

۲۰۷۸۸۶۶

بلاک چین در تئوری و عمل

نگاه‌های آمیخته به فناوری رمزارزها، بیت کوین،
تمرکززدایی و قراردادهای هوشمند

مؤلف

عمران بشیر

مترجم

محمد حسین مهری خوانساری

سرشناسه	پیشیر، عمران - Bashir, Imran
عنوان و نام پدیدآور	بلاک چین در تئوری و عمل (عمران پیشیر) مترجم: محمد حسین مهری خوانساری
مشخصات نشر	تهران: انتشارات ناقوس، ۱۳۹۸.
مشخصات ظاهری	۵۳۲ ص
شابک	۹۷۸-۶۰۰-۴۷۳-۲۴۸-۲
وضعیت فهرست نویسی	فیبیا
یادداشت	Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained
موضوع	بلاکچین (پایگاه های اطلاعاتی)
موضوع	Blockchains (Data bases)
موضوع	انتقال الکترونیکی وجوه
موضوع	Electronic funds transfers
موضوع	بیتکوین
موضوع	Bitcoin
شناسه افزودنی	مهری خوانساری، محمد حسین، ۱۳۶۸-، مترجم
رده بندی کنگره	HG
رده بندی دیویی	۳۳۲/۱۸۰۲۰۰
شماره کتابشناسی ملی	۹۹۷۲۱۱



برای خرید آنلاین با آدرس زیر مراجعه کنید:

www.naghoos.com.ir

انتشارات ناقوس

چاپ اول

در نسخه چاپ اول از دستگاه چاپ دیجیتال استفاده شده است

کلیه حقوق برای ناشر محفوظ است.
تکثیر تمامی یا قسمتی از این اثر به صورت حرفه‌ای یا چاپ مجدد، چاپ افست، پلی‌کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

نام کتاب	بلاک چین در تئوری و عمل
ناشر	انتشارات ناقوس
مولف	محمد حسین مهری خوانساری
چاپ اول	۱۳۹۸
تیراژ	۵۰۰ جلد
چاپ و صحافی	برجسته
ناظر چاپ	یاسمن تجملی محدث
قیمت	۱,۲۰۰,۰۰۰
شابک	۹۷۸-۶۰۰-۴۷۳-۲۴۸-۲
ISBN	978-600-473-248-2

انتشارات ناقوس

بلوار کشاورز - خیابان ۱۶ آذر - کوچه پارسی - پلاک ۱۰
تلفاکس: ۶۶۴۷۸۹۵۷ - ۶۶۴۷۸۹۵۸

پیش گفتار مولف

هدف اصلی این کتاب، آشنا ساختن خوانندگان با جنبه‌های نظری و عملی فناوری بلاک چین می‌باشد. تقریباً هر مطلب مورد نیاز برای تبدیل شدن به یک متخصص فنی بلاک چین در این کتاب آورده شده. از زمان انتشار اولین ویرایش کتاب، پیشرفت‌های بسیاری در این حوزه از فناوری صورت گرفته و بسیاری از ابزارها و تکنیک‌ها دستخوش تغییر شده‌اند در نتیجه نیاز به بروزرسانی محتوای کتاب کاملاً محسوس بود.

مباحث متعددی بدست آمده از پیاده سازی فناوری بلاک چین در حوزه‌های مختلف علاقمندی فراوانی را میان پژوهشگران آکادمیک و صنعتی به این فناوری ایجاد نموده است. در نتیجه پژوهش‌های بی‌وقفه در این زمینه، کنون کنفرانس‌ها، پروژه‌ها، تیم‌های فنی و افراد متخصص متعددی درگیر توسعه و پیشرفت این فناوری شده‌اند. ویرایش دوم این کتاب نگاهی عمیق‌تر به مفهوم تمرکززدایی، قراردادهای هوشمند و پلتفرم‌های متعدد بلاک چین همچون بیت کوین، اتریوم و هایپرلجر دارد. انتظار می‌رود که خوانندگان پس از مطالعه این کتاب درک عمیق‌تری از سازوکار داخلی فناوری بلاک چین بدست آورده و بتوانند با توسعه برنامه‌های کاربردی مبتنی بر این فناوری را داشته باشند.

