

ارتقای امنیت سایبری با بلاک چین

مترجمین:

فاطمه توکلی - آذر مهدوی دایرایی

گوپتا، راجنیش Gupta, Rajneesh :
 ارتقای امنیت سایبری با بلاک چین / [راجنش گوپتا]: مترجمین فاطمه توکلی، آذر مهدوی دهکردی.
 تهران: شمس دانش، ۱۳۹۸.
 ۲۷۳ ص.: مصور (بخشی رنگی)، جدول، نمودار.
 ۹۷۸-۶۰۰-۹۸۳۳۵-۴-۲-۳ ریال: ۴۹۵۰۰۰

رشناسه
 وان و نام پدیدآور
 مشخصات نشر
 مشخصات ظاهری
 بایک

نوعیت فهرست نویسی
 داشت

داشت

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

موضوع

شناسه افزوده

شناسه افزوده

رده بندی کنگره

رده بندی دیویی

شماره کتابشناسی ملی

فیب
 عنوان اصلی: Hands-on cybersecurity with Blockchain : implement DDoS protection, PKI-
 ۲۰۱۸FA, and DNS security using Blockchain, 2based identity,
 کتاب نامه: ص. ۲۷۳؛ همچنین به صورت زیر نویس.
 کامپیوترها -- ایمنی اطلاعات
 Computer security
 شبکه های کامپیوتری -- تدابیر ایمنی
 Computer networks -- Security measures
 بلاک چین (پایگاه های اطلاعاتی)
 (Blockchains) (Databases)
 پایگاه های اطلاعاتی -- امنیت
 Database security
 حمله های منجر به قطع سرویس دهی
 Denial of service attacks
 توکا، فاطمه، مترجم
 مهدوی دهکردی، آذر، مترجم
 ۹۷۴/
 ۵/۸
 ۹۷۸۱۹۶۵۳

عنوان کتاب: ارتقای امنیت سایبری با بلاک چین

مترجمین: فاطمه توکلی - آذر مهدوی دهکردی

ویراستار، صفحه آرا و طراح جلد: آریتا رفعت

نوبت چاپ: اول ۱۳۹۸

شمارگان: ۱۰۰۰ نسخه

ناشر: شمس دانش

شابک: ۹۷۸-۶۰۰-۹۸۳۳۵-۴-۲-۳

قیمت: ۴۹۵۰۰۰ ریال

حق چاپ محفوظ است و متعلق به انتشارات شمس دانش می باشد

shamse.danesh@gmail.com

تلفن: ۰۲۱۶۶۱۹۸۹۳۳-۰۹۳۹۱۸۸۱۳۸۸

http://shamse-danesh.ir

فهرست مطالب

۱	پیشگفتار مترجمان
۳	پیشگفتار نویسنده
۷	فصل ۱: حجم انداز تهدید سایبری و چالش‌های امنیتی
۹	چشم‌انداز تهدیدات فعلی
۱۰	باج‌افزار
۱۱	کسب درآمد از هک کردن
۱۱	WannaCry
۱۲	NotPetya
۱۲	SimpleLocker
۱۳	TeslaCrypt
۱۳	CryptoLocker
۱۴	PC Cyborg
۱۴	حملات تکذیب سرویس توزیع شده (DDoS)
۱۴	از اسکریپت kiddies به ژئوپولیتیک
۱۵	سهولت راه اندازی حمله DDoS
۱۵	کشورهایی که در راس هدف قرار دارند
۱۶	تهدیدات داخلی

- ۱۶..... برخی از روش‌های دیگر برای تعریف تهدیدهای داخلی
- ۱۷..... نمایه‌ای از تهدیدات داخلی
- ۱۸..... نقض داده‌ها
- ۱۹..... نقض‌های داده‌ای جدید و قابل توجه
- ۲۰..... تاثیر نقض داده‌ها
- ۲۱..... تهدید پایدار پیشرفته (APT)
- ۲۳..... دیدگاه دافعان
- ۲۳..... دولت‌ها
- ۲۳..... ایالات متحده (USA)
- ۲۴..... انگلستان (UK)
- ۲۵..... اروپا
- ۲۶..... هند
- ۲۶..... شرکت‌های بزرگ
- ۲۷..... شناسایی نقطه پایانی و واکنش سازمان داده (EDR)
- ۲۷..... تکنولوژی فریب
- ۲۸..... هوش تهدید سایبری (CTI)
- ۲۸..... انجام حمله‌ی زنده
- ۳۴..... چالش‌های امنیتی جدید
- ۳۵..... خلاصه
- ۳۵..... مسئله‌ها
- ۳۶..... مطالعه بیشتر

