

# فعالان عرصه امنیت سایبری جذب کدام شهرها می شوند؟

میترا جلیلی  
خبرنگار

خبره نیاز دارد. در این زمینه کشورهای مختلف برنامه‌ریزی‌های متفاوتی دارند. حتی برخی دامنه آموزش را به سنین بسیار پایین کشانده‌اند تا کودکان از سن کم با مفاهیم کلی امنیت سایبری، کدنویسی، مقابله با تهدیدات سایبری و... آشنا شوند و درصورت شناسایی استعدادهایی در این زمینه بلافاصله آنها را به سمت این حوزه و آموزش‌های مرتبط با آن هدایت کنند. به این ترتیب در آینده می‌توان تعداد زیادی متخصص حوزه امنیت سایبری با سابقه بالا در جهان داشت تا مقابل مجرمان سایبری قد علم کنند. اما برترین شهرها برای فعالان این حوزه کدام است؟

## ■ بهشت فعالان حوزه امنیت سایبری

با توجه به چالش‌ها و فرصت‌های مختلف در زمینه امنیت سایبری، شرکت Techshielder مستقر در بریتانیا که در مورد امنیت و حریم خصوصی اینترنت مشاوره می‌دهد، یک نظرسنجی جهانی در مورد اینکه چگونه یک متخصص امنیت سایبری می‌تواند پیشنهاد شغلی پر درآمد دریافت کند، انجام داده است و در این میان معیارهای متعددی از جمله متوسط میزان حقوق، در دسترس بودن شغل و هزینه زندگی برای یافتن بهترین مکان برای زندگی متخصصان امنیت سایبری و همچنین مهارت‌های مورد نیاز برای یادگیری در سال ۲۰۲۱ را مورد توجه قرار داده است.

به‌رحال با توجه به افزایش میزان حملات سایبری در جهان، دنیای امنیت سایبری در حال رشد انفجاری است و این عرصه همچنان روبه توسعه و گسترش است. به همین دلیل هم میزان تقاضا برای به کارگیری متخصصان حوزه مشاغل مرتبط با امنیت سایبری روبه فزونی است و در بیشتر نقاط جهان شاهد استقبال از فعالان این عرصه هستیم و تنها به شهرهای معرفی شده در این گزارش نباید بسنده کرد.

طبق این گزارش جهانی، واشنگتن دی سی، سنگاپور، برلین و لوکزامبورگ بهشت فعالان حوزه امنیت سایبری هستند و این افراد می‌توانند با سرعت کار مورد نیاز خود را با حقوقی مناسب پیدا کنند. حضور واشنگتن دی سی در صدر جدول چندان تعجب‌آور

روند رو به رشد حملات سایبری در جهان که از مدارس گرفته تا بیمارستان‌ها و حوزه‌های انرژی و...را تحت تأثیر قرار می‌دهند، موضوع امنیت سایبری را با یک چالش بی‌سابقه مواجه کرده است. به همین دلیل هم آموزش متخصصان به منظور پاسخگویی به نیازهای رو به رشد تهدیدات روزافزون حملات سایبری و به کار گرفتن آنها در بخش‌های مختلف مورد توجه قرار گرفته است. اما کدام شهرهای جهان می‌توانند متخصصان این حوزه را بیشتر جذب کنند و کدام بخش‌های سایبری باید بیشتر در کانون توجه این افراد ماهر قرار گیرد؟

## ■ هر ۴ ثانیه یک حمله سایبری

مطالعات مؤسسه Accenture نشان می‌دهد که هر ۴۰ ثانیه یک حمله سایبری در نقطه‌ای از جهان رخ می‌دهد و هریک از این حملات به طور متوسط ۱۳ میلیون دلار برای سازمان‌ها هزینه دربر داشته است. از سوی دیگر بسیاری، ۶ ماهه نخست ۲۰۲۱ را یک آزمون بزرگ برای صنعت امنیت سایبری در تاریخ می‌دانند که عملکرد مناسبی نداشته چراکه تعداد این حملات و زیان اقتصادی ناشی از آن به طور چشمگیری بالا رفته و ازسوی دیگر ۲۲ درصد از حمله‌های سایبری نیمه نخست ۲۰۲۱ ازنوع حملات باج افزاری بوده‌اند.

