
بسم الله
الرحمن
الرحيم

سیستم‌های فناوری دفترکل توزیع‌شده

یک چارچوب مفهومی

انتشارات راه‌پرداخت

عنوان :	سیستم‌های فناوری دفترکل توزیع‌شده (یک چارچوب مفهومی)
نویسندگان:	میشل راکس ... [و دیگران]
مترجمان:	ریحانه خیربخش، فاطمه عبداله.
مشخصات نشر :	تهران: راه پرداخت، ۱۴۰۰.
مشخصات ظاهری :	۲۰۸ ص.؛ ۱۴/۵ + ۲۱/۵ س‌م.
شابک:	۹۷۸-۶۲۲-۷۷۰۲-۰۰-۲
وضعیت فهرست نویسی :	فیپا
یادداشت : عنوان اصلی:	Distributed Ledger Technology Systems: A, ۲۰۱۸. Conceptual Framework
موضوع :	خدمات مالی -- نوآوری
موضوع :	Financial Services industry -- Technological innovations
موضوع :	بلاک‌چین (پایگاه‌های اطلاعاتی)
موضوع :	Blockchains (Databases)
شناسه افزوده :	راوچز، مایکل
شناسه افزوده :	Rauchs, Michel
شناسه افزوده :	عبداله، فاطمه، ۱۳۶۹ -، مترجم
شناسه افزوده :	خیربخش، ریحانه، ۱۳۶۰ -، مترجم
رده بندی کنگره:	HG۱۷۳
رده بندی دیویی :	۶/۳۳۲
شماره کتابشناسی ملی :	۷۶۱۶۲۳۳
وضعیت رکورد :	فیپا

سیستم‌های فناوری دفترکل توزیع‌شده

یک چارچوب مفهومی

نویسندگان:
میشل راکس
اندرو گلیدن
برایان گوردون
جینا پیترز

مترجمان:
ریحانه خیربخش
فاطمه عبداله

انتشارات راه‌پرداخت

عنوان:	سیستم‌های فناوری دفترکل توزیع‌شده (یک چارچوب مفهومی)
ناشر:	راه پرداخت
نویسندگان:	میشل راکس ... [و دیگران]
مترجمان:	ریحانه خیربخش، فاطمه عبداله.
ویراستار محتوایی:	اسماعیل حصاری
صفحه‌آرا:	فاطمه بذرافشان
ناظر چاپ:	قادر شهبازی
نوبت چاپ:	اول ۱۴۰۰
شمارگان:	۱۰۰۰ نسخه
شابک:	۹۷۸-۶۲۲-۷۷۰۲-۰۰-۲
تلفن:	۰۲۱-۴۴۴۳۹۶۶
دورنگار:	۸۹۷۸۴۹۰۲
ایمیل:	info@way2pay.press
وب‌سایت:	way2pay.shop
لیتوگرافی:	هنر اشکان
چاپ و صحافی:	واژه

فهرست

[یادداشت مترجمان]

این روزها صحبت از رمزارزها، بلاکچین و دنیای غیرمتمرکز به یکی از عناوین اصلی تحقیقاتی و کسب‌وکارها تبدیل شده است. «فناوری دفترکل توزیع‌شده» به‌عنوان فناوری زیربنایی ابزاری بین‌رشته‌ای به حساب می‌آید و در بسیاری از ساختارها و سیستم‌ها انقلاب ایجاد کرده است. با توسعه بیشتر این فناوری، منابع علمی متعددی در حال تولید است، ولی منابع مفید فارسی در این زمینه در حال حاضر محدود هستند.

کتاب پیش رو، ترجمه یکی از گزارش‌های «مرکز مالی جایگزین کمبریج»[1] است و با هدف کمک به طیف گسترده‌ای از مخاطبان شامل دانشجویان، مهندسان، طراحان سیستم‌های توزیع‌شده، سرمایه‌گذاران، قانون‌گذاران و کارآفرینان فارسی‌زبان منتشر شده است. «مرکز مالی جایگزین کمبریج» یک مؤسسه تحقیقاتی است که در سال ۲۰۱۵ به‌عنوان بخشی از دانشکده کسب‌وکار جاج کمبریج[2]، از بهترین دانشگاه‌های جهان در رشته کسب‌وکار، در کمبریج انگلستان تأسیس شده است. تحقیقات این مرکز بر حوزه کانال‌ها و ابزارهای مالیِ جایگزینی که خارج از اکوسیستم‌های مالی سنتی ظاهر می‌شوند و نیز فناوری‌های زیربنایی این ابزارها متمرکز است. از زمان تأسیس، فعالیت تحقیقاتی اصلی این مرکز انجام مطالعات تطبیقی در زمینه رشد «دانش

1 The Cambridge Centre for Alternative Finance (CCAF)
2 Cambridge Judge Business School

مالی جایگزین»[1] در مناطق و کشورهای مختلف جهان بوده که در قالب گزارش‌های سالیانه منتشر می‌شوند[2]. از دیگر زمینه‌های تحقیقاتی این مرکز سیستم‌های پرداخت جایگزین، مانند مطالعات در مورد بلاکچین، رمزارزها، دفاترکل توزیع‌شده، رمزدارایی‌ها و نیز پیامدهای ظهور شرکت‌های فین‌تک در حوزه قانون‌گذاری است. گزارش‌های این مرکز در بسیاری از مقالات سیاستی و رگولاتوری و توسط برخی سازمان‌های بین‌المللی و ارگان‌های دولتی، مانند بانک جهانی[3]، سازمان همکاری اقتصادی و توسعه[4] و سازمان بین‌المللی کمیسیون‌های اوراق بهادار[5] و پارلمان انگلستان، مورد ارجاع قرار گرفته‌اند.

