

نگاهی تحلیلی بر معماری فناوری زنجیره بلوکی و بررسی پلتفرم های منتخب

نویسندگان:

زهرا گل‌میرزایی

ابوذر عرب‌سرخی

زهرا معزکریمی

سیما زمانی

فاطمه عبداله‌ئی



انتشارات آوای قلم

پیشگفتار

طی سال گذشته زیرساخت‌های پولی و مالی و قوانین مربوطه دستخوش تغییر شده‌است. در این زمینه موارد متعددی تاثیرگذار بوده‌اند. نیازهای عمومی مالی و تجاری حوزه کسب‌وکار، الزام‌های محیطی و نیز توانمندی‌های فناوری‌های اطلاعات کاربردی، این حوزه از عمده این موارد هستند. زنجیره بلوکی معرف یکی از فناوری‌های نوظهور حوزه ارتباطات و فناوری اطلاعات است که طی چند سال اخیر از منظر توسعه فنی، دامنه و سطح نفوذ فناوری و نیز چارچوب‌ها و آئین به‌کارگیری در حوزه‌های کاربرد رشد چشمگیری را تجربه نموده است. در نگاه اول، دامنه نفوذ زنجیره بلوکی در فضاء پولی و مالی بسیار پر رنگ‌تر است. با این وجود توسعه ظرفیت‌های فنی و نیز شناخت قابلیت‌های این فناوری زمینه استفاده از آن را در حوزه‌های مختلف فراهم آورده است. این موضوع با ذوق‌زدگی ناشی از ورود فناوری زنجیره بلوکی در سطح دولت مردان، کسب‌وکارهای و صنایع موجب افزایش تلاش‌ها و سرمایه‌گذاری در این حوزه گردیده است.

علی‌رغم افزایش سرمایه‌گذاری در حوزه زنجیره بلوکی ما شاهد نرخ شکست فزآینده پروژه‌های این حوزه هستیم. بخشی از چالش‌های پیش‌روی تصمیم‌سازان به عدم درک مناسب ظرفیت‌های فناورانه و نیز عدم توجه به موضوع‌هایی مربوط می‌شود که زمینه‌ساز موفقیت یا شکست پروژه‌های زنجیره بلوکی محسوب می‌شوند. ملاحظه‌های معماری معرف یکی از عوامل کلیدی موفقیت پروژه‌های زنحیره بلوکی است. این معماری، اصول حاکم بر آن و ظرفیت‌های ناشی از استقرار درست آن از یک پلتفرم زنجیره بلوکی به پلتفرم دیگر دستخوش تغییر می‌شود. این موضوع و همراستایی آن با نگرش‌ها، نیازها و نیز مشخصه‌های فنی و زیرساختی حوزه هدف معرف عاملی مهم در موفقیت به‌کارگیری فناوری زنجیره بلوکی است. براین‌اساس در کتاب حاضر ضمن بررسی مفاهیم پایه، معماری مرجع زنجیره بلوکی و مؤلفه‌های سازنده آن، نسبت به مقایسه پلتفرم‌های مختلف این فناوری براساس یک چارچوب واحد اقدام گردیده است. نتایج بررسی‌های به‌عمل‌آمده پیرامون پلتفرم‌های مختلف زنجیره بلوکی از چند جهت حائز اهمیت است. اول آنکه درک مخاطب از مؤلفه‌های فناوری در پلتفرم‌های مختلف را ارتقاء می‌دهد. دوم آنکه ارائه‌گر یک چارچوب مقایسه‌ای ما بین پلتفرم‌های مختلف براساس مجموعه‌ای از معیارهای استاندارد شده و مشترک است. سوم آنکه نتایج مقایسه پلتفرم‌های زنجیره بلوکی به‌عنوان یک ساختار دانشی پشتیبان تصمیم برای انتخاب پلتفرم مناسب در حوزه‌های کاربردی مختلف عمل می‌نماید.

باید به این موضوع توجه داشت که بسیاری از پلتفرم‌های زنجیره بلوکی در حوزه رمزارزها کاربرد دارند. البته تعدادی از آن‌ها کاربردهای غیر رمزارزی را نیز پشتیبانی می‌نمایند. بنابراین ارزیابی این دو دسته از پلتفرم‌های زنجیره بلوکی در قالب دو فصل متمایز این کتاب ارائه و مورد توجه قرار گرفته‌است.

