



سازمان جواد دانشگاهی صنعتی شریف

زنجیره بلوکی

دکتر علی کهنی

استادیار دانشگاه تهران

با همکاری

مهديه دهقانی

پاییز ۱۳۹۸

سرشناسه:	کمندی، علی، ۱۳۵۸-
عنوان و نام پدیدآور:	رنجیره بلوکی/ علی کمندی؛ با همکاری مهدیه دهقانی.
مشخصات نشر:	تهران: جهاد دانشگاهی، واحد صنعتی شریف، ۱۳۹۸
مشخصات ظاهری:	۲۱۶ ص: مصور، نمودار.
شابک:	۹۷۸-۹۶۴-۶۴۴۵-۴۸-۲
وضعیت فهرست‌نویسی:	قیفا
یادداشت:	کتابنامه: ص. ۲۱۵-۲۱۶.
موضوع:	بلاک چین (پایگاه‌های اطلاعاتی)
موضوع:	Blockchains (Databases)
موضوع:	انتقال الکترونیکی وجوه
موضوع:	Electronic funds transfer
موضوع:	بازرگانی الکترونیکی
موضوع:	Electronic commerce
موضوع:	رمزگذاری داده‌ها
موضوع:	Data encryption (Computer science)
موضوع:	بیت‌کوین
موضوع:	Bitcoin
شناسه افزوده:	دهقانی، مهدیه، ۱۳۷۴-
شناسه افزوده:	جهاد دانشگاهی، واحد صنعتی شریف.
رده بندی کنگره:	۳۷۱۷۰
رده‌بندی دیوینی:	۳۳۱، ۷۸۰۲،
شماره کتابشناسی ملی:	۵۹۵۸۰۰



سازمان جهاد دانشگاهی صنعتی شریف

عنوان کتاب: رنجیره بلوکی
مولفان: علی کمندی و مهدیه دهقانی
ناشر: جهاد دانشگاهی صنعتی شریف
طراح جلد: سید حسن کمالی
صفحه‌آرایی: وحیده حسین‌زاده شانه‌چی
نوبت چاپ: اول
تاریخ چاپ: پاییز ۱۳۹۸
تیراژ: ۱۰۰۰ نسخه
قیمت: ۴۰۰۰۰۰ ریال

ISBN: 978-964-6445-48-2

شابک: ۹۷۸-۹۶۴-۶۴۴۵-۴۸-۲

نشانی: تهران، خیابان آزادی، شمال دانشگاه صنعتی شریف، خیابان شهید قاسمی، پلاک ۷۱
تلفن: ۶۶۰۷۵۰۱۱، نمابر: ۶۶۰۷۵۲۵۰، پست الکترونیکی: journal@jdsharif.ac.ir

فهرست مطالب

عنوان

صفحه

۱۵	پیشگفتار.....
۱۷	فصل اول: مقدمه.....
۱۹	۱-۱ مقدمه.....
۲۵	فصل دوم: سید-تم‌های توزیع شده.....
۲۷	۱-۲ سید-تم‌های متمرکز، نیمه-متمرکز و توزیع شده.....
۳۰	۲-۲ تعریف سیستم‌ها- توزیع شده.....
۳۲	۳-۲ اهداف استفاده، از سید-تم‌های توزیع شده.....
۳۲	۱-۳-۲ اشتراک منابع.....
۳۳	۲-۳-۲ درگیر نکردن کاربر جزئیات.....
۳۴	۳-۳-۲ باز بودن سیستم.....
۳۵	۴-۳-۲ مقیاس پذیری.....
۳۷	۴-۲ قضیه CAP.....
۴۱	فصل سوم: معرفی زنجیره بلوکی.....
۴۴	۱-۳ کارکرد زنجیره بلوکی.....
۴۵	۲-۳ ساختار شبکه‌های زنجیره بلوکی.....
۴۵	۱-۲-۳ بلوک.....
۴۵	۲-۲-۳ زنجیره.....
۴۶	۳-۲-۳ شبکه.....
۴۷	۳-۳ پلتفرم‌های مبتنی بر زنجیره بلوکی.....
۴۸	۴-۳ روند اجماع.....
۴۹	۵-۳ کاربردها.....
۵۰	۶-۳ انواع شبکه‌های زنجیره بلوکی.....
۵۱	۷-۳ تفاوت بین پلتفرم‌ها.....

