Deloitte.

디지털 신뢰: 현재와 미래의 투자처

Jesse Goldhammer 외 4인

2022년 03월
Deloitte Insights

서론

이해관계자의 신뢰를 떨어트리는 디지털 위협이 만연한 시대에 조직들은 '디지털 신뢰'(digital trust)를 쌓는 데 투자해야 한다. 다시 말해 사기와 범법으로부터 데이터와 정보를 보호하여 여태껏 쌓아온 관계와 명성을 유지하고 수익을 지켜내야 한다. 기술이 발전하면서 디지털 신뢰에 대한 위협 또한 진화하고 있기 때문에 이는 그 어느 때보다 더 어려운 일이 될 것이다. 예를 들어 한 번의 클릭으로 AI를 통해 가짜 디지털 영상, 비디오 및 오디오를 만들어내는 첨단 조작 기술인 딥페이크(deepfake)는 이미 사람을 사칭할 수 있는 지경에 이르렀다. 이러한 사칭으로 인해 2019년 한 에너지 회사의 최고경영자(CEO)가 미화 24만3,000달러를 허구의 공급업체로 송금하는 것을 승인하는 일이 발생하기도 했다.[1] 딥페이크 사기는 비교적 최근에 등장한 위협이지만, 2017년부터 2019년 사이 매년 900% 이상 증가했으며,[2] 2020년 동안 기업들에게 2억5,000만 달러 이상의 손실을 입힌 것으로 추정된다.[3]

이와 관련한 위험 부담이 크고, 어떠한 실수라도 고객 충성도와 재무 성과, 브랜드 자산에 영향을 미칠 수 있으며 궁극적으로는 신뢰를 구축하고 유지하는 조직의 능력을 저해할 수 있다. 설문 조사에 따르면 81%의 소비자가 이러한 디지털 침해 사건을 경험한 후 브랜드에 대한 신뢰를 잃으며, 25%는 브랜드와의 상호 작용을 완전히 중단하는 것으로 나타났다.[4] 팬데믹이 디지털 업무 인프라 구축을 가속화하고[5] 새로운 기술 보안 전략 및 솔루션에 대한 지출이 급증함에 따라 위험 부담이 더더욱 커졌다.[6]

많은 리더들이 디지털 신뢰에 대한 위협을 이해하지만, 보다 발전된 솔루션으로 기존의 사이버 보안 조치를 강화하는 것은 어렵다고 느낄 것이다. 오늘날 디지털 신뢰 요구를 해결할 수 있는 것은 무엇일까? 미래를 준비할 때 디지털 신뢰 솔루션에 대해서는 어떤 투자가 가장 효과적일까? 다양한 선택지가 존재한다. 분석 결과 2015년에서 2020년 사이 디지털 신뢰 분야와 관련된 특허가 매년 최소 2,000건이 제출된 것으로 파악되는데,[7] 이는 그만큼 올바른 도구를 선택하는 것이 어려울 수 있음을 의미한다.

리더들이 디지털 신뢰를 개선하기 위해 어디에 투자해야 할지 고려할 때 인력, 절차, 지배구조, 규제 등을 아우르는 엔드투엔드(end-to-end) 접근 방식을 고려해야 하며, 여기에 기술이 핵심 요소로 작용할 수 있다. 본 연구에서는 조직이 기존 사이버 대책을 넘어 디지털 신뢰를 강화하기 위해 탐색할 수 있는 첨단 조력 기술에 초점을 맞춘다. 해당 분야 글로벌 전문가 및 리더 15명과의 인터뷰를 통해 네 가지 유망한 기술 솔루션(▶AI기반 데이터 모니터링 ▶클라우드 지원 데이터 신탁(data trust) ▶블록체인 ▶양자 기술)을 파악했다. 또한 디지털 신뢰에 관한 이러한 새로운 기술의 성숙도를 측정하기 위해 지난 5-6년간 승인된 디지털 신뢰 관련 특허의 트렌드를 분석하여 이러한 조사 결과를 검증했다. 특허를 받지 않은 상용화된 솔루션 중에도 많은 혁신 사례가 있지만, 본 연구에서는 특허를 통해 광범위한 혁신 영역과 성숙도를 엿볼 수 있어 이에 대해 살펴본다. 또한 승인을 받은 특허만 분석했는데, 이는 등록 특허가 실로 차별성 있고 신뢰할 만한 혁신 지표이기 때문이다(부록 참조, '디지털 신뢰 혁신 연구'). 이러한 솔루션의 성숙도로 볼 때, 두 가지 솔루션이 오늘날의 요구를 충족할 수 있을 것으로 보인다. 나머지 두 가지는 장단기적인 미래를 위한 투자인데, 이를 통해 조직들이 가까운 미래에 진화하고 있는 위협보다 앞서 나가는 데 도움이 될 수 있다.

‘디지털 신뢰’란

딜로이트의 ‘신뢰’에 대한 정의를 바탕으로,[8] 본고에서는 ‘디지털 신뢰’를 ‘이해관계자 경험, 전략적 통찰력, 조직 플랫폼, 네트워크 연결 등에 걸쳐 디지털 자산(데이터/정보, 아키텍처, 애플리케이션, 인프라 등)의 무결성을 구축하고 유지하는 조직의 능력에 대한 고객, 직원, 협력사, 기타 이해관계자들의 신뢰’로 정의한다.[9] 이러한 디지털 신뢰는 투명성과 접근성, 보안과 신뢰성, 개인 정보 보호와 통제, 윤리와 책임을 보장한다.[10]

오늘날 디지털 신뢰를 높이는 솔루션

오늘날 디지털 신뢰를 높이고자 하는 조직은 이미 비교적 성숙한 일반적인 솔루션에 투자할 수 있다. 그러나 현재는 소수의 산업과 사용 사례에만 국한되어 있는 첨단 솔루션이 새로운 가능성을 열 잠재력이 있다. 이러한 첨단 솔루션은 기존의 사이버 대책을 대체하지는 않을 것이며, 오히려 보완적이고 부가적인 디지털 신뢰 이점을 가져올 수 있다. 본 연구는 조직이 현재 채택을 고려할 수 있는 AI 기반 데이터 모니터링과 데이터 신탁, 두 가지 첨단 솔루션을 파악했다.

AI 기반 데이터 모니터링과 데이터 접근 및 사용

본 연구는 디지털 신뢰를 개선하기 위해 AI를 적용할 수 있는 많은 적용 사례 중, 상황별 데이터 정확성을 검증하고 생태계 전반에서 참여자의 데이터 접근 및 사용을 통제할 때 AI 모니터링이 도움이 될 수 있는 몇 가지 비즈니스 사례를 발견했다.

