

فراگیری بلوک‌های زنجیره‌ای

شرح دفتر کل توزیع شده، مرکززدایی

و قراردادهای هوشمند

نویسنده:

ایمران بشیر

مترجم:

امیر دین‌اوژن

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

مرکز انتشارات راهبردی

تهران - بهار ۱۳۹۹

سرشناسه	: بشیر، عمران Bashir, Imran
عنوان و نام پدیدآور	: فراگیری بلوک‌های زنجیره‌ای: شرح دفتر کل توزیع‌شده، مرکز زدایی و قراردادهای هوشمند/نویسنده ایرمان بشیر؛ مترجم امیر رئیس‌اوزن؛ ویراستار علمی حامد حاجی‌ملا میرزایی؛ ویراستار ادبی اکبر بتونی.
مشخصات نشر	: تهران: دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، مرکز انتشارات راهبردی، ۱۳۹۹.
مشخصات ظاهری	: ۶۲۴ ص: مصور، جدول.
شابک	: ۹۷۸-۶۰۰-۵۳۹۱۰۷-۷
وضعیت فهرست نویسی	: فیبا
یادداشت	: Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained.
یادداشت	: کتاب حاضر با عنوان "بلاک چین در تئوری و عمل" و ترجمه محمدحسین مهری خوانساری توسط انتشارات ناقوس، ۱۳۹۸ (۵۰۷ ص) فیبا دریافت کرده است.
موضوع	: بلاک‌چین (پایگاه‌های اطلاعاتی)
موضوع	: Blockchains (Databases)
شناسه افزوده	: دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، مرکز انتشارات راهبردی
رده بندی کنگره	: HG۱۷۱۰
رده بندی دیویی	: ۳۳۲/۱۷
شماره کتابشناسی ملی	: ۶۱۳۳۳۲۱



فراگیری بلوک‌های زنجیره‌ای

نویسنده: ایرمان بشیر
توژمه: امیر رئیس‌اوزن
ویراستار علمی: حامد حاجی‌ملا میرزایی
ناظر ویراستار: مرتضی چشمه نور
صفحه‌آرا: مینا مجلسی
طراح جلد: زهرا مهدوی
نوبت چاپ: اول- ۱۳۹۹
ناشر: انتشارات دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
شمارگان: ۱۰۰۰ نسخه
قیمت: ۱۲۱۰۰۰۰ ریال

همه حقوق چاپ و نشر این کتاب محفوظ است.

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

مرکز انتشارات راهبردی

نشانی انتشارات: تهران، ضلع شمالی بزرگراه شهید بابایی، بعد از اتوبان هنگام،

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، انتشارات دانشگاه عالی دفاع ملی

نشانی اینترنتی: www.sndu.ac.ir

تلفن: ۲۲۹۷۰۳۴۳

سخن ناشر

دانشگاه پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی با هدف نهادینه‌سازی مرجعیت علمی در توسعه مفاهیم گفتمان و تفکر راهبردی در کشور و بهره‌گیری از بنیان‌ها و نظریه‌های بومی، رصد تدریجی و ارائه راهبردهای تعالی‌بخش، علمی و تخصصی است. این دانشگاه از مراکز علمی کلیدی و حساس در عرصه مسائل راهبردی است که از بدو تشکیل و در دگردیسی و بازطراحی سازمانی پس از انقلاب شکوهمند اسلامی به‌منظور کادرسازی در تراز انقلاب اسلامی در سطح مدیران عالی کشوری و لشکری مکلف بوده و وظیفه خطیر خود در جهت تربیت و آموزش فرماندهان و مدیران عالی رتبه کشور را سرلوحه تمامی برنامه‌ها قرار داده است.

اهمیت این امر هنگامی نمود بیشتری می‌یابد که نگاه ژرف و آینده‌پژوهانه به پیرامون کشور، منطقه و جهان داشته باشیم؛ چراکه با ظهور تهدیدات نوین در عرصه بین‌الملل، لزوم داشتن چنین کانونی برای به‌هنگام نگاه‌داشتن مدیران عالی و فرماندهان نظامی کاملاً ملموس خواهد بود. از سوی دیگر چشم‌انداز ایجاد تمدنی بزرگ موجب می‌شود تا این تلاش و تعهد سبب ترغیب سازمان‌هایی گردد که برای پیروی از این هدف متعالی و ایجاد تحول در برنامه‌ها و فعالیت‌های خود نیازمند راهبردهای تخصصی و علمی منبعث از گفتمان و تفکر راهبردی این دانشگاه و پژوهشگاه باشند. با نگرش به این رویکرد و اهمیت

