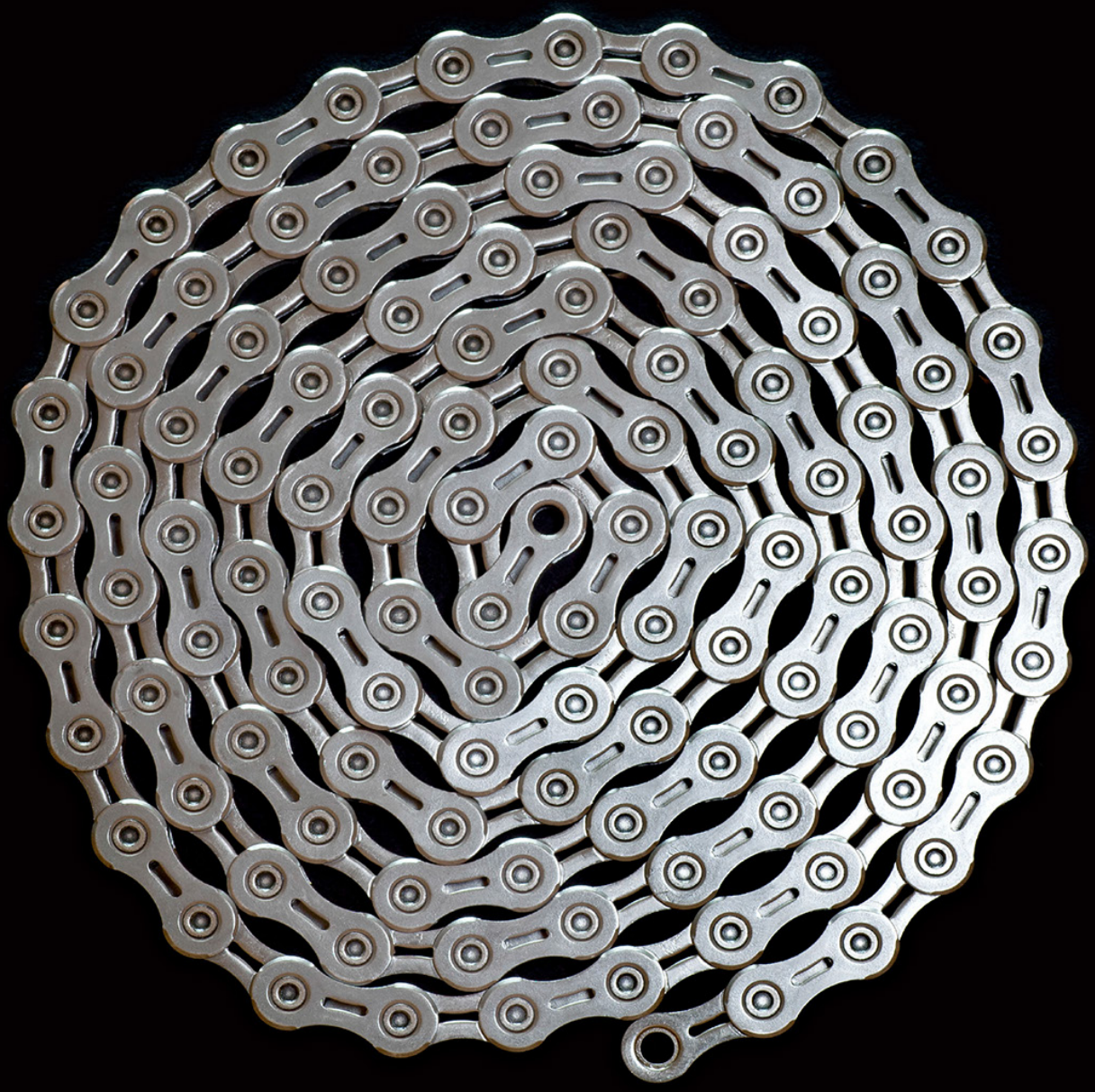
Deloitte.



شش اصل کنترلی

برای بلاکچین‌های خدمات مالی

اکتبر ۲۰۱۷

ققنوس
راه‌پرداخت

این نشریه در تابستان ۲۰۱۷ میلادی و به کوشش آزمایشگاه بلاکچین ای‌ام‌ای‌ای (EMEA) دیلویت در دوبلیـــن و با یاری دیلویت هنگ کنگ و ایالات متحده آمریکا تهیه شده اســـت و بر روی شش اصل کنترلی ضروری برای پذیرش بلاکچین در مقیاس جهانی تمرکز دارد:

۱) بهترین عملکرد- استانداردهایی برای توسعه بلاکچین
۲) تعامل‌پذیری و کنترل یکپارچگی سیستم
۳) قوانین حسابرسی
۴) کنترل‌های امنیت سایبری
۵) بهبود کنترل‌های اطلاعات و ارتباطات سنتی
۶) و طرح استمرار کسب‌وکار

نویسندگان

لوری کو (Lory Kehoe)
مدیرعامل، دیلویت ایرلند
E:lkehoe@deloitte.ie

اریک پسینی (Eric Piscini)
سرپرست، دیلویت آمریکا
E:episcini@deloitte.com

پائول سین (Paul Sin)
عضو، دیلویت هنگ کنگ
E:psin@deloitte.com.hk

ایان کونولی (Eoin Connolly)
معمار فنی، دیلویت ایرلند
E:econnolly@deloitte.ie

تقدیر ویژه از

نیام اوکانل (Niamh O`Connell)
مشاور، دیلویت ایرلند
E:nioconnell@deloitte.ie

گیلهرم کمپوس (Guilherme Campos)
مشاور ارشد، دیلویت ایرلند
E:gucampos@deloitte.pt

فهرست

۱. بست‌پرکتیس - استانداردی برای توسعه بلاکچین ۰۷
۱.۱ حکومت ۰۷
۱.۱.۱ کنسرسیوم ۰۸
۱.۱.۲ سرمایه‌گذاری مشترک ۰۹
۱.۱.۳ تشکیلات قانونی ۰۹
۱.۲ قانون و نظارت ۰۹
۱.۳ استانداردها ۱۰
۱.۳.۱ برقراری ارتباط با سازمان‌های استانداردسازی ۱۱
۱.۳.۲ پذیرش استانداردهای موجود و وضع استانداردهای فنی جدید ۱۱
۱.۳.۳ ارتقای قراردادهای هوشمند ۱۱
۱.۳.۴ امنیت سایبری قراردادهای هوشمند ۱۱
۱.۳.۵ رابط های قراردادهای هوشمند ۱۲

۲. تعامل‌پذیری و کنترل یکپارچگی سیستم ۱۵
۲.۱ ملاحظات امنیتی ۱۵
۲.۲ ادغام با سیستم‌های منسوخ ۱۵
۲.۳ ادغام داده‌ها ۱۶
۲.۴ سازوکارهای امنیتی ۱۷

۳. قوانین حسابرسی ۱۹
۳.۱ ثبت بدون تغییر ۱۹
۳.۲ حسابرسی قراردادهای هوشمند ۱۹
۳.۳ کنترل‌های فنی ۲۰
۳.۴ تحولات حسابرسی ۲۱

۴. کنترل‌های امنیت سایبری ۲۳
۴.۱ چالش‌های امنیت سایبری دفاتر کل توزیع شده ۲۳
۴.۲ قراردادهای هوشمند ۲۴
۴.۳ استانداردهای کنترل ۲۵
۴.۴ قدرت امنیت سایبری دفاتر کل توزیع شده ۲۵

۵. بهبود پروتکل‌های اطلاعات و ارتباطات سنتی ۲۷
۵.۱ مدیریت امنیت ۲۷
۵.۱.۱ طبقه‌بندی و حفاظت از اطلاعات ۲۷
۵.۱.۲ احراز هویت و کنترل دسترسی ۲۷
۵.۱.۳ مدیریت امنیت و نظارت ۲۷
۵.۲ مدیریت تغییر و توسعه سیستم ۲۷
۵.۳ پردازش اطلاعات ۲۸

۶. طرح استمرار کسب‌وکار و بلاکچین ۳۰
۶.۱ طرح استمرار کسب‌وکار ۳۰
۶.۲ طرح استمرار کسب‌وکار و زیرساخت کلیدی عمومی ۳۰
۶.۳ طرح استمرار کسب‌وکار گره‌های شبکه ۳۱
۶.۳.۱ شبکه‌های بلاکچین عمومی ۳۱
۶.۳.۲ شبکه‌های بلاکچین خصوصی ۳۱
۶.۴ متخصصین امنیتی ۳۱

همان‌طور که ساتوشی ناکاموتو (Satoshi Nakamoto) نیز در روایت پیپر بیت‌کوین در سال ۲۰۰۸ میلادی این نوآوری را «یک سیستم پول الکترونیکی همتا به همتا (Peer-to-Peer)» خطاب کرده بود، فناوری بلاکچین را می‌توان یک دفتر کل توزیع شده معرفی کرد که توانسته است توجهات زیادی را در حیطه خدمات مالی به سمت خود جلب کند.

CUSTOMER SER
SERVICE L
TIME SCALE
BIG DATA
FINANCE
NEW BUSINESS
CUSTOMER SERVICE
NEW INFORMATION
GLOBA
40%
27%

بست‌پرکتیس- استانداردی برای توسعه بلاکچین

همان‌طور که ساتوشی ناکاموتو (Satoshi Nakamoto) نیز در وایت پیپر بیت‌کوین در سال ۲۰۰۸ میلادی این نوآوری را «یک سیستم پول الکترونیکی همتا به همتا» خطاب کرده بود، فناوری بلاکچین را می‌توان یک دفتر کل توزیع شده معرفی کرد که توانسته است توجهات زیادی را در حیطه خدمات مالی به سمت خود جلب کند. محققان و سرمایه‌گذاران تمایل زیادی برای بررسی و بهره‌جویی از پتانسیل‌های ساختارشکنانه و تحول‌برانگیز این فناوری دارند تا در خلال آن به دستاوردهایی دست یابند نظیر:

- تسهیل تبادل ارزش
- امکان ذخیره‌سازی ایمن ارزش
- دستیابی به بهره‌وری عملیاتی
- صرفه‌جویی امن در هزینه‌ها
- افزایش شفافیت در صنعت
- ارتقای تجربه مشتری

در این مقاله، سعی کرده‌ایم سه فاکتور مهم تاثیرگذار در پذیرش و توسعه فناوری دفتر کل توزیع شده بلاکچین در صنعت خدمات مالی را مورد بحث و بررسی قرار دهیم.

این سه فاکتور عبارتند از:

۰۱. حکومت

۰۲. قانون و نظارت

۰۳. استانداردها

اگر چه این سه فاکتور، در این مقاله به صورت مجزا مورد بررسی قرار خواهند گرفت، اما بدیهی است که زمانی که پای فناوری دفتر کل توزیع شده به میان بیاید، صنعت خدمات مالی هر سه فاکتور را به شکلی مرتبط و وابسته به یکدیگر پیش رو خواهد داشت.

۱.۱. حکومت

اولین فاکتور کلان حکومت است. گزارش ریسک جهانی اقتصاد (The World Economic Global Risk Report) که در سال ۲۰۱۷ میلادی منتشر شده است، نشان می‌دهد که یک سیستم جامع، یکپارچه و موثر مدیریتی، لازمه پذیرش و به تبع آن توسعه هر نوآوری یا فناوری نوظهوری است.

برای پذیرش و توسعه فناوری دفتر کل توزیع شده بلاکچین در زیرساخت‌های خدمات مالی جهان، در حالت کلی، سه مدل حکومتی می‌تواند پیاده‌سازی شود: کنسرسیومی، سرمایه‌گذاری مشترک و تشکیلات قانونی.

الف) مدل کنسرسیومی، به حالتی اشاره دارد که مجموعه‌ای از دست‌اندرکاران صنعت در خلال تشکیل کنسرسیومی گرد هم آمده و برای دستیابی به هدفی خاص همکاری می‌کنند.

ب) سرمایه‌گذاری مشترک، در حقیقت یک نهاد مجزا و مستقل است که توسط دو یا چند شرکت به وجود می‌آید تا مالکیت، بازگشت سرمایه و ریسک‌های احتمالی را بین این شرکت‌ها تسهیم کند.

پ) سازمان یا تشکیلات قانونی نیز بدنه‌ای است که تشکیل می‌شود تا در خلال آن، کلیه الزامات و ملاحظات نوآوری‌ها و پیاده‌سازی‌ها تحت کنترل یک مقام رگولاتوری انجام گیرند.

بر اساس مدل مدیریتی و حکومتی انتخابی، نحوه حسابرسی‌ها و این‌که چه کسی این حسابرسی را بر عهده خواهد داشت متفاوت خواهد بود. به عنوان مثال، در مدل کنسرسیومی، کمیته حسابرسی منصوب هیات مدیره مسئولیت حسابرسی و ارائه گزارش از نحوه عملکرد کنسرسیوم را برعهده دارد. در مورد فرایند حسابرسی و حسابرس، در فصل سوم به تفصیل بحث خواهد شد.

(الف) کنسرسیوم

ادامه کار در یک مدل حکومتی کنسرسیومی، مبتنی بر تصمیماتی است که توسط اعضای کنسرسیوم اتخاذ می‌شوند. در حقیقت، در چنین مدل‌هایی خبری از نهاد نظارتی و یا چارچوب‌های رگولاتوری نیست و هر یک از شرکت‌کنندگان، گره خود را کنترل و مدیریت می‌کنند. اعضای شرکت کننده در این کنسرسیوم‌ها منابع مختلف را به اشتراک گذاشته و با هم در راستای پیشبرد اهداف کلی کنسرسیوم همکاری می‌کنند. هر بانک، یک نماینده از جانب خود می‌فرستد تا در مباحث شرکت کرده و از منافع آن دفاع کند.

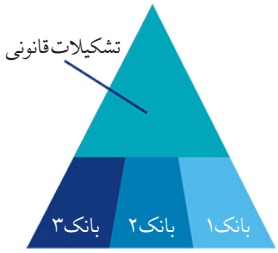
(ب) سرمایه‌گذاری مشترک

ایجاد یک نهاد قانونی و نظارتی مستقل و مجزا، که صاحب پلتفرم است و آن را توسعه می‌دهد. این پلتفرم، ابزاری برای شرکت کنندگانی است که هر یک گره‌های خود را مدیریت و کنترل می‌کنند.

این نهاد به صورت مشترک توسط اعضا (به عنوان مثال بانک‌ها) سرمایه‌گذاری و راه‌اندازی شده است. اعضایی که در حقیقت سهام‌داران اصلی کمیته اجرایی هستند.

(پ) تشکیلات قانونی

این مدل به راه‌اندازی نهاد قانونی کاملا مجزایی اشاره دارد که می‌تواند جداگانه عمل کرده و پلتفرم مشترکی را هدایت و مدیریت کند. کلیه مسئولیت‌های تامین مالی، مدیریت، مالکیت و توسعه پلتفرم در سیستم به عهده این نهاد است. اعضای شرکت کننده در شبکه از دستورالعمل‌های این نهاد نظارتی تبعیت می‌کنند که به پیشبرد اهداف کلی سیستم می‌انجامند. این سازمان می‌تواند نمایندگانی از بانک‌ها را نیز شامل شود.



۱.۱.۱. کنسرسیوم

شکل‌گیری کنسرسیوم برای بسیاری از دفاتر کل توزیع شده خصوصی، یکی از پدیده‌های رایجی است که در دنیای مدرن امروز بسیار به چشم می‌خورد. اعضای کنسرسیوم کلیه هزینه‌های راه‌اندازی، تنظیم و نگهداری را با یکدیگر سهیم می‌شوند، منابع را به صورت مشارکتی گردآوری می‌کنند، تحقیقات لازمه را به انجام می‌رسانند و استانداردهای موردنیاز برای راه‌اندازی و پیاده‌سازی دفاتر کل توزیع شده موردنظر برای اکوسیستم را در کنار هم تعریف و تبیین می‌کنند. استانداردهایی که می‌توانند فرایندها و عملیات اکوسیستم را در چارچوبی که اعضا مدنظر دارند نگه دارند و بلاکچین را کنترل کنند. هر عضو، دارای یک نماینده در کمیته فرماندهی است که از جانب آن‌ها در مذاکرات شرکت کرده و در اتخاذ تصمیمات نهایی دخالت می‌کند. مثال بارزی از این قبیل کنسرسیوم‌ها، کنسرسیوم جدیدی است که بین یوبی‌اس (UBS)، بی‌ان‌وای ملون (BNY Mellon) و دویچه بانک (Deutsche Bank) تشکیل شده است و اخیرا نیز با انجام پروژه Utility Settlement Coin، نوآوری جدیدی در حیطه بلاکچین در صنعت خدمات مالی به بازار معرفی کرده است.