از نظر مترجمان، نقطه قوت این کتاب معرفی عملیاتی پروژه‌های مختلف و تحلیل آنها بر اساس چارچوب مفهومی مطرح‌شده در کتاب است. نکته قابل توجه در این زمینه این است که اطلاعات ارائه‌شده در مورد این پروژه‌ها بر اساس واقعیت‌های موجود و منتشرشده در زمان نوشتن متن اصلی کتاب (سال ۲۰۱۸) است و این اطلاعات در ویرایش بعدی به‌روزرسانی خواهد شد. بنابراین، برای به دست آوردن اطلاعات به‌روز درباره این پروژه‌ها، لازم است خواننده خود اقدام به تحقیق کند. در این راستا، آخرین بخش کتاب، پی‌نوشت، می‌تواند نقطه شروع خوبی برای تحقیق خواننده باشد. در بخش مذکور، علاوه بر معرفی منابع استفاده‌شده در تهیه کتاب، در موارد زیادی نکات بسیار مفیدی در تکمیل مطالب متن اصلی کتاب ارائه شده و توصیه می‌شود در حین مطالعه کتاب به این منابع رجوع شود.

در کتاب حاضر، در انتخاب معادل‌های فارسی برای اصطلاحات تخصصی، علاوه بر مراجعه به متون فارسی موجود، دقت نظر بسیاری صورت گرفته و از نظر مترجمان در برخی موارد بهبودهایی در معادل‌های موجود صورت گرفته است. در مورد اصطلاحات تخصصی که معادل فارسی مناسبی برای آنها یافت نشد، با مشورت و استفاده از نظرات

---

1 Alternative Finance

۲ جهت دریافت متن اصلی گزارش و نیز سایر گزارش‌ها به وب‌سایت مرکز به آدرس زیر مراجعه کنید:
www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance

3 The World Bank

4 The Organization for Economic Co-operation and Development

5 The International Organization of Securities Commissions

استادان این حوزه، معادل‌سازی انجام شده است. نام‌های خاص افراد، پروژه‌ها و شرکت‌ها (به‌جز در برخی موارد محدود) بنا بر تلفظ‌شان در زبان انگلیسی با الفبای فارسی نوشته شده‌اند. مخفف‌ها، عباراتی مانند DLT و Pow، جهت خوانایی بیشتر، به همان صورت انگلیسی‌شان در متن آمده‌اند و در همه موارد ذکرشده، اصل عبارت انگلیسی در اولین محل مورد استفاده در متن کتاب به‌صورت پی‌نوشت ارائه شده است. جهت سهولت در یافتن معادل‌های فارسی انتخاب‌شده و نیز مراجعه‌های ناگزیر در حین مطالعه، واژه‌نامه‌ای نیز به انتهای کتاب افزوده شده است. علاوه بر آن، بخش تعاریف اصطلاحات تخصصی، «ضمیمه ج» کتاب، برای بسیاری از عبارت‌های اولیه مورد نیاز در زمینه فناوری دفاترکل توزیع‌شده، تعریف مختصر و مفیدی ارائه می‌دهد. مواردی نیز از سمت مترجمان به آن افزوده شده است. پیشنهاد مترجمان این است که پیش از شروع مطالعه کتاب، این تعاریف مطالعه شوند.

بر خود لازم می‌دانیم از عزیزانی که در این مسیر با ما همراهی داشتند، قدردانی کنیم؛ از جمله خانم فاطمه بذرافشان که در صفحه‌آرایی و بازطراحی تصاویر کتاب صبر و دقت بسیاری داشتند، آقای اسماعیل حصاری که در بازخوانی نسخه اولیه فارسی و پیشنهادهای اصلاحی بسیار مفید بودند، همچنین آقای محمد جباری در بازخوانی متن نهایی و آقایان رضا نورمحمدی، حجت عباسی، عباس امامی و علی‌رضا رادفر در معادل‌سازی اصطلاحات تخصصی و ارائه پیشنهادهای اصلاحی همکاری داشتند.

در پایان لازم به ذکر است که اگرچه در ترجمه و تهیه کتاب دقت بسیاری شده، اما نتیجه حاصل را عاری از خطا نمی‌دانیم. از خوانندگان محترم درخواست می‌شود چنانچه موردی را قابل بهبود یا اصلاح دانستند، ما را از لطف خود محروم ندارند.