ابوذر عرب سرخی

فهرست مطالب

عنوان صفحه

نگاهی اجمالی بر کتاب ۱۷

فصل اول: مقدمه‌ای بر زنجیره بلوکی ۱۹

۱-۱- مقدمه ۲۱

۱-۲- سیر تحول‌های حاکم بر زنجیره بلوکی ۲۲

۱-۳- معرفی زنجیره‌بلوکی..... ۲۵

۱-۴- ویژگی‌های زنجیره‌بلوکی..... ۲۸

فصل دوم: معماری زنجیره بلوکی ۳۳

۲-۱- مقدمه ۳۵

۲-۲- معماری کلان زنجیره‌بلوکی از منظر آی.بی.اِم ۳۶

۲-۲-۱- شبکه عمومی ۳۷

۲-۲-۱-۱- خدمات لبه ۳۸

۲-۲-۱-۲- کاربران ۳۹

۲-۲-۲- شبکه ابر ۴۱

۲-۲-۲-۱- برنامه‌های کاربردی زنجیره بلوکی ۴۱

۲-۲-۲-۲- مدیریت واسط برنامه‌نویسی کاربردی ۴۲

۲-۲-۲-۳- پلتفرم زنجیر ه بلوکی ۴۲

۲-۲-۲-۴- یکپارچگی سیستم..... ۴۵

۲-۲-۲-۵- دگرگونی و اتصال..... ۴۶

۲-۲-۳- شبکه سازمانی ۴۷

۲-۲-۳-۱- پوشه کاربر سازمانی ۴۷

۲-۲-۳-۲- برنامه‌های کاربردی سازمانی ۴۷

۲-۲-۳-۳- داده‌های سازمانی ۴۷

۲-۲-۴- خدمات پایه زنجیره بلوکی ۴۸

۲-۲-۴-۱- حاکمیت ۴۸

۲-۲-۴-۲- امنیت ۴۸

۲-۲-۴-۳- پایش و هوشمندی ۴۹

عنوان **صفحه**

۲-۲-۴-۴- مدیریت شبکه زنجیره بلوکی ۴۹
۲-۲-۴-۵- فرآیند اجرا ۴۹
۲-۳- معماری زنجیره‌بلوکی از منظر آی.تی.یو ۵۳
۲-۴- مؤلفه‌های اصلی پلتفرم‌های زنجیره بلوکی ۵۷
۲-۴-۱- خدمات رمزنگاری ۵۸
۲-۴-۱-۱- شناسه تراکنش ۵۸
۲-۴-۱-۲- اثرانگشت بلوک ۵۹
۲-۴-۱-۳- رمزنگاری کلید نامتقارن ۵۹
۲-۴-۱-۴- آدرس‌ها و آدرس‌های اشتقاقی ۶۰
۲-۴-۲- تراکنش‌ها ۶۰
۲-۴-۳- دفترکل ۶۱
۲-۴-۳-۱- بلوک‌ها ۶۲
۲-۴-۳-۲- زنجیر نمودن بلوک‌ها ۶۵
۲-۴-۴- اجماع ۶۵
۲-۴-۴-۱- مدل اجماع مبتنی بر اثبات کار ۶۶
۲-۴-۴-۲- مدل اجماع مبتنی بر اثبات سهام ۶۸
۲-۴-۴-۳- مدل اجماع دور رابین ۷۰
۲-۴-۵- قرارداد هوشمند ۷۰
۲-۴-۶- پروتکل ارتباطی ۷۲
فصل سوم: پلتفرم‌های زنجیره‌بلوکی با تمرکز بر رمزارزها ۷۵
۳-۱- مقدمه ۷۷
۳-۲- بیت‌کوین ۷۷
۳-۲-۱- معرفی بیت‌کوین ۷۷
۳-۲-۱-۱- اهداف و کاربردهای بیت‌کوین ۷۸
۳-۲-۱-۲- واحد ارز مبادلاتی بیت‌کوین ۷۸
۳-۲-۱-۳- ویژگی‌های اصلی بیت‌کوین ۷۹
۳-۲-۲- شبکه بیت‌کوین ۸۱
۳-۲-۲-۱- انواع گره‌ها در ساختار شبکه بیت‌کوین ۸۱
۳-۲-۲-۲- انواع کاربران و راه‌های ارتباط با شبکه بیت‌کوین ۸۳