با افزایش حملات سایبری، بیش از پیش کمبود نیروهای متخصص امنیت سایبری در جهان احساس می‌شود و مشاغل مرتبط با تأمین امنیت سایبری همچنان تقاضای زیادی در سراسر جهان دارند. از آنجا که در حملات هکری، فعالیت مجرمان سایبری که از ناحیه برخی دولت‌ها حمایت می‌شوند پیچیده‌تر می‌شود، برای شرکت‌ها بسیار مهم است که توانایی پاسخگویی خود را افزایش دهند و در این مسیر، استخدام نیروی کار ماهر سایبری در اولویت است.

اما مشکل اینجاست که متأسفانه مشاغل سراسر جهان با کمبود فزاینده متخصصان امنیت سایبری روبه‌رو هستند و تازه‌ترین گزارش سالانه Cybersecurity Workforce نشان می‌دهد که این صنعت در حال حاضر به حدود ۳ میلیون فعال امنیت سایبری

## گام بلند اسنپ چت

**علیرضا احمدی** - با شیوع کرونا میزان حضور کاربران در فضای مجازی و استفاده آنها از شبکه‌های اجتماعی روندی صعودی به خود گرفته است و اسنپ چت نیز روزهای پررونقی را می‌گذراند.

همین چند سال پیش نگرانی‌های زیادی وجود داشت که اسنپ، شرکت مادر اسنپ چت نتواند به عنوان یک شرکت مستقل زنده مانده و به فعالیت خود ادامه بدهد. قیمت سهام این شرکت به دنبال یک طراحی مجدد فاجعه بار و نامناسب باعث شد تا رشد کاربر برای این پلتفرم را بسیار کاهش دهد و شرکت‌های تبلیغاتی هم علاقه چندانی به همکاری با اسنپ نداشته باشند اما پس از مدتی این کمپانی با ارائه اسنپ چت به عنوان زیرمجموعه خود موفق شد تا حد زیادی ناکامی‌های خود را جبران کند به گونه‌ای که حالا دیگر این برنامه پیام رسان ۲۹۳ میلیون کاربر فعال روزانه دارد.

به هر حال اکنون اوضاع بسیار متفاوت شده است و اسنپ چت از سال ۲۰۱۷ یعنی سال انتشار عمومی، رشدی بسیار سریع داشته است. این پیام رسان مبتنی بر دوربین بتازگی در گزارشی اعلام کرده است که در سه ماهه دوم سال ۲۰۲۱ روزانه ۱۳ میلیون کاربر جدید جذب کرده است که این رقم نشان از افزایش ۲۳ درصدی نسبت به مدت مشابه سال قبل دارد. این بدان معناست که روزانه ۲۹۳ میلیون نفر در سراسر جهان از اسنپ چت استفاده می‌کنند، این در حالی است که این رقم در چهار سال پیش حدود ۱۷۳ میلیون نفر بوده است. اگر بخواهیم به موفقیت این اپلیکیشن بیشتری ببینیم تنها کافی است نگاهی مقایسه‌ای با توئیتر داشته باشیم. برای توئیتر در سه ماهه دوم سال ۲۰۲۱ روزانه ۲۰۶ میلیون کاربر گزارش شده است. بنابراین اسنپ چت موفق تر عمل کرده است. میزان درآمد اسنپ نیز با افزایش ۱۱۶ درصدی نسبت به سال گذشته به ۹۸۲ میلیون دلار رسیده است و می‌توان گفت که در این بخش هم این بهتر از توئیتر یا فیس بوک عمل کرده است.

ایران اقدام جدید در نتیجه پاندمی کرونا به دست آمده است، چراکه مردم بیشتر وقت خود را به صورت آنلاین می‌گذرانند. ایوان اشیپگل، مدیرعامل اسنپ هم گفته است: انتظار می‌رود با پایان یافتن کرونا و قرنطینه در جهان، همچنان تعداد کاربران این پیام رسان با سرعت بیشتری رشد کند، چراکه اسنپ چت با هدف حضور در کنار دوستان طراحی شده است.