ریحانه خیربخش

فاطمه عبداله

بخش ۱

مقدمه

مفهوم فناوری دفترکل توزیع‌شده[۱] پیش از بیت‌کوین[۲] و فناوری بلاک‌چین[۳] وجود داشت. مسئله ژنرال‌های بیزانسی[۴] که لمپورت[۵] و همکاران وی در سال ۱۹۸۲ مطرح کردند به تشریح این مسئله می‌پرداخت که چگونه «سیستم‌های کامپیوتری [...] باید اطلاعات متناقض را در یک محیط خصمانه[۶] مدیریت کنند» [۱]. تحقیقات بعدی، منجر به ظهور اولین الگوریتم برای سیستم‌های با دسترسی بالا[۷] شد؛ الگوریتمی که با افزایش کمی تاخیر[۸]، خطای بیزانسی را تحمل می‌کرد [۲]. اولین نمونه‌های ظهور مفهوم «بلاک‌چین» را می‌توان در سال‌های ۱۹۹۱ و ۱۹۹۲ در مطالعات هابر[۹] و همکاران [۳] وی ردیابی کرد [۴]؛ آنها مفهوم زنجیره‌ای از بلوک‌های داده، که با رمزنگاری به یکدیگر مرتبط شده‌اند را معرفی کردند. این زنجیره در سیستم‌های توزیع‌شده و با استفاده ازتوابع هَش رمزنگاری[۱۰] و درخت‌های مِرکِل[۱۱]، به شکلی امن و کارا، به داده‌های

1 Distributed Ledger Technology (DLT)
2 Bitcoin
3 blockchain
4 Byzantine Generals Problem
5 Lamport
6 adversarial environment
7 highly available systems
8 latency
9 Haber
10 cryptographic hashing functions
11 Merkle trees

دیجیتال برچسب زمانی[1] می‌زند.

اما این پیشرفت‌ها، در مقایسه با جذابیتی که اخیرا فناوری‌های رمزارز[2] و بلاک‌چین پیدا کرده‌اند، توجهی را به خود جلب نکردند. اقبال اخیر به فناوری بلاک‌چین باعث جذب سرمایه‌های هنگفتی شده است و در نتیجه‌ی آن، شاهد تحول سریع کاربردها و انواع سیستم‌های DLT هستیم، سیستم‌هایی که بسیاری از آنها شباهتی به بیت‌کوین و مقلدان بی‌شمار آن ندارند.

مفهوم سیستم‌های DLT در سال ۱۹۸۲ پدید آمد، در حالی که قدیمی‌ترین ردپای مفهوم «بلاک‌چین» به سال ۱۹۹۱ باز می‌گردد.

DLT چیست؟

عبارت فناوری دفترکل توزیع‌شده (DLT) به عنوان یک چترواژه[3]، برای معرفی سیستم‌های چندحزبی[4] به کار می‌رود که بدون وجود اپراتور یا قدرت مرکزی در یک محیط خصمانه کار می‌کنند؛ محیطی که احزاب آن ممکن است غیرقابل اعتماد و یا مخرب باشند. فناوری بلاک‌چین زیرمجموعه مشخصی از دنیای گسترده‌ترِ DLT است که ساختار داده[5] خاصی دارد، زنجیره‌ای از بلوک‌های داده که با استفاده از هش به یکدیگر مرتبط[6] شده‌اند.

1 timestamp
2 cryptocurrency
3 umbrella term (توضیح مترجم: چترواژه عبارتی است که چندین عبارت دیگر را دربرمی‌گیرد).
4 multi-party systems
5 data structure
6 hash-linked

گسترش و تحول انواع DLT و کاربردهای آن با استفاده‌ی گسترده از زبان و اصطلاحات تخصصی همراه بود، اصطلاحاتی که در اکثر مواقع گیج‌کننده و نادقیق بوده و در پروژه‌های مختلف، متناقض هستند. نگرانی ما از تداومِ استفاده‌ی بی‌قاعده از زبان و اصطلاحات تخصصی باعث تدوین این نوشتار شد. زیرا اگر این شرایط ادامه یابد، ممکن است توسعه این فناوری متوقف شود و جامعه و صنعت با مخاطرات قانونی و مالی ناشناخته‌ای مواجه شوند.

در حال حاضر بخش زیادی از اقبال عمومی به این حوزه متوجه توکِن‌های دیجیتالی[1] است، دارایی‌های دیجیتالی که با رمزنگاری امن شده‌اند[2] و آنها را می‌توان با استفاده از سیستم‌های DLT منتشر و جابجا کرد. اما پیش از تحلیل ویژگی‌های این دارایی‌ها، لازم است درک بسیار خوبی از زیرساخت‌ها[3] و نیز چگونگی تاثیرگذاری تصمیمات طراحی بر ماهیت داده‌های ثبت شده داشته باشیم.

اهداف

هدف این نوشتار ارائه چارچوب مفهومی[4] و مجموعه اصطلاحات تخصصی‌ای‌است که به آسانی برای سیستم‌های DLTی پیش از رمزارزهایی مثل بیت‌کوین و نیز سیستم‌های DLT مشابه با بیت‌کوین یا الهام گرفته از آن، قابل استفاده باشند. همچنین، تلاش می‌شود تا این فناوری‌های جدیدتر، از پایگاه‌داده‌های سنتی[5] و دیگر سیستم‌ها متمایز شوند. هدف این چارچوب مفهومی، ارائه‌ی ابزاری چند بُعدی برای بررسی و مقایسه‌ی سیستم‌های DLT موجود، رفتارها و ویژگی‌های آنها است. همچنین، در بررسی طرح‌های پیشنهادی سیستم‌های DLT جدید، این چارچوب می‌تواند به عنوان یک ابزار تحلیلی مفید استفاده شود.