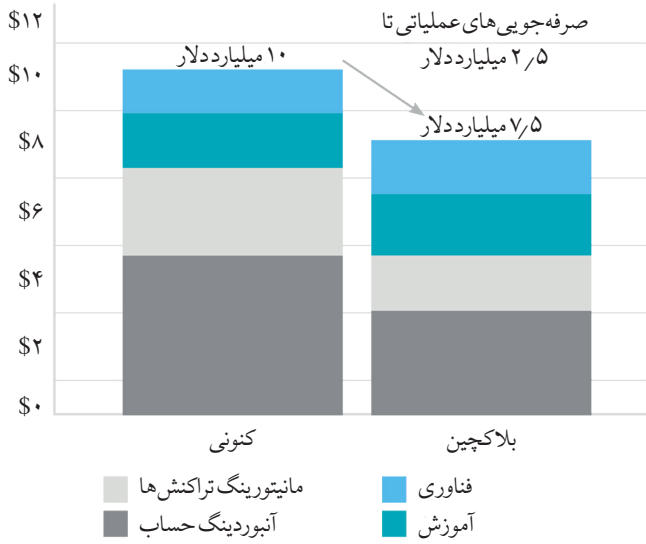
مدل کنسرسیوم، به ویژه در شرایطی که اعضا تمایل زیادی به استفاده از داده‌های به اشتراک گذاشته شده نشان می‌دهند بسیار کاربردی است. اخیرا، کنسرسیوم کاربردی مبتنی بر بلاکچین جدیدی تحت عنوان شناخت مشتری (Know Your Customer) راه‌اندازی شده است که به اعضا این امکان را می‌دهد تا سرمایه‌گذاران بالقوه موجود در سطح بازار را شناسایی کرده و برای استفاده از سرمایه‌های کلان آن‌ها اقدام کنند.

دنیایی را متصور شوید که در آن، فاکتور شناخت مشتری تنها از عهده یک نهاد واحد برآید، این نهاد تنها نهادی است که اطلاعات لازم پیرامون فاکتور شناخت مشتری را گردآوری می‌کند، سرمایه‌گذاری‌ها و هزینه‌های کلان مرتبط با این فاکتور مهم را به دوش می‌کشد و دیگر شرکت‌ها و سازمان‌ها، تنها کافی است در فرایندهای اعتبارسنجی و تایید کنسرسیوم شرکت کرده و از داده‌های به اشتراک گذاشته شده نهایت استفاده را ببرند.

بر اساس گزارشی که در سال ۲۰۱۶ میلادی از سوی گلدمن ساکس (Goldman Sachs) منتشر شده است، فناوری «بلاکچین: گذار از تئوری به عمل» است و سیستم‌های بانکداری می‌توانند از قبل این گذار، بالغ بر ۱۰ درصد از هزینه‌های سرانه خود را بکاهند و کنترل‌های تراکنشی خود را نیز تا بیش از ۳۰ درصد افزایش دهند. این گزارش تخمین می‌زند که مجموع صرفه‌جویی در هزینه‌های ناشی از این فناوری ساختارشکن می‌تواند مرز ۲.۵ میلیارد دلار را نیز رد کند که رقمی قابل تامل است.

با وجود این که منافع مشترک مدل کنسرسیومی نظیر ریسک، دانش و آی‌پی (IP) مشترک جذاب هستند، با این حال ممکن است فرایندهای تصمیم‌گیری در این قبیل مدل‌ها وقت‌گیر باشند. به ویژه که امکان به وجود آمدن درگیری میان اعضای کنسرسیوم در برخی شرایط بالا است.

بدیهی است، در شرایطی که سطح اعتماد در کنسرسیوم پایین است، اعضا تنش‌های بسیاری را هنگام فرایندهای تصمیم‌گیری متحمل خواهند شد و این تنش‌ها، بیش از پیش نیز به عدم اطمینان جاری و ساری در اکوسیستم خواهد افزود. این مشکل، موضوع مهمی است که با استفاده از فناوری، چه دفتر کل توزیع شده و چه سایر فناوری‌ها، قابل حل نیست. در همین راستا، در صورت اتخاذ مدل کنسرسیومی به عنوان مدل حکومتی اکوسیستم، کلیه پروتکل‌های تصمیم‌گیری باید در ابتدای امر تعریف شده، مورد بحث و بررسی قرار گیرند و کلیه اعضا در مورد آن‌ها به توافق نظر برسند تا در دراز مدت، از درگیری‌های احتمالی و تنش بین اعضا جلوگیری شود.



۱.۱.۲. سرمایه‌گذاری مشترک

سرمایه‌گذاری‌های مشترک، نهادهای جداگانه‌ای هستند که توسط دو یا چند شرکت تشکیل شده‌اند و می‌توانند با سرعت بخشیدن به اتخاذ تصمیمات، بسیاری از روندها و فرایندهای سازمانی را تسهیل و تسریع کنند. از آن‌جایی که شرکت‌ها و سازمان‌ها اشخاصی حقوقی در نظر گرفته می‌شوند، پروتکل‌ها، استانداردها و دستورالعمل‌ها در این مدل مدیریتی در همان ابتدای امر تعریف می‌شوند و در حالت کلی، درگیری و اختلاف برای تصمیم‌گیری نیز در این مدل نسبت به مدل کنسرسیومی بسیار کمتر است. مدل سرمایه‌گذاری مشترک، روی فرایندها و فعالیت‌هایی تمرکز دارد که می‌توانند سودآوری و بهره‌وری در اکوسیستم را افزایش دهند. این روند، به ویژه زمانی که سهامداران و دست‌اندرکاران اکوسیستم در حیطه‌های مختلفی مشغول فعالیت باشند بسیار نتیجه‌بخش است.

تامین مالی تجاری، یکی از حوزه‌هایی است که می‌تواند مثال خوبی برای این مدل مدیریتی جامع باشد. سیستم‌های بانکداری، رگولاتورها و شرکت‌های وارد کننده و صادرکننده محصولات در اکوسیستمی گرد هم آمده و یک نهاد مبتنی بر سرمایه‌گذاری مشترک راه‌اندازی می‌کنند که بر پایه فناوری بلاکچین بنا شده است. کلیه استانداردها و پروتکل‌ها در همان ابتدای راه‌اندازی و با توافق کلیه اعضا تعریف می‌شوند و دفتر کل توزیع شده به وجود آمده، کلیه اطلاعات، دارایی‌ها و فاکتورهای لازم برای سودآوری و بهره‌وری را در خود نگهداری کرده و مدیریت می‌کند.

در این مدل، کلیه کنترل‌ها و تصمیم‌گیری‌ها توسط نهاد سرمایه‌گذاری مشترک صورت می‌گیرد و اعضا، به صورت مستقیم نقشی در این تصمیم‌گیری‌ها نداند. سود به دست آمده در خلال این مشارکت نیز نسبت به سهمی که هر یک در نهاد سرمایه‌گذاری مشترک دارند تسهیم می‌شود و بدین ترتیب، بهترین تصمیم، در سریع‌ترین زمان، به ساده‌ترین روش و بدون درگیری اتخاذ می‌شود.

در دنیای مدرن امروز، تشکیل نهادهای سرمایه‌گذاری مشترک بین شرکت‌های فین‌تکی و سیستم‌های بانکداری بسیار شایع شده است. به عنوان مثال، شرکت فین‌تکی چینی کردیت (Credit China Fintech) با بیتفیوری (Bitfury) وارد معامله‌ای ۳۰ میلیون دلاری شده است تا در خلال تشکیل یک نهاد سرمایه‌گذاری مشترک، روی بازار چین تمرکز کنند. نوآوری‌های این نهاد، تاکنون منجر به ارائه یک نمونه آزمایشی سیستم وام‌دهی همتا به همتا و یک دفتر کل توزیع شده برای فرایندهای پرداخت شده است.

در حال حاضر، بهترین راه برای مشارکت سیستم‌های بانکداری با شرکت‌های فین‌تکی همین کنسرسیوم‌ها و نهادهای مشترک است. رویکردی که به بانک‌ها این امکان را می‌دهد تا از دستاوردها و نوآوری‌های عجیب و جالب توجه شرکت‌های فین‌تکی استفاده کنند و برای شرکت‌های فین‌تکی نیز فرصتی را فراهم می‌سازد تا از پایگاه کاربری هنگفت سیستم‌های بانکداری بهره‌مند شوند و با تکیه بر توانمندی‌های کلان موسسات مالی ایده‌های خود را عملی سازند.

فناوری بلاکچین، یکی از فناوری‌های نوظهور و ساختارشکنی است که عمده نوآوری‌ها و محصولات شرکت‌های فین‌تکی را به خود اختصاص داده است و در این میان، با توجه به این‌که این فناوری هنوز در نخستین مراحل رشد و پویایی خود قرار دارد، انتظار می‌رود طی سال‌های اخیر سال‌های تشکیل نهادهای سرمایه‌گذاری مشترک و کنسرسیوم‌های بسیاری مبتنی بر این فناوری باشیم. بدون شک، حجم قابل توجهی از موسسات مالی و سیستم‌های بانکداری به سمت این قبیل مشارکت‌ها سرازیر خواهند شد تا شانس خود را برای پیاده‌اسزی این نوآوری نوظهور آزموده و سپس آن را در زیرساخت‌های بانکی خود نهادینه کنند.

۱.۱.۳. تشکیلات قانونی

در مدل تشکیلات قانونی، اعضای شرکت کننده (از جمله سیستم‌های بانکداری و موسسات مالی)، ملزم به پیروی از دستورالعمل‌های این سازمان و حرکت به سمت هدفی هستند که از سوی آن تبیین شده است. به عنوان مثال، اداره سازمان پولی پرداخت الکترونیک سنگاپور (Monetary Authority of Singapore Electronic Payment System)، یک سیستم پرداخت بین بانکی و سیستم نقل و انتقال موجودی آنلاین است که تحت پوشش تشکیلات قانونی فعالیت می‌کند. از جمله مزایای مهم این مدل مدیریتی، شفافیت و تسلط بر داده‌ها است.

رگولاتورهایی که به عنوان ناظرین و کنترل کنندگان اکوسیستم انتخاب می‌شوند، این امکان را به سایر اعضا می‌دهند تا در نهایت شفافیت و اعتماد فعالیت کنند و مسئولیت تعریف و پیاده‌سازی استانداردها را نیز بر عهده دارد. البته، انتخاب این عنصر رگولاتور، خود از اهمیت بالایی برخوردار است چرا که باید بتواند صحت و کفایت استانداردهای تبیین شده را تضمین کرده و آن‌ها را موازی با حریم خصوصی اعضا به پیش ببرد. ضمن این‌که، این عنصر باید قادر باشد به کلیه اصول پایبند بوده و حقوق اعضا را تامین کند و در عین حال، کمترین حاشیه ریسک را برای اکوسیستم رقم بزند. مدل تشکیلات قانونی را می‌توان مناسب‌ترین گزینه برای گزارشات رگولاتوری تلقی کرد.

دفاتر کل توزیع شده خصوصی، این قابلیت را دارند تا در چارچوب مدل تشکیلات قانونی، منبعی برای ثبت و نگهداری داده‌های سیستم‌های بانکداری و سیستم‌های رگولاتوری باشند و با به اشتراک‌گذاری این داده‌ها، هر دو سیستم را اغنا سازند. با این حال، با توجه به این‌که سیستم‌های رگولاتوری چندان تمایلی به فناوری‌های مدرن نشان نمی‌دهند و به ویژه در مورد فناوری دفتر کل توزیع شده بلاکچین موضع مغرضانه‌ای در پیش گرفته‌اند، این مدل با برخی ابهامات و ناملایمات نیز روبه‌رو خواهد بود. مگر این‌که سیستم‌های بانکداری، خود در میان خود تصمیم به اتخاذ این مدل و ثبت و ذخیره‌سازی داده‌های مالی روی یک دفتر کل توزیع شده گرفته باشند و متعاقب آن، سیستم‌های رگولاتوری را نیز برای نظارت بر این دفتر کل توزیع شده متقاعد سازند.

۱.۲. قانون و نظارت

برای به حداکثر رساندن اثربخشی، تجاری‌سازی فناوری دفتر کل توزیع شده بلاکچین مستلزم قانون و چارچوب‌های رگولاتوری و نظارتی است. بنابراین، دومین فاکتور تاثیرگذار در پذیرش و به دنبال آن توسعه راهکارهای مبتنی بر فناوری بلاکچین در صنعت خدمات مالی قانون و نظارت است.

هر سه مدل مدیریتی که در بالا توضیح داده شدند، به قانون و چارچوب‌های رگولاتوری نیازمند هستند. تشکیل کمیته‌هایی قانونی و حقوقی که بتواند این نیاز مهم را به ویژه در دنیای پرهرج و مرج و داده‌محور امروز پاسخ گوید، از اهمیت بالایی برخوردار است.

به این منظور، بسیاری از شرکت‌های فین‌تکی، موسسات مالی و سیستم‌های بانکداری یا هر نهادی که در حیطه خدمات مالی فعالیت می‌کند، سعی می‌کند تا با نهادهای رگولاتوری همکاری کند و از قدرت و قابلیت‌های این نهادها برای پذیرش و توسعه نوآوری‌های مبتنی بر فناوری دفتر کل توزیع شده خود بهره جوید.

از منظر فنی و حقوقی، فقدان وضوح کافی پیرامون قراردادهای هوشمند، از جمله ابهاماتی است که سبب کندتر شدن پذیرش و توسعه فناوری بلاکچین شده و ریسک‌هایی را در پیاده‌سازی این فناوری در مقیاس عملی به وجود آورده است. برای رفع این ابهامات و پاسخ‌گویی به این ریسک‌ها، قراردادهای هوشمند مبتنی بر دفتر کل توزیع شده بلاکچین نیز باید تحت

چارچوب‌های رگولاتوری و به روشی مشابه با قراردادهای عادی انجام شوند.

تعهدات زمان واقعی، پاداش‌ها و تحریم‌ها، از جمله موارد مهمی در بلاکچین هستند که باید تحت نظارت کامل و با توجه به عملکرد هر یک از اعضای شبکه انجام شوند. یکی از مهم‌ترین تفاوت‌هایی که قراردادهای هوشمند مبتنی بر دفاتر کل توزیع شده با قراردادهای به اصطلاح کاغذی حال حاضر دارند این است که در این قراردادها، طرف اول قرارداد را به زبانی کاملا علمی و کامپیوتری نگارش کرده و در بستر بلاکچین ارائه کرده است و طرف یا طرفین دوم نیز این قرارداد را بی‌کم‌وکاست دریافت کرده‌اند؛ بدون این‌که پای شخص ثالثی در میان باشد.

در نتیجه، برخی ابهامات در این فرایند وجود دارد و طرفین، رلاهی ندارند جز این‌که به یکدیگر اطمینان داشته باشد (چرا که شخص ثالث مورد اعتماد هر دو طرف که قرارداد را نیز ضمانت می‌کند وجود ندارد). البته، این قراردادها مزایای فراوانی را برای موسسات مالی و سیستم‌های بانکداری در پی دارند و در صورتی که قانون و نظارت درستی روی آن‌ها پیاده شود، بسیار کارآمد هستند. از جمله مزایای قراردادهای هوشمند برای دست‌اندرکاران صنعت خدمات مالی، اجرای توافق‌نامه‌های حقوقی از طریق کد، دسترسی به یک پایگاه-یا فروشگاه-داده جامع و غیرقابل تغییر بدون نیاز به وجود عناصر سوم شخص قابل اعتماد و همچنین پتانسیل به اشتراک‌گذاری داده‌ها با تنظیم‌گنندگان و رگولاتورهای مالی است.