۵۳	فصل چهارم: ارزشهای رمز پایه
۵۵	۱-۴ بیت کوین
۵۵	۱-۱-۴ مروری مختصر بر تاریخچه بیت کوین
۵۶	۱-۲-۴ نحوه ذخیره‌سازی اطلاعات بیت کوین
۵۸	۱-۳-۴ آینده بیت کوین
۵۹	۱-۴-۴ محدودیت‌های بیت کوین
۵۹	۱-۵-۴ باورهای عمومی در مورد بیت کوین
۶۱	۲-۴ اتریوم
۶۱	۱-۱-۴ مرور اجمالی تاریخچه اتریوم
۶۲	۱-۲-۴ مدل اجماع
۶۳	۱-۳-۴ اتر، نام، متن‌باز
۶۳	۱-۴-۴ رمز ارز
۶۴	۱-۵-۴ استخراج
۶۴	۲-۴ ریپل
۶۵	۱-۳-۴ تاریخچه
۶۸	۲-۳-۴ روش اجماع
۶۸	۳-۳-۴ تفاوت ریپل با دیگر زنجیره‌ها: بلوکی
۷۰	۴-۳-۴ ریسک‌ها
۷۱	۴-۴ فکتوم
۷۱	۱-۴-۴ اعتماد
۷۳	۲-۴-۴ نوآوری‌های فکتوم
۷۵	۳-۴-۴ ساختار زنجیره
۷۶	۴-۴-۴ روش اجماع
۷۸	۵-۴-۴ توسعه به کمک فکتوم
۷۹	۶-۴-۴ آشنایی با فکتوید
۸۰	۷-۴-۴ ایجاد شفافیت در صنعت مرهونات
۸۱	۵-۴ لیبرا
۸۲	۱-۵-۴ ویژگی‌های منحصربه‌فرد لیبرا
۸۴	۲-۵-۴ نحوه کارکرد لیبرا
۸۴	۳-۵-۴ پیاده‌سازی ارز دیجیتال لیبرا
۸۵	۴-۵-۴ چالش‌های لیبرا

- ۸۶ ۴-۶ ملاحظات شبکه‌ها و رمز ارزها
- ۸۶ ۴-۶-۱ سریع پولدار شدن
- ۸۶ ۴-۶-۲ کلاهبرداری‌ها

۸۹ فصل پنجم: رمزنگاری

- ۹۱ ۵-۱ روش‌های سنتی رمزنگاری
- ۹۲ ۵-۲ توابع درهم‌سازی
- ۹۴ ۵-۳ توابع درهم‌سازی پرکاربرد در رمزنگاری
- ۹۴ ۵-۳-۱ خلاصه پیام
- ۹۴ ۵-۳-۲ تابع درهم‌ساز ایمن
- ۹۶ ۵-۳-۳ ریست
- ۹۷ ۵-۳-۴ ویرا بول
- ۹۷ ۵-۴ روش‌های مدرن رمزنگاری
- ۹۸ ۵-۴-۱ رمزنگاری متقارن
- ۹۸ ۵-۴-۲ رمزنگاری با زوج کل
- ۱۰۰ ۵-۵ امضای الکترونیکی
- ۱۰۲ ۵-۶ درخت مرکب