AI는 데이터가 정확한지, 변조되지 않고 신뢰할 만한지 확인하는 데 도움이 될 수 있다. 부정확한 데이터, 오래된 데이터, 누락된 데이터, 라벨이 잘못된 데이터 등 품질이 낮은 데이터를 수동으로 파악하고 정리하는 데는 많은 시간과 비용이 들 수 있다.[11] 조직들은 여기에 매년 평균적으로 1,300만 달러의 비용을 지출하고 있다.[12] 게다가 잘못된 데이터 모델을 사용할 경우 결과를 훼손하고 잘못된 정보의 영향을 증폭시킬 수 있다.[13] AI는 정보 정확성, 확실성, 맥락을 고려한 데이터의 신뢰성 등을 검증하는 데 도움이 될 수 있다.[14] 오늘날 AI 기반 솔루션은 누락 데이터, 이례, 예상치 못한 데이터 등을 실시간으로 감지할 수 있다.[15] 새롭게 등장한 AI 솔루션은 위조되었거나 조작된 문서와 영상, 딥페이크 비디오 등을 식별할 수 있다.[16] 딥페이크 감지 알고리즘은 조작된 부분의 경계에서 그레이스케일(grayscale) 픽셀의 유무 등 디지털 무결성을 검사할 수 있다.[17] 딥페이크 감지 알고리즘은 또한 부정확한 그림자 및 반사 등 물리적 정보의 이상한 점과 입술 움직임, 눈 깜빡임, 동공 모양과 같은 생체 인식 정보의 이상을 확인할 수 있다.[18] 페이스북과 미시간주립대학교의 모델은 AI를 만드는 데 사용된 AI의 특성을 역설계(reverse-engineering)함으로써 대략 70%의 정확도로 딥페이크를 식별한다.[19] 이러한 솔루션은 데이터, 관련 프로세스, 데이터에서 창출된 통찰 등에 대한 신뢰를 쌓는 데 도움이 된다.

AI는 신원(ID) 확인 및 접근 관리를 개선할 수 있다. 이는 인증되지 않은 데이터 접근을 표시하여 방지하고, 비정상적인 사용자 행위 또는 기타 이상 징후를 감지하는 데 도움이 될 수 있다.[20] 행위 관련 솔루션은 사용자와 기기 간의 상호 작용 패턴을 기반으로, 인증된 사용자 ID를 알아내고 봇(bot) 계정을 차단할 수 있다.[21] 악성 소프트웨어나 랜섬웨어로 시스템에 손상을 일으켜 데이터에 대한 접근 권한을 얻는 가장 일반적인 방법에는 피싱(phishing)과 사회공학적 공격(social engineering attack)이 있는데, 머신러닝 기반의 스팸 필터는 이를 통한 무단 접근 시도의 위험을 줄여준다.[22] 한 조사에 따르면 응답자의

75%가 행동 기반 애널리틱스만이 복잡한 랜섬웨어 공격을 잡을 수 있는 유일한 방법이라는 데 동의한다.[23] 행동 애널리틱스는 비지도(unsupervised) 머신러닝 알고리즘과 결합되면 보다 사전 예방적인 보안 조치를 가능하게 할 수 있다.[24] 실제로 AI 솔루션을 완전히 구축한 조직은 구축하지 않은 조직과 비교했을 때 데이터 침해 사고로부터 발생하는 비용 영향을 최대 80%까지 낮출 수 있다.[25]

AI는 데이터가 의도한 바에 맞게 사용되도록 할 수 있다 예를 들어, 조직은 공개 사이트나 플랫품을 AI로 모니터링하여 문서, 음악, 영상 등등의 디지털 자산에 대한 지적재산권 및 저작권 침해 여부를 찾아낸다. 유튜브의 AI 기반 'Content ID' 플랫폼은 저작권이 있는 콘텐츠를 식별하고 합법적인 소유자에게 연간 수십억 달러의 사용료가 지불되도록 해준다. [26]

조직은 디지털 신뢰 AI 사례를 활용하는 방안을 고려할 때 새로 등장한 개인정보보호 기법을 고려해볼 수 있다.[27] 동형암호(homomorphic encryption)를 사용하면 AI 솔루션이 암호화된 데이터를 직접 분석하여 기본 데이터를 해독하고 노출하지 않고도 인사이트를 도출할 수 있다.[28] 그리고 연합학습(federated learning) 기반 솔루션은 실제 데이터 접근이나 교환 없이 분산형 장치와 서버에 걸쳐 데이터를 분석하고 알고리즘을 교육시킬 수 있다.[29] 예를 들어 시큐어 AI 랩스(Secure AI Labs)는 민감한 건강 데이터를 분석하기 위해 연합학습을 활용하며,[30] 구글 광고는 사용자의 관심 분야를 지역적으로, 그리고 익명으로 분석하기 위해 연합 모델로 전환했다.[31] 이러한 접근법들을 통해 데이터 오남용 없이 인사이트를 도출하고 개인정보보호 및 보안을 강화하고 데이터 접근 및 사용 관리를 간소화하는 등의 결과를 얻을 수 있으며, 따라서 규제가 심한 산업에서 AI 활용 가능성이 점점 더 커지고 있다.

AI는 디지털 신뢰의 만병통치약이 아니며, 여전히 성장 가능성이 크다. 본 연구는 특정 사용 사례에 대한 AI의 적용 가능성과 관련된 몇 가지 취약점을 발견했다. 예를 들어, AI는 텍스트를 감시할 때 문맥에 대한 이해가 부족해 제 기능을 못할 수 있다. 이러한 경우, 인간과 AI 사이의 협업 구조가 도움이 될 수 있다. 이밖에 비윤리적이고 편향된 AI는 그 자체로 디지털 신뢰의 쟁점이 될 수 있다. 딜로이트의 연구에 따르면 AI 편향은 능동적이거나(인간의 행동에 기인) 수동적일 수 있으며, 조직이 실감하는 것보다 더 만연할 수도 있다. 교육과 인간 우선 접근법 외에 기술이 이러한 과제를 완화할 수 있는 방법 중 하나이다. 편견을 발견하고 모델 공정성을 보장할 수 있는 AI 솔루션이 일부 개발되고 있다.[32] 이러한 어려운 과제들에도 불구하고 우리가 분석한 결과 디지털 신뢰와 관련된 AI 혁신이 수년간 빠른 속도로 성장하고 있다.[33] AI 알고리즘이 보다 발전하고, 견고하며 광범위한 트레이닝 데이터 세트 및 상관관계가 가능해짐에 따라 사용 사례 전반에 걸쳐 솔루션이 보다 성숙해지고 자동화될 것으로 기대된다.