موضوع، لزوم تولید و توزیع ادبیات راهبردی در این دانشگاه که ماحصل تلاش اساتید و فرهیختگان متخصص در علوم دفاعی راهبردی و دانش‌آموختگان است، نمایان می‌گردد. در این راستا مرکز انتشارات راهبردی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی در سه حوزه مدیریت راهبردی، دفاع ملی و امنیت ملی با اهتمام به برنامه‌ها و در چارچوب اهداف و مفاهیم عالیه نظام مقدس جمهوری اسلامی ایران و تدابیر مقام معظم رهبری و فرماندهی کل قوا حضرت امام خامنه‌ای مد ظله العالی، سعی در انتقال مفاهیم و آموزه‌های خود به سطوح مختلف مدیران و ارکان جامعه داشته و در این بستر دست‌های پرتوانی را به این اهداف را تسهیل می‌نمایند، به گرمی می‌فشارد.

و ما توفیقنا الاً بالله علیه توکلنا و الیه ننبی
دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

فهرست مطالب

۳۳.....	مقدمه
۳۶.....	قراردادها
۳۷.....	بازخورد خواننده
۳۸.....	خدمات
۳۹.....	اشتباهات
۴۱.....	فصل اول: بلوک‌های زنجیره‌ای ۱۰۱
۴۵.....	ساختارهای توزیع شده
۴۷.....	نظریه و کد
۴۸.....	فرماندهان و شین
۴۹.....	همانگ‌سازی
۴۹.....	دستگاه‌های همانگ‌سازی
۵۰.....	انواع دستگاه‌های همانگ‌سازی
۵۰.....	نقص یزانتین براساس میزان تحمل آنتن
۵۰.....	دستگاه‌های همانگ‌سازی بر پایه راه‌ها:
۵۱.....	تاریخچه زنجیره بلوکی
۵۱.....	نقدینگی الکترونیکی
۵۲.....	مفهوم نقدینگی الکترونیکی
۵۵.....	آشنایی با زنجیره بلوکی
۵۶.....	نمایش شبکه زنجیره بلوکی
۵۷.....	تعاریف فنی مختلف زنجیره‌های بلوکی
۵۸.....	مؤلفه‌های کلی زنجیره بلوکی
۵۸.....	نشانی
۵۹.....	معامله
۵۹.....	بلوک
۵۹.....	شبکه نظیر به نظیر
۵۹.....	اسکریت‌نویسی یا زبان برنامه‌نویسی
۵۹.....	ماشین مجازی

۶۰.....	ماشین حالات
۶۰.....	گره
۶۰.....	قراردادهای هوشمند
۶۰.....	ویژگی های بلوک های زنجیره ای
۶۱.....	توافق توزیع شده
۶۱.....	تأییدیه عملکرد
۶۱.....	بسترهای نرم افزاری قراردادهای هوشمند
۶۱.....	انتقال اعتبار میان اعضا
۶۱.....	ایجاد رمزنگاری
۶۱.....	دارایی هوشمند
۶۲.....	ایمن ساز
۶۲.....	غیر قابل تغییر بودن
۶۳.....	منحصربه فرد بودن
۶۳.....	قراردادهای هوشمند
۶۳.....	برنامه های کاربردی فناوری بلوک های زنجیره ای
۶۴.....	بلوک های زنجیره ای چگونه تشکیل بلوک می دهند؟
۶۴.....	سطوح فناوری بلوک های زنجیره ای
۶۵.....	بلوک های زنجیره ای ۱،۰:
۶۵.....	بلوک های زنجیره ای ۲،۰:
۶۵.....	بلاک چین ۳،۰:
۶۵.....	نسل ایکس /بلوک های زنجیره ای ایکس:
۶۶.....	انواع بلوک های زنجیره ای
۶۶.....	بلوک های زنجیره ای عمومی
۶۶.....	بلوک های زنجیره ای خصوصی
۶۶.....	بلوک های زنجیره ای نیمه خصوصی
۶۷.....	زنجیره های جانبی
۶۷.....	بلوک های زنجیره ای جانبی
۶۷.....	دفتر کل مجاز
۶۸.....	دفتر توزیع شده