عنوان **صفحه**

۳-۲-۲-۳- محیط‌های اجرای بیت‌کوین ۸۴
۳-۲-۲-۴- پروتکل‌های بیت‌کوین ۸۵
۳-۲-۳- معماری بیت‌کوین ۸۸
۳-۲-۳-۱- مؤلفه‌های معماری بیت‌کوین ۸۹
۳-۲-۳-۲- زنجیره‌بلوکی بیت‌کوین ۹۱
۳-۲-۳-۳- ساختار بلوک‌ها ۹۲
۳-۲-۳-۴- ساختار تراکنش‌ها ۹۳
۳-۲-۳-۵- چرخه حیات تراکنش ۹۴
۳-۳- ویوز ۹۶
۳-۳-۱- معرفی ویوز ۹۶
۳-۳-۱-۱- اهداف و کاربردهای ویوز ۹۶
۳-۳-۱-۲- واحد ارز مبادلاتی ویوز ۹۷
۳-۳-۱-۳- ویژگی‌های اصلی ویوز ۹۷
۳-۳-۲- شبکه ویوز ۹۹
۳-۳-۲-۱- انواع گره‌ها در ساختار شبکه ویوز ۹۹
۳-۳-۲-۲- محیط‌های اجرای ویوز ۱۰۲
۳-۳-۲-۳- پروتکل‌های ویوز ۱۰۲
۳-۳-۳- معماری ویوز ۱۰۵
۳-۳-۳-۱- مؤلفه‌های معماری ویوز ۱۰۶
۳-۳-۳-۲- زنجیره‌بلوکی ویوز ۱۰۸
۳-۴- ریپِل ۱۱۳
۳-۴-۱- معرفی ریپِل ۱۱۳
۳-۴-۱-۱- هدف‌ها و کاربردهای ریپِل ۱۱۴
۳-۴-۱-۲- واحد ارز مبادلاتی ریپِل ۱۱۴
۳-۴-۱-۳- ویژگی‌های اصلی ریپِل ۱۱۴
۳-۴-۱-۴- تفاوت ریپِل و XRP ۱۱۶
۳-۴-۲- شبکه ریپِل ۱۱۸
۳-۴-۲-۱- انواع گره‌ها در ساختار شبکه ریپِل ۱۱۹
۳-۴-۲-۲- محیط‌های اجرای ریپِل ۱۲۰
۳-۴-۲-۳- پروتکل‌های ریپِل ۱۲۰
۳-۴-۳- معماری ریپِل ۱۲۵

عنوان **صفحه**

۳-۴-۳-۱- مؤلفه‌های معماری ریپل ۱۲۶
۳-۴-۳-۲- زنجیره‌بلوکی ریپل ۱۲۷
۳-۵- زی‌کَش ۱۳۴
۳-۵-۱- معرفی زی‌کَش ۱۳۵
۳-۵-۱-۱- اهداف و کاربردهای زی‌کَش ۱۳۵
۳-۵-۱-۲- واحد ارز مبادلاتی زی‌کَش ۱۳۶
۳-۵-۱-۳- ویژگی‌های اصلی زی‌کَش ۱۳۶
۳-۵-۲- شبکه زی‌کَش ۱۳۷
۳-۵-۲-۱- انواع گره‌ها در ساختار شبکه زی‌کَش ۱۳۸
۳-۵-۲-۲- انواع شرکت‌کنندگان زی‌کَش و راه‌های ارتباط با شبکه ۱۳۸
۳-۵-۲-۳- محیط‌های اجرای زی‌کَش ۱۳۹
۳-۵-۲-۴- پروتکل‌های زی‌کَش ۱۳۹
۳-۵-۳- معماری زی‌کَش ۱۴۶
۳-۵-۳-۱- مؤلفه‌های معماری زی‌کَش ۱۴۸
۳-۵-۳-۲- زنجیره‌بلوکی زی‌کَش ۱۴۹
فصل چهارم: پلتفرم‌های زنجیره‌بلوکی با تمرکز بر کاربردهای خاص ۱۵۷
۴-۱- مقدمه ۱۵۹
۴-۲- اِتریوم ۱۵۹
۴-۲-۱- معرفی اِتریوم ۱۵۹
۴-۲-۱-۱- اهداف و کاربردهای اِتریوم ۱۶۰
۴-۲-۱-۲- واحد ارز مبادلاتی اِتریوم ۱۶۳
۴-۲-۲- شبکه اِتریوم ۱۶۴
۴-۲-۲-۱- انواع گره‌ها در ساختار شبکه اِتریوم ۱۶۴
۴-۲-۲-۲- محیط‌های اجرای اِتریوم ۱۶۵
۴-۲-۲-۳- پروتکل‌های اِتریوم ۱۶۵
۴-۲-۳- معماری اِتریوم ۱۶۶
۴-۲-۳-۱- مؤلفه‌های معماری اِتریوم ۱۶۷
۴-۲-۳-۲- زنجیره‌بلوکی اِتریوم ۱۷۱
۴-۳- نِئو ۱۷۵