با وجود این‌که قراردادهای هوشمند این قابلیت را دارند تا به عنوان پلتفرم‌های قانونی عمل کنند، اما برای دستیابی به این مرحله، یک فرایند پیچیده دو مرحله‌ای نیاز است. قبل از این‌که موسسات مالی و سیستم‌های بانکداری نسبت به جایگزینی این قراردادهای نوین هوشمند با قراردادهای مبتنی بر کاغذ منسوخ کنونی اقدام کنند، لازم است برخی الزامات رگولاتوری روی آن‌ها پیاده‌سازی شود و این قراردادها، بر اساس برخی چارچوب‌های قانونی تعریف شوند تا در ادامه، مشکلی پدید نیاورند. الزاماتی که محلی و منطقه‌ای هستند و می‌توانند کلیه موسسات مالی، بانک‌ها، شرکت‌های فین‌تکی، کاربران و چارچوب‌های نظارتی و دولتی منطقه را تحت‌الشعاع قرار دهند. به علاوه، برای تسهیل تعاملات با سایر نهادهای برون مرزی نیز برخی الزامات و تمهیدات خارج از منطقه‌ای و غیربومی لازم است تا تعریفی یکپارچه و قابل اجرا از قراردادهای هشمند ارائه شود. تعریفی که بتوان در سایه آن، قراردادهای جامع، جهانی و قابل اعتمادی برای هر نقطه از جهان عرضه کرد. بدیهی است که دستیابی به چنین موقعیتی بسیار دشوار و هزینه‌بر خواهد بود. در غیاب مقررات پیشگیرانه و یا تصمیمات رگولاتوری در مورد نحوه اجرای قراردادهای هوشمند، ممکن است موسسات مالی و سیستم‌های بانکداری، در برخی از حوزه‌های قضایی قادر به توجیه و توسعه راهکارهای مدرن مبتنی بر فناوری بلاکچین خود نباشند و از ادامه مسیر باز بمانند.

سایر ملاحظات دستیابی به چارچوب‌های رگولاتوری و قوانین باکیفیت‌تر برای پذیرش و توسعه راهکارهای مبتنی بر دفاتر کل توزیع شده:

- همکاری بین نهادهای مبتنی بر سرمایه‌گذاری مشترک و مقامات صنعت خدمات مالی، به منظور تنظیم مقررات در سطح منطقه‌ای یا در مقیاس جهانی.
- بازنگری در نحوه قانونمندسازی شرکت‌کنندگان، و نحوه دسترسی سیستم‌های رگولاتوری به داده‌ها در زمان واقعی با استفاده از فناوری دفتر کل توزیع شده بلاکچین. فناوری بلاکچین، به این مفهوم نیست که سیستم‌های رگولاتوری به صورت مستقیم به کلیه داده‌ها و سیستم‌های داخلی بانک‌ها و موسسات مالی دسترسی داشته باشند، بلکه به مفهوم دسترسی به دفتر کل توزیع شده‌ای مشترک از داده‌ها است که در آن، همه اعضا به یک اندازه و در شفافیت کامل به اطلاعات دسترسی دارند و هیچ‌کس، حق هیچ‌گونه دستکاری یا تغییری در این داده‌ها ندارد.
- تعریف مجدد چارچوب‌های رگولاتوری به محض ورود به مقیاس برون مرزی

از آن‌جا که مدل مدیریتی تشکیلات قانونی از سوی بسیاری از شرکت‌ها و نقش‌آفرینان صنعت خدمات مالی مورد پذیرش واقع شده است، لازم است در مورد توافق کامل کلیه بانک‌ها و موسسات مالی با کمیته رگولاتوری و چارچوب‌های تبیین شده توسط این کمیته اطمینان حاصل شود. هرگونه مخالفت یا عدم موافقتی در این خصوص می‌تواند به شکست قطعی پروژه‌ها و نوآوری‌های مبتنی بر دفتر کل توزیع شده بلاکچین بیانجامد و سایر اعضای اکوسیستم را نیز از دستیابی به اهداف خود بازدارد.

قبل از سرمایه‌گذاری روی یک راهکار مبتنی بر فناوری دفتر کل توزیع شده، کلیه رویکردها، دستورالعمل‌ها و الزامات حفاظت از داده باید توسط سیستم‌های رگولاتوری به طور کامل مورد بررسی قرار گرفته و تایید شوند. کلیه خط مشی‌ها و پروتکل‌ها نیازمند ارزیابی و تایید توسط بدنه‌های رگولاتوری هستند تا پس از بررسی و تایید طراحی، اصلاح یا بازطراحی شوند و سپس مورد استناد و استفاده قرار گیرند.

در خلال پایبندی به حقوق مالکیت فکری (IP rights)، توصیف روشنی از صاحبان پروژه‌های مبتنی بر دفاتر کل توزیع شده وجود خواهد داشت و این‌که چه کسانی، راهکار مبتنی بر بلاکچین مورد را در اختیار دارند و این شفافیت می‌تواند در ادامه مسیر، منجر به پذیرش کامل دفتر کل، توسعه آن و بهره‌وری‌اش شود.

این موضوع می‌تواند هم در مورد خود دفتر کل توزیع شده و هم در مورد قراردادهای هوشمند مبتنی بر آن صادق باشد. به ویژه زمانی که از مدل مدیریتی کنسرسیومی استفاده می‌شود، تشخیص و تبیین این‌که چه کسی مالک، طراح یا ارائه دهنده حقیقی راهکاری مبتنی بر بلاکچین مورد نظر است بسیار دشوار است و در عین حال، رسیدن به توافق جمعی در مورد اعضای احتمالی نیز امری بسیار دشوار است. صرف نظر از مدل مدیریتی انتخاب شده، این مالکیت باید در چارچوب یک قرارداد قانونی نیز قابل اجرا باشد. از منظر حفاظت از اطلاعات نیز باید در نظر داشت که داده‌های آن چین (on-chain) باید دارای محدودیت‌هایی برای اعضا در برخی از فیلدها باشند در حالی که هیچ‌گونه محدودیتی برای داده‌های آف چین وجود ندارد و این داده‌ها می‌توانند به‌صورت آزادانه در خلال شبکه در جریان باشند. این امر، فارغ از نوع مدل مدیریتی اتخاذ شده، به نحوه تعریف پروتکل‌های دفتر کل توزیع شده بستگی دارد. علاوه بر این، انعطاف‌پذیری داده‌ها نیز باید توامان با پایبندی به مقررات حفظ حریم خصوصی و حفاظت از اطلاعات رعایت شود. اطلاعات شخصی قابل شناسایی، از جمله داده‌هایی هستند که علیرغم نیاز به انعطاف‌پذیری و اشتراک بین اعضا، از حساسیت بالاتری برخوردارند و ثبت آن‌ها، اشتراکشان و استفاده ابزاری از آن‌ها مستلزم برخی الزامات و ملاحظات ویژه از سوی کلیه اعضای شرکت کننده در اکوسیستم است.

در نهایت، نگهداری این داده‌ها نیز برخی ملاحظات را می‌طلبد. به عنوان نمونه، مهم‌ترین فاکتوری که باید در خصوص نگهداری از داده‌ها، به ویژه داده‌های شخصی قابل شناسایی کاربران مدنظر داشت، طراحی و تثبیت زیرساخت‌های شبکه است. زیرساخت‌هایی که در سایه فناوری بلاکچین، امکان هرگونه دستکاری، حذف یا ایجاد اختلال در داده‌ها را از کلیه اعضای اکوسیستم ساقط کرده و در خلال قوانین و چارچوب‌های رگولاتوری، ثبت و نگهداری این داده‌ها را به بهترین شکل ممکن کنترل می‌کند.

۱.۳. استانداردها

سومین فاکتور کلان تاثیر گذار روی پذیرش و توسعه راهکارهای مبتنی بر

بلاکچین در صنعت خدمات مالی استانداردها هستند. استانداردهایی که می‌توانند پذیرش فناوری دفتر کل توزیع شـــده در صنعت خدمات مالی را سرعت ببخشـــند و این فناوری را وارد زیرساخت‌های بانکی و مالی جهان کنند. مثال بارزی از این قبیل اســـتانداردها، اســـتاندارد آن ادیفکت (UN EDIFACT) ســـال ۱۹۸۷ میلادی و یا اســـتاندارد ISO 2002212 است که طی آن، ســـازمان‌ها و موسســـات مالی بنامی همچون سوئیفت (SWIFT)، ویزا (Visa) و آی‌اس‌دی‌ای (ISDA) پیام‌های مالی مبتنی بر ایکس‌ام‌ال (XML) خود را ارســـال می‌کنند. یکـــی از پروپوزال‌های استانداردسازی دفتر کل توزیع شده بلاکچین، که اخیرا توسط اداره استاندارد ملی استرالیا مطرح شده اســـت، در حال حاضر توسط سازمان بین‌المللی استانداردســـازی (International Organization for Standards) در حال بررسی اســـت. پروپوزالی که بر روی استانداردسازی فناوری دفتر کل توزیع شـــده بلاکچین برای تعامل‌پذیری و تبادل داده‌ها میان کاربران، اپلیکیشن‌ها و سیســـتم‌ها متمرکز شده اســـت. گفتنی است، اولین جلسه رسمی این استاندارد، در ماه آوریل سال ۲۰۱۷ میلادی در سیدنی برگزار شد.

۱.۳.۱. برقراری ارتباط با سازمان‌های استانداردسازی

ایجاد مشارکت و برقراری ارتباط با سازمان‌های استانداردسازی بین‌المللی، این فرصت را به یک شرکت می‌دهد تا به عنوان پیشتاز و رهبر سایر شرکت‌ها در زمینه تعریف و توســـعه اســـتانداردها حرکت کند. این که یک شـــرکت قادر باشـــد با ایجاد پـــل ارتباطی میان خـــود و ســـازمان‌های بین‌المللی استانداردسازی، در تعریف و تبیین استانداردهای فناوری دفتر کل توزیع شده مشارکت داشته و یکی از دست‌اندرکاران استارندردهای بلاکچین در سطح جهان باشد، امتیاز مهمی به شمار می‌آید.

این گروه‌های کاری استانداردسازی را می‌توان صرف‌نظر از مدل مدیریتی اتخاذ شده تشکیل داد. بدیهی اســـت که دست‌اندرکاران صنعت خدمات مالی، در صورتی که به دنبال پذیرش و به تبع آن توســـعه راهکارهای مبتنی بر فناوری دفتر کل توزیع شـــده بلاکچین در سطح جهانی و در سطح کلیه صنایع باشند، راهی ندارند جز این که در این قبیل گروه‌ها شرکت کنند و بدین ترتیب، با استانداردسازی راهکارهای بلاکچین خود در مقیاس منطقه‌ای و فرامنطقه‌ای، راه را برای موفقیت خود و نوآوری‌شان باز کنند. به عنوان مثال، می‌توان مشارکت دیلویت و ایریش فاندز (Irish Funds) را عنوان کرد که با تشکیل یک گروه در ایرلند، برای تعریف و توســـعه گواه اثبات مفهوم در این منطقه تلاش می‌کنند و سعی دارند روی بازپرداخت‌ها و بازگشت‌های صندوق سرمایه‌گذاری تمرکز کنند.

مشارکت و همکاری با بدنه‌های استانداردسازی، از این منظر نیز می‌تواند برای موسسات سودمند باشد که به آن‌ها نشان می‌دهد چه نوع مدل حکومتی را برای سیستم خود اتخاذ کنند تا موفق‌تر باشند. این که تشکیل کنسرسیوم سودمندتر است یا سرمایه‌گذاری مشترک.

با این حال، برای سیستم‌هایی که مدل تشکیلات قانونی را انتخاب کرده‌اند، علیرغم این که ایجاد، توزیع و اجرای اســـتانداردهای تعیین شده از سوی سیستم رگولاتوری با سرعت و سهولت بیشتری در میان اعضا انجام می‌شود، اما تعریف پارامترهای استانداردســـازی با مشکلات قابل توجهی در کوتاه مدت و میان مدت همراه خواهد بود. دلیل این امر نیز آن است که در برخی موارد، راهکارها و استانداردهایی که مطرح می‌شـــوند، نمی‌توانند توجه، اعتماد و تمایل همه رگولاتورها را به سمت خود جلب کنند.

۱.۳.۲. پذیرش استانداردهای موجود و وضع استانداردهای فنی جدید

توسعه استانداردهای فنی، این امکان را به موسسات مالی و بانک‌ها می‌دهد تا با بهره‌مندی از مکانیسم‌های ارتباطی متداول و متناسب، به مقیاس‌پذیری و تعامل‌پذیری قابل توجهی در سطح جهانی دســـت یابند. به عنوان مثال، استاندارد مجموعه قوانین متحدالشکل اعتبارات اسنادی (UCP600) یکی از استانداردهای رایجی است که می‌تواند کمک شایانی به مقیاس‌پذیری و تعامل‌پذیری سازمان‌های مالی در ســـطح جهانی کند. یا استاندارد ام‌تی ۷۹۸ (MT798) ســـوئیفت (SWIFT)، که در ثبت، صدور و تضمین اعتبارنامه‌ها نقش بسزایی دارد.

کار با رگولاتورها و ســـازمان‌های بین‌المللی، گامی اساســـی در توســـعه استانداردهای مبتنی بر داده الکترونیک در فناوری دفتر کل توزیع شده است. به ویژه زمانی که پای مدیریت قراردادهای هوشمند، امنیت و پروتکل‌های رابط کاربردی نیز به میان می‌آید.

استانداردهای فنی موردنیاز برای مدیریت قراردادهای هوشمند باید بتواند موارد زیر را پوشش دهد:

- ارتقاپذیری
- امنیت
- استانداردسازی رابط‌ها

۱.۳.۳. ارتقاپذیری قراردادهای هوشمند

قراردادهای هوشمندی که در ســـطح یک بلاکچین پیاده‌سازی می‌شوند، محتوی رابط‌های کاربردی، خط‌مشی‌های کسب‌وکاری و داده هستند. کلیه این پارامترها، در خلال طول عمر پلتفرم به مرور دســـتخوش تغییر و تحول می‌شوند. به همین دلیل نیز حیاتی است که الگوهای طراحی این قراردادها، به نحوی باشـــند که در صورت نیاز، امکان افزودن برخـــی توابع جدید و ضروری به سیســـتم را فراهم کنند یا بتوانند برخـــی از توابعی که غیرلازم، مشکل‌ساز یا خراب هســـتند را از شـــبکه حذف کنند. کدهایی که در این قراردادها پیاده‌شده‌اند، باید مدام قابل تغییر باشند حتی اگر این تغییرات برای حفظ سازگاری با نسخه‌های جدید پلتفرم اصلی بوده باشند. در عین حال، حتی کدهای نوشته شده برای پلتفرم‌های تغییرناپذیر نیز باید قابلیت تغییر داشته باشند تا از منسوخ شدن زودهنگام پلتفرم طی زمان جلوگیری شود. در آینده‌ای نه چندان دور، شاید امکان مهاجرت داده‌ها از یک قرارداد هوشمند مبتنی بر بلاکچین به قراردادی دیگر نیز وجود داشته باشد. به همین علت، طراحی، کدنویسی و تولید قراردادهای هوشمند باید به نحوی باشد که بتواند مهاجرت داده‌ها یا هر نوآوری نوین دیگری در این عرصه را پشتیبانی کند.

۱.۳.۴. امنیت سایبری قراردادهای هوشمند

با در نظر گرفتن قراردادهای هوشمند مبتنی بر فناوری دفتر کل توزیع شده بلاکچین، به عنوان قراردادهایی کاملا قانونی، برخی ملاحظات و الزامات امنیت ســـایبری جدید نیز نیاز خواهد بود تا امکان ثبت، ذخیره‌ســـازی و نگه‌داری امن داده‌ها در محیطی ســـالم را ضمانت کند. با این وجود، شاید خالی از لطف نباشـــد که بدانیم در حال حاضر نیز حجـــم این الزامات و ملاحظات کم نیســـت و راهکارهای امنیت ســـایبری متعددی روی دفاتر کل توزیع شـــده در حال اجرا اســـت. در عین حال، این نکته نیز از اهمیت بالایی برخوردار است که بدانیم بخش قابل ملاحظه‌ای از این استانداردها و ملاحظات امنیت سایبری، در سال‌های آتی نیز به کار خود ادامه خواهند داد. در فصل چهارم، به تفصیل در خصوص امنیت ســـایبری در بلاکچین بحث خواهیم کرد.

هر کدی که برای پوشش امنیتی قراردادهای هوشمند توسعه داده می‌شود، باید از بهترین راهکارهای امنیتی بهره برده باشـــد و توسط رگولاتورها نیز به صورت کامل مورد بررســـی و ارزیابی قرار گرفته باشد تا اطمینان حاصل شود که ناکارآمدی‌ها و نواقص موجود در کدهای سابق برطرف شده است

و راهکارهای جدید امنیتی نیز در این کدها جای داده شده است. ابزارهای خودکار، در حالی که در پلتفرم بلاکچین وجود داشته باشند، در حذف برخی از فرایندها و فعالیت‌های دستی مورد نیاز برای این بررسی‌ها و ارزیابی‌ها مفید خواهند بود.

