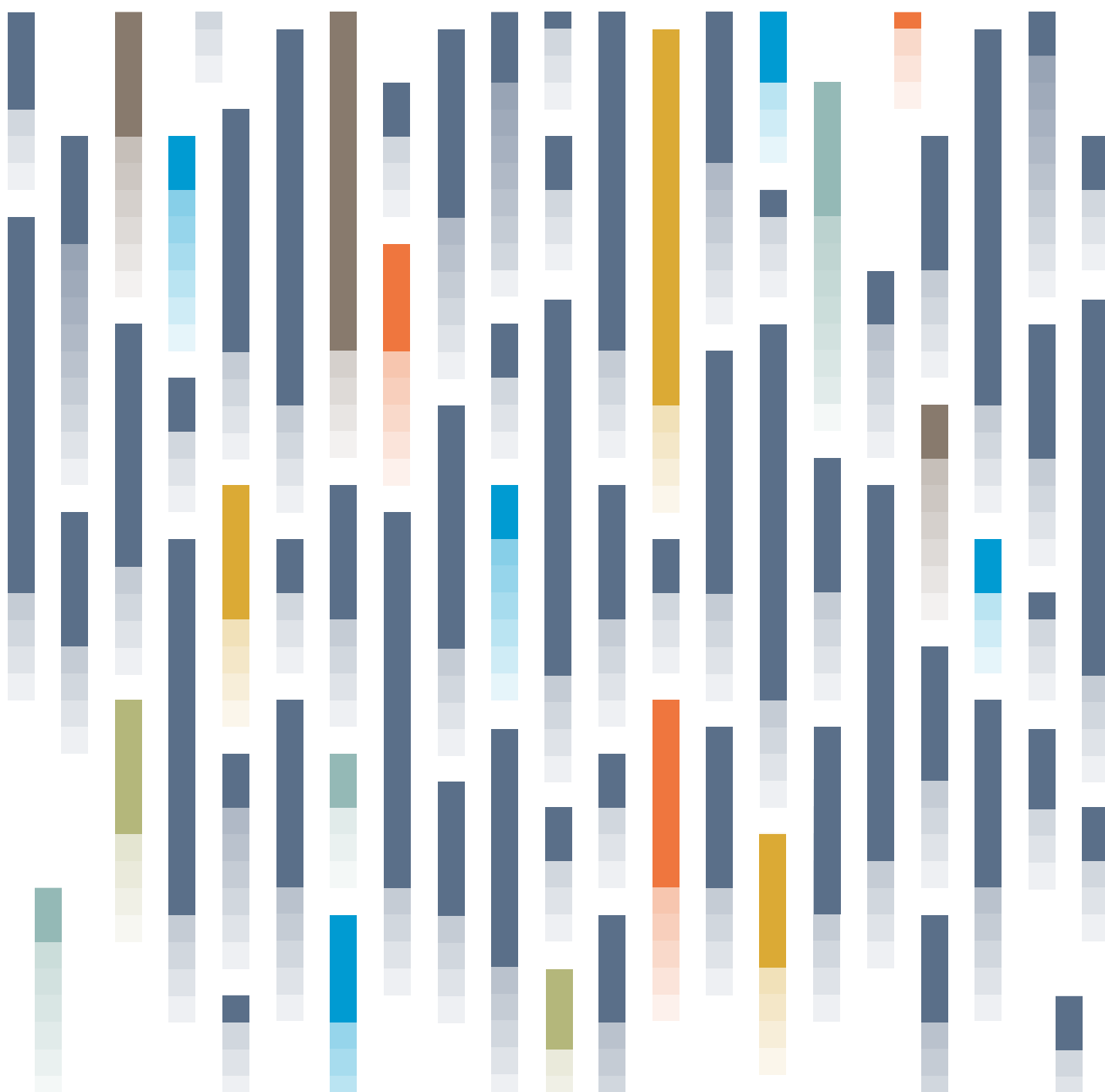
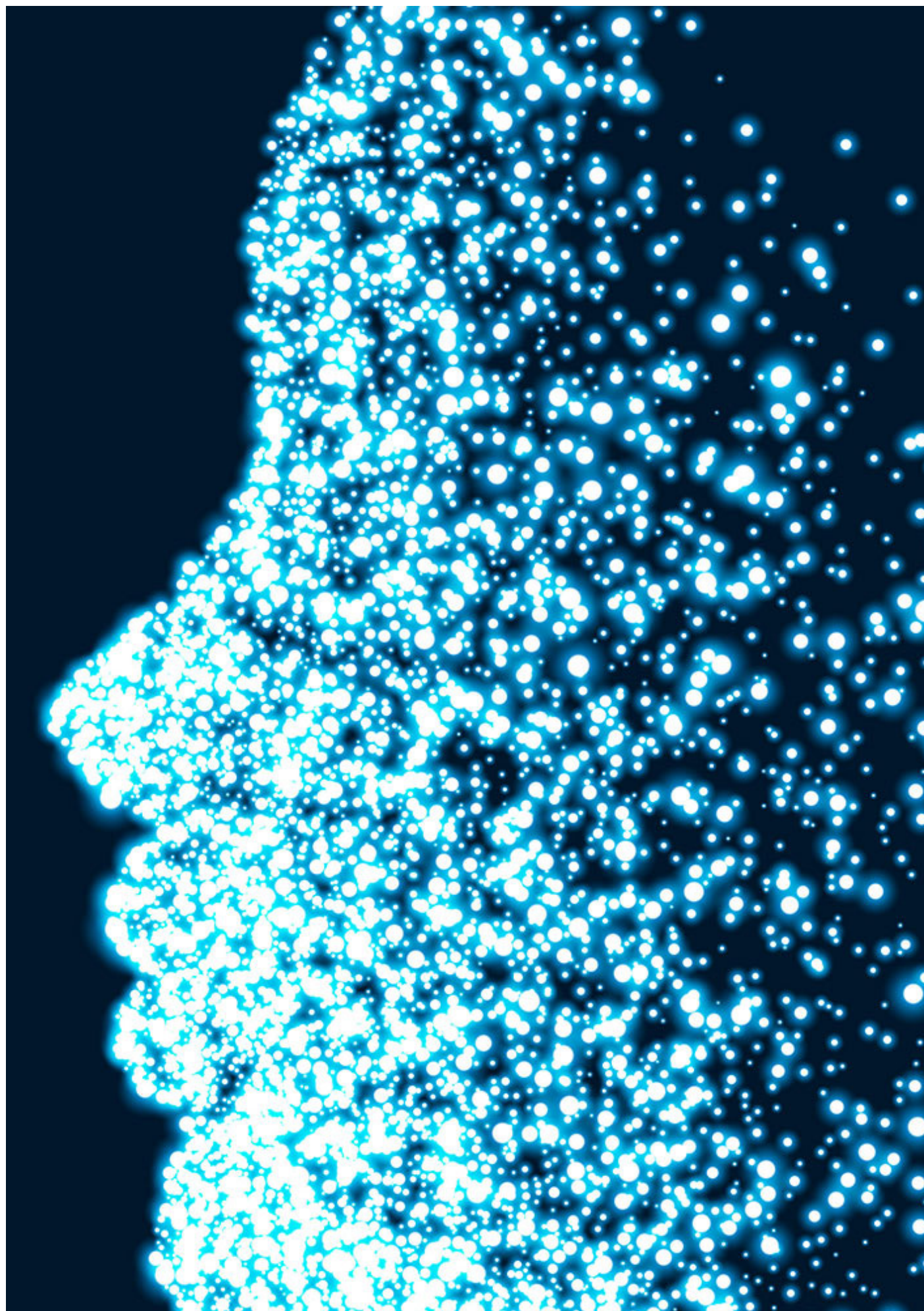


هویت دیجیتال





مقدمه

اینترنت طلیعه دار انقلابی در ارتباطات شد. با اینترنت می توانیم به صورت فوری اطلاعات و تقریباً هر چیز دیگری که می توان آن را دیجیتالی ساخت را با تمام افراد در جهان به اشتراک بگذاریم. پیامد آن انفجاری در بهره‌وری و به هم پیوستگی بود.

هر چند اینترنت از به اشتراک گذاشتن اطلاعات پشتیبانی می کند اما توانایی کمی در بررسی منبع و اعتبارسنجی داده‌ها دارد. این توانایی اندک به انواع مشکلات، از کلاهبرداری گرفته تا فیشینگ و اخبار جعلی در عرصه اینترنت دامن زد. همچنین عدم وجود یک لایه احراز هویت و در عین حال مناسب به این معناست که اینترنت یک کانال ایمن و یژه برای تراکنش‌ها نیست. این موضوع در عصری که تجارت الکترونیک در حال رونق است ممکن است تعجب‌آور به نظر رسد. حقیقت این است که وقتی از مرورگرهای خود جهت خرید چیزی به صورت آنلاین استفاده می کنیم، ماصرفا اطلاعاتمان مثل نام، شماره کارت اعتباری خود و غیره را ارسال می کنیم. این اطلاعات همچنان نیاز به بررسی و پردازش از طریق مسیرهای قدیمی دارند. تراکنش‌های الکترونیک حقیقتاً آنلاین نیستند.

اگر بخواهیم اقتصادی کاملاً دیجیتال داشته باشیم، نیازمند داشتن هویت‌های دیجیتال خواهیم بود. ما به عنوان یک بانک به طور کامل این مساله را درک می کنیم. هویت از ابتدا یک بخش اساسی از کسب و کار ما بوده است. امروزه ما نسبتاً در بررسی، حراست و استفاده از هویت‌ها در جهان آنالوگ خوب هستیم. هم اکنون چالش بزرگ این است که احراز هویت را به صورت دیجیتال و یکپارچه انجام دهیم.

جهان با سرعت زیادی در حال دیجیتالی شدن است و ما می توانیم یک نمای کلی احتمالی از یک اقتصاد کاملاً دیجیتال را مشاهده کنیم. اما در این مسیر با موانع زیادی هم مواجه هستیم. بخشی از مشکل این است که هنوز اتکای زیادی به جهان آنالوگ داریم. همان طور که از ما خواسته

می شود جهت باز کردن یک حساب بانکی یک گذرنامه فیزیکی یا شناسنامه ارائه دهیم، هویت‌های ما هم به همین ترتیب پیچیده هستند. از نام، آدرس و تاریخ تولد ما گرفته تا نوع پوشش و دایره دوستانمان، همه اطلاعات در مورد ما می تواند به هر نحوی جهت شناساییمان استفاده شوند. همچنین مشکلاتی جدی در مسیری که در حال حاضر از هویت در حوزه دیجیتال به کار گرفته می شود وجود دارد، از عدم امنیت اطلاعات گرفته تا نبود کنترل بر آن.

چنین مشکلاتی در یک دوره انتقال قابل درک است و چون هویت نقشی اساسی در آینده دیجیتال ما ایفا خواهد کرد، می توانیم این انتظار را داشته باشیم که نهادها و منابع متعددی در زمینه ارائه راهکارهای مناسب در این زمینه گام بردارند. در حال حاضر می بینیم که هویت دیجیتال یک موضوع داغ در میان دولت‌ها و رگولاتورها، بانک‌ها و شرکت‌های فناوری، NGOها و دانشگاه‌هاست. همچنین پروژه‌های زیادی در سراسر جهان در جهت ایجاد راهکارهای بهتر هویت دیجیتال در حال انجام هستند. ما انتظار داریم این تلاش‌ها تشدید شوند.

طبق دیدگاه ما، این حرکت‌ها هر چند به کندی پیش می روند اما در نهایت مطمئناً به یک پلتفرم هویت دیجیتال همه جانبه، منطقه‌ای و شاید جهانی منجر می شوند. ما می توانیم آن را به عنوان یک لایه پایه برای گردآوری، بررسی و به اشتراک گذاری هویت به صورت ایمن، ساده و در عین حال قدرتمند و همچنین به عنوان یک لایه ارتباطاتی که شاکله اینترنت را تشکیل می دهد، تصور کنیم.