عنوان **صفحه**

۴-۳-۱- معرفی نِئو ۱۷۵
۴-۳-۱-۱- ویژگی‌های اصلی نِئو ۱۷۶
۴-۳-۱-۲- واحد ارز مبادلاتی ۱۷۸
۴-۳-۱-۳- مقایسه نِئو و اِتریوم ۱۷۹
۴-۳-۲- شبکه نِئو ۱۸۱
۴-۳-۲-۱- انواع گره‌ها در ساختار شبکه نِئو ۱۸۱
۴-۳-۲-۲- محیط‌های پیاده‌سازی نِئو ۱۸۲
۴-۳-۲-۳- پروتکل‌های نِئو ۱۸۳
۴-۳-۳- معماری نِئو ۱۸۵
۴-۴- فَبریک ۱۸۷
۴-۴-۱- معرفی فَبریک ۱۸۷
۴-۴-۱-۱- اهداف و کاربردهای اصلی ۱۸۸
۴-۴-۱-۲- واحد ارز مبادلاتی ۱۸۹
۴-۴-۱-۳- ویژگی‌های اصلی فَبریک ۱۸۹
۴-۴-۲- شبکه فَبریک ۱۹۱
۴-۴-۲-۱- انواع گره‌ها در ساختار شبکه فَبریک ۱۹۳
۴-۴-۲-۲- محیط‌های اجرای فَبریک ۱۹۴
۴-۴-۲-۳- پروتکل‌ها ۱۹۵
۴-۴-۳- معماری فَبریک ۱۹۷
۴-۴-۳-۱- مؤلفه‌های معماری فَبریک ۱۹۹
۴-۴-۳-۲- زنجیره‌بلوکی فَبریک ۲۰۱
۴-۵- ساوتوث ۲۰۷
۴-۵-۱- معرفی ساتوث ۲۰۷
۴-۵-۱-۱- اهداف و کاربردهای اصلی ۲۰۸
۴-۵-۱-۲- ویژگی‌های اصلی ساوتوث ۲۰۹
۴-۵-۲- شبکه ساوتوث ۲۱۱
۴-۵-۲-۱- سیستم رخداد ۲۱۱
۴-۵-۲-۲- پیام‌ها ۲۱۱
۴-۵-۲-۳- پروتکل‌های ساتوث ۲۱۲
۴-۵-۳- معماری ساوتوث ۲۱۴
۴-۵-۳-۱- هَندلِرها ۲۱۵

عنوان **صفحه**

۴-۵-۳-۲- دفاترکل ۲۱۷
۴-۵-۳-۳- ژورنال ۲۱۸
۴-۵-۳-۴- تراکنش‌ها ۲۱۹
۴-۵-۳-۵- سلسله تراکنش‌ها ۲۲۰
۴-۶- مالتی‌چین ۲۲۲
۴-۶-۱- معرفی مالتی‌چین ۲۲۲
۴-۶-۱-۱- اهداف و کاربردهای مالتی‌چین ۲۲۳
۴-۶-۱-۲- ویژگی‌های اصلی مالتی‌چین ۲۲۴
۴-۶-۲- شبکه مالتی‌چین ۲۲۴
۴-۶-۲-۱- انواع گره‌ها در ساختار شبکه مالتی‌چین ۲۲۴
۴-۶-۲-۲- پروتکل‌ها ۲۲۵
۴-۶-۳- معماری مالتی‌چین ۲۲۶
۴-۶-۳-۱- مؤلفه‌های معماری مالتی‌چین ۲۲۷
۴-۶-۳-۲- زنجیره‌بلوکی مالتی‌چین ۲۳۰
۴-۷- کاردانو ۲۳۲
۴-۷-۱- معرفی کاردانو ۲۳۲
۴-۷-۱-۱- اهداف و کاربردها ۲۳۳
۴-۷-۱-۲- واحد ارز مبادلاتی ۲۳۵
۴-۷-۱-۳- ویژگی‌های اصلی کاردانو ۲۳۵
۴-۷-۱-۴- سیرتحولها و نقشهراه کاردانو ۲۳۷
۴-۷-۲- شبکه کاردانو ۲۳۸
۴-۷-۲-۱- انواع گره‌ها در ساختار شبکه کاردانو ۲۳۹
۴-۷-۲-۲- محیط‌های اجرای کاردانو ۲۴۰
۴-۷-۲-۳- پروتکل‌های کاردانو ۲۴۱
۴-۷-۳- معماری ۲۴۶
۴-۷-۳-۱- مؤلفه‌ها ۲۴۷
۴-۷-۳-۲- زنجیره‌بلوکی کاردانو ۲۵۱
واژه نامه ۲۶۲
جدول اختصارات ۲۷۴