گفته می‌شود بیشتر رشد کاربران اسنپ در سه ماهه دوم از خارج از بازارهای اصلی آن در امریکا، شمالی و اروپا حاصل شده است، جایی که تبلیغ کنندگان هزینه‌های بیشتری را برای دسترسی یافتن به مردم پرداخت می‌کنند. این بدان معناست که اسنپ کارهای زیادی پیش رو دارد تا بتواند از کاربران جدید خود به طور مؤثر درآمد کسب کند. همچنین باید گفت آنچه که بین اسنپ و فیس بوک مشترک است، علاقه به واقعیت افزوده (AR) را می‌توان مثال زد.

این فناوری از طریق صفحه نمایش تلفن یا عینک هوشمند، گرافیک رایانه را در دنیای واقعی نشان می‌دهد. اشیپگل سال‌هاست که سرمایه‌گذاری اسنپ در واقعیت افزوده را مطرح می‌کند و اخیراً این شرکت اقدام به ایجاد ویژگی‌های خرید کرده است. در نهایت این شرکت به هر کسی این امکان را می‌دهد تا اگر محصولی را با دوربین Snapchat اسکن کند، آن را عمل تجربه کرده و بدون اینکه از برنامه خارج شود، آن را خریداری کند. اسنپ اخیراً عینک‌های جدید Spectacles را هم با نمایشگرهای AR عرضه کرده هرچند این عینک‌ها فعلاً فقط برای سازندگان منتخب AR موجود است.



نیست زیرا پایتخت مقر ادارات دولتی امریکاست که بسیاری از متخصصان امنیت سایبری را استخدام می‌کنند. درحالی که این شهر با کسب نمره کلی ۱۷۰۵۸ در جایگاه نخست جهان قرار گرفته برای فعالان حوزه امنیت سایبری میانگین حقوق ۸۴ هزارو ۶۲۸ پوند را پرداخت می‌کند و متخصصان به این حوزه به میزان بالایی به شغل‌های مرتبط با تحصیلات خود دسترسی دارند که این شاخصی بسیار مناسب است.

جایگاه دوم این لیست هم با نمره کلی ۱۶۰۴۴ دراختیار سنگاپور قرار دارد. این شهر واقع در جنوب شرق آسیا البته ازنظر شاخص میزان دسترسی به شغل، از واشنگتن دی سی هم پیشی گرفته و با عدد ۱۰، بالاترین امتیاز را از بین تمام شهرهای مورد بررسی دارد. با وجود این، دستمزد متوسط ۵۵ هزارو ۵۷۷ پوند و هزینه بالای زندگی، این شهر را در رده دوم قرار می‌دهد. سنگاپور همچنین بیشترین تعداد فارغ‌التحصیلان را در زمینه امنیت سایبری دارد.

برلین هم با مجموع امتیاز ۱۵۰۴۱ سومین شهر مناسب جهان برای فعالان حوزه امنیت سایبری به شمار می‌رود که عدد دسترسی آنها به شغل مرتبط، ۳۰۱۸ و دستمزد متوسط آنها نیز ۷۰ هزارو ۱۴۱ پوند است. با وجود بالاتر بودن میزان درآمد، ولی شاخص‌های دیگر، رتبه کلی این شهر را پایین‌تر از سنگاپور و واشنگتن دی سی قرار داده است.

## چگونه فیلم‌ها را ویرایش کنیم؟

بسیاری از ما فیلم‌های خانوادگی از تولد، سفر، دورهمی‌ها و... را در سیستم‌های خود داریم که گاه زمان زیادی از آنها گذشته است. بی‌شک کیفیت دوربین‌ها در گذشته پایین‌تر بوده و همین موضوع باعث می‌شود تا این فیلم‌ها بی‌کیفیت به‌نظر بیایند. برای با کیفیت‌تر شدن، پررنگ شدن رنگ‌ها، استفاده از افکت‌های مختلف و... می‌توان از نرم افزارها استفاده کرد که یکی از بهترین نمونه‌ها در این زمینه، نرم افزار HitPaw Toolkit است.