---

1 digital tokens
2 cryptographically-secured digital assets
3 infrastructures
4 conceptual framework
5 traditional databases

طراحی این چارچوب مفهومی به صورت عمومی[۱] و ماژولار[۲] انجام شده تا بتواند برای هر نوع DLT به کار گرفته‌شود و نیز لایه[۳]ها، مولفه[۴]ها، پیکربندی[۵]ها و فرآیندهای جدید بتوانند مستقلا به آن اضافه شوند، به‌گونه‌ای که تاثیری بر اساس و بنیان این چارچوب نداشته باشند.

روش‌شناسی

رویکرد ما در این نوشتار «نگاه سیستمی»[۶] است. با این رویکرد می‌توانیم تشریح کنیم چگونه مجموعه‌ای از اجزاء با هم کار می‌کنند تا یک «کل عملکردی»[۷] خلق شود، به جای اینکه اجزاء را به صورت مجموعه‌ای از بخش‌های منفک از هم ارائه دهیم. رویکرد مذکور امکان ارزیابی رفتارهای یک سیستم را در بافت محیط آن، فراهم می‌کند. در حالی که مفهوم سیستم خود مفهوم عمومی‌تری است که بر جدا کردن بخشی از جهان از دیگر قسمت‌ها دلالت می‌کند، ایده‌ی نگاه سیستمی به معنای به کار گرفتن رویکردی غیرتقلیل‌گرایانه[۸] برای توصیف ویژگی‌های خود سیستم است. علاوه بر آن، تلاش ما بر این بوده است که این سیستم‌ها را در بافت محیطی یا اکوسیستم‌شان درنظر بگیریم، و نه به عنوان موجودیت‌هایی جداشده از محیط پیرامون. در نتیجه، خواننده می‌تواند تعاملات و ارتباطات بین یک سیستمDLT و محیط آن را بررسی کند.

این رویکرد تحلیلی از نظریه سیستم‌ها[۹] گرفته شده؛ نظریه‌ای که در خلال مجموعه‌ای از تحقیقات موازی توسعه‌یافته‌است. تحقیقات مذکور هر کدام جهتی مجزا

---

1 generic
2 modular
3 layer
4 component
5 configuration
6 systems perspective
7 a functional whole
8 non-reductionist approach
9 Systems Theory

و منحصربه‌فرد داشته و در دهه ۱۹۴۰ و با اثر لودویگ فون برتالانفی[۱] در سال ۱۹۴۹ آغاز شدند. برتالانفی مفهوم نظریه سیستم‌های عمومی[۲] را مطرح کرد [۵] که ماهیتی چندرشته‌ای دارد و علم عمومی «کلیت»[۳] را به عنوان سیستم‌ها بررسی می‌کند.

در سال ۱۹۷۲ اروین لازلو[۴] سازمانی از دانش را در زمینه‌ی سیستم‌ها، ویژگی‌های سیستمی و ارتباطات بین سیستمی پیشنهاد کرد و آن را «فلسفه‌ی سیستم‌ها»[۵] نامید [۶]. بعدها والتر باکلی[۶] در سال ۱۹۶۷ [۷] و جیمز گریر میلر[۷] در سال ۱۹۷۸ [۸]، نظریه سیستم‌های عمومی برتالانفی را به عنوان یک چارچوب نظری و روش مطالعه تصحیح کردند، به‌گونه‌ای که می‌توانست علاوه بر علوم اجتماعی، در علوم فیزیکی و زیست‌شناسی نیز به‌کار گرفته شود. خصوصاً مفهوم میلر در مورد «سیستم‌های زنده»[۸] قابل توجه بود که بیان می‌کند سیستم‌ها می‌توانند دارای سطوح سلسله‌مراتبی[۹] و لایه‌های زیرسیستم[۱۰] باشند که با جریان‌های اطلاعات، انرژی و ماده حفظ می‌شوند.

با استفاده از رویکرد مذکور، هدف ما این است که یک سیستم DLT را به عنوان مجموعه‌ای از مولفـه‌های به‌هم پیوستـه[۱۱] و دارای سلسه مراتب، به همراه فرآیندهای تعاملی بین آنها مفهوم‌سازی کنیم. به یاد داشته باشید آنچه که عملکرد و ویژگی‌های یک سیستم DLT را تعیین می‌کند پیکربندی مولفه‌های سلسله مراتبی و ارتباطات داخلی و تعاملات آنها است، و نه صرفا مجموعه‌ی ساده‌ای از اجزای مختلف.

---

1 Ludwig von Bertalanffy
2 general system theory
3 wholeness
4 Ervin Laszlo
5 systems philosophy
6 Walter Buckley
7 James Grier Miller
8 living systems
9 hierarchical
10 subsystem layers
11 interconnected

ساختار مطالب

ساختار ادامه‌ی این نوشتار به این شرح است:

بخش **۲** ادبیات موجود در این زمینه را مرور می‌کند و خلاصه‌ای از مفاهیم نظری و چارچوب‌ها را، به همراه محدودیت‌های آنها، ارائه می‌دهد. پس از آن، یک تعریف رسمی برای سیستم DLT ارائه می‌کند و معیارهای ضروری آن را برجسته و چندین اصطلاح کلیدی را تعریف می‌کند.

بخش **۳** ابزار پیشنهادی را به صورت اجمالی بررسی می‌کند و مولفه‌های مختلف چارچوب مفهومی مورد نظر را ارائه می‌دهد.