این کتاب مرجع جامعی از تمامی موضوعات مورد نیاز برای آشنایی با بلاک چین همچون رمزنگاری، رمزارزها، شبکه‌های بیت کوین و اتریوم، و همچنین پلتفرم‌ها و ابزارهای موجود برای توسعه بلاک چین می‌باشد. توصیه می‌شود که خوانندگان برای استفاده بیشترین مزیت از مطالعه این کتاب آشنایی اولیه با علوم کامپیوتر و برخی مفاهیم پایه برنامه نویسی داشته باشند اما این مساله ضروری نیست و هر خواننده علاقمند به آشنایی با این فناوری با هر سطح دانش می‌تواند با مطالعه این اثر درک مناسبی از سازوکار بلاک چین پیدا کند چرا که تمامی پیش‌نیازهای علمی در کتاب گنجانده شده است.

فهرست

فصل ۱: مقدمه‌ای بر بلاک چین	۱
۱.۱ مقدمه	۱
۱.۲ رشد فناوری بلاک چین	۱
۱.۳ سیستم‌های توزیع شده	۵
۱.۳.۱ مساله ژنرال‌های بیزانسی	۷
۱.۴ بل الکترونیک	۸
۱.۵ ظاهر بلاک چین	۹
۱.۶ تعریف بلاک چین	۱۰
۱.۷ عناصر عمومی بلاک چین	۱۴
۱.۸ سازوکار جام عملیات در بلاک چین	۱۷
۱.۹ مزایا و محدودیت‌های بلاک چین	۱۸
۱.۱۰ سطوح مختلف فناوری بلاک چین	۲۰
۱.۱۱ قابلیت‌های بلاک چین	۲۲
۱.۱۲ انواع بلاک چین	۲۶
۱.۱۲.۱ انواع جداول توزیع شده	۲۶
۱.۱۲.۲ فناوری جدول توزیع شده	۲۷
۱.۱۲.۳ بلاک چین‌های عمومی	۲۸
۱.۱۲.۴ بلاک چین‌های خصوصی	۲۸
۱.۱۲.۵ بلاک چین‌های نیمه خصوصی	۲۸
۱.۱۲.۶ زنجیره‌های جانبی	۲۹
۱.۱۲.۷ جداول با مجوز دسترسی	۲۹
۱.۱۲.۸ جداول اشتراکی	۳۰
۱.۱۲.۹ بلاک چین‌های کاملاً خصوصی و اختصاصی	۳۰
۱.۱۲.۱۰ بلاک چین‌های توکن دار	۳۰
۱.۱۲.۱۱ بلاک چین‌های بدون توکن	۳۰
۱.۱۳ مفهوم توافق و روش‌های دستیابی به آن	۳۱
۱.۱۳.۱ اثبات کار (PoW)	۳۴
۱.۱۳.۲ اثبات سهم (PoS)	۳۴
۱.۱۳.۳ اثبات سهم نیابتی (DPoS)	۳۴

۵۷	 مثال‌هایی از یک DApp
۵۸	 پلت‌فرم‌های تمرکز زدایی
۵۹	 خلاصه
۶۱	فصل ۳: رمزنگاری کلید متقارن (کلید خصوصی)
۶۱	 ۳.۱ مقدمه
۶۱	 ۳.۲ کار با OpenSSL
۶۲	 ۳.۳ مقدمات رمزنگاری
۶۳	 ۳.۴ ریاضیات رمزنگاری
۶۳	 ۳.۴.۱ مجموعه
۶۳	 ۳.۴.۲ گروه
۶۴	 ۳.۴.۳ میدان
۶۴	 ۳.۴.۴ میدان‌های
۶۴	 ۳.۴.۵ مرتبه
۶۴	 ۳.۴.۶ گروه آبدی
۶۴	 ۳.۴.۷ میدان اول
۶۵	 ۳.۴.۸ حلقه
۶۵	 ۳.۴.۹ گروه حلقوی
۶۵	 ۳.۴.۱۰ حساب پیمانه‌ای
۶۵	 ۳.۵ مبانی رمزنگاری
۶۶	 ۳.۵.۱ محرمانگی
۶۶	 ۳.۵.۲ یکپارچگی
۶۶	 ۳.۵.۳ احراز هویت
۶۶	 ۳.۵.۳.۱ احراز هویت موجودیت
۶۷	 ۳.۵.۳.۲ احراز هویت منشأ پیام
۶۸	 ۳.۵.۴ عدم انکار
۶۹	 ۳.۵.۵ مسئولیت پذیری
۶۹	 ۳.۶ رمزنگاری متقارن
۷۰	 ۳.۶.۱ الگوریتم‌های رمزنگاری جریانی
۷۱	 ۳.۶.۲ الگوریتم‌های رمزنگاری بلوکی
۷۵	 ۳.۷ الگوریتم DES