این موضوع که چنین پلتفرمی در نهایت چگونه به نظر می رسد بسیار واضح است. در این مقاله ما شمارا به سفری در طول این تکامل دیجیتال می بریم و همچنین آینده احتمالی آن و آنچه که آن‌ها برای ما به عنوان بانک، مشتری، و به طور کلی برای جهان در نظر گرفته اند، را بررسی خواهیم کرد.

پیش گفتار

در ژانویه سال ۲۰۱۶ مقاله‌ای را برای نشست مجمع جهانی اقتصاد در مورد فرارسیدن چهارمین انقلاب صنعتی منتشر و در آن پیشنهاد کردیم که اگر سه انقلاب صنعتی نخست، ما را از موتورهای بخار به تولید انبوه و از آن به سمت فناوری اطلاعات مدرن و ارتباطات انتقال داد، این عصر جدید برای مادیایی از اتوماسیون و اتصال به ارمغان خواهد آورد. مانند سه انقلاب نخست، این انقلاب نیز دگرگونی‌های بنیادینی در پی خواهد داشت.

از آن زمان، فرارسیدن چهارمین انقلاب صنعتی را با جزئیات بیشتر و از زوایای مختلف بررسی کرده‌ایم.

در نیمه سال ۲۰۱۶، مقاله مهمی را در رابطه با بلاکچین، (یک فناوری جدید) و از همه مهم‌تر در مورد قالب چهارمین انقلاب صنعتی منتشر کردیم، که معتقدیم ممکن است منجر به ساختار شکنی و تحولی عظیم در سیستم مالی جهانی یا فراتر از آن شود.

در پاییز سال ۲۰۱۶ مجمع آینده امور مالی را در UBS راه اندازی کردیم. در این سلسله رویدادها ما رهبران و متخصصانی از دانشگاه‌ها، شرکت‌های بزرگ، فین‌تک‌ها و رگولاتورها را گرد هم آوردیم تا به جنبه‌های چگونگی وقوع انقلاب چهارم صنعتی در اقتصاد و جامعه و به خصوص خدمات مالی نگاهی بیندازیم.

همچنین هویت دیجیتال را به عنوان یک موضوع کلیدی در مجمع آینده مالی انتخاب کردیم چون از طرفی هویت یکی از مهم‌ترین عناصر اقتصاد ماست و از طرف دیگر ایجاد یک اقتصاد کاملاً دیجیتال بدون همکاری از سوی شرکای بازار جهت برقراری هویت آنلاین، غیر ممکن خواهد بود.

این مقاله برای مخاطبان عمومی در نظر گرفته شده است. این بخشی از تلاش‌های مداوم ما جهت ارائه اطلاعات و بینش‌ها در مورد موضوعات مهم برای کسانی است که خدمات ارائه می‌دهند و همچنین به طور کلی برای تمام افراد جامعه است.

امید داریم که خواندن این مقاله برای شما تامل برانگیز باشد.

فهرست مطالب

مقدمه

پیش‌گفتار

۶ هویت امروز
کلید شاهراه (دیجیتال)
معمادریافته
چهره‌های متعدد من
بحران هویت

۱۱ راه پیش رو
شماره خودتان را بروید؛ من هم راه خودم را خواهم رفت
یک اپلیکیشن برای آن وجود دارد
بیشتر، لطفا
نه خیلی سریع
به هم آمیختن خلاقانه

۱۵ وضعیت آینده
یک نقش جدید
سرانجام خانه

۱۸ چالش‌ها و ریسک‌ها
اشکالات
چه کسی مسئول است؟
قشر مرفه

۲۳ خدمات مالی و هویت
نقشی برای بازی کردن
نگاهی به آینده

۲۴ در پایان

هویت امروز

در دنیای دیجیتالی امروز، هویت‌های ما به طور فزاینده‌ای به عنوان شبکه گسترده‌ای از داده‌های شخصی تعریف می‌شود که توسط نهادهای بی‌شماری تامین، گردآوری و به اشتراک گذاشته شده است. اگر چه اغلب سیستم‌های هویتی مفید و رایج در تلاشند تا امنیت، کنترل و سهولت استفاده را مطابق با چیزی که ما باید انتظار داشته باشیم ارائه دهند.

کلید شاهراه (دیجیتال)

ایجاد هویت یکی از پیش نیازهای کلیدی برای یک اقتصاد کارآمد است: شما نمی‌توانید دارایی افراد را در یک حساب بدون این که آن‌ها را بشناسید نگهداری کنید؛ شما نمی‌توانید معاملات را بدون حصول اطمینان از طرفین قرارداد داشته باشید.

از زمانی که بانکداران دوره رنسانس جهت بررسی هویت بر روابط شخصی یا معرفی نامه‌های مهر و موم شده متکی بودند، مسیر طولانی را طی کرده ایم. امروز سیستم مالی ما تعداد غیرقابل شماری از افراد، سازمان‌ها، دارایی‌ها و ابزارهای مالی را در یک شبکه پویا و تودرتو به هم متصل می‌کند. برای انجام تراکنش‌ها و گردش اقتصادی، همه این نهادها نیاز دارند که مکرراً، به طور منحصربه‌فرد و درست شناسایی شوند تا حرکت خود را در سیستم آغاز کنند.

امروزه انجام چنین کاری یک چالش است. هر چه که در جهت توسعه یک اقتصاد کاملاً دیجیتال تلاش کنیم، چالش‌ها صرفاً افزایش خواهند یافت. از یک سو، تعداد نهادهای موجود در سیستم شروع به فوران کرده است. هر چه بیشتر جهانی شویم، مناطق بیشتری از جهان یعنی افراد و سازمان‌های بیشتری، به صورت آنلاین در خواهند آمد. هر چه اینترنت اشیا رشد کند، به موازات آن تعداد بیشتری از اشیا از یخچال‌ها گرفته تا کانتینرهای حمل و نقل به صورت آنلاین در خواهند آمد. اگر همه این نهادها به طور یکپارچه با هم معامله کنند، ما باید مسیرهای استاندارد را جهت برقراری و بررسی اینکه آن‌ها چه کسی و چه چیزی هستند داشته باشیم.

اما صرفاً مسئله در خصوص آمار و ارقام نیست. هر چه دنیای ما دیجیتالی می‌شود، فرآیندهای بیشتری خودکارتر خواهند شد. پیشرفت‌هایی مثل بلاکچین، قراردادهای هوشمند و هوش مصنوعی، به ماشین و دیگر چیزها این امکان را خواهند داد تا به نوبه خود به فعالان اقتصادی تبدیل شوند.

یک قرارداد هوشمند را می‌توان به عنوان یک کد مشترک در نظر گرفت که به طور مستقل اغلب روی یک بلاکچین اجرا می‌شود. قرارداد هوشمند می‌تواند جهت ذخیره ارزش (پول) استفاده و در تصمیم‌گیری در مورد آن چه باید با آن انجام گیرد برنامه‌ریزی شود. برای اثربخش بودن قراردادهای

هوشمند، نیازمند دسترسی به یک سیستم هویت خواهیم بود که نه تنها محفوظ از خطا و شکست باشد، بلکه بدون دخالت انسان کار کند.

به همین دلیل و دلایل دیگر، هویت دیجیتال می‌تواند به عنوان هسته یک اقتصاد دیجیتال در نظر گرفته شود - نخ تسبیحی که بخش‌های مختلف آن را به هم متصل می‌کند و کلیدی که پتانسیل آن را آزاد می‌کند. بنابراین ضروری است که ما آن را عملی کنیم.

معماد آینه

در دنیای امروز، هویت‌های ما از مجموعه بزرگی از اطلاعات تشکیل شده است. بعضی از این‌ها می‌تواند به عنوان بخشی از هسته هویت مادر نظر گرفته شود؛ برای مثال نام، تاریخ تولد و یا جنسیت. اطلاعات مقدماتی که جامعه از ما می‌خواهد به وسیله آنها خودمان را معرفی کنیم.

مهم‌تر از این ما لایه‌های مختلفی از ویژگی‌های هویتی داریم. بعضی از این‌ها بیومتریک هستند، مانند چهره، اثر انگشت، الگوهای صدا یا حتی DNA ما. برخی از این‌ها مانند وضعیت شهروندی، گواهی نامه رانندگی، کارت اعتباری یا دیگر شماره‌های حساب رسمی هستند. بعضی دیگر اجتماعی هستند، مانند افرادی که با آن‌ها ازدواج کردیم، اسامی فرزندانمان، سلايق مادر غذا، پوشش، عادات و غیره. با گردآوری تمام این داده‌ها کنار هم ما تصویر خوبی از آن چه که هستیم را به دست می‌آوریم.

به جز صفات بیولوژیکی ذاتی، بیشتر این ویژگی‌ها به ما نسبت داده می‌شوند یا به هر طریقی جمع‌آوری می‌شوند. این موضوع از زمانی که متولد می‌شویم و به زندگی ادامه می‌دهیم تا زمانی که فوت کنیم ادامه پیدا می‌کند و در بعضی جاها، یک گواهی برای تایید مرگ مادر یافت می‌کند.

امروزه نهادهای بی‌شماری وجود دارند که ویژگی‌های هویتی را تعیین می‌کنند. بعضی از آن‌ها آشکار هستند، مانند دولت‌ها، بانک‌ها، شرکت‌های کارت اعتباری، یا حتی پزشکان. اما شبکه‌های اجتماعی، شرکت‌های ارتباط از راه دور، موتورهای جستجو و تمام وبسایت‌هایی که ما به آن‌ها مراجعه می‌کنیم، از طریق جمع‌آوری اطلاعات درباره ما، در واقع خصوصیات هویتی را نیز برایمان تعیین می‌کنند؛ خواه از این موضوع آگاه باشیم یا نباشیم.

چهره‌های متعدد من

به طور کلی، نمی‌خواهیم تمام ویژگی‌های هویتی خود را با هر کسی به اشتراک بگذاریم و بنابراین ترجیح می‌دهیم که در صورت امکان خصوصیات خود را در گروه‌های مختلف یا پرسوনা‌های مختلفی دسته‌بندی کنیم، که هر کدام مناسب‌بستر متفاوتی هستند.

به عنوان مثال، ما ممکن است بخواهیم مجموعه‌ای از خصوصیات خود را فقط با پزشک‌مان به اشتراک بگذاریم (سوابق سلامتی، عادات غذایی)، مجموعه دیگری را با فروشندگان آنلاین (شماره کارت اعتباری، سن) و غیره. این مطلوب است که در صورت امکان قادر به کنترل و استفاده انتخابی از خصوصیات هویتی خود باشیم.

در حالی که این صفات به خودی خود ممکن است هیچ ارزش ذاتی نداشته باشند، اما از نظر کاری که ما را قادر به انجام آن می‌کنند، ارزشمند هستند. بدون یک نشان شهر وندی معتبر (گذرنامه یا مدرک ثبت نام رای دهنده)، نمی‌توانیم به خارج از کشور سفر کنیم یا در آینده سیاسی کشور خود مشارکت کنیم و بدون یک کارت اعتباری معتبر نمی‌توانیم برای مثال یک اتومبیل کرایه کنیم.

ویژگی‌های ما بر حسب آن چیزی که انجام آن را برای دیگران امکان‌پذیر می‌سازند نیز ارزشی دارند. امروزه شرکت‌ها میزان زیادی اطلاعات در مورد ما در جهت ارائه خدمات بهتر به ما، یا ایجاد درآمد جمع‌آوری می‌کنند (رایج‌ترین روش بازاریابی). می‌توانیم آینده‌ای را تصور کنیم که در آن، نقش‌ها برعکس می‌شوند و این ما هستیم که هویت‌های خود را کنترل می‌کنیم و داده‌های خود را به شرکت‌ها می‌فروشیم. در چنین جهانی، هویت دیجیتال ارزش بسیار ملموسی خواهد داشت.