디지털 정보 공유 방식으로서의 데이터 신탁

데이터가 새로운 화폐이다. MI 커넥션 사이언스 랩(connection Science Lab)의 이사인 알렉스 샌디 펜틀랜드(Alex Sandy Pentland)는 "돈을 위해서는 은행이 있지만, 데이터를 위해서는 동일한 인프라가 없다"고 했다. 그는 데이터 신탁이 그 공백을 메울 수 있다고 말한다.[34]

은행이 금융 자산을 보유하고 관리하는 것과 마찬가지로 데이터 신탁이나 협동조합이 데이터를 관리한다. 이 솔루션은 독립적인 제3자가 정보를 검증, 통제, 보호, 공유하는 비즈니스 모델로, 데이터의 적절한 사용을 통제하고 수혜자를 대신하여 법적 데이터 권한을 관리한다.[35] 고객의 데이터 공유 및 사용에 대한 보다 강력한 보안과 통제를 통해 고객에게 힘을 싣는 방법에는 다양한 접근법이 있는데, 데이터 신탁은 흥미로운 기술적-법적 접근법으로 부상하고 있다. 데이터 신탁은 데이터를 저장하고 집단적 인사이트를 공유하기만 하는 하나의 기업에서부터, 집단적 이익을 위해 협력하는 신뢰할 만한 제3자들로 이뤄진 그룹에 이르기까지 다양한 형태로 나타날 수 있다.[36] 예를 들어 의료 데이터 협동조합인 MIDATA는 회원 스스로가 개인 정보 흐름을 통제하도록 해, 전 세계적으로 의료 연구에 적극 기여할 수 있도록 한다.[37] 영국에서는 '컨스트럭션 데이터 트러스트'(Construction Data Trust)가 설립되어 신뢰할 만한 정보 공유를 촉진한다.[38] 데이터 생산자나 고객의 관점에서 데이터 신탁의 이점은 분명하지만, 제3자의 역할이 투명하지 않거나 본질적으로 신뢰하지 못할 수 있다. 따라서 조직은 고객이 데이터를 관리하기 위해 누구를 받아들일지, 이에 대해 어떻게 커뮤니케이션해야 하는지, 프로세스 중 언제 어디에서 고객을

참여시킬지에 대해 신중하게 고려해야 한다.[39]

비즈니스 관점에서 데이터 신탁은, 윤리적이고 투명한 데이터 수집 및 사용으로 브랜드 평판을 개선하는 것은 물론 데이터 사일로(silo) 감소, 통제력 강화, 감사를 받은 신뢰할 만한 정보에 대한 접근성 등 다양한 이점을 실현하는 데 도움이 될 수 있다. 본 연구를 위해 진행된 인터뷰에 따르면 디지털 신뢰가 데이터 신탁으로 인해 강화될 것으로 나타났는데, 이는 조직이 데이터와 데이터에서 생성된 인사이트로 더 많은 신뢰를 얻을 수 있기 때문이다.

IT 관점에서 데이터 신탁은, 하나의 신뢰할 수 있는 정보 출처를 검증하여 데이터 관리와 공유를 보다 용이하게 하고 신뢰도를 높임으로써 디지털 신뢰를 개선할 수 있다. 또한 조직은 데이터 팽창을 피하고 중개자를 통해 필요한 데이터와 인사이트에만 접근하여 프라이버시와 보호 영역을 한층 강화할 수 있으며,[40] 동시에 데이터 손실이나 데이터 침해, 관리 실수, 사기 등의 위험을 최소화할 수 있다.[41] 데이터 신탁은 또한 사물인터넷(IoT)과 센서에서 발생한 방대한 양의 데이터를 관리하고 공유하는 솔루션으로도 부상하고 있다.[42] 오픈데이터인스티튜트(Open Data Institute)는 런던의 다양한 스마트시티 사용 사례를 대상으로 데이터 신탁 시범 사업을 진행하고 있다.[43] 클라우드 기술은 데이터 신탁으로 하여금 높아진 디지털 신뢰를 가지고 네트워크 전반에 공유되어야 하는 디지털 정보를 보다 효과적으로 관리할 수 있도록 한다. 예를 들어, 마스터카드는 IBM과 함께 고객의 재무 정보를 안전하게 익명으로 관리하기 위해 독립적인 데이터 신탁인 트루아타(Trūata)를 설립했으며, 클라우드는 신뢰할 수 있는 다른 디지털 솔루션에서 이러한 데이터를 사용할 수 있도록 지원한다.[44]

데이터 신탁은 디지털 신뢰를 유지하는 중요한 모델이지만, 어려운 해결과제들이 따른다. 분산형 클라우드 시스템을 사용하면 데이터 공유가 쉬워지지만 제대로 관리되지 않을 경우 데이터 주권과 규정 준수 문제가 발생할 수 있다. 예를 들어 한 국가에 저장된 데이터가 비즈니스 연속성과 재해 복구 목적으로 다른 국가에 위치한 데이터 센터에 복제되어 있을 수 있는데, 이로 인해 적절한 지배구조 및 통제 조치가 제대로 설정되어 있지 않을 때 현지 데이터 표준 및 개인정보 보호법과 관련된 문제가 발생할 수 있다. 또한 데이터 신탁은 가치가 높은 데이터를 집계하므로 데이터가 물리적으로 분산되어 있더라도 여전히 사이버 공격의 대상이 된다. 이 문제를 해결하기 위해 연합 클라우드 보안 모델(federated cloud security model)을 고려할 수 있다. 조직에서는 클라우드 데이터 패브릭(cloud-data fabric, 다양한 출처와 인프라에 걸쳐 원활하게 연결된 데이터)을 활용하여 데이터가 소비될 때 데이터를 추출하고 보다 효과적으로 보호하는 계층형 보안 모델을 만들 수 있다.[45] 이러한 조치를 염두에 두면 데이터 신탁은 다양한 산업의 조직들이 디지털 신뢰를 개선하기 위해 추구할 수 있는 실행 가능한 모델이다.

미래 디지털 신뢰를 바꿀 수 있는 혁신

클라우드로 지원되는 데이터 신탁과 AI 모니터링은 핵심적인 사이버 솔루션을 넘어 데이터 및 정보를 위한 디지털 신뢰를 구축하는 데 도움이 될 수 있는 혁신을 빠르게 발전시키고 있다. 그러나 조직은 또한 기술이 나아가고 있는 방향을 이해하고, 현재의 인프라뿐 아니라 미래 대비를 위해 향후 디지털 신뢰에 혁신을 일으키거나 개선할 기술을 위해 준비해야 한다. 따라서 본고는 질적 연구와 특허 분석을 바탕으로 블록체인과 양자 기술이라는 두 가지 주제를 검토한다. 디지털 신뢰에 대한 이 기술들의 혁신적인 잠재력을 감안할 때 두 가지 기술 모두 조직의 레이더망 안에 있어야 한다.