نرم افزار HitPaw Toolkit یک نرم افزار ویرایش حرفه‌ای فیلم است که ابزارهای گوناگون و گسترده‌ای را در اختیار کاربران خود قرار می‌دهد تا فیلم‌ها را مطابق سلیقه‌شان تغییر بدهند.

شما به‌عنوان کاربر با کمک این نرم افزار می‌توانید ویدیوهایی خیره کننده و فوق‌العاده را ایجاد کنید. همچنین می‌توانید ویدیوهای خود را در HitPaw Toolkit ویرایش کرده و عملیاتی نظیر برش، چرخش، تنظیم سرعت، افزودن افکت و... را روی آنها انجام دهید.

## روبات خاص مناطق ناهموار ساخته شد



می‌ماند. گفتنی است، اگر این روبات با مانعی مانند چوب یا الوارهای افتاده در جنگل، جاده و... یا سنگ‌های بزرگ روبه‌رو شود، می‌تواند بازوهای جلویی خود را در بالای جسم بالا بیاورد و آنها برای بالا بردن بارها استفاده کند. همچنین

و صنعت همکاری کنند. آماده‌سازی بهتر فارغ‌التحصیلان جدید و تجهیز آنها به مهارت‌های مورد نیاز برای موفقیت در حرفه امنیت سایبری هند در کانون توجه قرار گرفته است.

## ■ نیجریه و پاکستان در قعر جدول

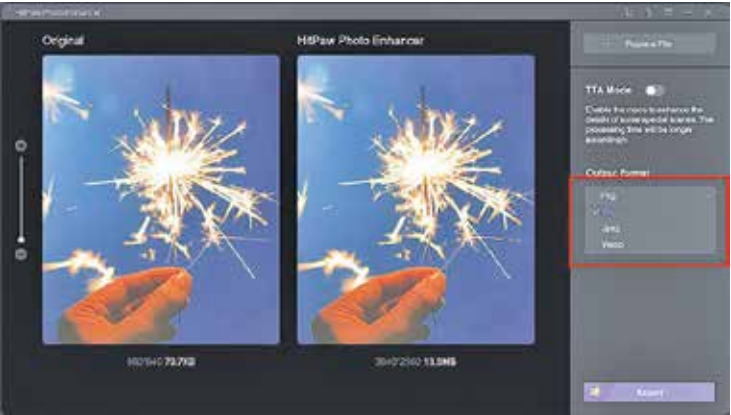
در آن سوی دیگر این فهرست نام آبوja از شهرهای نیجریه را می‌بینیم که کمترین درآمد را برای فعالان این حوزه رقم می‌زند و متخصصان این حوزه علاقه چندانی به فعالیت در این شهر ندارند. اسلام آباد پاکستان هم از شهرهایی است که فرصتی بسیار محدود برای فعالان این حوزه دارد و درمجموع رتبه ۱۰۱ را به خود اختصاص داده است که یکی از کمترین امتیازهای موجود است.

در این گزارش همچنین اشاره شده است که همزمان با شیوع کرونا، برزیل در زمینه تأمین امنیت سایبری کارمندان دورکار بسیار خوش درخشید و به برترین کشور جهان در این زمینه تبدیل شد که بخش عمده آن را مدیون فعالان عرصه امنیت سایبری است. کلمبیا پس از برزیل از نظر این شاخص در جایگاه دوم جهان قرار گرفت و پرتغال هم وضعیت نسبتاً مناسبی دارد.