بحران هویت

در حالی که راه طولانی را در بیست سال اخیر در توسعه ارتباطات آنلاین پیموده ایم، هنوز مشکلاتی جدی در مسیر به کار گرفته شدن هویت دیجیتال وجود دارد که می توان به موارد زیر اشاره کرد

هویت به اندازه کافی ایمن نیست. هک های عمده منجر به این شد که انتشار اطلاعات خصوصی به طور فزاینده ای رایج شود و سرقت هویت گسترش یابد. هویت های آنلاین امروزی، افراد را در مورد میزان امنیت آن ها در امور مهم خصوصی خود نگران ساخته است.

هویت غیر ضروری است. سیستم های هویتی به خوبی با یکدیگر در ارتباط نیستند، همان طور که هر بار مجبوریم برای ورود به یک وبسایت جدید دوباره ثبت نام کنیم، یا اسناد مشابهی تولید کنیم، که البته این موضوع تازگی ندارد، به همین ترتیب وقتی یک حساب بانکی در یک بانک جدید نیز باز می کنیم، این روند تکراری احراز هویت مجددا اتفاق می افتد.

هویت استاندارد سازی شده نیست. افزونگی و حشو محصول این واقعیت است که ما هیچ وسیله استاندارد دی جهت تعیین، فهرست کردن و به اشتراک گذاشتن هویت ها نداریم. هر ارائه دهنده خدمات مرتبط با هویت، چه یک دولت، بانک یا شرکت تلفن، اطلاعات هویتی را با روش خود ذخیره می کند.

هویت پراکنده است. اطلاعات در مورد مادر مکان های مختلفی از دیتابیس های دولتی و بانک ها گرفته تا بازار یاب ها و مجرمان گردآوری و ذخیره می شوند.

هویت تحت کنترل ما نیست. با توجه به موارد بالا، این موضوع در صورتی که غیر ممکن نباشد، برای ما سخت است که در دورانی که در جهان دیجیتال، اطلاعات مربوط به ما می تواند به آسانی و بدون اجازه نگه داری، کپی و استفاده شود، در مورد اینکه چه کسی چه اطلاعاتی مربوط به ما را نگه داری می کند دورنمایی داشته باشیم.

طرز اداره هویت نه کامل و نه هماهنگ است. بسیاری از مسائل قانونی مواجهه با هویت همچنان باید شناسایی شوند، برای مثال چه کسی مسئول شکاف در داده هاست؟ و اگر چه رگولاتورها در برخی حوزه های قضایی این مشکلات هویتی را شناسایی کرده اند اما چارچوب قانونی با رگولاتوری به هیچ وجه کامل یا هماهنگ نیست.

هویت جهانی نیست. میلیون ها نفر در جهان وجود دارند که هیچ گونه هویت رسمی ندارند و در نتیجه اغلب از مزایا و حمایت های جامعه برخوردار نمی شوند. در یک اقتصاد دیجیتال، فقدان چنین اعتبارنامه هایی آن ها را بیش از پیش محروم خواهد ساخت.

خبر خوب این است که تغییرات در حال وقوع هستند. شتاب روزافزون انقلاب صنعتی چهارم و حرکت فزاینده به سمت یک اقتصاد دیجیتال باعث آگاهی در مورد مشکلات هویتی در میان مردم، دانشگاه ها، دولت ها و بخش های خصوصی می شود.

ما همچنین شاهد تعداد قابل توجهی از پیشرفت های فناورانه هستیم، از بلاکچین گرفته تا بیومتریک ها که می توانند نقش مهمی در غلبه بر مشکلات فوق ایفا کنند و پلتفرم های هویت دیجیتال آتی را قابل دوام سازند.

به همین دلایل، ما فکر می کنیم که ممکن است به نقطه عطف مسیر رسیدن به راهکار نهایی دست یافته باشیم.

«یک سیستم هویت الکترونیک موفق

به کاربران این امکان را خواهد داد که به

آسانی هویت های مختلف خود را در میان

سازمان های مختلف مدیریت کنند. این

سیستم حریم خصوصی آنلاین کاربران را

محافظت خواهد کرد».

جان کامنیش، IBM

شرکت کننده در مجمع آینده امور مالی

فراسوی دریاها

در دوران بازارهای جهانی سازی شده کنونی، مانیز عادت کرده ایم که تراکنش ها را در آن سوی مرزها بدون هیچ گونه پیچیدگی انجام دهیم. معمولاً وقتی یک شرکت یا یک فرد پولی را جهت خرید کالا و خدمات به خارج ارسال می کند یا به دوستان یا اقوامش می فرستد، تراکنش از چندین ریل پرداخت از بانک های مبدأ از طریق تعدادی از بانک های کارگزار به بانک گیرنده فرستاده می شود. اگر چه بعضی راهکارهای نوظهور فین تکی وجود دارد که به تسهیل فرآیند کمک می کنند، اما استفاده از بانک ها برای تراکنش های بین المللی می تواند چندین روز پیش از تسویه به طول بینجامد.

یک دلیل، که به هیچ وجه تنها دلیل برای تاخیر نیست، الزامات مختلف مرتبط با شناسایی دقیق طرف قرارداد است. از آن جایی که هیچ وسیله استاندارد برای به اشتراک گذاشتن اطلاعات هویتی مناسب باشد وجود ندارد، و چون قوانین و مقررات می توانند در میان حوزه های قضایی متفاوت باشند، هر موسسه در طول زنجیره در هنگام شناسایی یک فرد اغلب مجبور است که از صفر شروع کند و این موضوع می تواند شامل بررسی های پیچیده شناسایی هویت مشتری (KYC) و ضد پولشویی هم باشد. اگر اطلاعات مفقود، مبهم یا اشتباه باشند، بررسی های بیشتری (اغلب دستی) نیاز است که انجام گیرد. این امر باعث افزایش تاخیر و هزینه می شود، نه صرفاً به این خاطر که سیستم رایج در معرض کلاهبرداری یا سایر خطاهای انسانی است.

اگر راهی برای داشتن یک هویت دیجیتال مورد اعتماد، ایمن و به صورت جهانی پذیرفته شده برای طرف ارسال کننده و دریافت کننده وجود داشته باشد، آنگاه فرآیند می تواند تسهیل شود، میزان خطاها کاهش یابد، و انطباق با قوانین رگولاتوری آسان تر شود. این موضوع می تواند به صرفه جویی قابل توجهی در هزینه و زمان، افزایش اعتماد و کاهش کلاهبرداری منجر شود. همچنین ممکن است از طریق ارائه یک تجربه مشتری بهتر، جریان درآمدی بیشتری را ایجاد کند. حل چالش هویت دیجیتال می تواند این موضوع را به یک واقعیت تبدیل سازد.

نمونه‌هایی از نوآوری‌های هویت دیجیتال

کانادا

شناسه دیجیتال و انجمن احراز هویت کانادا (DIACC)

این انجمن در نتیجه کار گروه دولت برای بازبینی سیستم پرداخت‌ها ایجاد شد. DIACC یک ائتلاف غیرانتفاعی از رهبران بخش‌های عمومی و خصوصی است که ملزم به توسعه یک شناسه دیجیتال کانادایی و ایجاد یک چارچوب احراز هویت جهت امکان‌پذیر کردن مشارکت کامل و ایمن کانادا در اقتصاد دیجیتال جهانی هستند. اعضای DIACC شامل نمایندگان از سطوح دولتی فدرال و استانی و همچنین رهبران بخش‌های خصوصی است. SecureKey یک ارائه‌دهنده برجسته هویت دیجیتال در کانادا است.

سوئد

BankID

BankID یک راهکار شناسایی شهروندان است که به شرکت‌ها، بانک‌ها و آژانس‌های دولتی این امکان را می‌دهد تا از طریق اینترنت توافق‌نامه‌های میان افراد را تایید و منعقد کنند.

فنلاند

TUPAS

TUPAS یک سیستم هویتی در فنلاند است. در این کشور تمام بانک‌های پیش‌وارانه‌دهنده هویت دیجیتال هستند. افراد می‌توانند از طریق اعتبارنامه‌های بانکی خود طیف گسترده‌ای از خدمات را دریافت کنند.

انگلستان

GOV.UK Verify

GOV.UK Verify یک ورود واحد و مورد اعتماد به خدمات دیجیتال دولتی انگلستان ایجاد کرده است. مردم از بین چندین شرکت ارائه‌دهنده خدمات مبتنی بر هویت مورد تایید دولت، یکی را انتخاب می‌کنند. این ارائه‌دهندگان بررسی می‌کنند که آیا افراد در مورد این که می‌گویند چه کسی هستند و چه زمانی هویت خود را ثبت و احراز کرده‌اند، صادق هستند یا نه و راه آسانی را برای آن‌ها جهت استفاده از سیستم‌های دولتی به ارمغان می‌آورند. GOV.UK Verify روش پایداری را جهت اثبات هویت هنگام دسترسی به خدمات آنلاین دولتی ارائه می‌دهد.

هند

DigiLocker و Aadhaar

Aadhaar یک شماره دیجیتالی ۱۲ رقمی منحصر به فرد است که به هر شهروند هندی که از ورودی‌های بیومتریک استفاده می‌کند، داده می‌شود. این شماره می‌تواند به عنوان تایید هویت یک فرد عمل و همچنین به آن‌ها جهت دسترسی به خدمات دولتی به صورت یکپارچه کمک کند. هند همچنین در تلاش برای تبدیل شدن به کشوری بدون کاغذ از طریق DigiLocker است. DigiLocker این فرصت را برای سازمان‌ها و افراد فراهم می‌کند که همه اسناد قانونی خود را صادر، تایید و ذخیره کنند و به آن‌ها دسترسی داشته باشند.

دانمارک

NemID

NemID یک شناسه الکترونیک ملی و زیرساخت امضای دیجیتال است که با همکاری نزدیک با بخش‌های بانکی توسعه یافته است و توسط یک ارائه‌دهنده خصوصی خدمات مبتنی بر هویت، برای دولت و بانک‌های دانمارکی به کار گرفته می‌شود. این سیستم که به صورت رایگان برای شهروندان دانمارکی ارائه شده، یک روش شناسایی مشترک را برای شهروندان جهت دسترسی به خدمات عمومی و خصوصی ارائه می‌کند.

استونی

e-Residency

e-Residency یک هویت دیجیتال فراملیتی است که برای هر شخصی در جهان که علاقه‌مند به اداره یک کسب‌وکار مستقل از مکان و به صورت آنلاین باشد، در دسترس است. به علاوه، e-Residency خدمات دیجیتالی ایمن و مناسبی که تامین اعتبار و اعتماد را به صورت آنلاین تسهیل می‌کنند را امکان‌پذیر می‌سازد.

راه پیش رو

تغییر فناوریانه تمایل دارد از الگویی پیروی کند که تلاش‌های فردی و پروژه‌های کوچک فناوری را به جلو سوق می‌دهد، که این روند به پلتفرم‌های بزرگ‌تر و در نهایت به یکپارچه‌سازی و استانداردهای همه‌جانبه منجر می‌شوند. ما فکر می‌کنیم که احتمالاً این مورد برای هویت دیجیتال هم اتفاق بیفتد

ما در مورد هویت در اقتصاد دیجیتال مشخص است: مارا هکاری می‌خواهیم که به روشی بی‌خطر، ایمن و به صورت صریح تمام افراد و چیزهایی که با آن‌ها تعامل می‌کنیم را شناسایی کنیم. از طرفی این راهکار به کاربران این امکان را بدهد که تنها خصوصیات ضروری خود را برای یک معامله به اشتراک بگذارند، در حالی که به طرفین قرارداد نسبت به معتبر بودن این خصوصیات اطمینان کامل می‌دهد. چطور به آن نقطه برسیم؟ اگر تاریخچه فناوری چراغ راه ما باشد، تکامل چنین چارچوب هویت دیجیتال همه‌جانبه‌ای احتمالاً مبتنی بر مراحل متعددی خواهد بود.