블록체인과 데이터 출처 및 소유권

종종 신뢰가 필요 없는(trust-less) 솔루션으로 언급되는 블록체인은 독립적으로 검증 가능하며 불변하고 신뢰할 수 있는(trusted) 데이터베이스나 원장을 통해 개인과 조직, 계약 세부 사항 등을 신뢰하는 메커니즘을 제공한다. 조직들이 이 기술 자체를 신뢰하기 때문에 신뢰할 수 있는 제3자의 필요성이 줄어들 수 있다. 일관적이며 지속적으로 감사가 가능한 시스템은 승인 과정과 보안, 개인 정보 보호를 간소화하여, 결국 서로 다른 시스템이 서로 연결되어야 하는 수고를 덜 수 있다.[46] 블록체인 기술과 관련하여 혁신이 빠르게 일어나고 있으며, 프로젝트들은 점차 초기 개념 증명 또는 시범 사업 단계를 넘어서고 있다.[47] 디지털 지문, 디지털 ID, 디지털 자산, 스마트 계약 등이 블록체인의 주요 사용 사례 중 일부이며, 신뢰할 수 있는 관계를 위한 견고한 프레임워크를 제공하는 데 서로 얽혀 있다.[48] 블록체인은 신뢰할 수 있는 거래 기록을 유지하는 데 도움이 될 수 있다. 이해당사자들은 데이터와 그 지문을 추적함으로써 투명성을 높이고 용이하게 데이터 진정성과 무결성을 달성할 수 있다. 복잡한 글로벌 공급망에 걸쳐 제품과 해당 정보를 추적할 수 있는 블록체인 기반 시스템의 도입이 점차 증가하고 있다.[49] 노르웨이 알루미늄 제조업체인 하이드로(Hydro)와 글로벌 인증 기관 DNV는 블록체인 솔루션의 시범 사업을 진행했는데, 이를 통해 도시 내 가로시설물을 이용하는 사람이 간단하게 바코드를 스캔하여 공원 벤치나 쓰레기 통에 사용된 지속가능한 알루미늄을 추적하여 그것의 원재료에서 발생한 이산화탄소 배출량을 확인할 수 있다.[50] 미디어 산업 또한 잘못된 정보 등의 문제에 대응하고 공개적으로 이용 가능한 정보에 대해 디지털 신뢰를 구축하기 위해 블록체인 활용을 모색하고 있다. 세이프닷프레스((Safe.press) 컨소시엄은 회원사 출판물에 블록체인에 연동된 디지털 인감을 추가한다. 새로운 뉴스 출처가 기사나 참고 문헌에 추가될 때마다 해당 키가 추적되므로 소비자들은 그 출처를 추적할 수 있으며 뉴스 위조가 어려워진다.[51]

블록체인은 신뢰할 수 있는 신원 확인에 도움이 될 수 있다. 이는 모든 디지털 관계나 거래에 있어 핵심 요소이다. 블록체인은 신원의 세부 사항을 드러내지 않으면서도 자격 인증이 가능하며, 탈중앙화된 변조 방지 자기주권신원(self-sovereign identity)을 가능하게 해[52] 다양한 상업적 서비스 및 정부 서비

스에 활용이 가능하다. 예를 들어 스위스의 추크(Zug) 시정부는 시민들을 위해 디지털 분산형 주권적 신원을 만들어 투표 및 정부 서비스 접근과 같은 활동에 참여할 수 있게 했다.[53] 이와 유사하게 MIT는 졸업생들이 안전하고 용이하게 외부에 공유할 수 있는 블록체인 기반의 검증 가능한 변조 방지 졸업장을 시범 운영했다.[54]

블록체인은 자산 소유권을 확고히 할 수 있다. 디지털 자산, 특히 암호화폐는 현재 대규모로 도입된 사용 사례이다. 딜로이트의 2021년 글로벌 블록체인 설문조사에 따르면 응답자의 약 40%가 디지털 자산이 준법 및 투명성 향상, 위험 감소, 신뢰성 제고에 상당히 긍정적인 영향을 미칠 것이라고 응답했다.[55] 블록체인에 저장된 유일의 교체 불가능한 데이터 단위인 NFT(Non-fungible token, 대체 불가 토큰)가 디지털 자산의 소유권을 인증하는 솔루션으로 떠오르고 있다.[56] NFT는 복사가 가능한다 하더라도 제작자와 소유자는 여전히 공개적으로 표시된다.[57] 이는 현재 미술 시장과 스포츠 수집품 분야에서 인기를 끌고 있지만[58] 여러 산업에 걸쳐 광범위하게 적용될 가능성이 있다. 예를 들어 NFT는 건강 데이터를 신원 증명서 및 소유권 보증의 형태로 한 특정 개인에게 속하는 것으로 표시할 수 있다. 이를 통해 환자는 데이터가 어떻게 사용되고 있는지 알 수 있으며 수익을 창출할 수도 있다.[59]

마지막으로 블록체인은 더 빠른 법적 합의를 가능하게 하고 신뢰를 자동화할 수 있다. 블록체인을 기반으로 하는 스마트 계약은 당사자들로 하여금 제3자인 중개자나 에스크로(escrow) 없이 조건에 합의하거나 거래할 수 있도록 하고, 오류나 조작의 위험이 감소된 환경에서 자동적으로 실행된다고 신뢰할 수 있다.[60] 미국의 한 주요 금융서비스 회사와 싱가포르 테마섹(Temasek), DBS의 합작 회사인 파르티오르(Partior)는 효율성과 신뢰를 높이기 위해 블록체인과 스마트 계약을 기반으로 하는 국가 간 결제 시스템을 시범 운영하고 있다.[61] 이 회사는 이 플랫폼을 대규모로 도입하기까지 3~5년의 시간이 걸릴 것으로 전망하고 있다.[62] 이 기술은 항만의 정보 및 다지털 자금 자동 검증에도 사용할 수 있어 선박의 처리와 출항 시간을 단축할 수 있다.