۲۱۰		الگوریتم‌های بازتنظیم درجه سختی	۸.۳
۲۱۱		Kimoto Gravity Well الگوریتم	۸.۳.۱
۲۱۲		Dark Gravity Wave الگوریتم	۸.۳.۲
۲۱۲		DigiShield الگوریتم	۸.۳.۳
۲۱۳		MIDAS الگوریتم	۸.۳.۴
۲۱۳		محدودیت‌های بیت کوین	۸.۴
۲۱۴		پروتکل‌های ترکیبی	۸.۴.۱
۲۱۴		پروتکل‌های ترکیبی ثالث	۸.۴.۲
۲۱۵		گمنامی ذاتی	۸.۴.۳
۲۱۶		پروتکل‌های توسعه یافته بر بستر بیت کوین	۸.۵
۲۱۶		سکه‌ها، رنگی	۸.۵.۱
۲۱۷		پلتفرم Counterparty	۸.۵.۲
۲۱۸		توسعه ارزهای جایگزین	۸.۶
۲۲۰		پروژه Namecoin	۸.۷
۲۲۲		معاملات Namecoin	۸.۷.۱
۲۲۲		بدست آوردن Namecoin	۸.۷.۲
۲۲۴		تولید رکوردهای Namecoin	۸.۷.۳
۲۲۶		پروژه Litecoin	۸.۸
۲۲۹		معاملات Litecoin	۸.۸.۱
۲۲۹		استخراج Litecoin	۸.۸.۲
۲۳۰		پروژه Primecoin	۸.۹
۲۳۱		معاملات Primecoin	۸.۹.۱
۲۳۱		استخراج Primecoin	۸.۹.۲
۲۳۳		پروژه Zcash	۸.۱۰
۲۳۵		معاملات Zcash	۸.۱۰.۱
۲۳۶		استخراج Zcash	۸.۱۰.۲
۲۳۹		تولید آدرس	۸.۱۰.۳
۲۳۹		ماینینگ GPU	۸.۱۰.۴
۲۴۰		ماینینگ در مخازن ابری	۸.۱۰.۵
۲۴۰		دانلود و کامپایل nheqminer	۸.۱۰.۶
۲۴۲		پیش فروش سکه‌ها (ICO)	۸.۱۱
۲۴۳		توکن‌های ERC20	۸.۱۲

۲۴۴	 خلاصه ۸.۱۳
-----	------------------

فصل ۹: قراردادهای هوشمند ۲۴۵

۲۴۵	 مقدمه ۹.۱
۲۴۶	 تعریف قراردادهای هوشمند ۹.۲
۲۴۹	 قراردادهای ریکاردی ۹.۳
۲۵۲	 قالب قراردادهای هوشمند ۹.۴
۲۵۴	 پیشگوها ۹.۵
۲۵۶	 پیشگوهای هوشمند ۹.۶
۲۵۷	 استقرار قراردادهای هوشمند بر بستر بلاک چین ۹.۷
۲۵۸	 پروژه The DAO ۹.۸
۲۵۹	 خلاصه ۹.۹