۱۰۷ فصل ششم: الگوریتم‌های اجماع

- ۱۰۹ ۶-۱ الگوریتم‌های اجماع در سیستم‌های توزیع شده
- ۱۱۱ ۶-۱-۱ پکس
- ۱۱۵ ۶-۱-۲ رفت
- ۱۱۷ ۶-۱-۳ الگوریتم اجماع با استفاده از همگامی جزئی
- ۱۱۷ ۶-۱-۴ بی‌بی‌اقتی
- ۱۱۸ ۶-۲ الگوریتم‌های توافق در زنجیره بلوکی
- ۱۱۸ ۶-۲-۱ روش اثبات کار
- ۱۲۳ ۶-۲-۲ چندشاخه شدن زنجیره
- ۱۲۹ ۶-۲-۳ گواه اثبات سهام وثیقه
- ۱۳۱ ۶-۲-۴ روش اثبات سهام وکالتی
- ۱۳۲ ۶-۲-۵ گواه اثبات ظرفیت
- ۱۳۲ ۶-۲-۶ گواه اثبات زمان سپری شده

- ۶-۲-۷ گواه اثبات سوزاندن..... ۱۳۳
- ۶-۲-۸ گواه اثبات فعالیت..... ۱۳۴
- ۶-۲-۹ گواه اثبات وزن..... ۱۳۶
- ۶-۲-۱۰ تحمل‌پذیری خطای بیزانس..... ۱۳۶
- ۶-۲-۱۱ الگوریتم توافق سومراگی..... ۱۳۷

فصل هفتم: قراردادهای هوشمند شرکت‌های خودگردان غیرمتمرکز..... ۱۳۹

- ۷-۱ مفهوم قراردادهای هوشمند..... ۱۴۱
- ۷-۲ شرکت‌های خودگردان غیرمتمرکز..... ۱۴۴

فصل ۸: سیستم‌های پیاده‌سازی..... ۱۴۹

- ۸-۱-۱ هایدلبر..... ۱۵۱
- ۸-۱-۱-۱ معرفی هایدلبر..... ۱۵۲
- ۸-۱-۲ فابریک..... ۱۵۳
- ۸-۱-۳ پروژه‌ی آیر..... ۱۵۶
- ۸-۲-۱ مایکروسافت آژور..... ۱۵۸
- ۸-۲-۱-۱ بلچلی: زنجیره بلوکی برای..... ۱۵۸
- ۸-۲-۲ کریپتلت..... ۱۶۰
- ۸-۲-۳ استفاده از زیست‌بوم آژور..... ۱۶۲
- ۸-۲-۴ ابزارهای زنجیره بلوکی در آژور..... ۱۶۳
- ۸-۳ زنجیره بلوکی آی‌بی‌ام..... ۱۶۵

فصل نهم: کاربردهای زنجیره بلوکی..... ۱۷۳

- ۹-۱ خدمات مالی..... ۱۷۵
- ۹-۱-۱ بانکداری..... ۱۷۵
- ۹-۱-۲ تغییر در ماهیت سرمایه‌گذاری..... ۱۷۷
- ۹-۱-۳ خدمات نوین پرداخت..... ۱۷۸
- ۹-۱-۴ خرد-پرداخت‌ها..... ۱۷۹
- ۹-۱-۵ بیمه..... ۱۷۹
- ۹-۱-۶ تغییر در شیوه ارائه اطلاعات..... ۱۸۳
- ۹-۱-۷ شناسایی تقلب در لحظه..... ۱۸۴
- ۹-۲ دولت‌های چابک..... ۱۸۵