## ■ مهارت‌های سایبری مورد نیاز ۲۰۲۱

اما بیشترین مهارت‌های مورد نیاز حوزه امنیت سایبری در سال ۲۰۲۱ کدامند؟ در حال حاضر جهان حداقل به ۳ میلیون فعال حوزه امنیت سایبری نیاز دارد و یکی از پرتقاضاترین مهارت‌های مورد نیاز در این عرصه، تأمین امنیت شبکه است. پس از آن، شناسایی تهدیدات سایبری از اهمیت بالایی برخوردار است و تقاضا برای آن بالاست. توانایی ارزیابی تهدیدات احتمالی و ممانعت از موفقیت هکرها هم از نیازهای اصلی هراس‌زمان، کسب و کار و هر کاربر اینترنت به شمار می‌رود.

همچنین از آنجا که تعداد زیادی از داده‌ها امروزه در فضاهای ابری ذخیره می‌شود، بنابراین ایجاد زیرساخت‌های ابری و تأمین امنیت آنها اهمیت زیادی دارد و فعالان حوزه سایبری در این فضا فرصت‌های شغلی ویژه‌ای دارند تا از نشت داده‌ها با حذف و سرقت احتمالی دیتاها جلوگیری شود.



یکی از ویژگی‌های فوق‌العاده و منحصر به فرد این برنامه، این است که می‌توانید در عرض چند دقیقه ویدیوی خود را حتی بدون داشتن دانش تکنولوژی زیاد، به GIF تبدیل کنید اما این همه ماجرا نیست و با کمک این نرم افزار شما می‌توانید عملاً به ویدیوهای خود موسیقی را نیز اضافه کنید. در واقع نرم افزار HitPaw Toolkit این امکان را

به شما می‌دهد که در کوتاه ترین زمان ممکن تغییرات مورد نظر تان را در یک فیلم ویدیویی اعمال کنید و از دیدن آن لذت ببرید. اگر شما هم علاقه مندید این نرم افزار را بدون داشتن دانش تکنولوژی زیاد، به GIF تبدیل کنید اما این همه ماجرا نیست و با کمک این نرم افزار شما می‌توانید عملاً به ویدیوهای خود موسیقی را نیز اضافه کنید. در واقع نرم افزار HitPaw Toolkit این امکان را

به شما می‌دهد که در کوتاه ترین زمان ممکن تغییرات مورد نظر تان را در یک فیلم ویدیویی اعمال کنید و از دیدن آن لذت ببرید. اگر شما هم علاقه مندید این نرم افزار را بدون داشتن دانش تکنولوژی زیاد، به GIF تبدیل کنید اما این همه ماجرا نیست و با کمک این نرم افزار شما می‌توانید عملاً به ویدیوهای خود موسیقی را نیز اضافه کنید. در واقع نرم افزار HitPaw Toolkit این امکان را

با حضور وزیر ارتباطات و فناوری اطلاعات

## آخرین جلسه شورای معاونان وزارت ارتباطات برگزار شد



آخرین جلسه شورای معاونان وزارت ارتباطات با موضوع آخرین اقدامات و فعالیت‌های معاونت‌ها و سازمان‌های تابع این وزارتخانه برای انجام بهینه انتقال اطلاعات و تجارب به وزیر جدید برگزار شد. به گزارش «ایران»، محمدجواد آذری جهرمی وزیر ارتباطات در آخرین جلسه شورای معاونان وزارت ارتباطات، از معاونان که طی ۴ سال وی را همراهی کردند قدرانی کرد. وی با برشمردن بخشی از دستاوردهای کلان وزارت ارتباطات در این سال‌ها و نحوه مواجهه با موانع و مشکلات و تعامل با دیگر دستگاه‌ها، موفقیت‌های به دست آمده را حاصل همدلی و تلاش مجدانه و مستمر معاونان و مدیران و کارشناسان وزارت ارتباطات دانست. آذری جهرمی گفت: تمام تلاش ما تحقق آرمان دسترسی همگانی و عدالت ارتباطی بود که با اتصال همه شهرها و بیش از ۹۸ درصد روستاهای کشور به شبکه پایداری و پرسرعت تا حدود زیادی محقق شد. در این جلسه همه معاونان گزارش کوتاهی از عملکرد مجموعه تحت مدیریت خود و نحوه انتقال مدیریت و تجربیات هر بخش را به وزیر و تیم جدید ارائه کردند.