۱.۳.۵. رابط های قراردادهای هوشمند

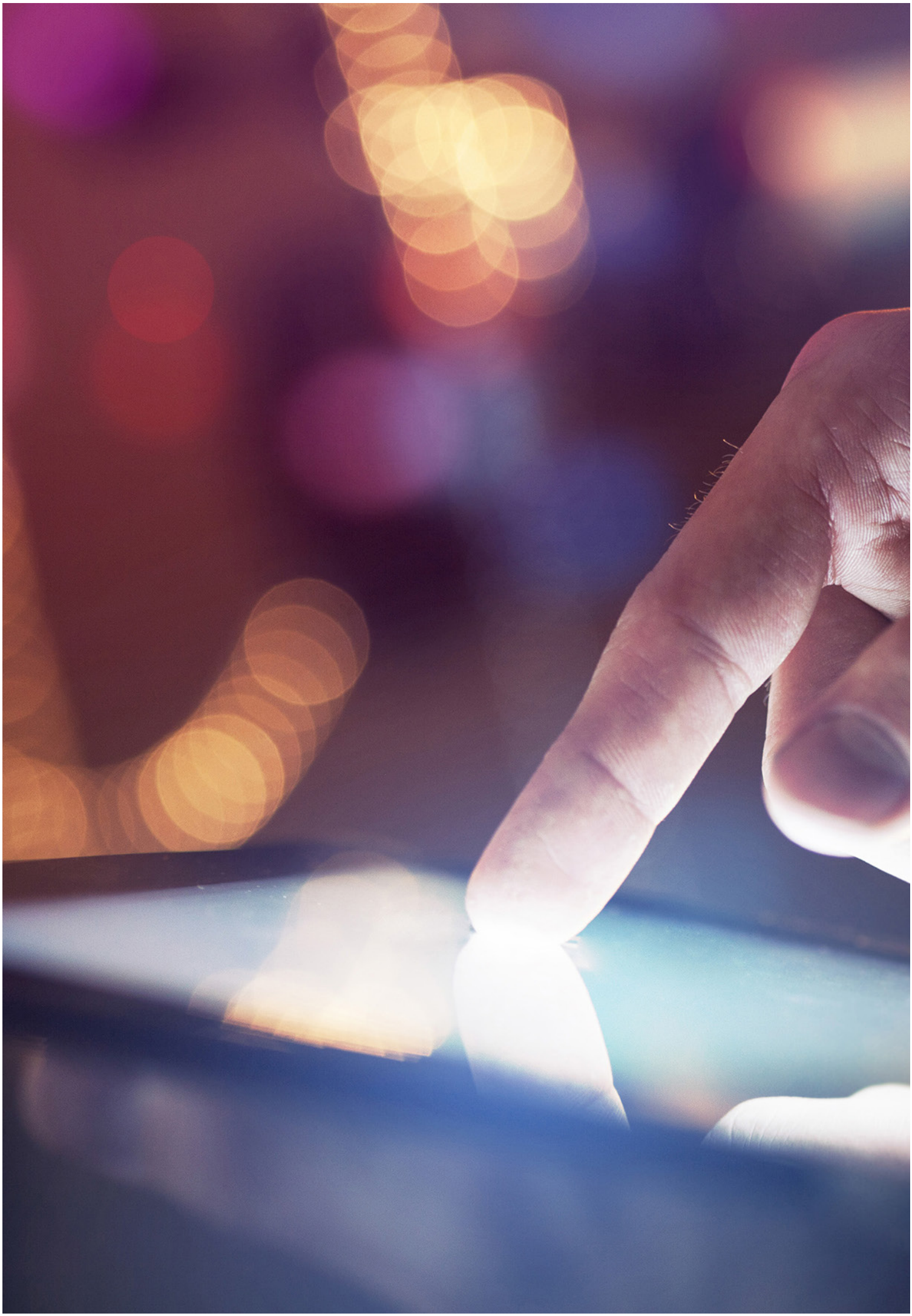
در مبحث قراردادهای هوشمند مبتنی بر دفاتر کل توزیع شده بلاکچین، دو نوع رابط باید مد نظر قرار گیرد. اولین رابطی که در این قراردادها باید مد نظر قرار گیرد، رابط های بین قراردادها هستند. رابط هایی که تعیین کننده نحوه ورود و خروج داده‌ها به قراردادها و میزان تعامل‌پذیری فی‌مابین قراردادهای هوشمند و سیستم‌های خدمات مالی مختلف هستند. معمولا، این سطح از تعامل‌پذیری نتیجه کدنویسی سطح بالای قراردادهای هوشمند است، به ویژه زمانی که استانداردهای مناسبی نیز برای سیستم تعریف شده باشند. این رابط‌ها می‌توانند عملکرد قراردادهای هوشمند و تعاملات با سایر قراردادها و سیستم‌ها را به روش‌های متنوعی از جمله سرویس‌های امن وب یا فایل‌های ثابت شده در خلال یک پوشه هدایت کنند.

این، نوع اول رابط‌های قراردادهای هوشمند است که برای هر قرارداد، به شکلی منحصر به‌فرد اعمال می‌شود. نوع دوم رابط‌ها، رابط هایی هستند که مختص یک قرارداد هوشمند خاص نیستند و سایر قراردادها نیز می‌توانند به آن‌ها دسترسی داشته باشند. توسعه رابط‌ها در سطح قراردادهای هوشمند، با فراهم ساختن امکان استفاده قراردادهای هوشمند از هم و داده‌های هم، قابلیت‌های سیستم را ارتقا بخشیده و برنامه‌های کاربردی مبتنی بر بلاکچین بسیاری را در اختیار آن قرار می‌دهد که نهایتا به بهبود نتایج نهایی می‌انجامد. مثال‌های بسیاری برای توسعه این قبیل رابط‌ها وجود دارند که سیستم‌های احراز هویت مدرن مبتنی بر بلاکچین، دارایی‌های توکن‌سازی شده (مثل رابط توکن استاندارد ERC20 اتریوم) و توابع کتابخانه‌ای از آن جمله‌اند.

برقراری ارتباط با قراردادهای هوشمند به روشی متحدالشکل، مستلزم تعریف و توسعه رابط‌های منحصر به‌فرد و مناسبی است که بتوانند نیازهای گروهی موسسات مالی و سیستم‌های بانکداری را برآورده کنند. توسعه خطوط مشی و ابزارهای کنترلی نیز رویکردی است که می‌تواند ادغام موثر و کارآمد سیستم‌های مدرن مبتنی بر قراردادهای هوشمند با سیستم‌های کنونی را فراهم سازد. در فصل سوم این مقاله، در خصوص این موضوع به تفصیل صحبت خواهد شد.

به طور خلاصه، سیستم‌های بانکداری و موسسات مالی ملزم به پذیرش استانداردهای موجود فعلی هستند تا بتوانند از صحت و سقم طراحی، توسعه و نگهداری راه‌کارهای مبتنی بر دفتر کل توزیع شده بلاکچین در محیطی امن اطمینان حاصل کنند. در این میان، برخی استانداردهای جدید نیز باید تعریف شده و در سطح قراردادهای هوشمند توسعه یابند تا بتوانند عملکرد فناوری ساختارشکن بلاکچین در صنعت خدمات مالی را تضمین کرده و به این فناوری در سطح زیرساخت‌های کنونی سیستم‌های بانکداری و سایر موسسات مالی جامه عمل بپوشانند.

سیستم‌های بانکداری و موسسات مالی ملزم به پذیرش استانداردهای موجود فعلی هستند تا بتوانند از صحت و سقم طراحی، توسعه و نگهداری راه‌کارهای مبتنی بر دفتر کل توزیع شده بلاکچین در محیطی امن اطمینان حاصل کرده و از انطباق این راهکارها با شیوه‌های صحیح صنعتی مطمئن شوند.



تعامل‌پذیری و کنترل یکپارچگی سیستم

هنگام معرفی فناوری دفتر کل توزیع شده بلاکچین برای شرکت‌ها، قابلیت تعامل‌پذیری و ادغام این سیستم با سایر سیستم‌ها، از جمله راهکارهای مبتنی بر بلاکچین دیگر یا سایر فناوری‌ها از اهمیت بالایی برخوردار است. حتی در راه‌اندازی دفاتر کل توزیع شده خصوصی نیز فناوری بلاکچین، جزئی بسیار کوچک از شبکه‌ای گسترده است که حاوی تعداد زیادی رابط، سیستم‌های پیام‌رسان، داده‌ها و توابع مربوط به آن‌ها و غیره است و به همین دلیل نیز تمام شرکت‌ها، روی نحوه و میزان تعامل‌پذیری این حجم از سیستم با یکدیگر، ارتباط میان‌آن‌ها و اتصالشان حساس هستند.

۲.۱. ملاحظات امنیتی

یکی دیگر از چالش‌هایی که فناوری دفتر کل توزیع شده با آن روبه‌رو است، ادغام و ائتلاف با ماژول‌های امنیتی سخت‌افزاری (HSMs) برای تولید و ذخیره‌سازی و همچنین زیرساخت‌های امنیتی همچون شبکه‌های خصوصی مجازی (VPNs) است.

چالش‌های مربوط به یکپارچگی دفاتر کل توزیع شده، بیشتر به جنبه‌های امنیتی و مدل امنیتی این فناوری‌ها برمی‌گردد که عمدتا نیز ناشی از زیرساخت کلیدی عمومی (public key infrastructure) است. ثبت و نگارش داده‌ها روی یک بلاکچین، نیازمند یک کلید خصوصی مخصوص است در حالی که خواندن این داده‌ها و اطلاعات از روی آن، مستلزم دسترسی به فایل اصلی است که در تعداد متعددی سرور ذخیره‌سازی شده است و این دسترسی نیز نیاز به وجود مکانیسم‌های رابط در فناوری دفتر کل توزیع شده را پررنگ‌تر می‌سازد.

این رابط‌ها یا اینترفیس‌ها، اغلب با استفاده از یک سیستم اعتبارسنجی شبکه (متصل به دایرکتوری شرکت) یا از طریق یک مکانیسم احراز هویت مبتنی بر پسوورد سفارشی ایمن شده‌اند. این مکانیسم‌های امنیتی چندگانه، باید بتوانند بدون افزایش سطح تماس با حملات سایبری عمل کنند، در حالی که کلیه اطلاعات خودکت و سایر شرکت‌های در ارتباط را نیز در کمال صحت و سلامت نگهداری می‌کنند یا به اشتراک می‌گذارند. این قابلیت، به ویژه در مورد مدل‌های کنسرسیومی، از اهمیت ویژه‌ای برخوردار است.

۲.۲. ادغام با سیستم‌های منسوخ

راهکارهای مبتنی بر فناوری دفتر کل توزیع شده، برای این‌که بتوانند در صنعت خدمات مالی موثر واقع شوند، نیاز به ادغام و ائتلاف با سیستم‌های منسوخ و میرای مالی کنونی دارند که در بسیاری از موارد، هنوز هم حرف اول را می‌زنند. ابررایانه‌ها، سرورهای وب، سرورهای پایگاه داده و امثال آن، هنوز هم جزو مهم‌ترین زیرساخت‌ها، سیستم‌ها و عناصر صنعت خدمات مالی هستند و بلاکچین، در صورتی که به دنبال پذیرش و توسعه باشد، باید بتواند با این سیستم‌ها از در سازگاری وارد شود. مبحث ادغام با سیستم‌های میرا، در حال حاضر یکی از مهم‌ترین مباحث صنعت خدمات مالی است که بسیاری از شرکت‌ها و موسسات مالی را نیز درگیر خود ساخته است.

به عنوان مثال، در یک موسسه مالی که از پردازنده مرکزی استفاده می‌کند، ممکن است داده‌ها و اطلاعات ورودی یا خروجی روی بلاکچین نیاز به بررسی و اعتبارسنجی از طریق سیستم سنتی را داشته باشند تا از پایبندی به خط مشی چندین و چندساله شرکت اطمینان حاصل شود. در چنین حالتی، بدیهی است که سازگاری و ائتلاف بلاکچین با سیستم منسوخ سازمان، از حساسیت بالایی برخوردار خواهد بود.

یکی از مهم‌ترین مشکلاتی که در خصوص فناوری دفتر کل توزیع شده مطرح است، محدودیت دسترسی این فناوری به منابع داده است چرا که یک بلاکچین، تنها به داده‌هایی دسترسی دارد که روی زنجیره آن ثبت شده‌اند. حتی در مورد بلاکچین‌هایی که مجهز به قراردادهای هوشمند هستند نیز، از جمله بلاکچین اتریوم، منابع داده خارج از قرارداد عملا غیرقابل اعتماد و نامعتبر هستند (چرا که این داده‌ها جزو دفتر کل غیرقابل تغییر اصلی به حساب نمی‌آیند). با توجه به این محدودیت ذاتی مهم بلاکچین و قراردادهای هوشمند، بدیهی است که این داده‌ها باید از طریق مکانیسم‌های قابل اطمینانی همچون اوراکل‌ها (oracles) به تعامل درآیند.

رابط‌هایی که بین قراردادهای هوشمند و داده‌های خارج از زنجیره قرار می‌گیرند و تا حدودی این مشکل دفتر کل توزیع شده را حل می‌کنند. این اوراکل‌ها، به قراردادهای هوشمند این امکان را می‌دهند که داده‌های آف‌چین را جذب کرده و از آن‌ها برای نیازهای شبکه استفاده کنند. این رویکرد، چندان هم بی‌تاثیر نبوده است و در حال حاضر، رویکردهای فنی مانند کریپتلس (Cryptlets) در یکی از پروژه‌های مایکروسافت توانسته است با معرفی برخی اوراکل‌های جدید، تا حدودی مشکل دسترسی بلاکچین به منابع داده‌آف‌چین را حل کند.

اغلب مشکلاتی که در خصوص دفتر کل توزیع شده مطرح هستند و نیاز به پاسخ‌گویی دارند، به زیرساخت دفتر کل توزیع شده، مدل‌های امنیتی و پیچیدگی نحوه دسترسی قراردادهای هوشمند مبتنی بر این فناوری به داده‌های آف‌چین برمی‌گردد. پاسخ‌گویی به این مشکلات، مستلزم یک معماری امنیتی جامع است که بتواند، سیستم کلمه عبور و

پسوردی منسوخ کنونی را به زیرساخت‌های کلیدی عمومی مختص دفاتر کل توزیع شده ارتباط داده و هر دو را پشتیبانی کند. در این میان، این‌که اجزای امنیتی و حساس شبکه، توسط عناصری که دارای حساسیت امنیتی اندکی هستند کنترل نشده یا وارد تعاملات بین شبکه‌ای نشوند از اهمیت بالایی برخوردار است. به عنوان مثال، زیرساخت سخت‌افزاری کلید عمومی بلاکچین، یکی از اجزای حساس شبکه است که نباید به دست رابط‌های برنامه‌نویسی کاربردی (APIs) باز سپرده شود. الزامات عملیاتی پیاده‌سازی فناوری بلاکچین در سطح صنعت خدمات مالی، می‌تواند به مفهوم ائتلاف سیستم ثبت مبتنی بر کلید عمومی بلاکچین با دایرکتوری کاربر داخلی یا با برخی دایرکتوری‌های خارجی باشد که توسط همه اعضای کنسرسیوم نیز قابل دسترسی است. البته، رویگرد دیگری نیز برای این ادغام و ائتلاف‌ها وجود دارد و آن، تخصیص حقوق دسترسی به کاربران از طریق نصب یک سیستم اعتبارسنجی و تایید روی سخت‌افزار آن‌ها است که به کاربران این امکان را می‌دهد تا در صورت تایید، از کلیه داده‌های خارج از شبکه (که عموما روی شبکه ابری ثبت و ضبط شده‌اند) استفاده کنند.