فصل ۱۰: آشنایی با اتریوم ۲۶۱

۲۶۱	 مقدمه ۱۰.۱
۲۶۲	 تعریف اتریوم ۱۰.۲
۲۶۲	 انواع شبکه‌های اتریوم ۱۰.۳
۲۶۴	 مولفه‌های اکوسیستم اتریوم ۱۰.۴
۲۶۵	 ۱۰.۴.۱ کلیدها و آدرس‌ها
۲۶۵	 ۱۰.۴.۲ حساب‌های کاربری
۲۶۶	 ۱۰.۴.۳ انواع تراکنش‌ها
۲۶۹	 ۱۰.۵ حالت جهانی
۲۷۰	 ۱۰.۶ ماشین مجازی اتریوم (EVM)
۲۷۱	 ۱۰.۶.۱ عملیات EVM
۲۷۲	 ۱۰.۷ زبان‌های برنامه نویسی اتریوم
۲۷۳	 ۱۰.۸ مفهوم سوخت (Gas)
۲۷۴	 ۱۰.۹ انشعابات در اتریوم
۲۷۵	 ۱۰.۱۰ سختی استخراج بلوک
۲۷۶	 ۱۰.۱۱ عملیات ماینینگ در اتریوم
۲۷۶	 ۱۰.۱۱.۱ سازوکار توافق در اتریوم
۲۷۸	 ۱۰.۱۱.۲ الگوریتم Ethash

۴۶۱	۱۷.۲ مقیاس پذیری
۴۶۴	۱۷.۲.۱ افزایش اندازه بلوک
۴۶۴	۱۷.۲.۲ کاهش زمان بین بلوکی
۴۶۵	۱۷.۲.۳ جداول جستجوی بلوم فیلتر معکوس پذیر
۴۶۵	۱۷.۲.۴ برش افقی
۴۶۶	۱۷.۲.۵ کانال‌های حالت
۴۶۷	۱۷.۲.۶ بلاک چین خصوصی
۴۶۷	۱۷.۲.۷ استفاده از PoS به جای PoW
۴۶۷	۱۷.۲.۸ زنجیره‌های جانبی
۴۶۷	۱۷.۲.۹ ریززنجیره‌ها
۴۶۸	۱۷.۲.۱۰ زنجیره‌های درختی
۴۶۹	۱۷.۲.۱۱ انتشار
۴۶۹	۱۷.۲.۱۲ L'con, vG
۴۷۰	۱۷.۲.۱۳ Plasma
۴۷۰	۱۷.۳ حریم خصوصی
۴۷۱	۱۷.۳.۱ Indistinguishability Obfuscation (مبهم سازی تمییز ناپذیر)
۴۷۱	۱۷.۳.۲ رمزنگاری هم‌ریخت
۴۷۲	۱۷.۳.۳ اثبات‌های دانش صفر (ZKP)
۴۷۳	۱۷.۳.۴ کانال‌های حالت
۴۷۳	۱۷.۳.۵ محاسبات چندسویه امن (MPC)
۴۷۳	۱۷.۳.۶ به کارگیری سخت افزار برای فراهم سازی محرمانگی
۴۷۴	۱۷.۳.۷ CoinJoin
۴۷۴	۱۷.۳.۸ تراکنش‌های محرمانه
۴۷۵	۱۷.۳.۹ MimbleWimble طرح
۴۷۶	۱۷.۴ امنیت
۴۷۶	۱۷.۴.۱ امنیت قراردادهای هوشمند
۴۷۸	۱۷.۴.۲ واریسی و تحلیل رسمی قراردادهای هوشمند
۴۸۰	۱۷.۴.۳.۱ Oyente ابزار
۴۸۱	۱۷.۵ خلاصه