이러한 광범위한 활용 사례에도 불구하고 디지털 신뢰를 위한 블록체인 기술은 아직 초기 단계에 있다. 제한적인 트랜잭션(transaction) 처리량, 이용자 혼선, 플랫폼 상호운용성 등의 기술적 제약과 더불어, 개방형(public) 블록체인의 제한적인 인센티브 메커니즘, 산업 표준과 규제 조화의 부족 등의 기술 외 제약으로 인해[63] 디지털 신뢰를 향상시키는 견고한 솔루션을 구축하는 능력이 제한될 수 있다. 그러나 지속적으로 빠르게 혁신이 진행되며 이해관계자들이 성숙해지고 이해도가 향상되면서, 향후 몇 년간 이러한 제약 조건 중 다수가 해결되어 디지털 신뢰로 나아가는 혁신적인 변화가 일어날 것으로 예상된다. 따라서 조직은 미래의 솔루션을 육성하기 위해 다가오는 이 디지털 인프라를 이해하기 시작해야 한다.

양자기술

양자 기술은 세 가지 뚜렷한 방식으로 디지털 신뢰에 영향을 미칠 것으로 보인다.[64] 첫째, 양자 컴퓨터가 약속하는 엄청난 컴퓨팅 능력은 사이버 및 개인 정보 데이터에 대한 방대한 분석을 수행하여 비정상적이거나 의심스러운 행동을 탐지하는 데 적용될 수 있다. 둘째, 양자 기술의 물리적 특성은 암호키 생성과 배포 등 사이버 시스템에 향상된 구성 요소를 제공할 수 있다. 셋째, 양자 컴퓨팅이 완전히 성숙해지면 쇼어 알고리즘(Shor's algorithm)[65]을 구현할 수 있는데, 이 알고리즘은 일부 일반적인 암호화 기법을 해독하기 쉽게 만들어 데이터와 트랜잭션을 공격에 취약하게 만들 수 있다.[66] 양자 컴퓨터가 등장한 이후(postquantum) 시대에 디지털 신뢰를 유지하려면 다수의 역량을 활용해야 할 것으로 보이는데,[67] 특히 '양자 컴퓨팅 공격에 저항력 있는' 암호화 기법, 즉 양자 내성 암호(postquantum cryptography, PQC)의 활용이 두드러질 것으로 보인다. PQC는 고전적인 컴퓨터에서 실행되며 양자 컴퓨터가 해결할 수 없는 것으로 여겨지는 복잡한 수학적 문제를 사용한다. PQC는 현재의 커뮤니케이션 프로토콜 및 네트워크와 상호 운용될 수 있을 것으로 예상되어 보다 비용 효율적이며 유지관리가 용이할 것으로 예상된다.[68] 미국표준기술연구소(NIST)는 2024년까지 양자 내성 알고리즘을 표준화하는 것을 목표로 하고 있다.[69] 또한 조직들이 PQC를 기대하며 자신들의 기본 암호 프로세스를 검토하기 때문에, 전반적인 사이버 위생 수준이 향상되어 더욱 암호화 민첩성(crypto-agile)을 갖출 것으로 보인다.[70] 이렇게 암호 의존에 대한 인식이 향상되면 디지털 신뢰가

개선될 수 있다.

앞서 언급한 바와 같이, 양자 원리는 또한 양자 암호키 분배(quantum key distribution, QKD)와 같은 방법을 사용하여 데이터 암호화 시스템[71]을 개선할 수 있을 것으로 보인다.[72] QKD는 양자 역학을 사용하여 두 당사자 간에 암호 키를 배포한다. 승인 받지 않은 접근을 감지하는 양자 물리학의 고유의 특성 때문에 키를 도청하려는 시도를 감지할 것이다.[73]

그러나 QKD 기술은 복잡한 프로세스와 과도한 크기의 특수 장비, 높은 비용 등 몇 가지 한계점이 있다.[74] 양자 입자의 취약한 상태는 적용 범위 및 도달 범위를 크게 제한할 수 있다.[75] QKD가 실험적으로 소규모 실행된 사례가 일부 알려져 있다. 일례로 스위스의 한 주에서는 QKD를 받아들임으로써 선거 과정의 무결성과 보안을 보호한 바 있다.[76] QKD가 상업적으로도 인정을 받고 중요한 시스템에도 사용될 수 있으려면 한계점을 극복해야 한다. 미국 국가안전보장국은 현재 국가 보안 시스템 내 커뮤니케이션을 보호하기 위해 QKD 사용을 지원하는 것을 자제하고 있다.[77]

오늘날의 인터넷이 언제 미래 양자 해커들에게 취약해질지 예측하기 힘들며, 그러한 일이 일어난다면 디지털 신뢰에 치명적일 것이기 때문에 리더들은 이에 대한 인식을 가지고 가능한 한 일찍 준비를 시작해야 한다. 쇼어 알고리즘은 10~15년 후에나 구현될 것으로 예상되지만,[78] 전략적 사이버보안 자산인 암호 인벤토리(cryptographic inventory)를 모으고 거버넌스 프로세스를 구축하며[79] PQC 알고리즘을 선정 및 구현하는 데 걸리는 시간은 상당하다. 따라서 조직들은 양자 기술과 관련 암호 기법 전망에 대해 명확하게 알고 있어야 하며 암호화 민첩성과 인프라를 발전시키기 위한 기술 투자 및 인재 투자를 적시에 할 수 있도록 해야 한다.[80]

묘책은 없다

디지털 신뢰 문제를 해결할 수 있는 단일 솔루션은 없지만 AI 기반 모니터링, 데이터 신탁, 블록체인, 양자 기술 등이 가치 있는 역할을 할 수 있는 솔루션들이다. 이러한 디지털 신뢰 접근법이 귀사를 어떻게 보호할 수 있을까? 딥페이크가 조직에 미치는 위험에 대해 생각해보자. 회사의 CEO로 가장하여 허위 거래나 데이터 침해를 시도하려는 범법자가 귀사를 표적으로 삼았다고 가정해 보자. 조직의 네트워크와 애플리케이션에 내재되어 있는 AI 기반 모니터링 솔루션이 1차 방어선으로서 잠재적인 딥페이크에 대해 경고하여 추가적인 시도를 차단할 수 있다. 이를 놓칠 경우 강력한 블록체인 기반 솔루션이 트랜잭션 내역을 쉽게 검증하고 스마트 계약 내에 안전 보장 장치를 설정하는 데 도움이 될 수 있다. 또한 데이터 신탁 체제를 통해 손상된 데이터의 양을 최소화할 수 있다. 마지막으로 귀사에서 언젠가 네트워크 및 커뮤니케이션 채널 내에서 양자 내성 안전장치를 구현한다면 다른 조직에서도 귀사의 데이터 및 트랜잭션의 무결성에 대해 훨씬 더 신뢰할 수 있을 것이다.