۲.۳. ادغام داده‌ها

در کنار امنیت، ادغام با دفترهای کل توزیع شده از منظر داده و تعامل‌پذیری نیز یکی از موارد مهمی است که باید مد نظر قرار گیرد. پیاده‌سازی‌های مبتنی بر فناوری دفتر کل توزیع شده، در عادی‌ترین حالت منجر به تولید برخی رابط‌های برنامه‌نویسی کاربردی خواهد شد که در حقیقت، درست مثل جاوااسکریپت (JavaScript)، نت (NET)، جاوا (Java) یا پایتون (Python)، به نوعی زبان‌های برنامه‌نویسی سیستم هستند. این رابط‌های برنامه‌نویسی کاربردی در اصل وسیله‌ای برای تولید رابط‌های رست‌فول (RESTful) برای بلاکچین هستند و بسیار مهم‌اند. اکثر محیط‌های برنامه‌نویسی مدرن از این رابط استفاده می‌کنند تا بتوانند با بسیاری از سیستم‌های دیگر در ارتباط و تعامل باشند. سیستم‌های متبنی بر دفتر کل توزیع شده، رابط‌های برنامه‌نویسی کاربردی را برای نوشتن و خواندن داده‌ها ارائه می‌دهند. این رابط‌های برنامه‌نویسی کاربردی، قابلیت استفاده در بالاترین سطوح برنامه‌نویسی را دارند و می‌توانند امکان تعامل‌پذیری شبکه با گذرگاه‌های سرویس سازمانی (Enterprise Service Bus) موجود یا تازه راه‌اندازی شده را فراهم کنند. گذرگاه‌های سرویس سازمانی پلی قابل اطمینان برای تراکنش و تعامل سیستم‌های مدرن مبتنی بر دفتر کل توزیع شده با زیرساخت‌ها و سیستم‌های منسوخ هستند.

هنگام معرفی یک دفتر کل توزیع شده جدید، داده‌های سنتی کنونی باید مورد تجزیه و تحلیل قرار گرفته و در مواقعی که نیاز است وارد سیستم جدید شوند. این فرایند، از یک استاندارد مخصوص پیروی می‌کند که تحت عنوان پروسه ای‌تی‌ال (ETL) شناخته می‌شود و عبارت است از:
۱. استخراج (Extract) داده‌ها از سیستم سنتی
۲. انتقال (Transform) آن به فرمتی که برای سیستم جدید دفتر کل توزیع شده قابل فهم باشد.
۳. بارگذاری (Load) داده‌ها روی بلاکچین

این مکانیسم‌های استاندارد می‌توانند با تامین داده‌های مودنیاز دفتر کل توزیع شده و انتقال داده‌های مبتنی بر این فناوری به سایر سیستم‌ها، زمینه‌ساز ادغام موثر فناوری بلاکچین با سیستم‌های مالی سنتی شوند. مزیت‌های فراوانی می‌توان برای رابط‌های مبتنی بر فناوری دفتر کل توزیع شده برشمرد که این قابلیت را دارند تا تعریف جدیدی از داده‌های مالی و به تبع آن خدمات مالی ارائه دهند.

با توجه به فقدان وجود پیچیدگی در این قبیل مکانیسم‌های رابط، مهم‌ترین عنصر برای ادغام موفق سیستم‌های مدرن و میرا با یکدیگر، معماری عمومی داده‌های سیستم‌های سنتی و منسوخ کنونی و دفاتر کل توزیع شده جدیدی است. به منظور نقل و تبادل کارآمد و موثر داده‌ها و ارائه اطلاعات ضروری، نیاز به معماری جامع، معتبر و کامل کامل غیرقابل چشم‌پوشی است.

یکی از ملاحظات مهم دیگری که در خصوص ادغام فناوری دفتر کل توزیع شده با سیستم‌ها و زیرساخت‌های منسوخ کنونی وجود دارد، محدودیت‌هایی فنی موجود در برخی از پلتفرم‌ها است. نگه‌داشتن ساختار اطلاعاتی در ساده‌ترین حالت ممکن از اهمیت بالایی برخوردار است و به همین دلیل نیز باید، تنها داده‌هایی را روی سیستم جدید مبتنی بر بلاکچین بارگذاری کرد که برای شبکه موردنیاز و ضروری هستند.

از طرفی، سرعت نوشتن و خواندن داده‌ها در فناوری بلاکچین، برخلاف سیستم‌های سنتی دارای محدودیت است. مکانیسم‌های ذخیره داده آف‌چینی نظیر آی‌پی‌اف‌اس (IPFS)، دقیقا به همین منظور معرفی شده‌اند تا بتوانند داده‌های موردنیاز شبکه را از خارج از زنجیره تامین کرده، روی بلاکچین ذخیره‌سازی کنند و از یکپارچگی اطلاعات ثبت شده در زنجیره نیز اطمینان حاصل کنند.

۲.۴. سازوکارهای امنیتی

به طور خلاصه، سازوکارهای امنیتی مهم‌ترین جنبه‌ای هستند که هنگام ادغام سیستم‌های مدرن مبتنی بر فناوری دفتر کل توزیع شده با سیستم‌های سنتی و منسوخ قدیمی باید مد نظر قرار داده شوند. ادغام داده‌ها با استفاده از برخی رابط‌های برنامه‌نویسی ویژه صورت می‌پذیرد و در این میان، چنین فرض می‌شود که کلیه فرایندهای ادغام از استاندارد ای‌تی‌ال پیروی می کنند و در عین حال، به صورت کامل نیز الزامات امنیتی را رعایت می‌کنند. در صورتی که سیستم‌های مدرن مبتنی بر بلاکچین دارای سطح امنیتی قابل قبولی باشند و از رابط‌های استاندارد و ایمن برای ادغام داده‌ها و در حالت کلی زیرساخت‌ها استفاده کنند، این فرصت را خواهند داشت تا به یکی از مولفه‌های نوین سازمانی تبدیل شوند، هرچند که دارای ویژگی‌ها، مزایا و محدودیت‌های منحصر به‌فرد خود نیز باشند. این که یک فناوری مدرن بتواند داده‌های مالی را در خلال سیستمی غیر متمرکز به روشی غیرقابل تغییر و قابل اطمینان ثبت کند، دستاورد شگرفی است که در صورت پایبندی به الزامات سایبری و استفاده از مکانیسم‌های امنیتی، تحول عمیقی در صنعت خدمات مالی رقم خواهد زد.

البته، قابلیت دیگری که بلاکچین دارد این است که می‌تواند برای حفاظت از داده‌های سایر سیستم‌ها نیز مورد استفاده قرار گیرد. به عنوان مثال، این امکان وجود دارد که کلیه بک‌آپ‌های گرفته شده از پایگاه داده سیستم‌های دیگر روی بلاکچین ذخیره‌سازی شود تا از پیکپارچگی، عدم تغییر و ماندگاری آن‌ها اطمینان حاصل شود. برخی رویکردهای رمزنگاری همچون درخت‌های مرکل (Merkle)، این قابلیت را به وجود آورده‌اند تا حجم غیرقابل تصوری از داده‌ها، تنها با استفاده از یک هش جهانی روی یک بلاکچین منفرد ثبت شده و ذخیره‌سازی شوند.

در صورتی که سیستم‌های مدرن مبلتنی بر بلاکچین دارای سطح امنیتی قابل قبولی باشند و از رابط‌های استاندارد و ایمن برای ادغام داده‌ها و در حالت کلی زیرساخت‌ها استفاده کنند، این فرصت را خواهند داشت تا به یکی از مولفه‌های نوین سازمانی تبدیل شوند، هرچند که دارای ویژگی‌ها، مزایا و محدودیت‌های منحصر به‌فرد خود نیز باشند.

Monthly results
325
838
338
580
472
896
471
489
662
774

قوانین حسابرسی

ویل بیبل (Will Bible)، یکی از اعضای دیلویت، استدلال می‌کند که زمان، یکی از مهم‌ترین مسایلی است که کاربران هنگام رجوع به سیستم‌های مبتنی بر دفتر کل توزیع شده در کسب‌وکارهای‌شان با آن طرف هستند. قطعا استفاده از فناوری دفتر کل توزیع شده تاثیر بسزایی در روند انجام حسابرسی خواهد داشت.

البته، بلاکچین‌ها فرایندهای حسابرسی را به طور کامل خودکار نمی‌کنند و تا حدی نیستند که بتوانند نیاز به حسابرس‌های انسانی را به طور کامل از فرایندهای مالی حذف کنند، اما این قابلیت را دارند تا برخی از فرایندها را تغییر دهند. حسابرسان فنی و مالی، نقش پررنگی در روند حسابرسی و ارزیابی داده‌های مربوط به تراکنش‌های مالی دفاتر کل توزیع شده ایفا می‌کنند. همان‌طور که در سیستم‌های سنتی کنونی نیز ارزیابی داده‌های مالی و حسابرسی سازمان‌ها، در وهله اول به عناصر انسانی متکی است. علیرغم این‌که داده‌های مالی در یک مخزن آنلاین ذخیره‌سازی می‌شوند، اما داده‌های آف‌چین و آن‌چینی که وارد بلاکچین می‌شوند یا از آن خارج می‌شوند نیاز به ارزیابی دقیق و حسابرسی اصولی دارند.

بر همین اساس، در سال ۲۰۱۷ میلادی، دیولیوت نتایج تحقیقات گسترده خود روی روند حساتبرسی یک پروتکل مبتنی بر دفتر کل توزیع شده خصوصی را منتشر ساخت تا بتواند با استناد به آن، سطح اعتماد طیف گسترده‌ای از کاربران خود را به دست‌آورد. نتیجه نهایی این بود که یک بلاکچین، بعید است بتواند یک نمای کلی از صورت‌های مالی‌اش ارائه دهد و حسابرسان، در صورتی که به دنبال دستیابی به اطلاعات جامعی در این خصوص باشند، ناچارند به منابع اطلاعاتی خارج از زنجیره مراجعه کنند.

۳.۱. ثبت غیرقابل تغییر

کلیه داده‌هایی که در یک بلاکچین ثبت و ذخیره‌سازی می‌شوند، غیرقابل تغییر هستند. به این مفهوم که نمی‌توان آن‌ها را تغییر داد، حذف کرد یا به عبارتی دستکاری کرد. در یک بلاکچین، تنها امکان این وجود دارد که داده‌هایی به مجموعه داده‌های قبلی اضافه شوند، بدون این‌که تغییر در داده‌های قبلی اعمال شود. همین دنباله حسابرسی پایدار یا غیر قابل تغییر بلاکچین، یکی از جذاب‌ترین ویژگی‌های فناوری دفتر کل توزیع شده برای صنعت خدمات مالی که حسابرسان بسیاری را با آرزوی شفافیت بیشتر و اطمینان به سنت خود جذب کرده است.

این‌که این فناوری، امکان دسترسی به مجموعه‌ای از داده‌های مالی و حسابرسی را در اختیار حسابرسان قرار می‌دهد و این اطمینان را نیز به آن‌ها می‌دهد که هیچ‌گونه دستکاری از سوی هیچ عنصر فردی یا سازمانی در آن‌ها صورت نگرفته است. مزیت دیگری که این فناوری دارد این است که در سایه توکن‌های رمزنگاری شده، دفتر کل این قابلیت را دارد تا در خلال ذخیره‌سازی تراکنش‌ها و نقل و انتقالات، ارزش زمانی واقعی دارایی‌های مبدلاتی را نیز ذخیره‌سازی کند.

البته، علاوه بر ثبت و ذخیره‌سازی دارایی‌های فیزیکی نظیر توکن‌ها، برخی دارایی‌های غیرمادی نظیر مالیکت معنوی نیز می‌توانند در این شبکه مدرن ثبت و ذخیره شده و حتی به تعامل درآیند که ویژگی منحصربه‌فردی برای فناوری دفتر کل تعوزیع شده به شمار می‌رود.

البته، این به این معنی نسیت که حسابرسان برای انجام حسابرسی‌ها و ارزیابی‌های خود محدود به شبکه بلاکچین هستند و می‌توانند صرفا با تکیه بر یک زنجیره کلیه فرایندهای حسابرسی خود را طی کنند، بلکه برای انجام یک حسابرسی کامل، دسترسی به حجم انبوهی از داده‌های آن‌چین و آف‌چین و هم‌چنین تلفیقی از سیستم‌های بلاکچینی و سنتی نیاز است. همچنین لازم به ذکر است که داده‌های ثبت شده در یک بلاکچین، ممکن است به اندازه کافی نتوانند اطلاعات موردنیاز برای رسیدگی به برخی پرونده‌های کلان حسابرسی را تامین کنند.

به‌ویژه که همان‌طور که عنوان شد، تنها بخشی از داده‌ها وارد شبکه می‌شوند که ضروری بوده‌اند. در این میلان، برخی از داده‌ها نیز هستند که از اهمیت بالایی برخوردار هستند. داده‌هایی از قبیل هویت طرفین دریافت کننده تراکنش‌ها، حقوق عاملان تراکنش‌ها برای آغاز تراکنش و یا حق مالکیت طرفین ارسال کننده. ممکن است نیاز باشد تا ارتباط بین بلاکچین و سایر سیستم‌های غیر بلاکچینی در تراکنش با آن اعتبارسنجی و ارزیابی شود.

به همین دلیل نیز دفتر کل توزیع شده، یک نوآوری خارق‌العاده برای فرایندهای حسابرسی است چرا که مجموعه‌ای بی‌نقص، یکپارچه و غیرقابل دستکاری از داده‌های مالی را در اختیار حسابرسان قرار می‌دهد. هر چند که همان‌طور که اشاره شد، برخی محدودیت‌های این نوآوری در حیطه منابع اطلاعاتی جای بحث و کار دارد و نیاز به تامین داده از سایر سیستم‌ها غیرقابل چشم‌پوشی است.

۳.۲ حسابرسی قراردادهای هوشمند

قراردادهای هوشمند، به پیچیدگی فرایند حسابرسی فناوری دفتر کل توزیع شده می‌افزایند. قراردادهای هوشمند، در اعماق خود، اجرای کدهایی در بلاکچین هستند که برای اطمینان از کد پردازش معاملات ارائه شده‌اند و همچون بسیاری از فناوری‌های نوآورانه دیگر راهکاری برای بهبود

خدمات و فرایندهای مالی به شـــمار می‌روند. وجود این کدها در فناوری دفتر کا توزیع شده می‌تواند برخی سوالات حسابرسی را در پی داشته باشد که عبارتند از:

- چه کسی تغییرات لازم را روی پایگاه داده اعمال می‌کند؟
- نحوه دسترســـی به لیســـت‌های کنترلی در خلال اجـــرای قراردادهای هوشمند چگونه است؟
- چه چیزی تعیین کننده حق دسترسی به فرایندها و عملیات قراردادهای هوشمند است؟ آیا این سازوکار دسترسی به تمام قراردادهای هوشمند نیز بسط داده می‌شود؟
- در صورتی که کلیدهای خصوصی نادرست بوده یا در معرض خطر قرار گرفته باشند، چه اقدامات و فرایندهایی باید انجام پذیرند؟
- در صورتی که از اوراکل‌ها (منابع داده آف‌چین) استفاده می‌شود، نحوه ادغام با داده‌هایی که این اوراکل‌ها تامین می‌کنند چگونه است؟

طراحی و پیاده‌ســـازی ناکارآمد و نامناسب قراردادهای هوشمند می‌تواند سیستم دفتر کل توزیع شده را دســـتخوش آسیب‌پذیری‌های قابل توجهی کند. به عنوان مثال، این اتفاق برای سازمان غیر متمرکز مستقل (DAO) نیز اتفاق افتاد. آسیب‌پذیری بروز کرده در بلاکچین اتریوم سازمان غیر متمرکز مستقل باعث شد تا مبلغ قابل توجهی از سرمایه این سازمان (بالغ بر ۶۰ میلیون دلار در آن زمان) توسط یک مهاجم سایبری از سیستم ربوده شود.

به همین دلیل نیز با توجه به ریســـک بالایی که آسیب‌پذیری‌های ناشی از قراردادهای هوشمند برای سیســـتم در پی دارند و می‌توانند ثبت داده‌ها یا در حالت کلی دسترسی به سیستم را برای هکرها و عوامل خارجی تسهیل کنند، حسابرسان روی این قراردادها حساسیت بیشتری نشان می‌دهند و سعی می‌کنند با شناسایی آسیب‌پذیری‌های بلاکچین و حفره‌های سایبری احتمالی، به یکی از ستون‌های سایبری سیستم تبدیل شوند.

در نتیجه، می‌توان چنین برداشت کرد که نگرانی‌های سایبری و ریسک‌های امنیتی، جزئی لاینفک از حسابرســـی بلاکچین هستند و در حالت کلی، زمانی که پای فناوری دفتر کل توزیع شـــده به میان می‌آید، حسابرســـی حساسیت بیشتری می‌یابد.