۶۸.....	دفتر مشترک
۶۸.....	بلوک‌های زنجیره‌ای خصوصی و اختصاصی
۶۸.....	بلوک‌های زنجیره‌ای رمزنگاری شده
۶۸.....	بلوک‌های زنجیره‌ای فاقد رمزنگاری
۶۹.....	اجماع در بلوک‌های زنجیره‌ای
۶۹.....	اثبات کار
۶۹.....	اثبات سهام
۷۰.....	اثبات سهام محول شده
۷۰.....	اثبات زمان سری شده
۷۰.....	اجماع سری به سرده
۷۰.....	اثبات اهمیت
۷۱.....	اجماع یکپارچه یا اجماع باسی یکپارچه
۷۱.....	سازوکارهای مبتنی بر شمار
۷۱.....	تحمل خطای بی‌زاستی عملی
۷۱.....	نظریه «کپ» و بلوک‌های زنجیره‌ای
۷۲.....	مزایا و محدودیت‌های بلوک‌های زنجیره‌ای
۷۲.....	تمرکززدایی
۷۲.....	شفافیت و اطمینان
۷۲.....	تغییر ناپذیری
۷۲.....	دسترسی بالا
۷۳.....	ایمنی زیاد
۷۳.....	ساده‌سازی الگوهای موجود
۷۳.....	معاملات سریع‌تر
۷۳.....	مقرون به صرفه بودن
۷۳.....	چالش‌ها و محدودیت‌های فناوری بلوک‌های زنجیره‌ای
۷۴.....	خلاصه
۷۵.....	فصل دوم: تمرکززدایی
۷۷.....	تمرکززدایی به وسیله بلوک‌های زنجیره‌ای

۷۹	انواع شبکه / سامانه
۸۰	روش های تمرکززدایی
۸۰	واسطه زدایی
۸۰	به واسطه رقابت
۸۱	مقیاس تمرکززدایی
۸۲	روش های تمرکززدایی
۸۲	چگونه تمرکززدایی کنیم؟
۸۴	بلوک های زنجیره ای و تمرکززدایی تمام محیطی
۸۴	حافظه
۸۵	ارتباطات
۸۷	محاسبه
۸۸	قرارداد هوشمندانه
۸۹	سازمان های تمرکززدایی شده
۸۹	سازمان های خودمختار تمرکززدا
۹۱	شرکت های خودمختار تمرکززدا
۹۱	جوامع خودمختار تمرکززدا
۹۲	برنامه های تمرکززدا
۹۲	الزامات برنامه نامتمرکز
۹۳	عملیات برنامه های تقسیم شده
۹۳	کی.وای.سی - چین
۹۳	بازار آزاد
۹۴	بسترهای نرم افزاری برای تمرکززدایی
۹۴	اتریوم
۹۴	مایدسیف
۹۵	لیسک
۹۵	خلاصه
۹۷	فصل سوم: رمزنگاری و اصول فنی آن
۱۰۰	مقدمه

۱۰۰	ریاضیات
۱۰۰	مجموعه
۱۰۰	گروه
۱۰۱	گروه تناوبی
۱۰۱	گروه آبلی (گروه جابه‌جایی پذیر)
۱۰۱	هم‌نهشتی
۱۰۱	رمزنگاری
۱۰۱	حریم شخصی
۱۰۲	امانت
۱۰۲	اصالت سببی
۱۰۳	عدم انکار
۱۰۴	مسئولیت پاسخگو
۱۰۵	رمزنگاری اولیه
۱۰۶	رمزنویسی
۱۰۶	رمزنویسی متقارن
۱۰۶	رمز دنباله‌ای
۱۰۷	رمزگذاری قطعه‌ای
۱۰۹	حالت رمزگذاری بلوک
۱۰۹	حالت افزایش کلید اجرایی
۱۰۹	حالت تأیید پیام
۱۰۹	درهم‌سازی رمزنگاری
۱۱۰	رمزنامه الکترونیکی
۱۱۰	زنجیره رمزقطعه
۱۱۱	حالت شمارنده
۱۱۱	استاندارد رمزگذاری داده‌ها
۱۱۲	پیشروی استاندارد پنهانی
۱۱۲	مراحل استاندارد رمزنگاری پیشرفته
۱۱۶	رمزنویسی نامتقارن
۱۱۹	تجزیه عدد صحیح