فصل ۲: امنیت باید تکامل یابد..... ۳۷

اکوسیستم امنیت ۳۸

روش اعتبار حصر ۴۰

رویکرد نقض فرض ۴۱

تکامل در لایه پایه ۴۳

خلاصه ۴۳

مسئله ۴۳

مطالعه‌ی بیشتر ۴۴

فصل ۳: معرفی بلاک چین و اترיום ۴۵

بلاک چین چیست؟ ۴۵

تاریخچه‌ای مختصر ۴۷

اصول و اساس بلاک چین ۴۷

چگونه از بلاک چین استفاده می‌شود؟ ۴۸

اینترنت در مقابل بلاک چین ۴۹

بسته IP در مقابل بلوک ۵۱

Web app در مقابل dapp ۵۲

بلاک چین چگونه کار می‌کند؟ ۵۲

بلوک‌های سازنده‌ی بلاک چین ۵۳

بلوک ۵۳

رمزنگاری - امضای دیجیتال و الگوریتم hashing ۵۸

- ۶۵..... توافق - هسته‌ی بلاک چین
- ۶۷..... اتریوم
- ۶۷..... تاریخچه
- ۶۸..... اتریوم چیست؟
- ۶۸..... قرارداد هوشمند
- ۸۶..... EVM
- ۸۷..... گس
- ۸۷..... ۵۱pp
- ۸۸..... بلاک چین: عمده در برابر خصوصی
- ۸۸..... بلاک چین: عمومی
- ۸۹..... بلاک چین: خصوصی
- ۹۰..... انطباق کسب و کار
- ۹۱..... خلاصه
- ۹۲..... مسئله‌ها
- ۹۲..... مطالعه‌ی بیشتر
- ۹۳..... فصل ۴: بلاک چین - Hyperledger برای تجارت
- ۹۴..... نیازمندی‌های فنی
- ۹۴..... مروری بر هایپرلجر
- ۹۵..... بلاک چین به عنوان یک سرویس (BaaS)
- ۹۶..... هدف برنامه
- ۹۷..... معماری و اجزای اصلی

۹۹.....	مدل هایپرلجر فابریک
۱۰۰.....	اجزای اصلی هایپرلجر فابریک
۱۰۲.....	کارکردن هایپرلجر و روند معاملات
۱۰۸.....	بیت کوین در مقابل اتریوم در مقابل هایپرلجر
۱۱۰.....	قابلیت های هایپرلجر فابریک
۱۱۱.....	آزمایشگاه
۱۱۲.....	برنامه کاربرد TUNA
۱۲۰.....	خلاصه
۱۲۱.....	مسئله ها

فصل ۵: بلاک چین، امنیت سه گانه CIA..... ۱۲۳

۱۲۳.....	مدل سه گانه امنیتی CIA چیست
۱۲۴.....	محرمانگی
۱۲۴.....	درستی و صحت
۱۲۵.....	دسترس پذیری
۱۲۵.....	درک بلاک چین در مورد محرمانگی
۱۲۶.....	محرمانگی در مدل موجود
۱۲۶.....	کسب و کارها، بلاک چین و محرمانگی
۱۲۷.....	دستیابی به محرمانگی با هایپرلجر فابریک
۱۲۸.....	بلاک چین در درستی و صحت
۱۲۸.....	درستی و صحت در شبکه ی بلاک چین فعلی
۱۲۹.....	تنظیم بلوک و غیرقابل تغییر بودن آن

۱۲۹.....	دستیابی به درستی و صحت با هایپرلجر
۱۲۹.....	بررسی درستی و صحت زنجیره
۱۳۰.....	درک دسترس پذیری بلاک چین
۱۳۰.....	دسترس پذیری در شبکه بلاک چین فعلی
۱۳۰.....	تنها نقطه شکست نیست
۱۳۱.....	کسب و کار و دسترس پذیری
۱۳۱.....	خلاصه
۱۳۲.....	مسئله
۱۳۲.....	بیشتر بخوانید
۱۳۳.....	فصل ۶: استقرار شناسایی و مجوز بر PKI با بلاک چین
۱۳۴.....	PKI
۱۳۴.....	PKI به طور خلاصه
۱۳۸.....	تکامل PKI
۱۴۰.....	اجزا و مؤلفه ها
۱۴۰.....	رمزنگاری کلید نامتقارن
۱۴۲.....	گواهی
۱۴۴.....	مرجع صدور گواهی نامه (CA)
۱۴۶.....	مرجع ثبت نام (RA)
۱۴۷.....	مخزن گواهی (CR)
۱۴۸.....	معماری
۱۵۱.....	چرخه حیات گواهی