۳.۳. کنترل‌های فنی

صرفا وجود بلاکچین نمی‌تواند نیاز به کنترل‌های فنی در یک سازمان را از بین ببرد. کنترل‌هایی نظیر استاندارد امنیت داده و اطلاعات ایزو ۲۷۰۰۱ (ISO 27001)، با پیاده‌سازی فناوری دفتر کل توزیع شده نیز همچنان مورد استفاده قرار می‌گیرند. استانداردها و کنترل‌هایی که سازمان‌ها پس از پذیرش و به کارگماری فناوری بلاکچین نیز ناچار به پیروی از آن‌ها خواهند بود عبارتند از:

- سیاست‌های امنیت اطلاعات: این‌که چه کســـانی به داده‌ها دسترسی دارند؟ هدف از راه‌اندازی پلتفرم چیســـت؟ میزان حساســـیت داده‌های ذخیره‌سازی شده در سیستم چقدر است؟ این ســـوالات، تنها بخشی از سیاست‌های امنیتی هستند که باید در خلال یک سازمان پاسخ داده شوند.
- کنترل‌های امنیتی منابع انسانی: این موضوع، به پروتکل‌هایی برمی‌گردند که تغییر و به‌روزراسنی سیستم و دسترســـی به آن را هنگام تغییرات منابع انسانی ســـازمان تضمین می‌کنند. این‌که هنگام ترک کار توسط برخی از کارکنان یا تغییر سمت، دسترسی افراد به شبکه نیز تغییر پیدا کند.
- کنترل‌های مدیریت دارایی: کنترل دارایی‌ها و تعیین خط مشی برای حفظ حق مالکیت پلتفرم نیز جزو مواردی اســـت که با افزوده شدن بلاکچین به سازمان باید همچنان مد نظر قرار داده شود. این موضوع می‌تواند به حفظ حق مالیکت توکن‌های سخت‌افزاری و یا لپ‌تاپ‌ها برگردد.
- کنترل دسترسی‌ها: نقش‌ها و محدودیت‌های امنیتی و کلیه فرانیدهای کنترلی، بـــه این منظور دنبال می‌شـــوند که از دسترســـی، ثبت و خواندن اطلاعات موجود در بلاکچین سازمان توسط افراد غیرقابل اعتماد و مهاجم جلوگیری شود.
- امنیت محیطی و فیزیکی: دفتر کل توزیع شـــده، پس از پیاده‌سازی در یک ســـازمان نیاز به مدیریت دارد. این مدیریت کلیـــه ماژول‌های امنیتی ســـخت‌افزاری، اقدامات امنیتی فیزیکی نظیر دوربین‌های مدار بســـته و کنترل‌های دسترسی فیزیکی و کلیدهای امنیتی را شامل می‌شود.
- کنترل‌های امنیتـــی عملیاتی: این مـــورد می‌تواند کلیه اســـتانداردها و فرایندهـــای کنترلی زیرســـاختی از جمله برنامه‌های چـــک کردن وجود ویروس در سیســـتم، برنامه‌های تعمیراتی و نگهداری و مدیریت بک‌آپ را در بر بگیرد. حتی دفاتر کل توزیع شده عمومی نیز با وجود داشتن حتی یک نود، تلفیقی از داده‌ها و سیســـتم‌های مختلف هستند و به همین دلیل نیز کنترل‌های امنیتی عملیاتـــی در این این سیســـتم‌ها از اهمیت بالایی برخوردار است. به‌ویژه که اغلب اوقات، از وی‌پی‌ان‌ها استفاده می‌شود. این استانداردها می‌توانند محیط عملیاتی ایده‌آلی برای شبکه ایجاد کنند.
- کنترل‌های رمزنگاری: این موضوع، به خود پلتفرم برمی‌گردد که در آن، احراز هویت بر کلیدهای احراز هویت رمزنگاری منحصربه‌فرد سیستم مبتنی است.
- کنترل‌های مدیریت حـــوادث مبتنی بر امنیت اطلاعـــات: در صورت بروز نشت اطلاعاتی یا شکاف امنیتی در سیستم، این کنترل‌ها می‌توانند فرایندهای پیگیری، رسیدگی و پاسخگویی به مشکل یا حادثه بروز کرده را تسریع و تسهیل کنند و به همین دلیل نیز برای دفتر کل توزیع شده حیاتی‌اند. توجه داشته باشید که در ســـازمان‌هایی با مدل مدیریتی حکومتی، اعمال مجموعه‌ای استاندارد از کلیه کنترل‌ها بین اعضای شبکه الزامی است.

۳.۴. تحولات حسابرسی

پرواضح است که استفاده از فناوری دفتر کل توزیع شده در یک سازمان، نه نیاز به حسابرسی در سیستم را حذف می‌کند و نه نیاز به یک حسابرس مستقل را. در عوض، این فناوری، نحوه استخراج داده توسط این حسابرسان از سیستم، تست و ارزیابی و تجزیه و تحلیل این داده‌ها را دستخوش تغییر می‌کند.

در حقیقت، فناوری لایه‌بندی شده بلاکچین، این امکان را به سازمان‌ها می‌دهد تا از یک حسابرسی پیچیده‌تر، کامل‌تر و شفاف‌تر در سیستم خود بهره‌مند شوند و نتایجی زمانی واقعی از بلاکچین خود به دست آورند. دفاتر کل توزیع شده، با قابلیت ثبت داده‌ها به شکلی غیرقابل تغییر و ثابت، به بسیاری از فرایندهای حسابرسی کمک خواهند کرد و بسیاری از عملیات حسابرسی را نیز تسهیل خواهند کرد. با این حال، این نوآوری شگرف نیز دارای الزامات و ملاحظاتی است و از منظر حسابرسی، وجود برخی محدودیت‌های اطلاعاتی، وجود برخی نواقص فنی و مادی در سیستم و امثال آن‌ها می توانند فرایندهای حسابرسی در سیستم را با معظلاتی روبه‌رو کنند.

مشکلاتی که نیازمند پاسخگویی دقیق و مناسب هستند و این پاسخگویی، در نهایت به مفهوم تغییر فرایندهای حسابرسی کلی در سازمان است. در همین راستا، تشکیل برخی کارگروه‌های حسابرسی مدرن، با تخصص‌ها و تجارب مدرن و متناسب با فناوری دفتر کل توزیع شده، اولین تغییر مهمی است که در حسابرسی سازمان‌ها به وقوع می‌پیوندد. این گروه‌های متخصص، کلیه مسایل از جمله یکپارچگی داده‌ها، صحت و سقم آن‌ها و تمامیت‌شان را مورد ارزیابی قرارداده و با اعتبارسنجی و تایید داده‌ها و قراردادهای مندرج در دفتر کل توزیع شده غیرقابل تغییر بلاکچین، به اهداف حسابرسی جامه عمل می‌پوشانند.

پذیرش و پیاده‌سازی فناوری دفتر کل توزیع شده در مقیاس عملی، برخی تحولات را به تکنیک‌ها و روش‌های حسابرسی فعلی تحمیل خواهد کرد. حسابرسان، ملزم به تعریف و تبیین برخی قواعد و فرمول‌های حسابرسی جدید خواهند بود تا بتواند فناوری جدید را پوشش دهد. ضمن این‌که برخی مقررات و قواعد جدیدی مربوط به داده‌ها و معماری‌های فناورانه در سازمان نیز نیاز خواهند بود تا در فاز طراحی، به نحوی در سیستم پیاده‌سازی شوند که به حسابرسان اجازه استفاده از داده‌ها و در حالت کلی زنجیره دفتر کل توزیع شده را داده و در فرایندهای حسابرسی مثمرثمر باشند.

علاوه بر موارد عنوان شده، ادغام سیستم‌های منسوخ کنونی به سیستم‌های مدرن مبتنی بر دفتر کل توزیع شده، ممکن است مستلزم تغذیه اطلاعاتی از برخی فرایندهای کاغذبازی نیز باشد. این، بدان معنی است که اتوماسیون کامل یک سیستم متشکل از هر دو نسل فناوری، مستلزم اتوماسیون تک‌تک این فرایندها و سیستم‌ها است و عملا، تا زمانی که کلیه فرایندهای متصل خودکار نشده باشند، امکان اتوماسیون حسابرسی بلاکچین نیز وجود ندارد.

البته، فناوری بلاکچین بسیاری از فرایندهای ثبت و ضبط، خواندن و ارزیابی داده‌ها و حسابرسی آن‌ها را خودکار و تسهیل کرده است و این به این مفهوم است که این فناوری، حسابرسی را نیز وارد فاز تحولات دیجیتال کرده است. ضمن این‌که فناوری دفتر کل توزیع شده، با قرار دادن حجم قابل توجهی داده در اختیار حسابرسان و فرایندهای مدرن تست و تجزیه و تحلیل این داده‌ها، این فرصت را به حسابرسان داده است تا با طراحی برخی نرم‌افزارهای مانیتورینگ دفتر کل و داده‌ها در زمان واقعی، اطلاعات حسابرسی هنگفتی به دست‌آورده و ذینفعان سازمان را پشتیبانی کنند.

در نهایت، می‌توان چنین نتیجه گرفت که فناوری دفتر کل توزیع شده، فرایندها و نحوه حسابرسی حسابرسان را تغییر خواهد داد و در مقابل، حسابرسان نیز گروه‌های کاری خود را تغییر خواهند داد تا بتوانند با تخصص و تبحر بیشتری با این فناوری نوظهور و متفاوت رودررو شوند. با این حال، بلاکچین، هرگز به مفهوم جایگزینی یا حذف حسابرسان از صنعت خدمات مالی نیست و در آینده‌ای نه چندان دور، نقش حسابرسان در صنعت خدمات مالی، نه تنها کم‌رنگ‌تر نخواهد شد، بلکه با رنگی تازه نیز رخ خواهد نمود.

استفاده از فناوری دفتر کل توزیع شده در یک سازمان، نه نیاز به حسابرسی در سیستم را حذف می‌کند و نه نیاز به یک حسابرس مستقل را. در عوض، این فناوری، نحوه استخراج داده توسط این حسابرسان از سیستم، تست و ارزیابی و تجزیه و تحلیل این داده‌ها را دستخوش تغییر خواهد کرد.

0005 -4,85%
0003 -18,04%
0001 -50,00%
0003 14,29%
0005 12,50%

کنترل‌های امنیت سایبری

فنـــاوری دفتر کل توزیع شـــده، به صـــورت ذاتی با برخـــی الزامات و ملاحظات امنیت ســـایبری در هم تنیده اســـت. پایه و اساس فناوری بلاکچین، رمزنگاری‌های خصوصی و عمومـــی، امضای دیجیتال و هش رمزنگاری است.

توانایی نوشتن داده‌ها روی یک بلاکچین، در وهله اول مستلزم داشتن یک کلید خصوصی است و داشتن توکن‌های رمزنگاری‌شده نیز می‌تواند به معنای امکان دسترسی کاربران به شـــبکه و قراردادهای هوشمندی باشد که سطح بالایی از امنیت سایبری را می‌طلبند. در عین حال، امکان دسترســـی به داده‌ها و به عبارت دیگر خواندن داده‌هـــا از بلاکچین نیز مستلزم داشتن کلید رمزگشایی است.

راهکارهـــای مبتنی بـــر بلاکچین، ثبـــت و نگارش داده‌هـــا، خواندن آن‌ها یـــا هرگونه تبادل اطلاعاتی در خلال شـــبکه را با اســـتفاده از یک سری کلیدهای خصوصی به اعضای شـــبکه محدود کرده‌اند و در این میان، امنیت این کلیدهای امنیتی از اهمیت بالایی برخوردار اســـت.

مقاله‌ای که تحت عنوان «فناوری دفتر کل توزیع شده و امنیت سایبری (Distributed Ledger Technology & Cybersecurity)» از سوی انیســـا (ENISA) منتشر شده اســـت بیان می‌کند که «هنگام مدیریت کلیدهـــا، از جمله افراد، فرایندها و فناوری، سیاســـت‌های و روندهای دقیق و سخت ضروری است».

نواقصی از جمله ســـرقت یا کنترل‌های غیر مجاز این کلیدها می‌تواند موجب انشعاب در پلتفرم استفاده کننده از فناوری دفتر کل توزیع شده شود. در ســـال ۲۰۱۴ میلادی، یک گزارش مبنی بر خرابی در ورایزون (Verizon) منتشر شد که نشـــان می‌داد تنها ۱۵ درصد از نشت‌های اطلاعاتی صورت گرفته در این سیستم توانسته‌اند طی یک روز کشف شوند و ۶۹ درصد از نشت‌های امنیتی صورت گرفته، بیش از یک روز زمان بردند تا فاش شوند. این در حالی اســـت که شناسایی ۳۵ درصد از این نشـــت‌های اطلاعاتی، هفته‌ها یا حتی بیشـــتر زمان برده بود. در فصل آتی، در مورد تهدیدهای بالقوه بلاکچین‌های خصوصی، بیشتر صحبت خواهیم کرد اما قبل از آن، نیاز به بررسی چالش‌هایی داریم که سازمان‌های استقبال کننده از فناوری دفتر کل توزیع شده با آن روبه‌رو خواهند بود.

۴.۱. چالش‌های امنیت سایبری دفاتر کل توزیع شده

ملاحظات سایبری مربوط به ماهیت رمزنگاری و غیرقابل تغییر فناوری بلاکچین عبارتند از:

- مدیریت کلیدها
- غلبه بر ریسک‌های حمله به یک بلاکچین خصوصی
- متمرکزسازی قدرت در شبکه
- حریم خصوصی و حق فراموش شدن

همان طور که در فصل دوم نیز به تفصیل شرح داده شد، راه‌های مناسب مختلفی برای ذخیره‌ســـازی و انتقال کلیدهای خصوصی وجود دارد. این راهکارها می‌تواند شامل ماژول‌های ســـخت‌افزاری امن و برخی سیاست‌ها و دستورالعمل‌های بسیار دقیق باشـــد که باعث می‌شود تا کلیدهای خصوصی مبتنـــی بر بلاکچین، در معرض خطر نباشـــند یا دست کم، ریسک به مراتب کمتری را تحمل کنند. با این وجود، برخی راهکارهای هجومی نیز وجود دارند که به مهاجان این امکان را می‌دهند تا بدون نیاز به دسترسی به کلیدهای خصوصی، به سیستم نفوذ کرده و به خواسته‌های خود دست یابند.

حمله منـــع ســـرویس (denial of service)، جزو حملاتی اســـت که دسترســـی به سیســـتم و انجام فرایندها در خلال شبکه را از اعضای اصلی شبکه (کاربران مجاز دارای کلیدهای خصوصی) سلب می‌کند. هنگامی که دفتر کل توزیع شـــده، از گواه اثبات کار به عنوان مکانیسم اجماع استفاده می‌کند، یک هکر یا مهاجم (که می‌تواند یکی از اعضای شرکت‌های عضو در شبکه بوده باشد)، می‌تواند تعداد متعددی گره به نام خود ایجاد کرده و با معکوس‌سازی بلوک‌ها، تراکنش‌های تاریخی صورت گرفته در شبکه را در اختیار خود درآورد.

اگر هر یک از اعضای شرکت کننده در شبکه‌ای با مکانیسم اجماع گواه اثبات کار، با استفاده از ۱۰ گره فعالیت می‌کنند، تولید تعداد ۱۰۰۰ گره در بلاکچین‌های معتبری همچون آمـــازون یا آزور (Azure) می‌تواند منجر به معکوس شدن ۱۰۰ مورد از بلوک‌ها شده و دست مهاجم را برای دسترسی به تراکنش‌ها و داده‌ها باز بگذارد. به همین علت نیز مکانیسم اجماع گواه اثبات کار، برای بلاکچین‌های مجاز پیشنهاد نمی‌شود.

در عوض، باید از مکانیسم‌های اجماعی از قبیل گواه اثبات قدرت و یا تحمل خطای بیزانس عملی استفاده شود. البته، جمله به بلاکچین‌های عمومی بسیار دشوارتر است چرا که مهاجم باید بتواند ده‌ها هزار گره سخت‌افزاری تخصصی را تحت تاثیر قرار دهد. چنین هجومی، مستلزم قدرتی بسیار زیاد و هزینه‌های سخت‌افزاری کلانی است که معادل کل مصرف انرژی برق ایرلند است!