بخش **۴** به بررسی وابستگی‌های موجود بین لایه‌های مختلف یک سیستم DLT و همچنین تعاملات و ارتباطات آن با سیستم‌های خارجی می‌پردازد.

بخش **۵** به بررسی عمیق هر یک از مولفه‌های چارچوب مفهومی، همراه با بیان خلاصه‌ای از پیکربندی‌های بالقوه و تاثیرات آنها بر روی سیستم می‌پردازد. این موارد با استفاده از مثال‌هایی از سیستم‌های DLT موجود تشریح می‌شوند.

بخش **۶** چارچوب پیشنهادی را به عنوان یک ابزار تحلیلی برای بیت‌کوین به کار می‌گیرد و نتایج را با موارد دیگر، که طراحی‌های متفاوتی دارند، مقایسه می‌کند.

بخش **۷** مطالب بخش‌های قبل را خلاصه می‌کند و پیشنهادهایی جهت توسعه چارچوب مفهومی ارائه می‌دهد و به این مسئله می‌پردازد که این چارچوب در چه مواردی می‌تواند به کار گرفته شود.

ضمیمه‌ی (الف) کل این چارچوب را به صورت جدول نشان می‌دهد؛ ضمیمه‌ی (ب) بررسی مقایسه‌ای بین شش سیستم مختلف (بیت‌کوین، اتریوم[1]، ریپل[2]، آلاستریا[3]،

1 Ethereum
2 Ripple
3 Alastria

وریفاید.می[1] و پروژه X[2]) [۹] را خلاصه می‌کند و ضمیمه‌ی (ج) شامل مجموعه‌ای از پرکاربردترین اصطلاحات است.

1 Verified.Me
2 Project X

بخش ۲

سیستم‌هایِ DLT؛ صَحنه آرایی

۱.۲. سیستم‌های DLT در ادبیات موضوع

۱.۱.۲. تعاریف

در ادبیات موضوع، تعاریف زیادی برای سیستم‌های فناوری دفترکل توزیع‌شده (DLT) وجود دارد و بسیاری از آثار منتشرشده در این حوزه، تعریف منحصربه‌فرد خود را ارائه می‌کنند. برخی از این تعاریف بسیار محدودند، در حالی که برخی دیگر بسیار وسیع و گسترده‌اند و برخی دیگر با هم در تناقض‌اند. در نتیجه، می‌توان ادعا کرد هنوز یک تعریف مناسب و منجسم برای DLT ارائه نشده است.

برای مثال، بانک جهانی در سال ۲۰۱۷ سیستم‌های DLT را اینگونه تعریف می‌کند: «پیاده‌سازی خاصی از دفاترکل به اشتراک گذاشته‌شده[1] که به بیان ساده، به صورت رکوردهای[2] داده‌ی به اشتراک گذاشته‌شده در میان بخش‌های مختلف تعریف می‌شوند» [۱۰].

در سال ۲۰۱۶ پینا و روتنبرگ[3] از بانک مرکزی اروپا[4] DLT را به عنوان یک فناوری تعریف کرده‌اند که: «به کاربران خود اجازه می‌دهد تا اطلاعات مرتبط با یک سری از دارایی‌ها و صاحبانشان را در یک پایگاه‌داده‌ی به اشتراک گذاشته‌شده ذخیره کنند و به آنها دسترسی داشته باشند، این پایگاه‌داده حاوی تراکنش‌ها و موجودی حساب‌هایشان

1 shared ledgers
2 records
3 Pinna & Ruttenberg
4 the European Central Bank (ECB)

است. این اطلاعات بین کاربران توزیع شده‌است و آنها می‌توانند از آن داده‌ها برای نقل و انتقالات مالی، مانند جابجایی سهام و پول نقد، استفاده کنند بدون اینکه به یک سیستم مرکزی معتمد جهت تائید اعتبار تراکنش‌ها نیاز داشته باشند» [۱۱]. دیویدسون[۱] و همکاران وی در سال ۲۰۱۶، یک سیستم DLT را به عنوان یک «موتور اجماع[۲] توزیع‌شده که امنیت آن با استفاده از رمزنگاری تامین می‌شود و اقتصادِ رمزنگاری[۳] محرک آن است» تعریف می‌کنند [۱۲].

در مقابل بانک انگلستان[۴] در سال ۲۰۱۷، یک سری ویژگی‌های ساختاری کلیدی ارائه می‌کند که بر اساس آن سیستم‌های DLT اینگونه تعریف می‌شوند: «DLT یک پایگاه‌داده توزیع‌شده است که در آن هر گره[۵] یک کپی هماهنگ[۶] از داده‌ها را در اختیار دارد، اما از سه جهت با معماری پایگاه‌داده توزیع‌شده سنتی متفاوت است: (اول) عدم تمرکز[۷]، (دوم) قابلیت اطمینان در محیط‌های غیرقابل اعتماد و (سوم) رمزگذاری رمزنگاری[۸]». بانک انگلستان تعریف خود را اینگونه خلاصه می‌کند: «یک معماری برای پایگاه‌داده که می‌تواند حفظ و به اشتراک‌گذاری رکوردهای ثبت‌شده را به صورت توزیع‌شده و غیرمتمرکز[۹] امکان‌پذیر کند، در حالی که یکپارچگی داده‌ها را با استفاده از پروتکل‌های تائیدِ مبتنی بر اجماع و امضاهای رمزنگاری[۱۰] تضمین می‌کند» [۱۳].