۱۸۶	۱-۲-۹ پروژه شهر هوشمند سنگاپور
۱۸۶	۲-۲-۹ اقامت الکترونیکی استونی
۱۸۸	۳-۹ کاربردهای دیگر
۱۸۸	۱-۳-۹ دفترخانه‌ها در چین
۱۸۸	۲-۳-۹ لایه اعتماد برای اینترنت
۱۸۹	۳-۳-۹ اینترنت اشیاء و تغییر شکل گواهی‌نامه‌ها
۱۹۱	۴-۳-۹ استارت آپ‌ها
۱۹۲	۵-۳-۹ حقوق مالکیت فکری و هنری
۱۹۳	۴-۹ زنجیره بلوکی این بازار
۱۹۴	۵-۹ برنامه ویس مشارکتی
۱۹۴	۶-۹ ثبت امارات
۱۹۵	۷-۹ املاک و مستعلات
۱۹۷	۸-۹ شهرهای هوشمند
۱۹۸	۱-۸-۹ شهرهای هوشمند
۱۹۹	۲-۸-۹ چشم‌انداز لندن
۲۰۰	۳-۸-۹ ابتکار ۲۰۲۰ دویی
۲۰۳	فصل دهم: آینده زنجیره بلوکی
۲۰۵	۱-۱۰ واکنش‌ها نسبت به رمزارزها
۲۰۶	۲-۱۰ مقررات مرتبط
۲۰۷	۱-۲-۱۰ واکنش دولت‌ها
۲۰۸	۲-۲-۱۰ رویکرد ایالات متحده و اروپا
۲۱۰	۳-۲-۱۰ چین
۲۱۰	۳-۱۰ کشورهای در حال توسعه
۲۱۱	۴-۱۰ ایجاد تاریخچه دائمی
۲۱۳	۵-۱۰ ایجاد فرصت‌های برابر
۲۱۷	فهرست مراجع

پیشگفتار

زنجیره بلوکی یکی از چالشی‌ترین تکنولوژی‌هایی است که در سال‌های اخیر معرفی شده و چشم‌انداز شگفت‌انگیزی از رشد و توسعه و نیز کاربردهای متنوع آن در آینده‌ای نه‌چندان دور ترسیم شده است. برخلاف تصور عموم که زنجیره بلوکی را گاهی با ارزهای دیجیتال مترادف فرض می‌کنند، زنجیره بلوکی تکنولوژی زیربنای ارزهای دیجیتال است و کاربردهای آن مطلقاً به ارز دیجیتال محدود نیست. هرروز کاربردهای جدیدی برای تکنولوژی زنجیره بلوکی پیدا می‌شود و امروزه در تنوع گسترده‌ای از کاربردها چه در بخش خصوصی و چه در بخش دولتی به کار گرفته می‌شود و هرروز نیز به تعداد متنوع این کاربردها افزوده می‌شود.

مهم‌ترین دستاورد تکنولوژی زنجیره بلوکی قابلیت اعتماد بالا و اطمینان از صحت و اصالت و حفظ دائمی اطلاعات و عدم دست‌کاری اطلاعات پس از ثبت است. از طرف دیگر ماهیت توزیع‌شدگی، بر جذابیت‌های آن افزوده است.

در این کتاب به دنبال معرفی تکنولوژی زنجیره بلوکی، معرفی تکنولوژی‌ها و مفاهیم علمی بنیادین آن و همچنین شیوه اجرا و پیاده‌سازی و آشنایی با نمونه‌های متعددی از کاربردهای این تکنولوژی نوظهور هستیم. سعی شده است تا مطالب کتاب هم برای آشنایی عمومی با مبحث زنجیره بلوکی مفید واقع شود و هم برای دانشجویان و متخصصانی که به دنبال مباحث نظری زنجیره بلوکی هستند قابل استفاده باشد.

گروهی از دانشجویان تحصیلات تکمیلی دانشگاه تهران در تهیه مطالب کتاب و ترجمه برخی از مطالب از منابع اصلی همکاری داشته‌اند، به ویژه آقای مصطفی محمدی که زحمات زیادی را در ویرایش مطالب تقبل کردند، که در اینجا از زحمات و تلاش ایشان قدردانی می‌نماید. تمامی کامل‌تیم همکاران در صفحه بعد کتاب ذکر شده است.

امید است مطالب این کتاب در آشنایی با مبانی نظری و عملی زنجیره بلوکی مفید واقع شود و به خوانندگان کمک کند علاوه بر احاطه کلی به موضوع بتوانند کاربردهای این تکنولوژی جدید را در حوزه کسب‌وکار خود کشف نمایند.

دکتر علی کمندی

مردادماه ۱۳۹۸