از آن‌جا اجازه دسترسی به سیستم یا به عبارت بهتر اعتبارات در سیستم‌های کنونی به صورت متمرکز است - یک صادر کننده مرکزی افراد و اعضا را اعتبارسنجی کرده و کلید دسترسی به شبکه را در اختیار آن‌ها قرار می‌دهد - اعطای این مجوزها می‌تواند شبکه را در معرض خطر قرار دهد. به همین دلیل نیز امید می‌رود تا با پیاده‌سازی فناوری دفتر کل توزیع شده در سطح سازمان‌ها، دسترسی در شبکه به شکلی غیر متمرکز درآمده و بخش قابل توجهی از این ریسک کاهش پیدا کند.

حق فراموش شدن - نیاز به حذف داده‌ها - یکی از چالش‌های دیگر فناوری دفتر کل توزیع شده است چرا که دستیابی به این مهم در شبکه‌هایی با داده‌های غیرقابل تغییر، بسیار دشوار است. در برخی از بلاکچین‌ها، شبکه این امکان را دارد تا برخی از بلوک‌ها را که در زمان‌های مشخصی قبل‌تر ایجاد شده‌اند حذف کنند.

هرچند که این روند، در صورتی که داده‌های قدیمی با داده‌های پس از آن ارتباط و پیوند داشته باشند امکان‌پذیر نخواهد بود. یک رویکرد جایگزین برای مقابله با این چالش این است که اطمینان حاصل شود کلیه داده‌هایی که روی زنجیره به ثبت می‌رسند رمزنگاری شده‌اند. هنگامی که کلیدهای خصوصی مربوط به داده‌هایی باید فراموش شوند خراب شود، این داده‌ها دیگر قابل خواندن نخواهند بود. در صورتی که قرار بر اتخاذ این رویکرد باشد، رمزنگاری باید از نخستین داده‌ها آغاز شود که بعید به نظر می‌رسد رمزنگاری داده‌های اخیر کارساز واقع شود.

چالش دیگری که در مورد فناوری دفتر کل توزیع شده وجود دارد، پیشرفت‌های حاصل شده در محاسبات کوانتومی است. پیشرفت‌هایی که می‌توانند مولفه‌های رمزنگاری اصلی را منسوخ کرده یا به یکپارچگی داده‌های رمزنگاری شده با الگوریتم‌های توافقی آسیب بزنند. این پیشرفت‌ها، حتی به طور بالقوه این قابلیت را نیز دارند که حریم خصوصی داده‌ها را در سطح جهانی تحت‌الشعاع قرار دهند. در نتیجه، کلیه پیشرفت‌های صورت گرفته در این حیطه باید به صورت کامل مانیتورینگ شده و اطمنان حاصل شود که این قبیل پیشرفت‌ها و امثال آن‌ها، تمامیت و امنیت داده‌های رمزنگاری شده در شبکه بلاکچین را مورد تهدید قرار نمی‌دهند.

۴.۲. قراردادهای هوشمند

قراردادهای هوشمند نیز تهدیدها و ریسک‌های امنیت سایبری خود را دارند. با وجود این‌که یک بلاکچین با زبان قراردادهای هوشمند ماشین تورینگ کامل (Turingcomplete) دارای قابلیت‌های فراوانی است، اما باید توجه داشت که برای مهاجمان نیز سطح تماس وسیعی برای بهره‌برداری مهیا می کند (درست مثال همان چیزی که در مورد سازمان غیر متمرکز مستقل اتفاق افتاد و در فصل سوم نیز مطرح شد). اعضای داخلی شبکه، در چنین شرایطی این امکان را دارند که از قوانین کسب‌وکار به نفع خود بهره‌برداری کنند و همین امر نیز ایجاب می‌کند تا یکپارچگی برنامه در طول شبکه حفظ شود.

در این قبیل شبکه‌ها، بررسی مداوم کدها ضروری است به ویژه در مورد شبکه‌هایی که کدهای آسیب‌پذیر قادر باشند تمامیت و یکپارچگی بلاکچین را در خطر بیندازند. این بررسی‌ها، از منظر امنیتی باید به بهترین شکل ممکن صورت بگیرند. در صورت لزوم، شاید ممکن باشد از راهکارهای اتوماتیک برای بررسی کدها کمک گرفته شود تا اطمینان حاصل شود که کدها، عاری از هرگونه ریسک احتمالی برای شبکه هستند.

قرادادهای هوشمند، یک سری اجرای کد در شبکه بلاکچین هستند که در دسترس تمامی اعضا نیز قرار گرفته‌اند. بدیهی است که تغییر در این کدها، تغییراتی را کل اعضای شرکت کننده در زنجیره تحمیل خواهد کرد. زمانی که یک قرارداد هوشمند جدید به سیستم افزوده می‌شود یا قراردادی به‌روزرسانی می‌شود، لازم است که یک فرایند مدیریتی قدرتمند دنبال و پیاده شود. بلاکچین‌ها، به صورت خودکار مکانیسم های اجماع را امضا می‌کنند و این در حالی است که اعضای شرکت کننده در شبکه دفتر کل توزیع شده، قبل از این‌که فعال شوند بادی قراردادهای هوشمند را ارزیابی کرده و به اتمام برسانند.

به همین ترتیب، وظیفه اجرای انطباق داخلی با استفاده از دستورالعمل‌ها و کنترل‌های توافقی نیز به عهده خود بلاکچین است. کتابخانه‌های استاندارد نیز می‌توانند برای کاهش ریسک‌های امنیت سایبری قراردادهای هوشمند مورد استفاده قرار گیرند. ضمن این‌که، رابط‌های استاندارد توافق شده‌ای همچون استاندارد توکن ERC20 نیز حفره‌های امنیتی به وجود آمده در سیستم را می‌کاهند. حفره‌هایی که ناشی از عملکرد غیراستاندارد پلتفرم هستند.

۴.۳. استانداردهای کنترلی

استانداردهای کنترلی نظیر ISO 27001، کنترل‌های مرکز امنیت اینترنت (Center for Internet Security Controls) و کنترل‌های امنیت بحرانی اس‌ای‌ان‌اس (SANS)، بایستی به عنوان بخشی از برنامه کنترلی جامع امنیت سایبری هر شبکه پیاده‌سازی شوند و با بازنگری‌های منظم و حفظ انطباق نیز پشتیبانی شوند.
کنترل‌های مرکز امنیت اینترنت شامل موارد زیر می‌شود:

- ۱. موجودی دستگاه‌های مجاز و غیر مجاز
- ۲. موجودی نرم‌افزارهای مجاز و غیر مجاز
- ۳. پیکربندی ایمن برای سخت‌افزارها و نرم‌افزارهای روی گوشی‌های تلفن همراه، لپ‌تاپ‌ها، ایستگاه‌های کاری و سرورها
- ۴. ارزیابی و رفع آسیب‌پذیری مداوم
- ۵. کنترل استفاده از امتیازات اجرایی

۴.۴. قدرت امنیت سایبری دفاتر کل توزیع شده

دفاتر کل توزیع شده‌ای که از زیرساخت‌های کلیدی عمومی رمزنگاری شده برای حفظ تمامیت و امنیت شبکه خود استفاده می‌کنند، در قبال مهاجمانی که فاقد کلیدهای مجازند مقاوم‌هستند. زمانی که این قابلیت مهم را در کنار مزیت ضدجعل بودن داده‌های بلاکچین قرار می‌دهیم، به این نتیجه می‌رسیم که نوآوری دفتر کل توزیع شده، یک نوآوری با قدرت امنیت سایبری فوق‌العاده است. به همین علی نیز امید می‌رود که با استمرار کنترل‌هایی همچون مدیریت کلیدهای رمزنگاری، فناوری دفتر کل توزیع شده بیش از پیش در چشم‌انداز امنیت سایبری شتاب بگیرد. این روند پرشتاب، با ایجاد رمزهای دستی درشبکه به جای استفاده از کلیدهای رمزنگاری خصوصی، بیش از پیش نیز اوج خواهد گرفت.

تقویت پروتکل‌های اطلاعات و ارتباطات سنتی

فناوری اطلاعات و ارتباطات (Information and Communication Technology)، ابزارهای خودکار تولید، پردازش، ذخیره‌سازی و انتقال اطلاعات را شامل می‌شود و دستگاه‌های ضبط، شبکه‌های ارتباطی، سیستم‌های کامپیوتری و سایر ابزارها و تجهیزات الکترونیکی را تحت پوشش قرار می‌دهد. مدیریت این زیرساخت، مستلزم مجموعه‌ای از روش‌ها و دستورالعمل‌های خاص است تا بتواند شناسایی، ارزیابی، نظارت و کنترل ریسک‌های احتمالی سیستم را تضمین کند.

در راهنمای سیاست نظارت بر اصول عمومی مدیریت ریسک فناوری که توسط مقامات پولی هنگ کنگ (HKMA) گردآوری و منتشر شده است، کنترل‌های فناوری اطلاعات و ارتباطات به پنج دسته متخلف دسته‌بندی می‌شوند: مدیریت امنیت، مدیریت تغییر و توسعه سیستم، پردازش اطلاعات، شبکه‌های ارتباطی و مدیریت ارائه دهندگان خدمات مبتنی بر فناوری.

ماهیت غیرمتمرکز دفتر کل توزیع شده، مستلزم رویکردی متفاوت برای کنترل این مدیریت‌ها است:

۵.۱. مدیریت امنیت

فناوری دفتر کل توزیع شده بر رمزنگاری استوار است. در فصل چهارم، به تفصیل در مورد نحوه پاسخگویی این ماهیت به مشکلات سایبری مربوط به حفاظت از اطلاعات و احراز هویت کاربران اشاره کردیم.

۵.۱.۱. طبقه‌بندی و حفاظت از اطلاعات

از آن‌جا که فناوری دفتر کل توزیع شده بر الگوریتم‌های رمزنگاری استوار است، حفاظت از اطلاعات و رمزنگاری می‌تواند یکی از مزایای این قبیل شبکه‌ها قلمداد شود. با این حال، با توجه به این‌که شبکه بلاکچین‌ها قابلیت اتصال به سیستم‌های خارجی را نیز دارند و قطعا نیز نیاز به این اتصال وجود خواهد داشت، اطلاعات و داده‌های مندرج در شبکه در دسترسی برخی عناصر و سیستم‌های خارجی نیز قرار خواهد گرفت. این تبادل اطلاعاتی، مستلزم ارزیابی‌ها و کنترل‌های دقیق امنیتی است تا اطمینان حاصل شود داده‌ها و تراکنش‌ها، در اختیار طرفین قابل اعتماد و معتبری قرار می‌گیرند.

۵.۱.۲. احراز هویت و کنترل دسترسی

همان‌طور که مطرح شد، دسترسی کاربران به شبکه دفتر کل توزیع شده و اطلاعات ثبت شده در آن، مستلزم داشتن کلیدهای خصوصی و عمومی ارائه شده است. کلیه داده‌های محرمانه‌ای که نیاز به ثبت در سیستم بلاکچین دارند، به طوری که از دسترس عموم خارج باشند، باید با استفاده از کلیدهای خصوصی رمزنگاری شوند. هر سازمان، داده‌ها خود را با استفاده از کلیدهای خصوصی روی زنجیره رمزنگاری کرده و سپس کلیدها را نزد خود نگه می‌دارد (کلیدهایی که بدون وجود آن‌ها، امکان بازیابی و خواندن این داده‌ها وجود نخواهد داشت). این روند، حاکی از آن است که رویکردی دقیق و حساب شده برای حفاظت از کلیدهای خصوصی رمزنگاری وجود دارد تا داده‌های محرمانه سازمان‌ها، در دسترس عموم یا مهاجمین قرار نگیرد.

۵.۱.۳. مدیریت امنیت و نظارت

غیرمتمرکزسازی سیستم‌ها، مستلزم اصلاح بسیاری از پروتکل‌های امنیتی کنونی است. تعداد متعددی از گره‌هایی که به صورت مداوم داده‌ها و تراکنش‌ها را در طول شبکه رد و بدل می‌کنند، ریسک دسترسی افراد مهاجم به شبکه را افزایش می‌دهد. به همین دلیل نیز الزامی است که اطمینان حاصل شود تنها گره‌ها و کاربرانی به شبکه و داده‌های مندرج در آن دسترسی دارند که تایید شده‌اند. ممکن است برخی از گره‌های دارای دسترسی به سیستم، خارج از سازمان باشند و به همین علت نیز نیاز به نظارت و اجرای امنیت غیرقابل چشم‌پوشی است.

۵.۲. مدیریت تغییر و توسعه سیستم

ملاحظات امنیتی بیشتری که در مورد سازمان‌های استفاده کننده از فناوری دفتر کل توزیع شده وجود دارد، توجه به تغییرات و توسعه‌های صورت گرفته در خلال ارتباط با برخی نهادهای خارجی است. قبل از این‌که هرگونه ادغام یا حتی ارتباطی برقرار شود، لازم است که توافقی جمعی بین نهادها صورت بگیرد. از آن‌جا که در شبکه بلاکچین، تغییرات مورد نیاز این امکان را دارند تا از طریق هر گرهی با دسترسی به شبکه اعمال شوند، لازم است که گروهی خاص برای اعمال تغییرات به کار گمارده شوند.

فرایندهای پیاده‌سازی خاصی برای دفتر کل توزیع شده لازم است تا بتواند تغییرات و پیاده‌سازی جدید اعمالی به سیستم را به بهترین و موثرترین شکل ممکن مدیریت کند. به علاوه، کلیه اعضای شرکت کننده در شبکه باید از تغییرات و اهداف تغییرات اعمالی آگاهی کامل داشته باشند و آن را پذیرفته باشند.

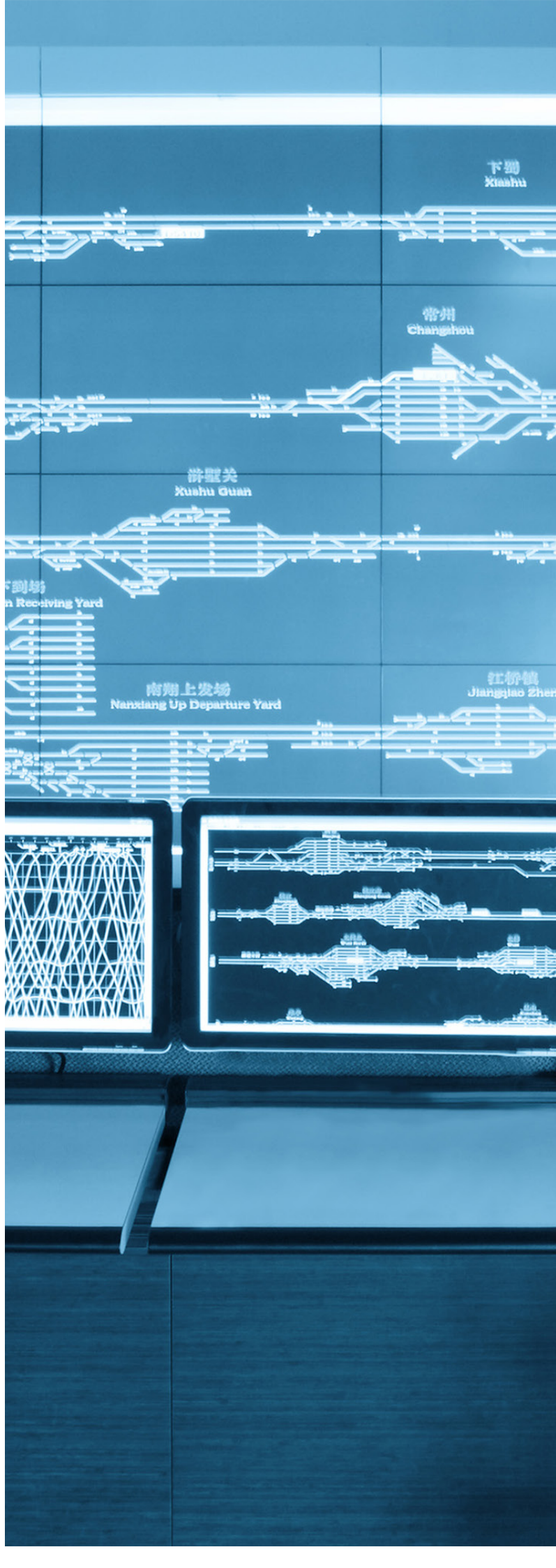
۵.۳. پردازش اطلاعات

اکثر فرایندهای فعلی که برای مدیریت عملیات فناوری اطلاعات، نظارت بر عملکرد و برنامه‌ریزی ظرفیتی، و همچنین تعمیر، تجهیز و نگهداری امکانات فناوری اطلاعات اعمال می‌شـــوند، در دفاتر کل توزیع شـــده نیز پیاده خواهند شـــد. به احتمال زیاد، بزرگترین تغییراتی که در پردازش اطلاعات شـــاهدش خواهیم بود، برنامه‌ریزی بـــرای ریکاوری حوادث خواهد بود. این مبحث را می‌توان در دو زیر مجموعه مورد بررسی قرار داد: سوء عملکرد شبکه، که می‌تواند منجر به از دست رفتن ارتباط با شبکه شود و از بین رفتن یکپارچگی داده‌ها، که می‌تواند در در وضعیت عادی، کلیه تغییرات اعمالی به سیستم را به عقب برگرداند (تغییرات را بی اثر کند).