به طور مشابه، تاسکا و تِسون[۱۱] مجموعه‌ای از ویژگی‌های کلیدی را که برای سیستم‌های DLT منحصر به فرد به نظر می‌رسند فهرست می‌کنند: «سیستم DLT دفترکل توزیع‌شده‌ای مبتنی بر اجماع گروهی است که در آن ذخیره‌ی داده‌ها بر اساس

---

1 Davidson
2 consensus engine
3 crypto economic
4 the Bank of England
5 node
6 synchronized
7 decentralisation
8 cryptographic encryption
9 decentralised
10 cryptographic signatures
11 Tasca & Tessone

زنجیره‌ای از بلوک‌ها نیست. ویژگی‌های اصلی این سیستم عبارتست از (۱) فرآیند اجماع غیرمتمرکز، (۲) شفافیت[۱]، و (۳) امنیت و تغییرناپذیری[۲]» [۱۴].

تعاریف دیگر منحصرا به «فناوری بلاک‌چین» اشاره می‌کنند و تمایزی بین DLT و بلاک‌چین قائل نمی‌شوند. برای نمونه، کانگ[۳] و هی[۴] بلاک‌چین را به عنوان یک «پایگاه‌داده توزیع‌شده که به طور مستقل لیستی از رکوردهای عمومی[۵] را که دائما در حال رشد است در واحد بلوک ذخیره می‌کند، به گونه‌ای که رکوردها از دستکاری و اصلاح مصون هستند» [۱۵] تعریف می‌کنند، در حالی که آتزوری[۶] آن را به عنوان یک «مخزن غیرقابل بازگشت[۷] و ضد دستکاری[۸] برای رکوردهای عمومیِ مستندات، قراردادها، مایملک و دارایی‌ها» تعریف می‌کند که «می‌توان از آن برای نگهداری اطلاعات و دستورالعمل‌ها در کاربردهای بسیار متنوعی استفاده کرد» [۱۶].

همانطورکه با این مثال‌ها نشان داده شد، هیچ تعریف اصیل و جهانی برای آنچه که سیستم DLT نامیده می‌شود وجود ندارد. آنچه باعث سخت‌تر شدن این چالش می‌شود این است که از یک سو، این تعریف‌ها گاهی بسیار خاص، فنی و برای مخاطب عام غیرقابل فهم می‌شوند؛ و از سوی دیگر، برخی از این تعاریف بسیار عام و ساده‌انگارانه هستند به گونه‌ای که هیچ تفاوت معناداری بین آنها و معماری پایگاه‌داده‌های سنتی مشاهده نمی‌شود. در هر دو حالت، فقدان اصطلاحات تخصصی رایج منجر به تصورات غلط و شکل‌گیری گسترده‌ی انتظارات غیرواقعی از پتانسیل‌های این فناوری شده است.

---

1 transparency
2 immutability
3 Cong
4 He
5 public
6 Atzori
7 irreversible
8 tamper-proof

۲.۱.۲. چارچوب‌های موجود

هستی‌شناسی[1] عبارت است از توصیف چیزهایی که وجود دارند و اینکه آنها چگونه می‌توانند با توجه به شباهت‌ها و تفاوت‌هایشان گروه‌بندی شوند. هستی‌شناسی به افراد اجازه می‌دهد برای رسیدن به اصطلاحات تخصصی مشترک در اکوسیستم‌های خاص، هم‌مسیر شوند. ما در تدوین این نوشتار، هستی‌شناسی‌هایی را که پیش از این جهت درک بهتر طبقه‌بندی‌های پیشنهادی برای اکوسیستم‌های DLT از سوی افراد دانشگاهی، متخصصان و نویسندگان در این حوزه ارائه شده بودند، مطالعه کردیم. در ادامه برخی از این چارچوب‌ها به صورت خلاصه بیان و نقایص آنها در بخش ۳.۱.۲ بررسی می‌شود.

در سال ۲۰۱۷ اوکادا[2] و همکاران وی طبقه‌بندی پیشنهادی خود را برای فناوری بلاک‌چین بر پایه دو بُعد ارائه می‌دهند: (۱) وجود یک قدرت مرجع و (۲) انگیزه‌ی مشارکت [۱۷].

لِمیوکس[3] در سال ۲۰۱۷ بلاک‌چین را از منظر علم بایگانی[4] بررسی می‌کند. علم بایگانی نظریه‌ی زیربنایی ثبت رکورد[5] و حفظ رکوردهای معتبر است. این تحقیق بلاک‌چین‌ها را در قالب سیستم‌های ثبت رکوردی چون «نوع آینه‌ای»[6]، «نوع رکورد دیجیتالی»[7] و «نوع توکن‌دار»[8] چارچوب‌بندی می‌کند و هر نوع را در رابطه با چارچوب ارزیابی نظری بایگانی رسمی[9] بررسی می‌کند [۱۸].

---

1 ontology
2 Okada
3 Lemieux
4 archival science
5 record keeping
6 mirror type
7 digital record type
8 tokenised type
9 formal archival theoretic evaluation framework

پلت[1] نیز در سال ۲۰۱۷ چارچوب دوبعدی ساده و در عین حال قدرتمندی را معرفی می‌کند که سیستم‌های DLT را با توجه به موارد: (۱) مدل انتشار داده‌ها[2] (سراسری[3] در مقابل محلی[4]) و (۲) عملکرد درون زنجیره‌ای[5] (دارای حالت[6] در مقابل بدون حالت[7]) طبقه‌بندی می‌کند [۱۹].

