصوصی، جلوگیری از جرائم و توسعه استانداردهای مرتبط این موارد به عنوان موانع غیر فنی برای توسعه فناوری زنجیره بلوک در حوزه کاربردهای خدمات مالی در کشور؛
- تدوین و انتشار دستورالعملی برای ثبت ماهیت حقوقی و همچنین ایجاد دسته‌بندی شرکت‌های فناور فعال در این حوزه به عنوان شرکت دانش‌بنیان با هدف استفاده از ظرفیت‌های حمایتی معاونت علمی و فناوری ریاست جمهوری؛
- توسعه کاربرد فناوری در کسب و کارها با مدل فضای آزمون نوآوری (Sandbox) در حوزه خدمات مالی و همچنین ایجاد زیرساخت‌های فنی مورد نیاز آن مانند امکان تأیید هویت مشتریان (KYC) برای مراکز مبادله ارزهای دیجیتال (صرافی‌های رمزارز) به صورت رسمی؛
- حمایت از راه‌اندازی دفاتر کل توسط دولت‌های محلی (استانی) و یا نهادهای حاکمیتی جهت آزمایش و کاربرد فناوری زنجیره بلوک برای مثال، توسعه کاربردهای کیف پول‌های چند امضایی^۱ (MCP) برای مشارکت بیشتر شهروندان و دولت به منظور دسترسی، کنترل و ارزیابی به داده‌های شهروندان و ایجاد ادبیات مشترک بین دولت و مردم.

سطح ۳: تعیین جایگاه حاکمیت در اکوسیستم نوظهور:

- تسریع در امر رگولاتوری و برنامه راهبردی، زیرا عدم ورود بهنگام و بهینه دولت در این حوزه می‌تواند منجر به از بین رفتن فرصت‌های پیش‌روی کشور گردد. پیشنهاد مشخص در اینجا می‌تواند ایجاد نهادی متمرکز ما بین دستگاه‌های دولتی برای توسعه فناوری مذکور و کاربردهایش باشد؛
- ایفای نقش دولت به عنوان یک مشتری هوشمند برای استفاده از کاربردهای زنجیره بلوک، برای مثال استفاده از توان نهادهای دولتی متولی حوزه فناوری اطلاعات و تجارت الکترونیک در وزارتخانه‌های تخصصی با هدف کاربردی‌سازی فناوری زنجیره بلوک برای نمونه در حوزه اولویت‌دار مدیریت زنجیره تأمین (رهگیری کالا)

¹ Multi party computing

نهادی مانند مرکز توسعه تجارت الکترونیک از وزارت صمت با برگزاری رویداد تقاضا محور می تواند چنین نقشی را ایفا نماید؛

- ایجاد بدنه‌ی تخصصی در قوه قضایه با دو هدف افزایش توان کارشناسی پرونده‌ها و صدور آرای قضایی مرتبط و همچنین کاربردی‌سازی فناوری زنجیره بلوک در مباحث حقوقی با استفاده از ظرفیت قراردادهای هوشمند.

1. B. H. A. K. a. N. G. Matthew Budman, "Delitte's 2019 global blockchain survey: blockchain gets down it business," Deloitte Insights contributors, 2019.
2. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, "Bitcoin and cryptocurrency technologies: a comprehensive introduction," in Bitcoin and cryptocurrency technologies: a comprehensive introduction, Princeton University Press. ISBN 978-0-691-17169-2, 2016 .
3. "Peck, Morgan (30 May 2012).” Bitcoin: The Crypto Anarchists’ Answer to Cash". IEEE Spectrum. Retrieved 8 January 2017".
4. Coinsutra, (2020). [Online]. Available: <https://coinsutra.com/bitcoin-double-spending/>
5. Patsnap, "An IP perspective on Blockchain: beyond the realm of cryptocurrencies," <https://www.patsnap.com>, 2019.
6. R. M. Visconti, "Blockchain Valuation: Internet of Value, digital networks and smart transactions," Università Cattolica Del Sacro Cuore, Milan, Italy, January 2019.
7. PWC, (2020). [Online]. Available: <https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/qa-what-is-blockchain.pdf>.
8. Gartner, [Online]. Available: "Hype Killer - Only 1% of Companies Are Using Blockchain, Gartner Reports | Artificial Lawyer". Artificial Lawyer. 4 May 2018. Retrieved 22 May 2018.
9. T. Locher and S. O. a. Y.-A. Pignolet, "When Can a Distributed Ledger Replace a Trusted Third Party?" in IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), June 2018 .
10. Coinmarketcap, (2020). [Online]. Available: <https://coinmarketcap.com>.
11. WinterGreen Research, "Blockchain Market Shares, Market Strategies, and Market Forecasts, 2018 to 2024," WinterGreen Research, Inc., Lexington, Massachusetts, 2018.
12. Accenture, [Online]. Available: "The future of blockchain in 8 charts". Raconteur. 27 June 2016. Archived from the original on 2 December 2016. Retrieved 3 December 2016.
13. IBM, [Online]. Available: Corkery, Michael; Popper, Nathaniel (24 September 2018). "From Farm to Blockchain: Walmart Tracks Its Lettuce". The New York Times. Retrieved 5 December 2018.
14. D. Houlding, "Microsoft Blockchain in Healthcare," Microsoft, 2019.
15. Harvard Business Review Home, "The Truth about Blockchain," Harvard Business Review Home, 2017.
16. D. Alessie and M. A. V. L. Sobolewski, "Block chain for digital government: An assessment of pioneering implementations in public services," European commisson, Joint Research Center science for policy report, 2019.
17. Fintechnews, Fintechnews, 5 November 2019. [Online]. Available: <https://www.fintechnews.org/china-adopts-certification-system-for-finetech-products/>
18. V. Meguerditchian, "ROADMAP FOR BLOCKCHAIN STANDARDS," Standards Australia, 2017.
19. Johnston, crypto coin spy, 5 August 2018. [Online]. Available: <https://cryptocoinspy.com/turkey-launches-first-blockchain-center-at-bahcesehir-university/>
20. UAE Government, "The Emirates Blockchain 2021 Initiative: Innovation in the UAE," UAE Government, April 2018. [Online]. Available: <https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021>.