شماره خودتان را بروید؛ من هم راه خودم را خواهم رفت

در مرحله اول، ما ذی‌نفعان یا گروه‌هایی که روی راهکارهایی برای حل مسائل مرتبط با هویت یا یوزکیس‌های خاص هویت دیجیتال کار می‌کنند را شناسایی می‌کنیم. این اتفاق همین امروز در حال روی دادن است. به عنوان مثال دولت‌ها علاقه زیادی به هویت با هدف کمک به خدمت، حفاظت و درک نیازهای شهروندان خود دارند. ما در حال حاضر شاهد راهکارهای نوآورانه دولت الکترونیک مانند e-ID در کشورهای شمال اروپا، برنامه Gov.UK Verify در بریتانیا، یا کارت هویت الکترونیک همه‌کاره در استونی هستیم. ما می‌توانیم و باید در انتظار موارد بیشتری باشیم.

رگولاتورها به هویت دیجیتال به عنوان روشی برای حفاظت از مشتریان و تثبیت بازارها توجه می‌کنند، و به طور فزاینده‌ای به دنبال نوشتن قوانینی هستند که این کار را انجام دهد. مقررات عمومی حفاظت از داده در اتحادیه اروپا، که یک تلاش رگولاتوری همه‌جانبه و برجسته جهت کمک به حفاظت از داده‌های شخصی شهروندان اتحادیه اروپاست و یک محیط رگولاتوری یکپارچه را برای هویت در منطقه ارائه می‌کند.

سازمان‌های غیردولتی و بین‌المللی مانند پروژه ID۲۰۲۰ سازمان ملل، یا بنیاد جهانی هویت، به موضوع هویت دیجیتال جهت شناسایی نیازهای مردم کشورهای در حال توسعه و فقیر جهان که بسیاری از آن‌ها به دلیل نداشتن اعتبارنامه از اقتصاد دیجیتال محروم هستند توجه دارند.

شرکت‌های بخش خصوصی چه برای مدیریت و درک روابط بی‌شمار خود با مشتریان، تامین کنندگان و شرکا و چه برای فراهم کردن دسترسی آسان و ایمن مشتریان به خدمات آنلاین بیشتر، نیاز بسیار زیادی به سیستم‌های

هویت دیجیتال جامع و مقیاس پذیر دارند.

شرکت‌هایی مانند مایکروسافت، اوراکل یا سلفورس از این نیازها با CRM (مدیریت ارتباط با مشتری) پیچیده و خدمات مرتبط با هویت استقبال می‌کنند. گوگل، لینکدین و یوتیوب که مدل‌های کسب و کاری آن‌ها تا حد زیادی مبتنی بر جمع‌آوری و مدیریت داده‌های هویتی است، در حال یافتن راه‌هایی برای گسترش خدمات و تخصص‌های خود به اشخاص ثالث هستند؛ مانند زمانی که شما از «Facebook login» جهت دسترسی به یک اپلیکیشن غیرفیس‌بوکی استفاده می‌کنید.

صنایع به طور کلی چالش‌های هویت دیجیتال را اغلب از طریق کنسرسیوم‌ها می‌گشایند. سیستم TUPAS در فنلاند، برای مثال، توسط بنیاد خدمات مالی فنلاند جهت ارائه یک استاندارد هویتی غیررسمی برای مشتریان بانک‌های فنلاند ایجاد شد.

یک اپلیکیشن برای آن وجود دارد

دلیلی وجود ندارد که فکر کنیم با افزایش سرعت دیجیتالی شدن سراسر جهان چنین تلاش‌هایی تشدید نخواهد شد. دیجیتالی شدن به نوبه خود پیشرفت‌هایی را در فناوری‌های اصلی و روش‌های ارتباط با پلتفرم‌های هویتی آینده هدایت می‌کند.

به عنوان مثال، ما به احتمال زیاد شاهد این خواهیم بود که تکنیک‌های بیومتریک به عنوان یک وسیله احراز هویت به رشد خود ادامه دهند. در حال حاضر استفاده از اثر انگشت جهت باز کردن قفل دستگاه هوشمند امری عادی است. هم‌اکنون فناوری‌ها برای انجام کارهای مشابه با نشانگرهای بیولوژیکی مانند شبکه چشم، ضربان قلب، الگوی وریدی، صدا یا حتی DNA ما توسعه یافته‌اند.

معیارهای رفتاری و جغرافیایی همچنین می‌تواند به عنوان یک وسیله احراز هویت عمل کند. جایی که ما هنگام دسترسی به اطلاعات حضور داریم، یکی از تکنیک‌هایی است که قبلاً نیز استفاده شده است، زیرا هر کس می‌داند چه کسی از یک مکان جدید وارد گوگل یا آی‌کلود شده است. فناوری‌ای که نحوه استفاده از دستگاه‌هایمان را کنترل می‌کند (برای مثال چطور ما آن‌ها را نگه می‌داریم و یا چطور از یک صفحه کلید استفاده می‌کنیم) نیز در دسترس است و می‌تواند جهت بررسی اینکه آیا مادر حال کنترل این دستگاه‌ها هستیم یا افراد ناشناس دیگری کنترل آن را بر عهده دارند، مورد استفاده قرار گیرد.

زندگی اجتماعی ما نیز می تواند به عنوان نشانگرهای هویت عمل کند. نمودارهای اجتماعی - نقشه های شبکه اجتماعی ارتباطات حرفه ای ما - به عنوان مثال می تواند به ما این امکان را بدهد که به آسانی «جان اسمیت» از لندن در کشور انگلستان را از «جان اسمیت» از لندن در انتاریو کشور کانادا متمایز کنیم، بدون این که مجبور باشیم از هر کدام اطلاعاتی بگیریم. ما همچنین پیش بینی می کنیم که پیشرفت هادر رمزنگاری و زمینه های مرتبط با آن به کمک توانایی ما جهت احراز هویت، ذخیره و به اشتراک گذاشتن اطلاعات که شامل داده های شخصی می شود به صورت ایمن ادامه خواهد داد. در این زمینه باید توجه ویژه ای به فناوری بلاکچین، صورت گیرد، چون این فناوری تعدادی قابلیت جذاب دارد که می تواند جهت توسعه پلتفرم های هویتی غیر متمرکز و متن باز مورد استفاده قرار گیرد.

و در آخر، هوش مصنوعی با اشکال مختلف خود احتمالاً در بسیاری از حوزه های هویتی به کار گرفته خواهد شد. به عنوان وسیله ای جهت تجزیه و تحلیل مقادیر زیاد داده ها و الگوهای یافته شده، هوش مصنوعی می تواند نقش مهمی در شناسایی کلاه برداری از طریق تشخیص رفتارهای غیر عادی ایفا کند. هوش مصنوعی می تواند به شرکت ها جهت گردآوری مجموعه بزرگی از خصوصیات هویتی جهت ارزیابی ریسک یا طبقه بندی مشتری کمک کند.

بیشتر، لطفاً

از آن جایی که این موضوع و دیگر پیشرفت ها به افزایش استفاده از ویژگی های هویتی منجر می شود، ما می توانیم در انتظار آگاهی نسبت به این باشیم که چگونه هویت می تواند نقشی در رشد اقتصاد دیجیتال در میان کسانی که از آن استفاده می کنند، داشته باشد.

به احتمال زیاد بخش اعظمی از این امر تاثیر مثبتی خواهد گذاشت. با ورود سیستم های هویت دیجیتال همه جانبه، مردم با توجه به منافع خود از نظر راحتی و امنیت شروع به استفاده از آن خواهند کرد. هر چه که مادر مورد این که چگونه اعتبار نامه ها را به اشتراک بگذاریم بیشتر آگاه شویم، شرکت ها قادر خواهند بود که به طور فزاینده ای تجربه مشتری خوشایند و یکپارچه ای را ارائه کنند. طبق دیدگاه ما، این تقاضای بیشتری را به دنبال خواهد داشت و از آن مهم تر، حداقل انتظارات از آن چه که راهکارهای هویتی باید ارائه دهند را افزایش خواهد داد.

می توانیم انتظار استقبال مشابهی را از سوی دولت ها و بخش های خصوصی داشته باشیم، به خصوص چون مزایای بهره وری از پلتفرم های هویت دیجیتال روشن تر شده است. با یک تخمین، به عنوان مثال، مجموع هزینه مدیریت هویت دیجیتال در بریتانیا با هزینه های دولتی پراکنده جاری خود، به بالای سه میلیارد پوند انگلیس می رسد. استاندارد سازی می تواند به آسانی این رقم را تا ۱۵۰ میلیون کاهش دهد و قطعاً هزینه های کلاه برداری از هویت که توسط بانک ها و سایر تامین کنندگان خدمات مالی متحمل می شود را کاهش می دهد. این را می توان به عنوان یک محرک قدرتمند معرفی کرد.

«یک زیرساخت هویت دیجیتالی قدرتمند برای آینده معاملات مبتنی بر اینترنت، حیاتی است. زیرساختی که اشتراک گذاری مقیاس پذیر داده های شخصی را در قالب یک روش حفظ حریم شخصی به عنوان پایه و اساسی برای خصوصیات دیجیتالی بسیار ایمن یکپارچه می کند. مراجع مورد اعتماد توزیع شده در اینترنت که توسط محاسبات ایمن توزیع شده روی شبکه های همتا به همتا و بلاکچین پشتیبانی می شوند، به طور فزاینده ای به ویژگی های بنیادین این زیرساخت آتی تبدیل خواهند شد. ما خوشحالیم که شاهد این هستیم که UBS در حال هدایت این تلاش ها در انجمن خدمات جهانی بایک زیرساخت هویت دیجیتالی قدرتمند است.»
توماس هاردجونو، MIT
شرکت کننده در مجمع آینده امور مالی

نه خیلی سریع

از سوی دیگر، مردم احتمالا به طور فزاینده‌ای آگاهی بیشتری نسبت به مشکلاتی که می‌تواند در خصوص هویت‌های آنلاین رخ دهد داشته باشند.

پیش از این گفته شد که امنیت نگرانی و دغدغه مهمی است. در یک اقتصاد کاملاً دیجیتال، سرقت هویت به مراتب خطرناک‌تر از چیزی خواهد شد که اکنون وجود دارد، این موضوع چنین نگرانی‌هایی را حاد می‌سازد. ادامه هک‌های پر مخاطره (شامل حملات با پشتوانه دولتی که اخیراً نیز گزارش شده است) و افزایش زیاد تعداد افرادی که در نتیجه آن‌ها صدمه می‌بینند، احتمالا درخواست برای سیستم‌های ایمن‌تر را تشدید و پذیرش سیستم‌های با امنیت کمتر را کند خواهد کرد.

امروز ما به شرکت‌هایی که مایل به جمع‌آوری هرچه بیشتر اطلاعات در موردمان هستند، عادت کرده‌ایم. نقض داده‌ها در یک اقتصاد پیش از پیش دیجیتالی ممکن است به طور متناقضی این روند را معکوس کند. شرکت‌هایی که داده‌های مربوط به ما را جمع‌آوری می‌کنند، می‌توانند طبق قانون موظف باشند که این داده‌ها را ایمن نگه دارند و در صورت ناتوانی مسئولیت آن را می‌پذیرند. این موضوع می‌تواند داده‌های شخصی را به یک دارایی یا یک بدهی تبدیل کند و در صورت رخداد آن، دیگر اثری از شرکت‌هایی که مشغول جمع‌آوری اطلاعات هستند، باقی نمی‌ماند.

همچنانکه شرکت‌ها اطلاعات بیشتری را در مورد ما جمع‌آوری می‌کنند، احتمال بیشتری وجود دارد که بدون اطلاع ما داده‌های جعلی به سیستم آن‌ها وارد شود و سبب تصمیم‌های آن‌ها را تحت تأثیر قرار دهد. می‌توان انتظار داشت که این منجر به مشکلات بیشتر و بیشتر برای مشتریان شود، و هم چنین باعث درخواست‌هایی مبنی بر کنترل بیشتر افراد روی داده‌های خود شود. ما فکر می‌کنیم این احتمال وجود دارد که آگاهی نسبت به مشکلات هویت دیجیتال، درخواست‌ها برای حفظ حریم خصوصی و گمنامی در فضای مجازی را افزایش خواهد داد، در کنار آن سهولت در به

اشتراک‌گذاری ویژگی‌های هویتی را در صورت تمایل نیز افزایش خواهد یافت.