د کریوف[8] و ویگاند[9] در سال ۲۰۱۷ تلاش می‌کنند تا به ادبیات بلاک‌چین سازمانی[10] رسمیت ببخشند. کریوف از هستی‌شناسی سازمانی استفاده می‌کند تا بین سطوح داده‌ای[11]، ساختار اطلاعاتی[12] و لایه‌ی اساسی تراکنش‌های بلاک‌چین و قراردادهای هوشمند[13] تفاوت قائل شود [۲۰].

ژو[14] و همکاران وی نیز در ۲۰۱۷ یک رویکرد لایه‌ای[15] را برای چارچوب فعلی توسعه دادند. هدف مطالعات آنان بررسی تاثیر تصمیمات طراحی بلاک‌چین بر معماری نرم‌افزار است. رده‌بندی[16] پیشنهادی آنان در جهت کمک به ملاحظات معماری (نرم‌افزاری) در مورد عملکرد و کیفیت سیستم‌های مبتنی بر بلاک‌چین است [۲۱].

گلیزر[17] در تحقیق خود در سال ۲۰۱۷ از مجموعه اصطلاحات تخصصی واضح و روشنی استفاده می‌کند. این مجموعه اصطلاحات به شکل‌گیری مبنای مشترکی

---

1 Platt
2 data diffusion model
3 global
4 local
5 on-chain functionality
6 stateful
7 stateless
8 De Kruijff
9 Weigand
10 enterprise blockchain
11 datalogical
12 infological
13 smart contracts
14 Xu
15 layer approach
16 taxonomy
17 Glaser

جهت بحث و تبادل نظر در این حوزه کمک می‌کند. وی این مجموعه اصطلاحات را با مدل‌های بازار دیجیتال[1] مرتبط می‌کند تا از این طریق پیامدهای بازار هر مولفه را مشخص کند [۲۲]. ایده گلیزر در این تحقیق از کار مشترکی که در سال ۲۰۱۵ با بزنگر[2] انجام داده بود الهام گرفته شده‌است؛ مطالعات مشترکی که تلاش داشت تا ابزار اولیه‌ای جهت طبقه‌بندی سیستم‌های انتقال همتا به همتا[3] و سیستم‌های اجماع غیرمتمرکز به دست دهد [۲۳].

و در نهایت هم تاسکا و تسون در سال ۲۰۱۸ تلاش کردند تا فراتر از تمامی تعاریف قبلی، یک چشم‌انداز کلی از سیستم‌های DLT ارائه دهند. این هستی‌شناسی پیشرفته تقریبا جامع بوده و شامل جزئیات لازم برای طبقه‌بندی فناوری‌های بلاک‌چین است [۲۴].

۳.۱.۲. محدودیت‌های آثار قبلی

تعاریف ارائه‌شده برای فناوری‌های دفترکل توزیع‌شده متعدد است و هر کدام در جزئیات با یکدیگر تفاوت‌های زیادی دارند. این امر، رسیدن از این تعاریف خاص به یک تعریف کلی و چارچوب ماژولار که بتواند انواع مختلف سیستم‌های DLT را توصیف و طبقه‌بندی کند، دشوار ساخته است.

بحث بیشتر در این زمینه به دلیل تعریف مبهم مولفه‌های سیستم DLT در کارهای قبلی، با مشکل روبرو می‌شود. برای مثال، غالبا با «عدم تمرکز» در سیستم‌های DLT به عنوان یک ویژگی «صفر و یکی»[4] برخورد می‌شود، به جای آنکه به صورت یک متغیر پیوسته در نظر گرفته شود که نتیجه تعامل بین لایه‌های مختلف و زیرسیستم‌های تو در توی داخل آن سیستم‌ها است. این مسئله تا حدی به نمونه‌های موجود در ادبیات

1 digital market models
2 Bezzenberger
3 peer-to-peer transfer systems
4 binary

کنونی این حوزه مرتبط است که در آنها سیستم به مولفه‌های مختلف شکسته نمی‌شود و روابط، وابستگی‌ها و اثرات متقابل بین عناصر مختلف آن بررسی نمی‌شوند.

برای رفع این محدودیت‌ها، این مطالعه سعی دارد تعریف مفیدی برای سیستم‌های DLT ارائه دهد و با اتخاذ رویکردی جامع، از لایه‌ی پردازش شروع کرده و تا توسعه ابزاری عمومی و پایدار پیش رود. از چارچوب مفهومیِ حاصل می‌توان در مقاصد مختلفی از جمله ارزیابی یک سیستم موجود، بررسی مقایسه‌ای بین چندین سیستم و توسعه‌ی سیستم‌های جدید، بهره گرفت.

۲.۲. سیستم DLT چیست؟

در بخش ۱.۲ چندین تعریف متناقض برای «بلاک‌چین» یا «دفترکل توزیع‌شده» ارائه شد. مجموعه اصطلاحات غیرشفاف و مرزهای گیج‌کننده باعث شده‌اند تا DLT به چترواژه‌ای تبدیل شود که برای مجموعه متنوعی از مفاهیمی که ارتباط کمی با یکدیگر دارند، استفاده شود (که در کنار موارد دیگر، شامل بلاک‌چین‌ها نیز می‌شود).