فصل ۱۸: چشم اندازی فعلی و آینده بلاک چین ۴۸۳

۴۸۳	۱۸.۱ مقدمه
-----	------------

۴۸۳	۱۸.۲ روندهای در حال ظهور
۴۸۳	۱۸.۲.۱ بلاک چین‌های خاص کاربرد (ASBC)
۴۸۴	۱۸.۲.۲ بلاک چین‌های درجه سازمانی
۴۸۴	۱۸.۲.۳ بلاک چین‌های خصوصی
۴۸۵	۱۸.۲.۴ علاقمندی پژوهشی بالا
۴۸۵	۱۸.۲.۵ استارت آپ‌ها
۴۸۵	۱۸.۲.۶ استاندارد سازی
۴۸۶	۱۸.۲.۷ بهبودها
۴۸۷	۱۸.۲.۸ پیاده سازی‌های واقعی
۴۸۷	۱۸.۲.۹ پاسخ به چالش‌های فنی
۴۸۸	۱۸.۲.۱۰ همگرایی با سایر فناوری‌ها
۴۸۸	۱۸.۲.۱۱ سایر رمزنگاری‌ها
۴۸۹	۱۸.۲.۱۲ موسساتها، شغلها
۴۸۹	۱۸.۲.۱۳ اقتصاد رمزنگاری
۴۸۹	۱۸.۲.۱۴ تحقیقات در حوزه رمزنگاری
۴۸۹	۱۸.۲.۱۵ تحقیق و توسعه در سخت افزار
۴۹۰	۱۸.۲.۱۶ تحقیقات در حوزه روش‌های رسمی و امنیت
۴۹۰	۱۸.۲.۱۷ جایگزین‌های بلاک چین
۴۹۱	۱۸.۲.۱۸ قابلیت تعامل شبکه‌های بلاک چین
۴۹۱	۱۸.۲.۱۹ بلاک چین به عنوان سرویس
۴۹۲	۱۸.۲.۲۰ تحقیقات مرتبط با کاهش مصرف انرژی
۴۹۲	۱۸.۳ سایر چالش‌ها
۴۹۲	۱۸.۳.۱ تنظیم مقررات
۴۹۳	۱۸.۳.۲ سوی تاریک فناوری بلاک چین
۴۹۵	۱۸.۴ حوزه‌های پژوهشی
۴۹۵	۱۸.۴.۱ مشکلات متمرکز سازی
۴۹۵	۱۸.۴.۲ محدودیت توابع رمزنگاری
۴۹۶	۱۸.۴.۳ الگوریتم‌های توافق
۴۹۶	۱۸.۴.۴ مقیاس پذیری
۴۹۶	۱۸.۴.۵ مبهم سازی کد
۴۹۷	۱۸.۵ پروژه‌های قابل توجه

۴۹۷	۱۸.۵.۱	زی کش بر بستر اتریوم
۴۹۷	۱۸.۵.۲	ColiCo پروژه
۴۹۷	۱۸.۵.۳	Cello پروژه
۴۹۷	۱۸.۵.۴	Qtum پروژه
۴۹۸	۱۸.۵.۵	Bitcoin-NG پروژه
۴۹۸	۱۸.۵.۶	Solidus پروژه
۴۹۸	۱۸.۵.۷	Hawk پروژه
۴۹۸	۱۸.۵.۸	Town-Crier پروژه
۴۹۹	۱۸.۵.۹	SETLCoin پروژه
۴۹۹	۱۸.۵.۱۰	TEEChan پروژه
۴۹۹	۱۸.۵.۱۱	Falcon پروژه
۵۰۰	۱۸.۵.۱۲	Bletchley پروژه
۵۰۰	۱۸.۵.۱۳	Cerberus پروژه
۵۰۱	۱۸.۶	سایر ابزارهای توسعه
۵۰۱	۱۸.۶.۱	افزونه Solidity برای رتوال استودیو
۵۰۱	۱۸.۶.۲	MetaMask
۵۰۱	۱۸.۶.۳	Stratis
۵۰۲	۱۸.۶.۴	Embark
۵۰۲	۱۸.۶.۵	DAPPLE
۵۰۲	۱۸.۶.۶	Meteor
۵۰۳	۱۸.۶.۷	uPort
۵۰۳	۱۸.۶.۸	INFURA
۵۰۳	۱۸.۷	همگرایی با سایر صنایع
۵۰۴	۱۸.۸	آینده بلاک چین
۵۰۶	۱۸.۹	خلاصه