باید هم چنین به یاد بیاوریم که افراد تنها ذی‌نفعان اقتصاد دیجیتال نیستند. هر چه اینترنت اشیا رشد می‌کند، ماشین‌های ما، از یخچال‌ها گرفته تا کانتینرهای حمل و نقل، به طور فزاینده‌ای به فعالانی مستقل تبدیل خواهند شد و این موضوع اهمیت بیشتری پیدا خواهد کرد که آن‌ها می‌دانند ما چه کسی هستیم. شاید جالب و خنده‌دار باشد که اگر ما بتوانیم خودمان را به خانه هوشمندمان معرفی کنیم و پشت در بمانیم؛ یا مثلاً اگر اتومبیل خودکار ما فکر کند که ما شخص دیگری هستیم و توانیم از آن استفاده کنیم.

در هم آمیختن خلأ قان

پیش‌بینی می‌کنیم که ترکیبی از پروژه خاص کاربردی، بهبود فناوری و فشار از سوی کاربران، پلتفرم‌های هویت را به جلو سوق می‌دهد. در نتیجه، باید این انتظار را داشته باشیم که شاهد رشد پیچیدگی، امنیت بهتر و افزایش قابلیت همکاری باشیم که از استانداردها و رقابت ناشی می‌شود.

این موضوع هم اکنون در حال وقوع است. سیستم TUPAS فنلاند، که توسط بانک‌ها ابداع شده است، می‌تواند جهت دسترسی به خدمات دولتی نیز مورد استفاده قرار گیرد. SecureKey در کانادا، دیگر پلتفرم هویتی که توسط بانک‌ها به کار گرفته می‌شود، اخیراً در حال گسترش با هدف تبدیل به یک پلتفرم هویتی ملی جهت دسترسی به طیف گسترده‌ای از خدمات عمومی و خصوصی است.

اما این انتظار هنوز وجود دارد که این تکامل به صورت تدریجی اتفاق بیافتد. این موضوع احتمالا منجر به ترکیبی از پلتفرم‌های هویتی با اندازه‌ها و اشکال مختلفی خواهد شد که در مناطق و صنایع مختلف به کار گرفته می‌شود و مبتنی بر فناوری‌ها و استانداردهای مختلفی است و سطوح مختلفی از امنیت و تسهیلات را ارائه می‌کند. این گام، سفر ما را آغاز می‌کند؛ اما هنوز مقصد نهایی نیست.



ما شما را می شناسیم!

بسیاری از ما احتمالاً این تجربه را داشته ایم: قصد باز کردن یک حساب بانکی داریم و از ما خواسته می شود که یک عدد یا تعدادی مدارک هویتی با خود بیاوریم. این ها اغلب اسناد فیزیکی هستند، مانند یک گذرنامه، قبض خدماتی یا پرونده مالیاتی. زمانی که بانک اطلاعات را بررسی کند، ما به سیستم آن ملحق می شویم و می توانیم به محصولات و خدماتش دسترسی داشته باشیم. اما چه می شود اگر بخواهیم حسابی را در یک بانک دیگر باز کنیم؟ پاسخ این است که مجبوریم دوباره همین روند را تکرار کنیم.

ممکن است خیلی دردسرساز به نظر نرسد، اما در خصوص میلیون ها حساب باز شده بین بانک ها و مشتریان آن ها، این روند تکرار می شود، چنین فعالیت های تکراری ای باعث افزوده شدن هزینه و پیچیدگی قابل توجهی به سیستم می شود.

یک راهکار هویت دیجیتال می تواند این روند را با قادر ساختن مشتریان در راستای نگهداری و کنترل دسترسی به نسخه های دیجیتالی شده مدارک هویتی توسط خودشان، تسهیل کند. در ادامه نحوه عملکرد آن آمده است:

بیا بید فرض کنیم که کاربری اپلیکیشن موبایلی دارد که آن را یک کیف پول می نامد. کیف پول به صورت محلی یک کپی از گذرنامه (تصویر اسکن شده)، یک کپی از یک قبض خدماتی و یک کپی از یک قبض مالیاتی را ذخیره می کند. کاربر اولین حساب بانکی را باز می کند و اسناد اصلی را به بانک ارائه می دهد. بانک اسناد را بررسی می کند، یک کپی دیجیتال از مدارک تهیه و سپس به صورت دیجیتالی آن را امضا می کند. این فرآیند تایید می کند که بانک سند اصلی را دیده است و دارد اطلاعاتی را منعکس می کند که برای دارنده کیف پول روی پرونده قرار گرفته است. این کپی امضا شده سپس به کیف پول مشتری بازگردانده می شود.

وقتی که مشتری به بانک دوم تغییر مکان می دهد آن ها می توانند تصمیم بگیرند که بعضی یا همه اسنادی که قبلاً امضا شده را از طریق کیف پول از بانک اول به بانک دوم ارائه دهند. مشتری می تواند حتی انتخاب کند که تنها بخش های خاصی از اطلاعات را ارائه دهد، مثلاً ملیت خود را از گذرنامه اش بگوید اما تاریخ تولد را نه. از آن جایی که سند شامل یک مدرک دیجیتال است که بانک اول اسناد هویتی اصلی را دیده، بانک دوم می تواند تصمیم بگیرد که آیا با توجه به مفاد بررسی خود به آن ها اعتماد کند یا خیر. چون این یک تراکنش ۱۰۰٪ دیجیتال است، فرایند بسیار راحت است.

می توانیم یک قدم جلوتر رویم. به عنوان مثال یک مدرک برای آدرس محل سکونت، می تواند به طور مستقیم توسط یک شرکت ارائه دهنده خدمات شهری صادر و امضا شود. بنابراین بانک های درگیر لزوماً نیاز نیست که به یکدیگر اعتماد کنند، اما در عوض مرجعی که سند را صادر می کند، تصدیق و گواهی را روی بلاکچین به اشتراک می گذارد، یک تحول بالقوه در اینجا وجود دارد. این کار نه تنها کارایی بیشتری را موجب می شود، بلکه اسناد دیجیتالی امضا شده در کیف پول مشتری را قابل اطمینان تر می سازد، چون صرفاً آن دسته نهادهایی که مراجع معتبری برای حوزه های خود هستند جهت امضای اسناد مربوطه به صورت دیجیتال واجد شرایط می شوند.

وضعیت آینده

همان طور که هویت دیجیتال رشد می کند، نیازهای جدیدی در اکوسیستم هویت به وجود خواهد آمد و به همین ترتیب محصولات و خدمات جدیدی که آن نیازها را پوشش دهند نیز به وجود می آیند. هر چند هنوز سخت است که بگوییم سفرمان در دنیای هویت دیجیتال دقیقاً به کجا خواهد رسید، اما فکر می کنیم که سه سناریوی احتمالی در نهایت وجود خواهد داشت.

یک نقش جدید

از دیدگاه مافاز بعدی تکامل هویت دیجیتال، با بلوغ و یکپارچه سازی مستمر مشخص خواهد شد و تا حد زیادی توسط نیروهایی که در فصل قبل اشاره شد، هدایت می شود. با تکامل پلتفرم ها، فکر می کنیم که شاهد نیازی برای محصولات و خدمات جدیدی خواهیم بود که نیازهای هویت دیجیتال را پوشش دهند. این موضوع می تواند توسط سازمان های موجود یا نهادهای جدیدی که انواع جدید کسب و کارها را می سازند، تامین شود. برای مثال، نیازهای روبه افزایشی جهت خدمات در زمینه مدیریت (و در موارد خاص، در زمینه ایجاد) هویت های دیجیتالی وجود خواهد داشت. بنابراین می توانیم ظهور تامین کنندگان هویت را به عنوان یک نهاد مجزا ببینیم.

چنین خدماتی، احتمالاً نیازمند سطح مشخصی از به رسمیت شناختن است. به عنوان مثال در سیستم GOV.UK Verify، دولت انگلستان به شرکت های خصوصی این مجوز را می دهد که به عنوان تایید کننده هویت برای دسترسی به خدمات دولتی عمل کنند. شرکت های ارائه دهنده خدمات مبتنی بر هویت کارهای اولیه افرادی که متقاضی استفاده از سیستم های دولتی هستند که شامل جمع آوری، بررسی و حراست از داده های آن ها مطابق با استانداردهای تعیین شده است، را انجام می دهند. زمانی که هویت یک فرد توسط یکی از این شرکت ها ثبت می شود، او می تواند از آن هویت جهت دسترسی به انواع محصولات و خدمات استفاده کند و از طرفی می تواند به تامین کننده جهت مدیریت داده ها اعتماد کند. ما این فرآیند را به عنوان الگویی برای انواع خدماتی که تامین کنندگان هویت ممکن است فراهم کنند، در یک مقیاس بزرگتر در آینده می بینیم.

تامین کنندگان هویت احتمالاً برای تایید اطلاعات به خدمات شاهدان هویتی مختلف متکی هستند. شاهد هویت، مرجعی است که به نوعی تایید می کند که یک خصوصیت هویتی خاص صحیح است. یک بانک می تواند گواهی دهد که شما دارای یک حساب هستید، یک دولت می تواند گواهی دهد که شما شهروند یک کشور هستید، شورای شهری که در آن زندگی می کنید و یا باشگاه شای محلی که شما عضو آن هستید، نیز

می توانند چنین کاری انجام دهند.

ما فکر می کنیم که اعطای گواهی به طور روبه رشدی به یک امر مهم تبدیل خواهد شد اما ارزش چنین گواهی دادن هایی متفاوت خواهد بود. یک درجه بندی اعتباری که توسط یک بانک مستقر مانند UBS تصدیق می شود ممکن است ارزشمندتر از یک گواهی شایستگی اعتباری از سوی یک شبکه اجتماعی باشد. هر چه گواهی مهم تر شود و به طور گسترده تر مورد استفاده قرار گیرد، به طور فزاینده ای مورد تقاضا قرار خواهد گرفت. ما می توانیم تصور کنیم که شرکت های تخصصی برای تامین گواهی به وجود آمده اند، یا منابع مورد اعتماد موجود (بانک ها، به عنوان مثال) گواهی را به عنوان یک خدمت اضافه کنند. این موضوع می تواند در عوض منجر به بازاری شود که در آن شاهدان یا یکدیگر به رقابت می پردازند و این رقابت موجب پیشرفت می شود.

همچنین می توانیم تعدادی از خدمات هویتی تخصصی جانبی را پیش بینی کنیم. برای مثال، ممکن است شاهد ظهور کارگزارانی باشیم که با کاربران در مدیریت هویت های خود همکاری می کنند، شاید به واسطه کمک آن ها داده های هویتی خود را جمع آوری و از آن در زمینه های مختلف استفاده کنند. چنین کارگزارانی همچنین ممکن است در حفاظت از کاربران از طریق بروز نگه داشتن جزئیات شاهدان هویتی مورد اعتماد، یاری رسان باشند. بعلاوه این کارگزاران ممکن است تبدیل به سازندگان بازارچه های هویتی شوند.

ممکن است شاهد انواع مختلفی از ارزیابان هویتی باشیم که رتبه بندی کلی هویتی را برای افراد بر پایه داده های شخصی آن ها ارائه می دهند، همان طور که موسسه اعتبار پژوهی هم اکنون این کار را برای شایستگی اعتباری انجام می دهد. همچنین احتمالاً شاهد ظهور ارائه خدمات بیمه هویت باشیم که هم از کاربران در برابر خسارت ناشی از دست رفتن یا به سرقت رفتن داده های هویتی محافظت می کند و هم از مادر برابر در دروس های مرتبط با شکاف در داده ها یا خرابی سیستم حراست می کند. با توجه به این موضوع، اهمیت ماموران حفاظت هویت که به کاربران کمک می کنند تا به صورت ایمن داده های هویتی خود را ذخیره و در صورت لزوم بازیابی کنند، افزایش خواهد یافت.