۱۱۹	تابع گسته
۱۱۹	خط منحنی بیضی
۱۲۰	کلیدهای عمومی و خصوصی
۱۲۱	آراس ای
۱۲۲	خاستگاه کلید عمومی
۱۲۲	تولید کلید اختصاصی
۱۲۲	رمز گذاری و رمز گشایی با آراس ای
۱۲۲	رمزنویسی منحنی بیضی
۱۲۳	ریاضیات در ح. ای. سی. سی
۱۲۵	نقطه ضمیمه‌ای
۱۲۷	دو برابر کردن نقطه
۱۳۳	جفت کلید خصوصی و عمومی: سی. سی. سی
۱۳۶	پایه رمزنگاری
۱۳۷	پایه رمزنگاری
۱۳۷	توابع هش
۱۳۸	فشرده سازی پیام‌های دلخواه به هضم طول ثابت
۱۳۸	محاسبه آسان
۱۳۸	مقاومت قبل از تصویر
۱۳۸	دومین تصویر قبل از تصویر
۱۳۹	مقاومت در برابر برخورد
۱۳۹	پیام دایجست (امدی)
۱۴۰	توابع امن هش
۱۴۱	طراحی توابع امن هش
۱۴۲	پیش پردازش
۱۴۲	محاسبات هش
۱۴۳	طراحی اس‌اچ‌ای ۳ (کیکاک)
۱۴۵	کدهای تأیید اعتبار پیام (مک)
۱۴۵	ساخت مک با استفاده از بلوک‌های رمز گذاری شده
۱۴۵	اچ‌مک‌ها (مک‌های مبتنی بر هش)

۱۴۶	درخت مرکل
۱۴۷	درخت پاتریشیا
۱۴۷	توزیع جداول هش (دی‌اچ‌تی)
۱۴۸	امضای دیجیتال
۱۴۹	ابتدا ثبت نام، سپس رمزگذاری
۱۵۰	ابتدا رمزگذاری، سپس امضا
۱۵۰	منحنی القای تابع امضای دیجیتال
۱۵۵	رمزنگاری هومورفیک
۱۵۶	علامت‌گذاری
۱۵۶	گواهی
۱۵۷	امضای کور
۱۵۷	طرح‌های رمزگذاری
۱۵۸	بازارهای مالی و تجارت
۱۵۸	بازرگانی
۱۵۹	بازار مبادلات
۱۵۹	سفارش‌ها و ویژگی‌های آن
۱۶۰	سفارش سامانه‌های مدیریت و مسیریابی
۱۶۰	اجزای تجارت
۱۶۰	ابزار اصلی
۱۶۱	ویژگی‌های عمومی
۱۶۱	اقتصادی
۱۶۱	حراجی
۱۶۱	طرف قرارداد
۱۶۱	چرخه تجاری
۱۶۲	پیش‌بینی‌های خرید
۱۶۲	دستکاری بازار
۱۶۳	خلاصه
۱۶۵	فصل چهارم: بیت‌کوین

۱۶۹		بیت کوین
۱۷۰		تعریف بیت کوین
۱۷۰		کلیدها و عناوین
۱۷۱		کلیدهای عمومی در بیت کوین
۱۷۲		کلیدهای خصوصی در بیت کوین
۱۷۳		واحدهای ارز بیت کوین
۱۷۴		رمز گذاری پیس ۵۸ چک
۱۷۴		نشانی های تجمل
۱۷۴		نشانی رمز عمومی در کد کیو آر
۱۷۵		معاملات
۱۷۶		ساختار معامله
۱۷۸		زبان اسکریپت
۱۷۸		آپ کدهای متداول
۱۷۹		انواع تراکنش
۱۸۲		معامله های بر پایه سکه
۱۸۲		هزینه معامله
۱۸۳		قراردادها
۱۸۳		معاملات انعطاف پذیر
۱۸۴		منع معاملات
۱۸۴		تأیید معامله
۱۸۵		بلوک های زنجیره ای
۱۸۶		بلوک تولید کننده یا منشأ
۱۸۹		استخراج
۱۹۰		وظیفه استخراج کنندگان
۱۹۱		اثبات کار
۱۹۲		تابع اثبات کار
۱۹۲		نرخ هش
۱۹۳		روش های استخراج
۱۹۴		آرایه دریچه ای برنامه پذیر