증가하는 비즈니스 영향을 고려할 때 디지털 신뢰는 더 이상 최고정보관리책임자(CIO)나 최고정보보호책임자(CISO)만의 문제가 아니다. CEO를 비롯한 비즈니스 리더들은 현재와 미래의 기술 투자에 참여해야 한다. 리더들에게 기다릴 여유란 없다. 급격한 기술 혁신으로 인해 새로운 디지털 위협이 너무나도 빠르게 등장하고 있다. 리더들은 선제적으로 혁신의 기회를 감지하고 이에 발맞춰 투자하여 디지털 신뢰를 보강해 나가야 한다. 이는 현재와 미래의 디지털 신뢰를 유지하고 발전시키기 위해 규칙적 리듬과같이 지속적으로 해 나가야 한다.

부록: 디지털 신뢰 혁신 연구

특허 분석 결과 2015년과 2020년 사이에 승인 받은 디지털 신뢰 관련 총 특허 수가 점진적으로 증가한 것으로 나타났다(매년 약 15% 증가).[81] 해당 자료에 따르면 특정 신흥 기술군이 훨씬 빠른 속도로 증가하고 있어 상대적인 중요성과 인기가 있는 것으로 나타났다. 추가 분석 결과 다음과 같은 트렌드가 나타나고 있다(그림 1).

- 클라우드 기술은 혁신 주기가 비교적 성숙했다. 클라우드는 다른 기술을 가능케 하며 어떤 경우에는 다른 기술의 보안과 효율성을 개선하는데, 이를 고려하면 클라우드는 조직의 디지털 신뢰 전략의 필수 기술일 수 있다.

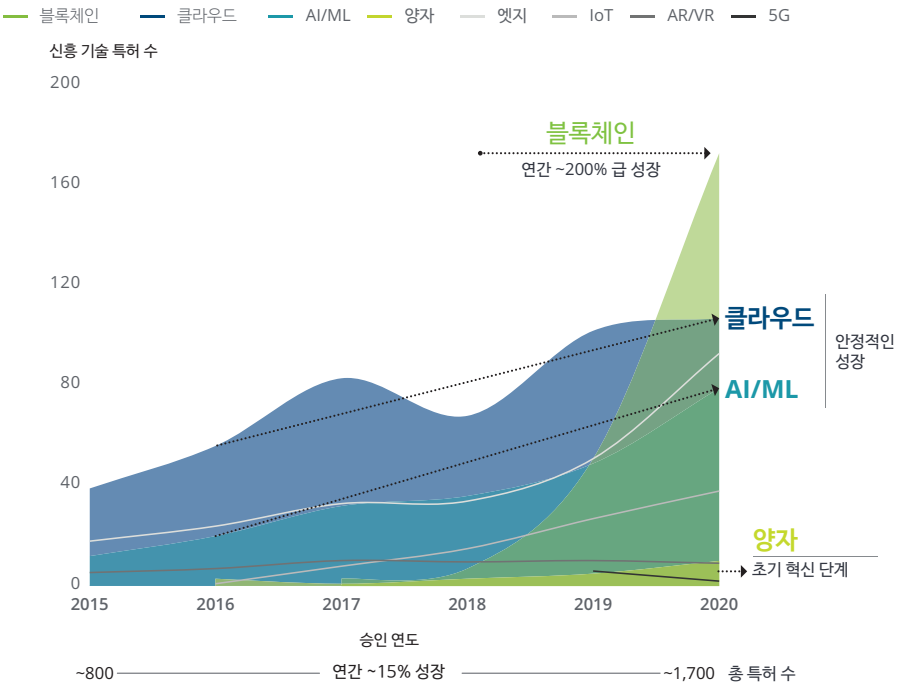
- AI와 머신러닝 특허는 빠른 속도로 증가하고 있으며(35%), 적용 및 사용 사례 전반에 걸쳐 디지털 신뢰를 강화할 수 있는 수많은 방법을 조직에 제공하고 있다.

- 반면 블록체인은 초기 급성장 단계에 접어든 것으로 보인다. 블록체인 특허는 지난 3년간 매년 약 200%씩 성장했다. 이는 블록체인이 점차 실현 가능한 디지털 신뢰 솔루션으로서 유망한 성장 잠재력을 가지고 있을 수 있으나 아직 성숙도의 정점에 도달하지는 않았음을 보여준다. 블록체인 프로젝트들은 초기 개념 증명 또는 시범 사업에서 벗어나 본격적인 구현 단계로 점차 들어서고 있으며,[82] 따라서 가까운 미래에 블록체인은 기업과 생태계 전반에 걸친 디지털 신뢰를 구축하는 데 실질적으로 주춧돌 역할을 할 수 있을 것이다.[83]

- 양자 기술은 혁신 곡선 상에서 훨씬 초기 단계에 있다. 그러나 전문가들은 핵심 양자 컴퓨팅 기능이 성숙함에 따라 민감한 디지털 자산의 보안을 보장하는 데 필수가 될 수 있다고 말한다.[84]

그림 1

2015년~2020년 사이 매년 승인된 디지털 신뢰 특허



참고: 모든 특허 정보는 Quid(https://quid.com)를 통해 Derwent World Patents Index를 참고했다. 분석의 목적은 디지털 신뢰의 일반적인 테마를 파악하는 것이다. 딜로이트는 이 분석을 준비하는 데 있어 개별 특허를 검토하지 않았다.
출처: 딜로이트 분석

주석

1. Catherine Stupp, “Fraudsters used AI to mimic CEO’s voice in unusual cybercrime case,” Wall Street Journal, August 30, 2019.
2. Johannes Tammekänd, John Thomas, and Kristjan Peterson, Deepfakes 2020: The tipping point, Sentinel, October 2020.
3. Jeff Pollard, “Predictions 2020: Cyberattacks influence society in a broader way,” Forrester, October 30, 2019.
4. Ping Identity, 2019 Consumer survey: Trust and accountability in the era of data misuse, October 8, 2019.
5. David Linthicum et al., The future of cloud-enabled work infrastructure: Making future business infrastructure ready, Deloitte Insights, September 23, 2020.
6. Spiceworks Ziff Davis, The 2022 State of IT, accessed January 21, 2022.
7. All information on patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in digital trust. Deloitte did not review individual patents while preparing this analysis.
8. Deloitte defines organizational trust as the foundation of a meaningful relationship between an entity and its stakeholders, at both individual and organizational levels. Trust is built through actions that demonstrate a high degree of competence and the right intent, which result in demonstrated capability (possessing the means to meet expectations), reliability (consistently and dependably delivering upon promises made), transparency (openly sharing information, motives, and choices in plain language), and humanity (genuinely caring for the experience and well-being of others). For more information, please visit: Importance of Trust in your organization | Deloitte US.
9. Rich Nanda et al., A new language for digital transformation, Deloitte Insights, September 23, 2021.
10. Nancy Albinson, Sam Balaji, and Yang Chu, Building long-term trust in digital technology, Deloitte Insights, September 23, 2019.
11. Gil Press, “Cleaning big data: Most time-consuming, least enjoyable data science task, survey says,” Forbes, March 23, 2016.
12. Manasi Sakpal, “How to improve your data quality,” Gartner, July 14, 2021.
13. Don Fancher et al., AI model bias can damage trust more than you may know. But it doesn’t have to, Deloitte Insights, December 8, 2021.
14. Debbie Walkowski, “What is the CIA Triad?,” F5, July 9, 2019.
15. Ira Cohen, “The end to a never-ending story? Improve data quality with AI analytics,” Anadot, accessed January 21, 2022.
16. Sensity, “Fraudulent documents detection,” accessed January 21, 2022; Sentinel, “Defending against deepfakes and information warfare,” accessed January 21, 2022.
17. Mina Tocalini, “Living in a deepfake world,” Arts Management & Technology Laboratory, October 21, 2021.