۱۵۵	مدیریت کلید
۱۵۷	چالش‌های مدل PKI موجود
۱۵۸	چگونه بلاک چین می‌تواند کمک کند؟
۱۵۹	زیرساخت غیرمتمرکز
۱۶۰	روش استقرار
۱۶۱	الزامات
۱۶۲	آزمایشگاه
۱۶۴	تست
۱۶۷	خلاصه
۱۶۷	مسئله‌ها
۱۶۸	برای مطالعه بیشتر
۱۶۹	فصل ۷: احراز هویت دو عامل برای چین
۱۶۹	۲FA چیست؟
۱۷۰	تکامل احراز هویت کاربر
۱۷۲	چرا ۲FA؟
۱۷۳	چگونه کار می‌کند؟
۱۷۴	چالش‌ها
۱۷۵	بلاک چین برای ۲FA
۱۷۵	چگونه بلاک چین می‌تواند ۲FA را تغییر دهد؟
۱۷۶	معماری راه حل
۱۷۷	آزمایشگاه

۱۷۸.....	مولفه‌ها
۱۷۹.....	آماده‌سازی
۱۷۹.....	نصب Node.js
۱۸۰.....	اجرا اتریوم
۱۸۱.....	اجرا قرارداد هوشمند
۱۸۳.....	تست و تایید
۱۸۶.....	خلاصه
۱۸۶.....	مسئله
۱۸۶.....	بیشتر بدانید
۱۸۷.....	فصل ۸: پلت فرم اینترنت DNS مبتنی بر بلاک چین
۱۸۷.....	DNS
۱۸۹.....	درک مولفه‌های DNS
۱۸۹.....	فضای نام
۱۹۰.....	سرورهای نام
۱۹۲.....	تحلیل‌گر
۱۹۲.....	ساختار DNS و سلسله‌مراتب
۱۹۲.....	سرور نام ریشه
۱۹۳.....	ساختار TLD فعلی
۱۹۵.....	مرکز ثبت، ثبت‌کننده و متقاضی ثبت
۱۹۶.....	رکوردهای DNS
۱۹۹.....	توپولوژی DNS برای شرکت‌های بزرگ

۲۰۰	 معماری
۲۰۱	 چالش‌ها با DNS فعلی
۲۰۲	 DNS spoofing
۲۰۳	 راه حل DNS مبتنی بر بلاک چین
۲۰۴	 X.۵۰۹ جایگزین PKI
۲۰۴	 DNS MITM زیرساخت ضد
۲۰۴	 آزمایشگاه زیرساخت DNS مبتنی بر اتریوم
۲۰۵	 آماده‌سازی آزمایشگاه
۲۰۶	 نصب بلاک چین Namecoin
۲۱۰	 نصب PowerDNS
۲۱۳	 نصب DNSChain
۲۱۶	 خلاصه
۲۱۶	 مسئله‌ها
۲۱۷	 برای مطالعه بیشتر
۲۱۹	 فصل ۹: توسعه بلاک چین مبتنی بر حفاظت در برابر DDOS
۲۲۰	 حملات DDOS
۲۲۰	 یک حمله DDOS چیست؟
۲۲۱	 چگونه کار می‌کند؟
۲۲۲	 ساخت بات‌نت
۲۲۳	 شناسایی
۲۲۴	 سلاح‌سازی

۲۲۶	تحويل
۲۲۹	بهره‌برداری
۲۲۹	نصب و راه‌اندازی
۲۳۰	مدیریت و کنترل (C۲)
۲۳۰	اقدامات در جهت اهداف
۲۳۰	انواع حملات DDoS
۲۳۱	حملات با هدف منابع شبکه
۲۳۱	حملات سیل آسا پروتکل دیتاگرام کاربر (UDP)
۲۳۲	حملات سیل آسا ICMP
۲۳۳	حملات سیل آسا پروتکل مدیریت گروه اینترنت (IGMP)
۲۳۳	حملات تقویت
۲۳۴	حمله با هدف منابع سرور
۲۳۴	حملات سیل آسا TCP SYN
۲۳۵	حمله TCP RST
۲۳۶	حمله مبتنی بر لایه امن سوکت ها (SSL)
۲۳۶	حملات HTTP رمزگذاری شده
۲۳۶	حملات با هدف منابع برنامه‌های کاربردی
۲۳۷	حملات سیل آسا DNS
۲۳۷	حملات DoS عبارات منظم
۲۳۸	حملات DoS تصادم Hash
۲۳۸	چالش‌ها با راه حل‌های فعلی DDoS
۲۳۹	چگونه بلاک‌چین می‌تواند حفاظت در برابر DDoS را تغییر دهد؟