سرانجام، خانه

هر چه پلتفرم‌ها رشد کنند و یکپارچه‌سازی شوند و نقش‌های جدیدی به وجود آیند که نیازهای خاص حوزه هویت دیجیتال را برطرف کنند، ما به سمت ایجاد پلتفرم‌های هویتی در مقیاس بزرگ پیش خواهیم رفت. به عقیده ما، پیامد منطقی این سفر یک مجموعه نسبتاً کوچکی از پلتفرم‌های منطقه‌ای است که به عنوان پایه لایه هویتی برای اقتصاد دیجیتالی خدمت خواهند کرد. همانند اینترنت، این موضوع می‌تواند به صورت قابل‌تصور تغییر به یک پلتفرم جهانی شود.

پلتفرم‌هایی هویت دیجیتال به چه شکل خواهد بود؟ طبق دیدگاه شخصی ما، پاسخ دادن به این سوال در حال حاضر مشکل است. اما با در نظر گرفتن روندهای فعلی و قیاس آن با سایر فناوری‌ها، فکر می‌کنیم منطقی باشد که در انتظار یک یا شاید ترکیبی از سه سناریوی اساسی باشیم. هویت مبتنی بر دولت. در اولین سناریو، دولت‌ها نقش تأمین‌کننده هویت جهانی را بر عهده دارند. آن‌ها دارای لایه هویتی پایه هستند و آن را به کار می‌گیرند، هویت‌ها را صادر، ویژگی‌های هویتی را بررسی و کلیدهایی را برای استفاده از هویت فراهم می‌کنند. چنین سیستم‌های متمرکزی مزایایی را از جنبه استانداردسازی و قابلیت همکاری با سایر بخش‌ها ارائه می‌کنند. آن‌ها همچنین مزیت یک مرجع هویتی واحد مورد اعتماد را ارائه می‌دهند. اما سیستم‌های متمرکز معایبی هم دارند. آن‌ها تنها نقطه شکست، تنها هدف حمله و تنها منبع سوءاستفاده احتمالی هستند. سیستم‌های بزرگ و متمرکز به دلیل توانایی‌شان در نوآوری و تکامل شناخته نمی‌شوند و بعضی از دولت‌ها مورد اعتمادتر از سایرین هستند تا به نفع شهر و ندان‌شان عمل کنند.

هویت مبتنی بر کنسرسیوم‌ها. ممکن است در عوض شاهد یک سناریوی ترکیبی باشیم که در آن کنسرسیوم‌های نهادهای تجاری که با دولت همکاری می‌کنند، لایه هویتی را به عنوان بخشی از یک سیستم محرمانه و بسیار رگوله شده تأمین می‌کنند. این مشابه آن چیزی است که در بریتانیا، کانادا و شمال اروپا در حال وقوع است. این رویکرد ترکیبی از نظارت بخش عمومی و شرکت‌های خصوصی را ارائه می‌دهد. این سیستم به کاربران حق انتخاب می‌دهد و از نیروی رقابتی جهت کمک به هدایت نوآوری‌ها و کنترل هزینه‌ها استفاده می‌کند. در چنین مجموعه‌ای، ارائه‌دهندگان خدمات هویتی موجود، مانند بانک‌ها و شبکه‌های اجتماعی، می‌توانند آسان‌تر با یکدیگر متحد شوند. از آنجایی که این سیستم تعداد زیادی نهاد مستقل را در قیاس با یک رویکرد کاملاً متمرکز درگیر می‌کند، چنین سیستمی ذاتاً پیچیده‌تر است و مسائل مرتبط با قابلیت همکاری و اعتماد در آن پررنگ می‌شود. ممکن است کنسرسیوم‌های مختلف بتوانند ارتباط

را در قالب یک مدل فدرالی تر امکان‌پذیر کنند.

هویت خودمختار. دو سناریو فوق‌ر می‌توان به عنوان نتیجه‌گیری منطقی از روندهایی که در مورد آنها بحث کرده‌ایم، مشاهده کرد که شامل تأمین هویت توسط نهادهای خارجی می‌شود. با این حال ممکن است یک رویکرد کاملاً متفاوت را متصور شویم. رویکردی که در آن افراد مالک تمام داده‌های خود هستند و آن‌ها را کنترل می‌کنند.

در چنین پلتفرم هویتی خودمختاری، فرد نقش تأمین‌کننده هویت را بر عهده می‌گیرد که تمام ویژگی‌ها و خصوصیات هویتی در دسترس خود را گردآوری و آن‌ها را در یک کیف پول دیجیتال یا سیستم دیگری نگهداری می‌کند. (مشابه روشی که ما در نگهداری گذرنامه و شناسنامه در یک مکان ایمن در خانه داریم). در حال حاضر فناوری‌هایی داریم (برای مثال UBS Safe) که می‌تواند چنین سیستم‌هایی را عملی سازد. ما در UBS از طریق رمزنگاری می‌توانیم به طور ایمن شواهد خود را ضمن اطمینان از این که آن‌ها نمی‌توانند مورد جعل یا سوءاستفاده قرار گیرند، ذخیره کنیم و به اشتراک بگذاریم.

اعتقاد داریم چنین راهکاری به احتمال زیاد به نتیجه خوبی منجر می‌شود. این راهکار سطح بهینه‌ای از حفظ حریم خصوصی و امنیت را ارائه می‌دهد و تا زمانی که اکوسیستم اطراف به سمت آن هدایت شود، تقریباً به افراد توانایی کنترل کامل روی داده‌ها و پرسوئال‌های خود را ارائه می‌دهد. چنین سیستم غیر متمرکزی ممکن است تنها راهکار موجود در برابر فشارهای طولانی‌مدتی باشد که هر سیستم هویتی جهانی و به طور فزاینده‌ای پیچیده، احتمال دارد با آن‌ها مواجه شود.

جنبه‌های منفی نیز وجود دارند. در جهانی که شما مالک تمام مدارک هویتی خود هستید، گم کردن گذرنامه چیزی فراتر از صرفاً یک دردسر ساده خواهد بود. اما اشخاص ثالث، مانند آن‌هایی که در بالا اشاره شد، می‌توانند خدماتی ارائه دهند که به کاهش چنین ریسک‌هایی کمک کنند. به همین ترتیب، فکر می‌کنیم راهکارهای خودمختار باید به استاندارد بردی برسد که در آن به سیستم‌عامل‌های دیگر نیز احتیاج است.



چالش‌ها و ریسک‌ها

هر چند ما قویا معتقدیم که پلتفرم‌های هویت کاملاً دیجیتال باید تکامل پیدا کنند، بدون شک چالش‌هایی وجود خواهد داشت. از امنیت گرفته تا نظارت و پذیرش اجتماعی، می‌توان انتظار موانع بسیاری را در این مسیر داشته باشیم.

مسیرهای ممکن برای رسیدن به یک آینده هویت دیجیتالی توضیح داده شد، در این بخش نگاهی به بعضی از چالش‌ها می‌اندازیم.

اشکالات

بسیاری از این ریسک‌ها و چالش‌ها به لحاظ ماهیت، فنی خواهند بود. از مهم‌ترین آن‌ها:

امنیت. در میان تمام چالش‌های پیش روی هویت دیجیتال، امنیت احتمالاً آشکارترین و شاید مبهم‌ترین است. امروز، هویت‌های دیجیتال ما به هیچ وجه ایمن نیستند. ما شکاف‌های داده‌ای عمده‌ای داشته‌ایم، از Ashley Madison گرفته تا Target و گزارش‌های اخیر در مورد ۵۰۰ میلیون داده مشتریان که به طور بالقوه از Yahoo به سرقت رفت. چنین شکاف‌هایی چیزی فراتر از صرفاً یک دردسر هستند. آن‌ها همچنین هزینه‌های زیادی را تحمیل می‌کنند. به عنوان مثال، بریتانیا، هر ساله ۱۹۳ میلیارد پوند به دلیل سرقت هویت از دست می‌دهد. هک کردن هویت تبدیل به بخشی از زرادخانه‌های ربه‌رشد سلاح‌های سایبری می‌شود، در کنار این که هکرها هویت‌های به سرقت رفته را به عنوان راهی برای تسویه حساب با مخالفان خود فاش می‌کنند.

اگر بخواهیم یک اقتصاد واقعا دیجیتالی داشته باشیم، باید راهی برای ایمن ساختن هویت‌های دیجیتال پیدا کنیم. نکته منفی قضیه این است که قابلیت‌های امنیتی قوی، شامل هویت اطراف، به طور فزاینده‌ای به یک کسب‌وکار تبدیل خواهد شد. به عنوان مثال، می‌توانیم در انتظار یک افزایش نیاز به مدیریت و ایمن‌سازی گذرواژه‌ها و یک افزایش تمایل برای پرداخت هزینه خدمات در این خصوص باشیم.

زنده ماندن. یکی از جنبه‌های بسیار مهم هر چیز دیجیتال این است که با تکامل فناوری چه اتفاقی برایش می‌افتد. این موضوع از اهمیت زیادی در حوزه هویت دیجیتال برخوردار است. یک مورد این است که دیگر نمی‌توانیم اسناد WordStar را که شامل پایان‌نامه‌های دانشگاهی است که سی سال پیش نوشتیم را باز کنیم. مورد دیگر این است که اطلاعات هویتی حیاتی مادر قالب‌های داده‌های قدیمی تر و غیرقابل دسترسی خاک می‌خورد.

اگر سازمانی که کلید داده‌های هویتی را نگه‌داری می‌کند به هر دلیلی از این کسب‌وکار خارج شود ما نیز دچار مشکل مشابهی هستیم. هنگامی که Brothers Lehmann در سال ۲۰۰۸ ورشکست شد میلیاردها دلار از دست رفت یا متوقف شد. تصور رخ دادن اتفاقی مشابه برای هویت‌های دیجیتال افراد دشوار نیست. در همین راستا، چگونه یک فرد می‌تواند از داده‌های هویتی خود پس از مرگ محافظت کند؟ این جانیز، ممکن است نیازمند خدمات اشخاص ثالث برای جست‌وجوی اطلاعاتمان و در دسترس نگه‌داشتن آن‌ها برای وراثتمان باشیم، حتی اگر اصلاً تمایلی به این کار نداشته باشیم.

از هم‌گسیختگی. ما معتقدیم که عدم توافق در مورد فناوری‌ها و پلتفرم‌ها، همانند تضاد منافع در همکاری، یک ریسک برای توسعه سیستم‌های بنیادین هویت دیجیتال است. ما نیاز به حضور بنگاه‌های خصوصی و پیشگامانی که در این مسیر گام بردارند را درک می‌کنیم؛ اما همیشه این خطر وجود دارد که همان طوری که افراد راهکارهای متعلق به خود را ایجاد و پیاده‌سازی می‌کنند، ما به سمت از هم‌گسیختگی انبوه پیش رویم. در چنین حوزه‌های بنیادین و همه‌جانبه‌ای مانند هویت، احساس می‌کنیم که برای تمام ذی‌نفعان خیلی بهتر باشد که ابتدا با طرح کلی موافقت کنند و سپس به سمت این رویای مشترک حرکت کنند.

استانداردهای غیررسمی. با توجه به موارد فوق، این ریسک وجود دارد که یک یا چند نهاد (شاید شرکت‌های خصوصی) راهکاری را توسعه دهند که شاید ایده آل هم نباشد اما به دلیل راحتی و هزینه کم به طور بسیار گسترده‌ای مورد استفاده قرار گیرد. این موضوع می‌تواند طلیعه یک استاندارد هویتی غیررسمی باشد که به طور بالقوه متعلق به یک نهاد واحد باشد. هیچ تضمینی وجود ندارد که چنین پلتفرمی بتواند همه ویژگی‌ها و اقدامات حفاظتی را ارائه دهد؛ به خصوص اگر انگیزه اقتصادی کافی برای انجام این کار وجود نداشته باشد.