18. Matt Groh, “Detect DeepFakes: How to counteract misinformation created by AI,” MIT Media Lab, accessed January 21, 2022; Tammekänd, Thomas, and Peterson, Deepfakes 2020; Nadeem Sarwar, “Scientists discover trick to spotting deepfakes, but it’s not easy,” Screen Rant, September 13, 2021.
19. Jeremy Kahn, “Facebook says it’s made a big leap forward in detecting deepfakes,” Forbes, June 16, 2021.
20. Curt Aubley et al., Cyber AI: Real defense, Deloitte Insights, December 7, 2021.
21. Avi Turgeman, “Machine learning and behavioral biometrics: A match made in heaven,” Forbes, January 18, 2018.
22. Ben Dickson, “How machine learning removes spam from your inbox,” TechTalks, November 30, 2020.
23. Sentinel One, Global ransomware study 2018, accessed January 21, 2022.
24. Aubley et al., Cyber AI: Real defense.
25. IBM, How much does a data breach cost—Cost of a data breach report 2021, accessed January 21, 2022.
26. John Paul Titlow, “YouTube is using AI to police copyright—to the tune of $2 billion in payouts,” Fast Company, July 13, 2016.
27. Duncan Stewart, Gillian Crossan, and Ariane Bucaille, Keeping AI private: Homomorphic encryption and federated learning can underpin more private, secure AI, Deloitte Insights, December 1, 2021.
28. VentureBeat, “Meet the new twist on data encryption that promises better privacy and security for AI,” January 16, 2020; Bernard Marr, “What is homomorphic encryption? And why is it so transformative?,” Forbes, November 15, 2019.
29. Brendan McMahan and Daniel Ramage, “Federated learning: Collaborative machine learning without centralized training data,” Google AI Blog, April 6, 2017.
30. Zach Winn, “Enabling AI-driven health advances without sacrificing patient privacy,” MIT News, October 7, 2021.
31. Dieter Bohn, “Privacy and ads in Chrome are about to become FLoC-ing complicated,” Verge, March 30, 2021.
32. Fancher et al., AI model bias can damage trust more than you may know. But it doesn’t have to. Deloitte Insights, December 08, 2021.
33. All information on patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in digital trust. Deloitte did not review individual patents while preparing this analysis.
34. Jeffery Weirens, Michael Bondar, and Jennifer Lee, New models for building digital trust: An interview with MIT’s Sandy Pentland, Deloitte Insights, April 5, 2021.
35. Sylvie Delacroix and Jess Montgomery, “Data trusts and the EU data strategy,” Data Trusts Initiative, June 8, 2020; The Open Data Institute, “How do we unlock the value of data while preventing harmful impacts?,” accessed January 21, 2022.
36. Geoff Mulgan and Vincent Straub, “The new ecosystem of trust,” Nesta, February 21, 2019.
37. MIDATA, “My data—Our health,” accessed January 21, 2022.
38. Construction Data Trust website, accessed January 21, 2022.
39. Deloitte interview.
40. Deloitte, “To build trust, take data protection to the bank,” Wall Street Journal, July 14, 2021.
41. Weirens, Bondar, and Lee, New models for building digital trust.
42. Monique Crichlow and David Castle, “Examining the role of data trusts in smart cities,” Canadian Science Policy Centre, November 2019.
43. The Open Data Institute, “Greater London Authority and Royal Borough of Greenwich pilot: What happened when we applied a data trust,” April 15, 2019.

44. Tanya Andreasyan, “Mastercard and IBM join forces for new “data trust,” Truata,” FinTech Futures, March 19, 2018.
45. Deloitte interview; TIBCO, “What is data fabric?,” accessed January 21, 2022.
46. Deloitte, “To build trust, take data protection to the bank.”
47. Avivah Litan and Adrian Leow, Hype cycle for blockchain technologies, 2020, Gartner, July 13, 2020; Avivah Litan, “Hype cycle for blockchain 2021; More action than hype,” Gartner, July 14, 2021.
48. Deloitte interview.
49. Thomas Jensen, Jonas Hedman, and Stefan Henningsson, “How TradeLens delivers business value with blockchain technology,” MIS Quarterly Executive 18, no. 4 (2019): pp. 221–43; TradeLens, “Together, we can set trade free,” accessed January 19, 2022.
50. Elinar Stabel, “Hydro and DNV GL launch blockchain for greener metals,” Norsk Hydro ASA, March 1, 2021; Ledger Insights, “Aluminium firm Hydro pilots DNV blockchain solution for sustainable traceability,” March 2, 2021.
51. Safe.press, “News certification operated by blockchain,” accessed January 21, 2022.
52. Jai S. Arun and Alexander Carmichael, Digital identity on blockchain, IBM, April 1, 2017; Tykn B.V., “Self-sovereign identity: The ultimate beginners guide!,” accessed January 21, 2022.
53. Consensys, “Blockchain in digital identity,” accessed January 21, 2022.
54. Elizabeth Durant and Alison Trachy, “Digital diploma debuts at MIT,” MIT News, October 17, 2017.
55. Linda Pawczuk, Richard Walker, and Claudina Castro Tanco, Deloitte’s 2021 Global Blockchain Survey: A new age of digital assets, Deloitte Insights, 2021.
56. Sam Dean, “$69 million for digital art? The NFT craze explained,” Los Angeles Times, March 11, 2021.
57. Rebellion Research, “Why NFTs could be the solution to the DeepFake problem,” April 11, 2021.
58. Paul Lee et al., From trading cards to digital video: Sports NFTs kick sports memorabilia into the digital age, Deloitte Insights, December 1, 2021.
59. Chrissa McFarlane, “Tokenized blood? How NFTs are transforming healthcare,” Forbes, June 2, 2021.
60. Deloitte, “Getting smart about smart contracts,” accessed January 19, 2022.
61. Alex Rad, “Partior enters cross-border payments ecosystem as newcomer with big backers,” The Asian Banker, September 23, 2021.
62. Ledger Insights, “JP Morgan, DBS blockchain payment platform Partior launches first pilot,” October 26, 2021.
63. William D. Eggers and Ruth Hickin, Global technology governance report 2021: Harnessing Fourth Industrial Revolution technologies in a COVID-19 world, World Economic Forum, December 2021; Matthew Niemerg, “Private vs. public blockchains for enterprise business solutions,” InfoQ, September 21, 2021; Shea Ketsdever and Michael Fischer, “Incentives don’t solve blockchain’s problems,” accessed January 21, 2022.
64. Scott Buchholz, Deborah Golden, and Caroline Brown, A business leader’s guide to quantum technology, Deloitte Insights, April 15, 2021.
65. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” IEEE Xplore, August 6, 2002.
66. Deborah Golden et al., Preparing the trusted internet for the age of quantum computing, Deloitte Insights, August 6, 2021.
67. World Economic Forum, Quantum personas: A multistakeholder approach to quantum cyber risk management, 2021.
68. Buchholz, Golden, and Brown, A business leader’s guide to quantum technology; National Security Agency, “Quantum key distribution (QKD) and quantum cryptography (QC),” accessed January 21, 2022.
69. NIST, “Post-quantum cryptography (PQC),” June 14, 2021.