آزمایشگاه.....	۲۳۹
خلاصه.....	۲۴۷
مسئله‌ها.....	۲۴۷
برای مطالعه بیشتر.....	۲۴۷

فصل ۱۰: واقعیت‌هایی درمورد بلاک چین و امنیت سایبری..... ۲۴۹

مسیر تصمیم‌گیری برای بلاک چین.....	۲۴۹
چه زمانی باید از بلاک‌چین استفاده کرد؟.....	۲۵۲
چه وقت نباید از بلاک‌چین استفاده کرد؟.....	۲۵۴
چک‌لیست راه‌ها.....	۲۵۵
چالش‌های بلاک‌چین.....	۲۵۶
آینده امنیت سایبری با بلاک‌چین.....	۲۵۸
خلاصه.....	۲۵۹
مسئله‌ها.....	۲۵۹
برای مطالعه بیشتر.....	۲۶۰
ضمیمه ۱: ارزیابی.....	۲۶۱
ضمیمه ۲: اصطلاحات.....	۲۶۷
مراجع.....	۲۷۳

پیشگفتار مترجمان

بلاک چین (Blockchain) از دو کلمه Block (بلاک) و Chain (زنجیره) ایجاد شده است. این فناوری در زنجیره‌ای از بلاک‌هاست. به‌طور کلی بلاک‌چین یک نوع سیستم ثبت اطلاعات و گزارش است. تفاوت آن با سیستم‌های دیگر این است که اطلاعات ذخیره‌شده روی این نوع سیستم، میان همه اعضای شبکه به اشتراک گذاشته می‌شوند و با استفاده از رمزنگاری امکان حذف و دست‌کاری اطلاعات ثبت‌شده تقریباً غیرممکن است. در حقیقت بلاک چین‌ها شبکه‌های تراکنشی هستند؛ یک بلاک چین یک پایگاه داده امن است که به‌صورت جهانی تکثیر شده است. شما می‌توانید آن را به‌عنوان یک اکس‌اچ‌ان، تمبر، راپذیر و ماندگار در ابر در نظر بگیرید. این ناحیه مشخصاً حوزه‌ای است که احتمال رشد آن در سال‌های پیش رو وجود دارد. در گزارشی که توسط Grand View Research، به‌تازگی انجام شده است، گفته شده که بازار بلاک چین تا سال ۱۴۰۳ رشدی در حدود ۷,۷۴ میلیارد دلار خواهد داشت. از طرفی در دنیای سایبری، هر روز خبر جدیدی از به‌خطر افتادن اطلاعات کاربران شنیده می‌شود که امنیت سایبری مجموعه ابزارها، سیاست‌ها، مفاهیم امنیتی، دستورالعمل‌ها با رویکردهای مدیریت ریسک، آموزش بهترین شیوه‌ها و فن‌آوری‌هایی است که می‌تواند برای محافظت از محیط سایبری، سازمان‌ها و دارایی‌های کاربر استفاده شود. با توجه به ویژگی‌های بازار بلاک چین، به نظر می‌رسد بلاک چین فناوری دلگرم‌کننده‌ای برای حفظ امنیت زندگی آنلاین ما خواهد بود.

موضوع کتاب حاضر بررسی امنیت سایبری با بلاک چین است که با بررسی راه کارهای امنیتی ارائه‌شده توسط بلاک چین در مقابل حملات سایبری می‌پردازد.

با توجه به اینکه بلاک‌چین یکی بروزترین وقایع امروزه شناخته‌شده و باعث شده تا درک بسیاری از سازمان‌ها را تغییر داده و برای مواردی حیاتی همچون ذخیره‌سازی و برای انتقال ارز مورد استفاده قرار گیرد، ترجمه‌ی این کتاب ارائه‌شده تا خدمتی هرچند کوچک برای متخصصان، علاقه‌مندان و محققین پیرامون امنیت مجازی و یا هر ذینفع دیگری باشد.

نیاز به ترجمه‌ی کتابی مناسب در زمینه‌ی امنیت سایبری با بلاک چین ما را بر آن داشت تا پس از انتخاب یک کتاب مناسب (کتاب حاضر) در حد توان خود ترجمه‌ای صحیح و روان از آن را ارائه کنیم. کتاب موجود خالی از نقص نبوده و امکان وجود اشکالاتی در آن وجود دارد. بدین جهت از کلیه دانش‌پژوهان و خوانندگان عزیز می‌خواهیم که از این کتاب استفاده می‌کنند صمیمانه تقاضا می‌کنیم که نظرات خود را در جهت بهبود در ویرایش بعدی عنوان نمایند.

www.ketab.ir