قطع ارتباط با سیســـتم می‌تواند تبعـــات جبران‌ناپذیری را در پی داشـــته باشـــد. حتی اگر مقیاس این انقطاع در حد یک گره نیز باشد، سیستم از یکپارچگی و امنیت در خواهد آمد و در تعداد بالاتر نیز نتیجه کاملا روشن است. سازمان‌ها، برای این‌که بتوانند از این مشکل جان سالم به در ببرند، مجموعه‌ای از چندین گره را در مکان‌های مختلفی نگهداری می‌کنند تا ریسک از دست دادن ارتباط با شبکه را به حداقل برسانند.

با این حال، در صـــورت وقوع حوادث ناگواری همچون از دســـت رفتن ارتباطات اینترنتی، دیگر ســـازمان‌ها نیز قادر به اعتبارســـنجی و بررسی مجموعه گره‌ها نخواهند بود و تا زمانی که ارتباط مجددا برقرار شود و گره‌ها بتوانند با سایر گره‌ها هماهنگ شوند، سیستم در معرض ریسک قرار دارد.

پیکربندی شبکه باید به نحوی باشـــد که در ورت خارج شدن تعدادی از همتایان در سیستم، ســـایر اعضا بتوانند به فعالیت خود ادامه دهند. این، یکی از دلایل مهم اهمیت غیر متمرکزســـازی در فناوری دفتر کل توزیع شده اســـت. سیســـتم‌های همتا به همتای غیر متمرکز از درجه بالایی از انعطاف‌پذیری برخوردار هســـتند و همین ویژگی سودمند بلاکچین باید در سیستم‌ها و سازمان‌های خصوصی به کار گرفته شود.



ماهیت غیرمتمرکز دفتر کل توزیع شده، مستلزم رویکردی متفاوت برای مدیریت کنترل‌های اطلاعات و ارتباطات است.

طرح استمرار کسب‌وکار و بلاکچین

طرح استمرار کسب‌وکار (Business continuity planning) یکی از زیرمجموعه‌های مدیریت ریسک است. این طرح، با برخی از ریسک‌های بالقوه سیستم نظیر از دست رفتن زیرساختی که به ضرر شبکه تمام می‌شود سروکار دارد. ساختارشکنی در سیستم‌های می‌تواند به کاهش سودآوری و درآمدزایی، افزایش هزینه‌ها و کاهش بهره‌وری بیانجامد، ضمن این‌که این احتمال نیز وجود خواهد داشت که با افزایش آسیب‌پذیری سیستم و برخی اختلالات، اعتماد کاربران به شبکه نیز از دست برود.

با توجه به ماهیت دفتر کل توزیع شده، طرح استمرار شبکه، احتمال از دست رفتن داده‌ها و کاهش بهره‌وری و قدرت پردازش سیستم ناشی از از دست رفتن ارتباط را مورد بررسی قرار می‌دهد و ریسک‌هایی را در بوته ارزیابی قرار می‌دهد که می توانند به ضرر شبکه تمام شوند؛ ریسک‌هایی نظیر جرایم سایبری.

یک نمونه معمول از پیاده‌سازی طرح استمرار کسب‌وکار در سطح یک دفتر کل توزیع شده، باید بتواند طیف گسترده‌ای از پیچیدگی‌های فنی، از ذخیره‌سازی کلید تا بازسازی کلید به هنگام از دست دادن داده‌ها را تحت پوشش قرار داده و قادر باشد با ایجاد برخی کلیدهای جدید هنگام بروز جرایم سایبری از شبکه محافظت کند.

۶.۱. طرح استمرار کسب‌وکار

رویکردها و فعالیت‌های مبتنی بر طرح استمرار کسب‌وکار باید بتواند کلیه تهدیدها و ریسک‌های متوجه راهکار دفتر کل توزیع شده را تحت پوشش قرار دهد. فرایندهای تخفیفی مبتنی بر طرح استمرار کسب‌وکار، در حقیقت طراحی می‌شوند، پیاده‌سازی می‌شوند و مهم‌تر از همه تست می‌شوند تا در صورت بروز حادثه در شبکه بتوانند از آن حفاظت کنند و موجب ادامه حیات کسب‌وکار شوند.

علاوه بر این، این قبیل برنامه‌ها باید به صورت مداوم به‌روزرسانی شوند تا بتوانند در قبال ریسک‌های نوظهوری که همه‌روزه نیز به تعداد آن‌ها افزوده می‌شود نیز پاسخگو باشند. به عنوان مثال، پیشرفت در محاسبات کوانتومی می‌تواند امنیت رمزنگاری منحنی بیضوی (Elliptical Curve Cryptography) را تهدید کند و به همین دلیل نیز طرح استمرار کسب‌وکار، باید بتواند با پیشرفت خود و به‌روزرسانی مداوم، شبکه را برای تمهیدات امنیتی و سایبری مدرن‌تری که با این محاسبات نیز سازگاری داشته باشد تجهیز کند.

اغلب قابلیت‌ها و توابع رمزنگاری شده فناوری دفتر کل توزیع شده، بر اساس استانداردهای رمزنگاری (نظیر هش‌های SHA-۲۵۶ یا کلیدهای الگوریتم امضای دیجیتال منحنی بیضوی) ساخته‌اند. با این حال، برخی از سیستم‌ها نیز وجود دارند که از رمزنگاری‌های نوین و تست نشده‌ای استفاده کرده‌اند. بلاکچین‌هایی نظیر زیرکش (Zerocash) یا بلاکچین‌هایی که از رمزنگاری‌های هوموگرافیک استفاده می‌کنند.

چنین بلاکچین‌هایی، در صورتی که از حریم خصوصی و امنیت سایبری مناسب و مطمئنی برخوردار نباشد، در صورت بروز تغییرات دستخوش خرابی یا انقطاع کامل خواهند شد. به‌طور بالقوه، برخی از پیشرفت‌های محاسبات کوانتومی مدرن این قدرت را دارند امنیت اینترنت را نیز در کنار شبکه بلاکچین‌هایی با میلیارد دلار ارزش و حجم گسترده‌ای از کاربران مورد تعرض قرار دهند. در صورتی که محاسبات کوانتومی به قدر کافی پیشرفت کند، طرح استمرار کسب‌وکار در سازمان‌ها ملزم به نظارت مستمر روی دفاتر کل توزیع شده و آسیب‌پذیری‌های رمزنگاری خواهد بود تا بتواند از انقطاع و خرابی کامل شبکه در اثر تهدیدات تحمیلی ممانعت کند.

علاوه بر ریسک‌ها و تهدیدات رمزنگاری، سایر ریسک‌های بالقوه دفتر کل توزیع شده نظیر سرقت یا از دست رفتن کلیدهای رمزنگاری خصوصی یا رمزنگاری داده روی سیستم به وسیله بدافزارها نیز از اهمیت بالایی برخوردار است.

به عنوان مثال، باج‌افزار رمزنگاری (Crypto ransomware)، یکی از مهم‌ترین مواردی است که در حال حاضر کسب‌وکارها را تهدید می‌کند و این قابلیت را دارد تا با ایجاد محدودیت برای اعضای شبکه و کلیدهای باز رمزنگاری، آن‌ها را با مشکل مواجه کند. طبق اظهارات آزمایشگاه کیپراسکای لب (Kapersky Lab)، تعداد کاربرانی که در معرض حمه تروجان‌های رمزنگاری قرار گرفته‌اند، در سال ۲۰۱۶ بالغ بر ۱۸ درصد افزایش داشته است که که طیف گسترده‌ای از ۲/۳ میلیون کاربر از اقصی نقاط جهان را در بر می‌گیرد.

سیمانتک (Symantec) نیز اعلام کرده است که بالغ بر ۴۳ درصد از قربانیان تروجان‌های رمزنگاری، اعضای سازمان‌های جهانی و کارکنان آن‌ها بوده‌اند. حمله سایبری باج‌افزار واناکرای در سال ۲۰۱۷ میلادی نیز یکی از بزرگترین حملات سایبری تاریخ به شمار می‌آید که توانست تنها در همان چند روز نخست، صدها هزار کامپیوتر از سراسر جهان را تحت تاثیر خود قرار دهد.

۶.۲. طرح استمرار کسب‌وکار و زیرساخت کلیدی عمومی

در راهکارهایی که شامل زیرساخت کلیدی عمومی هستند، طرح استمرار کسب‌وکار تضمین یکپارچگی مکانیسم‌های تولید کلید (ماژول‌های امنیتی سخت‌افزاری، اعتبارسنجی و تایید افراد مجاز) را در بر می‌گیرد، فرایندهای کسب‌وکار تضمین نقل و انتقال ایمن کلیدهای خصوصی را در بر می‌گیرند و لایه اعتبارسنجی نیز کلیه این مکانیسم‌ها را پوشش می‌دهد. علاوه بر

این، برنامه‌های ریکاوری کسب‌وکار باید بتوانند با مسائلی نظیر افزایش یا از دست دادن داده‌ها نیز مقابله کرده و سطح تماس فرایندهای سیستم با مهاجمین سایبری را نیز به حداقل برسانند.
موفقیت طرح‌های استمرار کسب‌وکار، مستلزم عملکرد گروه‌های کاری امنیتی در داخل سازمان‌ها و اعتبارسنجی از متخصصین خارج از سازمان‌ها است تا اطمینان حاصل شود که بهترین رویکرد هنگام راه‌اندازی، پیاده‌سازی و تست اتخاذ شده است.
مارگارت هاروود جونز (Margaret Harwood-Jones)، در مقاله‌ای که در باب فناوری بلاکچین تالیف کرده است می‌گوید: «علیرغم این‌که طرفداران فناوری بلاکچین تاکید می‌کنند که این فناوری از امنیت سایبری خارق‌العاده‌ای برخوردار است، آن (بلاکچین) هنوز در مقیاس وسیع و در محیطی کاملا تحت نظارت و قانونمند امتحان نشده است. صرافی‌ها، بانک‌ها، کارگزاران و دلالان و همچنین مدیران صندوق‌ها، همگی تحت تاثیر جرایم سایبری قرار گرفته‌اند و رگولاتورها، به عملکرد این سازمان‌ها نیاز دارند تا اطمینان حاصل شود که نه تنها حفاظت سایبری این قبیل موسسات یکپارچه و جامع است، بلکه اقدامات سایبری در بستر ارائه دهندگان خدمات از جمله فروشندگان فناوری و استانداردها نیز حاکم است».

۶.۳. طرح استمرار کسب‌وکار در گره‌های شبکه

تاکنون، تمام آن‌چه که در مورد طرح استمرار کسب‌وکار مطرح شده بود، به سازمان‌ها و کسب‌وکارها باز می‌گشت. زمانی که پای خود فناوری دفتر کل توزیع شده و سرورهای آن به میان می‌آید، ماهیت غیرمتمرکز این فناوری کار را آسان می‌کند. هر دفتر کل توزیع شده، دارایی گره‌هایی است که وظیفه ثبت داده‌ها و پردازش آن‌ها را بر عهده دارند.

۶.۳.۱. شبکه‌های بلاکچین عمومی

در صورتی که از شبکه بلاکچین عمومی استفاده شده باشد، مانند شبکه بلاکچین‌های بیت‌کوین و اتریوم، از دست دادن داده‌ها امکان‌پذیر نیست، مگر این‌که بیش از ۱۰،۰۰۰ گره از اقصی نقاط جهان از دسترس خارج شده باشند.

۶.۳.۲. شبکه‌های بلاکچین خصوصی

در صورتی که از شبکه‌های خصوصی بلاکچین در راه‌اندازی و پیاده‌سازی فناوری دفتر کل توزیع شده در فضایی امن نظیر وی‌پی‌ان (VPN) استفاده شده باشد، گره‌ها باید به منظور جلوگیری از قطع جریان سیستم و از دسترس خارج شدن داده‌ها به صورت مجموعه‌هایی در جاهای مختلف نگهداری شوند.

با این حال، با توجه به ماهیت پیاده‌سازی فناوری دفتر کل توزیع شده، ممکن است برخی از گره‌ها، در زیرساخت‌های سایر شرکت‌ها یا سازمان‌ها (مثلا در زیرساخت موسسات مالی که عضو کنسرسیوم هستند) نیز وجود داشته باشد و داده‌ها در برخی گره‌ها تکرار شوند. این روند، ریسک از دست دادن داده‌ها را در سیستم کاهش می‌دهد. البته، برای بازیابی داده‌ها پس از رفع مشکلات و قطعی‌های به وجود آمده، باید اطمینان حاصل شود که سیستم، توانایی لازم برای برقراری ارتباط مجدد و ریکاوری داده‌ها را دارد و بلاکچین می‌تواند بازیابی و بازسازی شود.

۶.۴. متخصصین امنیتی

در این فصل، در این خصوص بحث کردیم که طرح استمرار کسب‌وکار چگونه می‌تواند برخی نگرانی‌ها و پیچیدگی‌های دنیای رمزنگاری و جرایم سایبری را از سر راه بردارد. متخصصین امنیتی، چه داخلی و چه خارجی، نقش مهمی در تضمین نحوه اجرای فرایندها مطابق با دستورالعمل‌های صادره و پیشرفت‌های رمزنگاری ایفا می‌کنند.
علیرغم این‌که بسیاری از نگرانی‌های طرح استمرار کسب‌وکار با روی کار آمدن فناوری دفتر کل توزیع شده، با ماهیت غیرمتمرکز آن کاهش یافته‌اند، اما باید در نظر داشت که کلیه این راهکارها، برای سیستمی وسیع‌تر، با سرورهای متمرکز و پایگاه‌های داده‌ای سنتی ارائه می‌شوند. به همین دلیل نیز حفظ تمامیت داده‌ها در سطح سیستم اصلی، و تداوم خدمات، بادید به صورت مستمر مد نظر قرار گیرد.
در نهایت، از آن‌جا که پیاده‌سازی فناوری دفتر کل توزیع شده در مقیاس عملی، هنوز آن‌گونه که باید جای نیفتاده و وارد فاز عملیاتی نشده است، خطراتی بدوی در همین ابتدای مسیر وجود دارند.
دلیل این امر نیز آن است که به احتمال زیاد، در صورت پیاده‌سازی کامل بلاکیچن در سطح شرکت‌ها، هر شکت از طرح استمرار کسب‌وکار ویژه و منحصر به‌فردی بهره خواهد برد و این موضوع، نیاز به اعتبارسنجی و هماهنگی خارجی را افزون‌تر می‌کند. بلاکچین، به تنهایی یک فناوری قدرتمند و جدید است که تنها برخی پیاده‌سازی‌های مرجع محدود برای آن صورت گرفته است، اما جنبه‌های اصلی این فناوری (نظیر زیرساخت‌های کلیدی عمومی، پاسخ‌های همتا به همتا، ثبت و ذخیره‌سازی داده و پیام‌رسانی)، دهه‌ها است که در سایر سیستم‌های سنتی وجود دارند.
بنابراین، علیرغم این‌که کل فناوری و مزایا و قابلیت‌هایی که ارائه می‌دهد جدید هستند، اجزای آن به خوبی قابل درک هستند. در نتیجه، تضمین کیفیت طرح‌های استمرار کسب‌وکار برای راهکارهای مبتنی بر فناوری بلاکچین، مستلزم گردآوری و تطبیق این فرایندهای موجود در یک پکیج یکپارچه است.

این گزارش با حمایت شرکت ققنوس توسط تیم راه پرداخت، ترجمه و بازتولید شده است