70. Golden et al., Preparing the trusted internet for the age of quantum computing.
71. Ibid.
72. Buchholz, Golden, and Brown, A business leader's guide to quantum technology.
73. QuantumXchange, "Quantum cryptography, explained," accessed January 21, 2022; Toshiba Clip, "Securing the future of a digital society: Achieving secure transfer of sensitive data between remote facilities on a single fiber," April 20, 2021.
74. NSA, "Quantum key distribution (QKD) and quantum cryptography (QC)."
75. Deloitte, "With quantum computing's rise, cybersecurity takes center stage," Wired, accessed January 21, 2022.
76. QuantumXchange, "Quantum communications in real world applications," accessed January 21, 2022.
77. NSA, "Quantum key distribution (QKD) and quantum cryptography (QC)."
78. Kylie Robison, "Here's how quantum computing could transform the future," Business Insider, March 2, 2021. Michele Moska and Marco Piani, Quantum threat timeline report 2020, Global Risk Institute, January 27, 2021.
79. Colin Soutar et al., "How the world can prepare for quantum-computing cyber risks," World Economic Forum, September 28, 2021.
80. Duncan Stewart et al., Quantum computing in 2022: Newsful, but how useful?, Deloitte Insights, December 1, 2021; Golden et al., Preparing the trusted internet for the age of quantum computing, Deloitte Insights, August 6, 2021.
81. The number of granted digital trust patents analyzed was approximately 7,000 (between 2015–20). All information on patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in digital trust. Deloitte did not review individual patents while preparing this analysis.
82. Litan and Leow, Hype cycle for blockchain technologies, 2020, Gartner, July 13, 2020; Litan, "Hype cycle for blockchain 2021; More action than hype," Gartner, July 14, 2021.
83. Gartner, "Gartner 2019 hype cycle shows most blockchain technologies are still five to 10 years away from transformational impact," press release, October 8, 2019; Deloitte interview.
84. Deloitte interview.

저자

Jesse Goldhammer I jgoldhammer@deloitte.com
Jesse Goldhammer is a managing director in Deloitte's cyber security practice and leads the firm's Trustworthy Institutions initiative. He is deeply committed to the safeguarding of public and private sector data, networks, systems, and people from a wide range of cyber threats. An accomplished instructor, author, and speaker, he has written articles and given presentations on a variety of cyberand trust-related topics.

Curt Aubley I caubley@deloitte.com
Curt Aubley is Deloitte's Cyber and Strategic Risk Groups managing director and general manager for the Threat Detection & Response. He leads the development of the vision, strategy, solution development, roadmap, go-to-market, sales, ecosystem, alliances, and overall execution in alignment with Deloitte's strategy.

Michael Morris I micmorris@deloitte.com
Michael Morris is a managing director in Deloitte's Cyber and Strategic Risk practice where he leads Engineering for Detect and Respond. He is responsible for the technical vision, technological development, operations engineering, and was the chief architect behind the Adversary Pursuit platform and methodology. He has experience in intelligence operations, advanced offensive and defensive cyber operations, and tactics and tool development.

Jay Parekh I japarekh@deloitte.com
Jay Parekh is a senior analyst with the Deloitte Center for Integrated Research. He has over six years of experience in research and analysis focused on emerging technologies and digital innovations related to cloud computing, augmented & virtual reality, the Internet of Things (IoT), and other advanced technologies. He also focuses on developing Deloitte's perspectives on cross-industry topics such as climate change and sustainability.

Diana Kearns-Manolatos I dkearnsmanolatos@deloitte.com
Diana Kearns-Manolatos is a senior manager in the Deloitte Center for Integrated Research where she analyzes market shifts and emerging trends across industries. She leads Deloitte's global research on digital transformation. Additionally, Kearns-Manolatos draws on almost 15 years of award-winning marketing communications expertise to align insights with business strategy.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Jesse Goldhammer
Managing director | Deloitte Risk & Financial Advisory
+1 415 783 7681 | jgoldhammer@deloitte.com

Jesse Goldhammer is a managing director in Deloitte's Cyber Security practice and leads the firm's Trustworthy Institutions initiative. He specializes in helping clients build new cyber and trust capabilities using cutting-edge technologies.

Deloitte Center for Integrated Research

Diana M. Kearns-Manolatos
Senior manager, subject matter specialist | Deloitte Services LP
+1 212 436 3301 | dkearnsmanolatos@deloitte.com

Diana M. Kearns-Manolatos is a senior manager with Deloitte Services LP's Center for Integrated Research, where she leads Deloitte's global research on digital transformation.

Deloitte.
Insights

딜로이트 안진회계법인·딜로이트 컨설팅
고객산업본부

오성훈 Partner
고객산업본부 본부장
sunoh@deloitte.com

김사헌 Director
딜로이트 인사이트 편집장
sahekim@deloitte.com

HOT LINE
02) 6099-4651