استانداردهای فناورانه. برای دستیابی به یک راهکار هویت دیجیتالی کارآمد، همانند هر توسعه فناورانه در مقیاس بزرگ، نیازمند حل مسائل مربوط به استانداردهای فناورانه و نظارت هستیم. این به معنای تصمیم‌گیری در مورد استانداردهای پایه، پروتکل‌های بنیادین و

«هویت مشترک دیجیتال پیش شرط تحویل ایمن، کارآمد و دیجیتال خدمات مالی، دولتی و غیره به مشتریان در سراسر جهان خواهد بود. مقررات مالی مانند بانکداری باز و دستورالعمل خدمات پرداخت ۲ (PSD2)، که موسسات مالی را ملزم می‌کند که برای اشخاص ثالث دسترسی به رابط برنامه‌نویسی کاربردی (API) را فراهم کنند، به علاوه نیاز به خدمات مالی و توانمند ساختن اشخاص ثالث، اعتماد به یک منبع و هویت کسب‌وکاری را برجسته خواهند کرد. با توجه به چالش‌های صنعت مالی در کنار پیاده‌سازی راهکارهای شناسایی هویت مشتری (KYC) مطابق با مقررات جرم مالی، این چالش قریب‌الوقوع چیزی نیست که دست کم گرفته شود.»

آجیت تریپاتی، PwC
شرکت‌کننده در مجمع آینده امور مالی

نظارت‌های اساسی است، همان‌گونه که امروزه شاهد TCP/IP، HTML یا ICANN در حوزه اینترنت و شبکه هستیم. البته که امکان پذیر است؛ اما نسبت به این که فرآیند توافق زمان‌بر و چندوجهی باشد، مشکوک هستیم. چه کسی مسئول است؟

تعدادی چالش نظارتی مهم که ماهیت فنی ندارند نیز وجود دارد. اشاره به مهم‌ترین آن‌ها ارزشمند است:

خودمختاری در مقابل نظارت‌سازمانی. فکر می‌کنیم این پرسش که چه کسی در نهایت مالک هویت‌های دیجیتال ماست و آن را کنترل می‌کند، یکی از مهم‌ترین مسائل اساسی در توسعه پلتفرم‌های هویت دیجیتال خواهد بود. پیش از این گفتیم که احتمالاً راهکارهای خودمختاری به وجود خواهد آمد که در آن‌ها فرد داده‌های هویتی خود را در اختیار دارد و بر استفاده از آن‌ها کنترل کامل دارد. در حال حاضر شاهد تکامل فناوری‌هایی هستیم که می‌تواند چنین راهکارهایی را امکان‌پذیر کند، اما آیا چنین راهکارهایی به لحاظ سیاسی یا اجتماعی قابل پذیرش خواهند بود؟ یا مادر عوض راهکارهای سنتی تر که در آن‌ها انواع مختلف سازمان‌ها، مانند دولت‌ها، تامین‌کنندگان دارندگان نهایی هویت‌های ما هستند را ترجیح خواهیم داد؟

چارچوب قانونی. در حال حاضر هیچ قانونی در خصوص هویت دیجیتالی وجود ندارد، اما وجود آن برای یک اقتصاد دیجیتال به شدت مورد نیاز است. برای مثال مسائل عمده‌ای وجود دارد: چه کسی مسئول از دست رفتن داده‌ها در اثر بروز یک نقص است؟ آیا هزینه مسئولیت هویت، شرکت‌ها را مجبور به صرف‌نظر کردن از در اختیار گرفتن داده‌های مشتری خواهد کرد؟

در یک اقتصاد دیجیتال رو به رشد، بیشتر معاملات ما با ظهور فناوری‌های جدیدی مانند بلاکچین و قراردادهای هوشمند خودکار خواهند شد.



اگر چه این یک مسئله کاملاً هویتی نیست، اما با وجود اتوماسیون ما باید پرسش‌های مربوط به الگوریتمی در مقابل حاکمیت انسان را پاسخگو باشیم. اخیراً شاهد تعدادی از مشکلات حاکمیت الگوریتمی بوده‌ایم (به عنوان مثال با سازمان خودمختار غیر متمرکز اتریوم یا همان DAO). در هر موقعیت قراردادی، مسائل هویتی نقشی کلیدی را ایفا خواهند کرد. به همین ترتیب، آن‌ها ممکن است فرصت‌های کسب و کاری جدیدی را ایجاد کنند، برای مثال برای تأمین کنندگان بیمه هویت. مسائل رگولاتوری، در ارتباط با قانون، تعداد زیادی مسئله رگولاتوری پیرامون هویت دیجیتال وجود خواهد داشت. یک نگرانی این است که قانون‌گذاری مسیرهای پرآکنده و بارویکردهای متفاوت در حوزه‌های قضایی مختلفی را طی کند. در حال حاضر تا حدودی شاهد کنترل‌های هویتی قدرتمند GDPR در اتحادیه اروپا با روش‌هایی هستیم که در هیچ حوزه قضایی دیگر دیده نمی‌شود. خطر دیگر، درست مشابه هر پلتفرم فناوریانه نوظهور، مقررات خوب اما ناکارآمد و زیان‌بخش است. رگولاتورها باید نسبت به فناوری و انشعابات آن آگاهی داشته باشند و ممکن است نیاز به مداخله در ایجاد یا بازسازی روندها داشته باشند.

قشر مرفه

در نهایت، به عقیده ما، احتمالاً چالش‌های اجتماعی زیادی جهت شناسایی وجود خواهد داشت. بر جسته‌ترین آن‌ها عبارت‌اند از:

تحصیلات. اگر چه شاید مشهود نباشد، اما فکر می‌کنیم که تحصیلات یک چالش اصلی در هویت دیجیتال است و دستیابی به این حق، یک عامل شتاب‌دهنده اساسی به سمت یک راهکار فراگیر و پایدار است. امروزه، عموم مردم، می‌توانند و شاید باید نسبت به مسائل مرتبط با هویت آگاهی بهتری داشته باشند. فکر می‌کنیم که بانک و سایر ارائه‌دهندگان خدمات مالی می‌توانند مسئولیت این چالش را بر عهده بگیرند. معتقدیم که یک نیاز رو به رشد و مبرم نسبت به آموزش مشتریان در مورد این که هویت دیجیتال به چه معنی است و این که چه اتفاقی برای داده‌های آن‌ها در حال وقوع است، وجود دارد. رهبران صنعت و تصمیم‌گیرندگان همچنین می‌توانند درک خود را نسبت به این که چگونه هویت دیجیتال با زنجیره‌های ارزش و مدل‌های کسب و کاری آن‌ها متناسب است، بهبود بخشند و همان‌طور که اشاره شد، رگولاتورها در همراهی با سیاست‌مداران، باید در این جانیز آگاهی خود را حفظ کنند و سیاست‌های خود را طبق آن تنظیم کنند.

ترس و عدم اطمینان. تازمانی که افراد در مورد مسائل هویت دیجیتال آگاهی کامل پیدا کنند، اغلب ترس و سردرگمی پیرامون آنها وجود دارد. قربانیان سرقت هویت، افرادی که در مورد جمع‌آوری اطلاعات شخصی توسط شرکت‌های خصوصی نگران‌اند، کسانی که از سیستم‌های هویتی متمرکز (ملی یا جهانی) هراس دارند، منجر به ایجاد سناریوهای «برادر بزرگ» می‌شوند - همه گروه‌هایی که نگرانی‌هایی دارند باید شناسایی شوند. چنین ترس‌هایی ممکن است مانع پیشرفت شوند.

همچنین ممکن است شاهد گروه‌های مختلفی باشیم که با روش‌های مختلفی در جستجوی هویت دیجیتال هستند. نسل‌های قدیمی‌تر شاید نسبت به سپردن اطلاعات شخصی خود به یک پلتفرم هویتی گسترده‌تر دید بیشتری باشند، در حالی که نسل دیجیتال ممکن است مشتاق‌تر باشند. شاید چنین روندهایی روی چگونگی نزدیک شدن افراد به مسائل حفظ

حریم خصوصی و هویتی در آینده تأثیرگذار باشد.

پذیرش و مقبولیت. در نهایت، ممکن است چالش‌های مهمی به لحاظ پذیرش راهکارهای هویت دیجیتال توسط مشتری وجود داشته باشد. احتمالاً این گونه به نظر می‌آید که استفاده از راهکار جدید هم گران‌تر از روشی است که هم اکنون به کار گرفته می‌شود و هم به اندازه روش فعلی کارآمد و مطلوب نیست. پذیرش، فقط به یک سیستم بنیادین بهتر نیاز ندارد، بلکه به یک تجربه کاربری سرتاسری بهتر نیز نیازمند است. با توجه به حق انتخاب، مشتریان ممکن است امنیت را فدای سادگی استفاده از یک پلتفرم کنند، که این می‌تواند در درازمدت به هویت آسیب برساند. ما فکر می‌کنیم که یک پلتفرم کاملاً محفوظ و ایمن باید یک تجربه کاربری که به طور گسترده‌ای به لحاظ تمام جنبه‌های اقتصادی مقبولیت داشته باشد نیز ارائه دهد. با این حال نباید خطرات تجاری و اعتباری ناشی از شکست یک پلتفرم هویت دیجیتال را کم‌اهمیت جلوه دهیم.

«آینده به احتمال زیاد توسط زیرساخت‌های دیجیتالی که از مبادلات بسیار غیر متمرکز و مبتنی بر اعتماد به فناوری واسطه‌ای پشتیبانی می‌کنند، شکل خواهد گرفت. این فرضیه بعضی از راهکارهای عملی را در مورد مسئله پیچیده هویت دیجیتال توزیع شده در بر می‌گیرد. پرداختن به مشکل هویت دیجیتال همچنین انواع جدیدی از نوآوری‌ها را در روابط مردم و ارائه‌دهندگان خدمات مبتنی بر هویت و همین‌طور تعامل شخص به شخص امکان‌پذیر می‌کند.»

کارستن سورنسن

مدرسه اقتصاد و علوم سیاسی لندن

شرکت‌کننده در مجمع آینده امور مالی

بسیار واجد شرایط

هویت صرفاً در مورد این نیست که ما چه کسی هستیم، بلکه در مورد این که ما توانایی انجام چه کارهایی را داریم نیز است، نه فقط در مورد هویت اصلی ما (نام، آدرس)، بلکه در مورد خصوصیات وابسته مرتبط با آن نیز هست. وقتی این به صورت چنین خصوصیات و پرسوناهایی در می‌آید، راهکارهای هویت دیجیتال می‌توانند امنیت و راحتی را به سیستم فعلی ما بیفزایند. به عنوان مثال مورد سرمایه‌گذاران واجد شرایط (QI) را در نظر بگیرید. در بسیاری از حوزه‌های قضایی در سراسر جهان مقرراتی وجود دارد که این الزام را به وجود می‌آورد که فقط آن دسته از سرمایه‌گذارانی که معیارهای خاصی دارند (برای مثال به لحاظ درآمد، ارزش خالص دارایی یا تجربه حرفه‌ای) امکان سرمایه‌گذاری در انواع خاص سرمایه‌گذاری‌های جایگزین مانند صندوق پوشش ریسک یا سرمایه‌گذاری خصوصی را دارند. این به جهت حفاظت از منافع سرمایه‌گذاران متوسطی است که ممکن است دانش لازم برای درک صحیح این سرمایه‌گذاری‌ها یا ریسک‌های وارده ندارند.

امروزه به طور کلی مسئولیت یک صادرکننده این است که بررسی کند (برای مثال با ملزم کردن سرمایه‌گذار در ارائه اسناد درآمدی، ثروت یا تجربه) که یک سرمایه‌گذار واجد شرایط است یا خیر، این موضوع سرمایه‌گذار را ملزم می‌کند تا اسناد را جمع‌آوری کند و ارائه دهد، و هم چنین صادرکننده را به بررسی آن‌ها ملزم می‌کند. فرآیند باید با جدیت تکرار شود.