۱۹۵.....	مدارهای مجتمع با کاربرد خاص
۱۹۵.....	منبع استخراج
۱۹۷.....	شبکه بیت کوین
۱۹۸.....	ارزش جادویی شبکه بیت کوین
۲۰۰.....	پروتکل نمایشی کشف گره
۲۰۵.....	کیف پول اینترنتی
۲۰۶.....	انواع کیف پول
۲۰۹.....	آرم مقبول بیت کوین
۲۱۰.....	سرمایه‌گذاری، و خرید و فروش بیت کوین
۲۱۲.....	نصب بیت کوین
۲۱۲.....	راه‌اندازی گره بیت کوین
۲۱۲.....	گام دوم
۲۱۳.....	راه‌اندازی بیت کوین
۲۱۴.....	راه‌اندازی bitcoin.conf
۲۱۴.....	راه‌اندازی گره در شبکه تست
۲۱۵.....	راه‌اندازی گره در تست رگرسیون
۲۱۵.....	راه‌اندازی گره در شبکه اصلی و زنده
۲۱۶.....	آزمایش با بیت کوین-کلی
۲۱۷.....	برنامه‌نویسی بیت کوین و رابط خط فرمان
۲۱۹.....	پیشنهادهایی برای بهبود بیت کوین
۲۱۹.....	خلاصه
۲۲۱.....	فصل پنجم: سکه‌های جایگزین
۲۲۷.....	پایه و اساس نظری
۲۲۷.....	جایگزین مقیاس کار
۲۳۰.....	اثبات حافظه
۲۳۰.....	اثبات سهام
۲۳۱.....	اثبات ضرب سکه
۲۳۱.....	اثبات سپرده

۲۳۱	اثبات سوختن
۲۳۱	اثبات فعالیت
۲۳۲	جدول‌های غیرقابل برون‌سپاری
۲۳۲	تنظیم سختی و هدف‌گذاری مجدد تابع
۲۳۴	چاه گرانش کیموتو
۲۳۴	موج گرانشی تاریک
۲۳۵	محافظ دیجیتال
۲۳۵	میداس
۲۳۶	محدودیت‌های بیت‌کرین
۲۳۶	حریم خصوصی و ناشناس
۲۴۱	توسعه ارزش‌های دیجیتال
۲۴۱	تابع توافقی
۲۴۱	تابع هش
۲۴۱	توابع تنظیم دشواری
۲۴۱	زمان بین بلوک
۲۴۲	امتیاز بلوک
۲۴۲	بهره‌مندی از نصف نرخ
۲۴۲	رده‌بندی بلوک و میزان تراکنش
۲۴۲	نرخ بهره
۲۴۲	سن سکه
۲۴۳	مجموع عرضه سکه
۲۴۳	ارز رمزگذاری
۲۴۵	تجارت نیم‌کوین
۲۴۵	به دست آوردن نیم‌کوین
۲۴۷	تولید داده‌های نیم‌کوین
۲۴۸	لیست کوین
۲۵۰	تابع اسکریپت
۲۵۱	لیست کوین تجاری
۲۵۱	استخراج لیست کوین

۲۵۱	کد منبع نرم افزار و کیف پول کد منبع
۲۵۲	پرایم کوین
۲۵۳	تجارت پرایم کوین
۲۵۳	راهنمای استخراج پرایم کوین
۲۵۵	زیکش
۲۵۷	تجارت زیکش
۲۵۸	راهنمای استخراج
۲۶۱	استخراج سی بی یو
۲۶۲	بارگیری و بردآوری <i>nheqminer</i>
۲۶۳	خلاصه
۲۶۵	فصل ششم: قراردادهای هوشمند
۲۶۷	تاریخچه قراردادهای هوشمند
۲۶۸	تعریف قراردادهای هوشمند
۲۷۱	قراردادهای ریکاردی
۲۷۴	قالب قرارداد هوشمند
۲۷۵	اوراکل
۲۷۸	اوراکل های هوشمند
۲۷۸	استقرار قراردادهای هوشمند در بلوک های زنجیره ای
۲۷۸	سازمان مستقل تقسیم شده (دی ای او)
۲۷۹	خلاصه
۲۸۱	فصل هفتم: اتریوم ۱.۰.۱
۲۸۳	اتریوم
۲۸۴	مشتریان اتریوم و انتشار آن
۲۸۵	پشته اتریوم
۲۸۶	بلوک های زنجیره ای اتریوم
۲۸۶	ارز اتریوم (ای تی سی و ای تی ای جی)
۲۸۷	فورک
۲۸۷	گاز