یک تفسیر از مفهوم DLT همان محدودترین تعریف آن است (که قدمت تاریخی نیز دارد): یک زنجیره‌ی فقط-افزودنی[1] از بلوک‌های داده که با رمزنگاری به یکدیگر مرتبط شده و توسط یک شبکه‌ی غیرمتمرکز حفظ و به‌روز رسانی می‌شوند. با استفاده از محرک‌های اقتصادی، گره‌های این شبکه تشویق می‌شوند تا با یکدیگر تعامل غیراستراتژیک داشته باشند [۲۵] و از این طریق سیستم را امن و پایدار نگه دارند، و در نتیجه داده‌ها - که در یک ساختار مشخص که اغلب از آن به عنوان «دفترکل جهانی» یاد می‌کنیم مرتب شده‌اند - در مقابل دخالت خصمانه، دوبار خرج کردن[2]، سانسور، جعل، تبانی، دستکاری یا هر گونه فعالیت مخرب دیگری پایدار بمانند.

با این وجود، چنین تعریف محدودی بسیاری از کاربردهای کنونی و بالقوه‌ی

1 append-only
2 double-spend

فناوری‌های دفترکل توزیع‌شده در آینده را شامل نمی‌شود. همچنین، این تعریف دربرگیرنده مواردی نیست که در آنها یک شرکت، اصطلاح DLT را در زمینه‌ای استفاده می‌کند که آنچنان گسترده است که مرز بین سیستم DLT و دیگر سیستم‌های توزیع‌شده سنتی واضح نیست و عناصر اصلی زیادی از این تعریف محدود، گم و یا کم‌اهمیت می‌شوند.

برای حل این مشکل، پیشنهاد می‌شود با استفاده از یک رویکرد جایگزین، تعادلی بین دو انتهای این گستره ایجاد کنیم؛ رویکردی که به جای تبیین مجموعه‌ی کامل ویژگی‌های یک سیستم DLT ایده‌آل، بر نیازمندی‌های حداقلیِ ضروری یک سیستم DLT تمرکز می‌کند (همان شرایط لازم و کافی). ما سیستم‌های DLT را به عنوان یک نوع یا زیرمجموعه‌ای از سیستم‌های توزیع‌شده در نظر می‌گیریم که واجد یک سری ویژگی‌های خاصی هستند که آنها را از سیستم‌های توزیع‌شده سنتی متمایز می‌کنند.

سیستم‌های DLT به گونه‌ای طراحی شده‌اند که بتوانند در محیط‌های خصمانه کارایی داشته باشند.

محیط خصمانه چیست؟

یک محیط خصمانه با حضور بازیگران خرابکار[1] در آن سیستم یا شبکه شناخته می‌شود؛ بازیگرانی که از سیستم در جهتی غیر از هدف آن استفاده می‌کنند تا سیستم تخریب و یا تضعیف شود. متخاصم[2] در یک سیستم DLT موجودیتی[3] است که تلاش می‌کند از قوانین اجماع به‌گونه‌ای بهره‌برداری کند

1 malicious actors
2 adversary
3 entity

که دارایی‌های دیگران را بدون اجازه جابجا کند، تراکنش‌های دیگران را سانسور کند و یا شبکه را مختل سازد. بازیگران خرابکار می‌توانند داخل و یا خارج از سیستم فعالیت داشته باشند [۲۶].

سیستم DLT در ذات خود یک «ماشین اجماع» است؛ یک سیستم چندحزبی که در آن شرکت‌کنندگان[1] در مورد یک مجموعه داده‌ی به اشتراک گذاشته‌شده و اعتبار آن به توافق می‌رسند، آن هم در نبود یک هماهنگ‌کننده‌ی مرکزی. آنچه باعث تمایز سیستم‌های DLT از پایگاه‌داده‌های توزیع‌شده سنتی می‌شود ویژگی‌هایِ طراحیِ ساختار آنها است؛ ویژگی‌هایی که قابلیت پشتیبانی از داده‌ها و حفظ تمامیت آنها در محیط خصمانه را فراهم می‌کنند.

سیستم‌های DLT، «ماشین‌های اجماع» چندحزبی هستند.

سیستم‌های DLT در بازه‌ی حدی خودشان می‌توانند اعمال بازیگران خرابکاری که به صورت فعالانه به سیستم حمله می‌کنند، و نیز بازیگران صادق اما در عین حال غیرقابل اعتماد را تحمل کنند [۲۷]. اما این تحمل کردن صرفا در مورد ثبت و پردازش داده‌ها صورت می‌گیرد. به این معنا که طرف‌هایی که می‌خواهند با یکدیگر تراکنش داشته باشند، ممکن است بتوانند به عملکرد سیستم اعتماد کنند، اما همچنان باید عموما به طرف مقابل خود اعتماد داشته باشند [۲۸]. به همین دلیل، سیستم‌های DLT را می‌توان به عنوان یک فناوریِ حذف‌کننده واسطه[2] در نظر گرفت که اعتماد کردن را به نقاط پایانی (به عبارتی همان کاربرهای) یک سیستم محول می‌کند [۲۹].

این ویژگی‌ها، به معماری و طراحی سیستم و نیز به محیطی که سیستم در آن

1 participants
2 disintermediating technology