در عوض، سناریویی را تصور کنید که در آن یک نهاد حوزه سرمایه‌گذاری، به عنوان مثال کمیسیون بورس و اوراق بهادار (SEC) در ایالات متحده، نقش تأیید اعتبارنامه یک سرمایه‌گذار و صدور مجوز «سرمایه‌گذار واجد شرایط» را به عهده بگیرد.

سرمایه‌گذار می‌تواند این اعتبار را برای هر صادرکننده‌ای که نیاز دارد؛ ارائه دهد. این کار هزینه‌های سرمایه‌گذاری‌های جایگزین را کاهش و سهولت استفاده از آن را افزایش خواهد داد. در صورتی که مرجع صادرکننده این قابلیت را داشته باشد که اعتبارات را به‌روز نگه‌داری کند، شاید با ملزم کردن سرمایه‌گذاران به تجدید اعتبار خود در یک بازه سالانه، تضمین صحت انطباق با قوانین در هر زمانی راحت‌تر باشد.

از این رو چنین فرآیندی احتمالاً امنیت را در سیستم افزایش خواهد داد و به رگولاتور تصویر بهتری از سرمایه‌گذار و نهاد‌های صادرکننده مجوز می‌دهد. یک نهاد مثل SEC این فرآیند را به عنوان یک پیشرفت طبیعی در محدوده کاری خود در ایفای این نوع از نقش بررسی می‌بیند.



خدمات مالی و هویت

بررسی و صیانت از هویت همیشه بخش مهمی در بانکداری بوده است. ما معتقدیم بانک‌ها برای کمک به تشکیل یک پلتفرم باز، مقرون به صرفه و به طور گسترده‌ای قابل دسترس برای هویت دیجیتال، دارای تجربه، تخصص و زیرساخت هستند.

نقشی برای بازی کردن

توسعه یک پلتفرم هویت دیجیتال همه‌جانبه برای بکارگیری یک لایه هویتی در اقتصاد دیجیتال نیاز به یک تلاش جمعی با مشارکت بخش خصوصی، دولت، رگولاتورها، دانشگاه‌ها و... خواهد داشت. با تجربه‌ای که آن‌ها دارند و درک این نکته که چگونه بانک‌ها دارای یک چشم‌انداز واحد نسبت به مشکلات مربوطه هستند، می‌توان نقش کلیدی در تسریع توسعه این راهکار ایفا کرد.

برای مثال، بانک‌ها در حال حاضر نقش مهمی در تامین هویت در حوزه اقتصاد به عنوان دارندگان حساب‌ها و انجام‌دهندگان تراکنش‌ها ایفا می‌کنند. ما می‌دانیم که چگونه افراد، موسسات و دارایی‌ها را روی این سیستم سوار کنیم. مادر بالاترین استانداردهای بررسی هویت، تجربه خوبی داریم. این موضوع هم به نفع خودمان است و هم در نتیجه اجرای مقررات سخت‌گیرانه شناسایی هویت مشتری (KYC)، ضد پولشویی و سایر مقررات هویتی که ما باید به آن‌ها پایبند باشیم. در نتیجه، ارائه هویت بانکی در حال حاضر در سطح پیشرفته‌ای قرار دارد و بسیار قابل اعتماد است.

از آن جایی که ما از مال خود حراست می‌کنیم (که در دنیای امروز به معنی حراست از داده‌هاست) در حفاظت از داده‌های دیجیتال متخصص هستیم. به همین دلیل، علی‌رغم بعضی‌ها که اخیراً، سیستم‌های بانکداری اغلب در بین ایمن‌ترین سیستم‌ها در جهان در نظر گرفته می‌شوند. چون این بخشی از عملکرد ماست تا تراکنش‌ها را در سایر موسسات تسهیل کنیم در نتیجه تجربه زیادی در ایجاد و نگهداری شبکه‌های پیچیده و ایمن که به صورت جهانی مبتنی بر هویت عمل می‌کنند، داریم. این بدان معنی نیست که فکر کنیم بانک‌ها باید تنها تامین‌کنندگان پلتفرم‌های هویتی باشند؛ کاملاً برعکس. اما هر چه به سمت یک آینده هویت دیجیتالی پیش می‌رویم، بانک‌ها می‌توانند تخصص و زیرساخت آن‌ها را تامین کنند. به نظر ما، بانک‌ها در موقعیتی هستند که می‌توانند نقش‌های متعددی در اقتصاد دیجیتال ایفا کنند، به عنوان مثال نقشی به عنوان شاهدان هویتی یا محافظان هویتی که به این ترتیب گامی فراتر از خدمات مالی سنتی بر می‌دارند.

نگاهی به جلو

فکر می‌کنیم که تجربه مادر مسائل هویتی به این معناست که می‌توانیم در گفتمان‌های پیرامون تنظیم پیش‌نویس قوانین حوزه هویت دیجیتال مشارکت داشته باشیم. پس مادر UBS در مورد این که آینده هویت دیجیتالی چگونه باید به نظر برسد چه فکری می‌کنیم؟

پلتفرم ایده‌آل ما - خواه به صورت یک پلتفرم واحد و جهانی و خواه به صورت مجموعه همه‌جانبه‌ای از آن‌ها - یکی از مواردی است که امنیت را در اولویت قرار می‌دهد. سیستمی که در آن سرقت اطلاعات و سپس سوء استفاده از آن‌ها را اگر نگوئیم غیر ممکن ولی دشوار است. همچنین سیستمی است که

از حریم خصوصی افراد محافظت می‌کند، به آن‌ها حق انتخاب زیادی در مورد این که کدام اطلاعات مربوط به خود را آشکار کنند و کدام را خصوصی نگه دارند، می‌دهد.

برای تکمیل این پلتفرم هویتی آینده، لایه‌های مختلف هویتی را که ما پیش‌تر در مورد آن‌ها بحث کردیم، از هویت اصلیمان گرفته تا تمام خصوصیات مختلف، باید با هم تطابق یابند. با انجام چنین کاری، این امکان به ما داده می‌شود که به آسانی از پرسونا‌های مختلف با محتواهای مختلف استفاده کنیم. این پلتفرم برای این که بتوانیم خصوصیات خود را به راحتی به اشتراک بگذاریم، بسیار تعامل‌پذیر است. این پلتفرم به یک فناوری منحصر به فرد اختصاصی متکی نیست، بلکه روی کانال‌های مختلفی که مردم در حال حاضر استفاده می‌کنند یا ممکن است در آینده چه در خانه و یا در جاده و چه به صورت درون مرزی و بیرون مرزی مورد استفاده قرار دهند، کار می‌کند. به نظر ما این موضوع بسیار مهم است که پلتفرم هم بسیار فراگیر و هم صرف‌نظر از جایی که افراد زندگی می‌کنند، قابل دسترس باشد.

در حالی که ممکن است بخش‌هایی از پلتفرم از طریق کار با نهادهای خصوصی برای رفع مشکلات هویتی خاص تکامل پیدا کنند، در صورت تکامل و بلوغ کامل، پلتفرم ما می‌تواند متعلق به هیچ شرکت یا سازمان خاصی هم نباشد. در عوض این پلتفرم متن‌باز و برای استفاده عموم‌رایگان است مثل وضعیتی که اینترنت امروزه دارد. این پلتفرم توسط قوانین و مقررات هویتی مشخص که در سراسر جهان هماهنگ است پی‌ریزی می‌شود، در نتیجه تمام کاربران نسبت به مسئولیت‌ها و تعهدات هویتی اطمینان خاطر دارند. سیستم ما هم چنین بر یک منبع گواهی هویتی، به عنوان مثال یک دولت، متکی نیست. در عوض این پلتفرم به یک شبکه مشخصی از تامین‌کنندگان هویت وابسته است، از دولت‌ها گرفته تا بانک‌ها و شبکه‌های اجتماعی، هر کدام از آن‌ها تکه‌ای از این پازل را تامین می‌کنند.

بنابراین ما همان‌طور که پیش‌تر نیز بدان اشاره کردیم از حامیان رویکرد «خودمختاری» هویت هستیم. این بدان معناست که در نهایت تمام تکه‌های پازل هویت در اختیار افراد جامعه قرار دارد. ما به عنوان مالکان هویت‌های خود، مطابق با قوانین حاکم، بر چگونگی به‌کارگیری هویت‌های خود کنترل کامل داریم. این کنترل هویت در کنار سیستمی که توسط سازمان‌های متصدی که از افرادی همچون خود ما پی‌ریزی می‌شود، قرار دارد.

در نهایت، سیستم ما ملموس و به لحاظ مدیریت و استفاده، آسان‌تر از سیستم‌هایی است که مادر در حال حاضر داریم. این سیستم به ما این امکان را می‌دهد که راحت‌تر به طیف گسترده‌ای خدمات دسترسی داشته باشیم و برای ما آسودگی بیش از پیشی را در کنار آرامش خاطر نسبت به این که هویت‌های ما ایمن و سودمند هستند به ارمغان می‌آورد.

در پایان

این وایت پیپر بینشی را در مورد جنبه مهمی از چهارمین انقلاب صنعتی ارائه داده است. دستیابی به حق هویت دیجیتال، کلیدی برای یک اقتصاد دیجیتال با کارکرد درست است و معتقدیم که بانک‌ها مسئولیت و توانایی بهبود این گفتمان را دارند، و شاید راهکار را معرفی کنند. این نکته که این راهکار چگونه است، اصلاً مشخص نیست. با این وجود، مطمئنیم که این راهکار باید ایمن، تعامل‌پذیر، مقیاس‌پذیر و جامع باشد. از طریق در اختیار گرفتن پتانسیل بیومتریک‌ها، نرم‌افزارهای موقعیت مکانی، بلاکچین و هوش مصنوعی، ما می‌توانیم راهکاری را توسعه دهیم که به لحاظ فنی، تمام انتظارات را برآورده کند. ما هم چنین اطمینان داریم که با سطح مناسبی از تعهد و همکاری، سفر ما به سوی یک راهکار هویت دیجیتال از نظر عملی ممکن، به لحاظ اقتصادی قابل دوام و از لحاظ سیاسی قابل پذیرش است. به علاوه، معتقدیم که فرصتی وجود دارد تا بازار دیجیتالی جدیدی برای هویت‌هایی که امروزه وجود ندارند، ایجاد کنیم. UBS تولد این راهکار را یک انفجار بزرگ نمی‌بیند و معتقد است که این یک فرآیند تکرار شونده و مستمر خواهد بود و پیشرفت احتمالاً مرحله به مرحله است. این مراحل می‌توانند و باید به سمت یک وضعیت نهایی که معمولاً مورد توافق است هم‌تراز شوند. با اتکای زیاد به یک راهکار کارآمد و متقابلاً سودمند، ما باید برای شروع، ابتدا در یک مسیر درست سرمایه‌گذاری کنیم. تعریف مشکلات و چالش‌ها و بررسی دقیق و کامل راهکار، یک نقطه معقول برای شروع است. ما باید متوجه چالش‌ها و ریسک‌ها و فرصت‌هایی که در این مقاله شرح داده شد باشیم و این را غنیمت بشماریم که ذی‌نفعان زیادی وجود دارند که علاقه‌مندند و نیاز خواهند داشت که یک کرسی را در اختیار بگیرند. هویت دیجیتال مفروض صرفاً در مورد ثبت این که ما چه کسی هستیم نیست و وسعت و پتانسیل بیشتری دارد. UBS دست به کار شده و مشارکتی را با سایر کسانی که می‌توانند نقشی در این مسیر ایفا کنند آغاز کرده است. این مبنای کار مجمع‌های آینده امور مالی UBS و مقاله‌هایی است که توسط اعضای آن منتشر می‌شود. در این رویدادها، و در مقاله‌های مربوطه، ما پیشگامان و متخصصین را از سراسر جهان گرد هم می‌آوریم تا بررسی کنند که چگونه چهارمین انقلاب صنعتی به طور کلی همه حوزه‌ها و صنایع و به ویژه خدمات مالی را توسعه می‌دهد. امیدواریم که این مقاله برای شما مفید واقع شده باشد و نسبت به ادامه این گفتمان علاقه‌مند باشید.