## هک آیفون فعالان سیاسی با جاسوس افزار «پگاسوس»

بررسی‌های مؤسسه سیتیزن لپ نشان می‌دهد حکومت بحرین با استفاده از نرم افزار جاسوسی پگاسوس، آیفون‌های فعالان سیاسی بحرینی را هک کرده است. به گزارش مهر، ان‌اس‌اوگروپ که یک شرکت فعال در خاک سرزمین‌های اشغالی است، بین ماه ژوئن سال ۲۰۲۰ تا ماه فوریه سال ۲۰۲۱ انواع ابزار جاسوسی و کنترل و نظارت را به حکومت آل خلیفه فروخته است تا از فعالان سیاسی و حقوق بشری جاسوسی کند و به گوشی‌های آنها نفوذ کند. بر اساس گزارش سیتیزن لپ، گوشی‌های آیفون ۹ فعالان سیاسی بحرینی با استفاده از برنامه جاسوسی پگاسوس شرکت ان‌اس‌اوگروپ هک شده و با استفاده از آسیب‌پذیری‌هایی در برنامه پیام‌رسان آی‌مسیج اپل برای سرقت اطلاعات این گوشی‌ها اقدام شده است. این دو آسیب‌پذیری که در سال‌های ۲۰۲۰ و ۲۰۲۱ شناسایی شده‌اند، به ترتیب KISMET و FORCEDENTRY نام دارند و به دولت بحرین کمک کرده‌اند محتوای آیفون‌ها فعالان سیاسی و حقوق بشری را هک کند. حداقل چهار نفر از فعالان سیاسی مذکور توسط هکری با نام مستعار LULU هک شده‌اند که از جمله اپراتورهای شرکت پگاسوس است که به‌شدت مورد اعتماد دولت بحرین بوده و بارها از پگاسوس به‌نفع حکام آل خلیفه سوء استفاده کرده است. دو نفر از این ۹ نفر فرد هک شده در لندن زندگی می‌کنند و یکی از آنها هم در زمان هک شدن آیفون خود در لندن بوده است. افراد یادشده به دو حزب سکولار و شیعه وعد و الوفاق وابستگی دارند. علاوه بر حکومت بحرین، دولت‌های عربستان سعودی و امارات هم از جاسوس افزار پگاسوس برای سرقت اطلاعات گوشی‌های شهروندان خود سوء استفاده کرده بودند.

## هوای مجوز خرید تراشه از امریکا را دریافت کرد

دولت امریکا بعد از مدت‌ها مجوزی به ارزش صدها میلیون دلار صادر کرد تا شرکت چینی هوای بتواند تراشه‌هایی برای برخی قطعات خود روهایی مختلف خریداری کند. به گزارش فارس، هوای مدت‌هاست که در فهرست سیاه وزارت بازرگانی امریکا قرار دارد و حق خرید هیچ تراشه یا سخت افزار پیشرفته‌ای را از شرکت‌های امریکایی ندارد. دلیل این مسأله نگرانی‌های امنیتی اعلام شده است. در عین حال هوای با تراشه‌های دیگر همچنان ارتباطی با دولت چین ندارد و داده‌های خصوصی کاربران را در اختیار افراد و شرکت‌های ثالث قرار نمی‌دهد. هوای بزرگ‌ترین شرکت سازنده تجهیزات مخابراتی در جهان است و محدودیت‌های تجاری دولت ترامپ در زمینه فروش تراشه و دیگر محصولات فناوریانه به آن مشکلاتی را برای ساخت گوشی و تجهیزات شبکه‌ای توسط هوای به وجود آورده است. باین نیز این ممنوعیت‌ها و محدودیت‌ها را تعدید کرده و مانع از فروش تراشه‌های مورد نیاز هوای برای راه‌اندازی شبکه‌های نسل پنجم می‌گردد است. تراشه‌هایی که هوای مجوز خرید آنها را از امریکا دریافت کرده برای ساخت نمایشگرهای ویدیویی و حسگرهای خودروها مورد استفاده قرار می‌گیرند. به نظر می‌رسد دولت امریکا به علت عدم حساسیت فناوری تراشه‌های یادشده اجازه فروش آنها را به چین صادر کرده است.

## بلاکچین فناوری پیشران در مدیریت شهری کار آمد

مهدی بیبا  
کارشناس بین‌المللی فناوری اطلاعات

این روزها با تحول دیجیتال رخ داده در دنیا، انتظارات برای توسعه شهرهای هوشمند افزایش یافته است. همچنین با رکود اقتصادی ناشی از COVID-۱۹، نیاز به مدیریت شهری کارآمدتر، بیش از پیش احساس می‌شود. بین سال‌های ۲۰۲۰ تا ۲۰۲۴، بازار توسعه شهرهای هوشمند، به میانگین نرخ سالانه ۲۲ درصد رشد می‌کند و مبلغ آن تقریباً ۲.۱ تریلیون دلار است. در این میان، فناوری‌های پیشران، از جمله بلاکچین می‌توانند نقش کلیدی در حل مسائل اجتماعی و دستیابی به مدیریت شهری کارآمد را ایفا کنند. بلاکچین، افراد در شبکه را قادر می‌سازد تا داده‌ها را با درجه اطمینان و شفافیت بالا بدون نیاز به مدیر متمرکز مبادله کنند. فناوری بلاکچین با پدیدار شدن در عرصه FinTech (فین تک)، اصطلاحاً نقل مجالس شد اما بتدریج سایر صنایع مثل اینترنت اشیا، هوش مصنوعی، واقعیت مجازی، کلان داده‌ها و البته حوزه مخابرات و ارتباطات هم از آن تأثیر می‌پذیرند. برنامه‌های نوآورانه و امکانات متنوع بلاک‌چین برای بهبود و نوسازی ساختار سنتی، معیوب و ناامن فعلی ارتباطات موبایلی و مخابرات نوید آینده بهتری برای این صنعت را می‌دهد. آینده‌ای که در آن مشترکان دغدغه از دست رفتن داده‌های شخصی را ندارند و می‌توانند به‌صورت کاملاً شفاف بسته‌های مصرفی را مشاهده کنند و در ضمن از خدمات ارزش افزوده هم بهره‌مند شوند. شهرهای هوشمند می‌توانند از چهارچوبی که اخیراً برای قابلیت همکاری منتشر شده است که یک مدل سه لایه برای استفاده از بلاک چین ارائه می‌دهد، یاد بگیرند. لایه اول شامل شبکه‌ای از مدل‌های حکمرانی، استانداردسازی داده‌ها، چهارچوب‌های قانونی و مدل‌های تجاری است. لایه بستر شامل مکانیسم‌های اجماع، قراردادهای هوشمند، احراز هویت و مجوز است. لایه زیرساخت شامل لایه ابر ترکیبی، بلاکچین مدیریت شده و اجزای اختصاصی است.

توجه به این نکته ضروری است که دستیابی به قابلیت همکاری بیش از حل یک مشکل فنی نیاز دارد. همچنین نیاز به حل مسأله‌ای از نظر حکمرانی، مالکیت داده‌ها و مدل‌های تجاری دارد که ذینفعان اکوسیستم را برای همکاری با یکدیگر ترغیب می‌کند. در واقع بلاکچین یک شبکه یک به یک است که برای رسیدن به توافق، به هیچ نهاد متمرکزی وابسته نیست. هراحد، در این تکنولوژی دفتر کل توزیع شده (Distributed Ledger Technology) یک نسخه از دفتر کل را دارا بود که هر تراکنش انجام شده به یک بلاک اختصاص پیدا می‌کند تا به روش توافق جمعی حاصل از بلاکچین مورد تأیید قرار گیرد. گفتنی است، هر بلاک به‌وسیله فرایندهای دیگری هم قابل تأیید است که اگر مورد تأیید قرار گیرد، امنیت سایبری آن تأمین شود و قابل دستکاری یا ویرایش نخواهد بود.