

IDG Deep Dive

“가능성과 버블사이”

2018 블록체인 비즈니스 현황 진단

많은 기업들이 블록체인을 활용한 비즈니스 혁신을 꾀하고 있다. 이미 공급망 및 물류 업계에선 블록체인 파일럿 테스트가 활발히 진행 중이며, 보다 위험 부담 없이 블록체인을 도입할 수 있도록 도와주는 블록체인 서비스(Blockchain-as-a-Services)도 다양하게 나와있는 상태. 하지만 블록체인이 모든 비즈니스에 적합한 것은 아니며, 초기 단계인 기술이기에 도입 과정에서 많은 시행착오를 겪을 수 있다는 전문가들의 지적도 있다. 블록체인 도입을 계획하고 있는 기업들이 알아두어야 할 블록체인의 현황과 문제점들을 살펴본다.

- ❖ “파일럿 넘어 현실로 간다” 블록체인 기술 현황 진단
- ❖ 블록체인에 뛰어들기 전 고려해야 할 사항
- ❖ ‘BaaS’ 쏟아진다... 위험부담 없이 기술 테스트 가능
- ❖ 우후죽순 속 옥석은?... 검토할 만한 블록체인 분야 스타트업 10곳
- ❖ 블록체인의 5가지 문제점



“파일럿 넘어 현실로 간다” 블록체인 기술 현황 진단

Bill Snyder | CIO

비트코인을 비롯해 수많은 암호 화폐를 지원하는 기술인 블록체인(Blockchain)이 주류 사업으로 거듭날 준비를 하고 있다. 이미 여러 업종의 다수 기업과 최소 3개국 정부가 시범 운영 또는 경우에 따라 실제 블록체인 애플리케이션 배치를 실시하고 있다. 공급망 관리와 식품 안전성 개선, 신원 확인, 부동산 거래 수행, 의료 기록 및 보험 거래 처리 등이 대표적인 초기 사용례다.

IBM, 마이크로소프트, 일련의 스타트업 기업들이 블록체인 플랫폼 구축과 관련해 상당한 규모의 비즈니스를 이미 펼치고 있으며 블록체인 엔지니어와 개발자의 몸값은 연일 올라가고 있다.

비즈니스 컨설팅 기업 액센추어의 금융 서비스 상무이사 데이비드 트리트는 “지난 2년 동안 많은 시범 프로젝트가 있었고 이제 진정한 블록체인 애플리케이션이 등장하고 있다”라며, “금융 서비스 외에 신원과 공급망이라는 압도적인 두 가지 테마가 존재한다”라고 말했다.

블록체인이 적합한 비즈니스

IDC는 최근 “블록체인 원장과 인터커넥션이 2021년까지 36개월 동안 꾸준히 발전할 것이며 글로벌 2000 기업 중 최소 25%가 블록체인을 대규모 디지털 신뢰를 위한 기초로 사용할 것”이라고 전망했다.

그러나 블록체인에 대한 혼란이 여전히 적지 않게 존재하고 있다. 액센추어의 트리는 “고객과의 만남에서 블록체인이 비트코인이 아니라고 설명하는 데 상당한 시간이 소요되곤 한다”라고 말했다.

기본적으로 블록체인은 네트워크의 참가자들 사이의 거래 이력을 기록하는 공유된 분산형 원장이다. 일련의 거래가 블록(block)이라는 기록에서 확인된다. 블록은 암호화되고 이전에 확인된 블록에 연결되어 체인을 구성한다.

이 기술에 대해 특히 낙관적으로 보는 이들이 있다. 포레스터의 수석 애널리스트 마르타 베넷은 “블록체인 솔루션을 지금 바로 도입해 배치해야 하는 것처럼 이야기하는 이들이 있다. 그러나 늘 그렇지는 않다”고 지적했다. 그는 이어 “오늘날 블록체인의 위치를 비유하자면 80년 말의 인터넷과 유사하다”고 말했다.

베넷은 업체가 블록체인 애플리케이션에 관해 홍보할 때 IT 임원들이 중요한 사항을 질문해야 한다고 조언했다. “블록체인이 다른 애플리케이션과 차별화되는 점은 무엇인가?”라는 질문이다.

베넷의 말은 블록체인에 비즈니스적 미래가 없다는 뜻이 아니다. 다른 애널리스트 및 산업 임원들과 마찬가지로, 먼저 발전할 가능성이 높은 사용례로 공급망과 물류를 지적하고 있다.

공급망에서의 블록체인

일반적으로 공급망에는 일련의 거래를 처리함에 있어 비즈니스 정보의 일부를 공유해야 하는 여러 당사자들이 관련된다. 그리고 각 당사자는 해당 정보가 변경되거나 삭제되지 않았음을 확인해야 한다. IDC의 블록체인 전략 연구이사 빌 페언리는 “진실을 보여주는 버전이 있어야 한다”라며, 그것이 블록체인의 최대 장점이라고 설명했다.

WHO(World Health Organization)가 2015년 말 설문조사 결과를 공개하기 전까지, 부패한 음식에 관한 문제가 얼마나 만연했는지 잘 알려지지 않았다. WHO에 따르면, 매년 약 10명 중 1명이 오염된 식품을 섭취해 질병을 앓고 있으며, 5세 이하의 아동 12만 5,000명을 포함한 42만 명이 이로 인해 사망하고 있다. 대부분은 아프리카와 동남아시아에서 발생하지만, CDC(Center for Disease Control)은 미국 내에서도 식품으로 인한 질병으로 매년 약 3,000명이 사망하고 있는 것으로 추정했다.

신선식품 유통업체인 드리스콜스(Driscoll's)의 CIO 톰 쿨렌은 식품을 원산지부터 시장까지 정확하게 추적할 수 있다면 식품으로 인한 질병의 근원을 지금보다 훨씬 쉽고 빠르게 찾아낼 수 있을 것이라고 본다. 드리스콜스는 부패 식품 추적 문제에 블록체인 기술을 적용하기 위해 IBM과 협력해 파일럿 프로그램을 진행한 13개 주요 식품 생산자 및 유통업체 중 하나다.

드리스콜스는 이미 미국 내, 미주, 아시아 태평양, 중동의 일부, 아프리카, 유럽에서의 수천 명의 독립 재배자를 아우르는 공급망에 대한 상당한 가시성을 확보하고 있다. 바코드와 QR 코드를 활용해서 과일의 원산지를 개인 재배자와 특정 수확물로 추적할 수 있다.



IBM은 부패한 식품 문제에 블록체인 기술을 적용하기 위해 13개 주요 식품 생산자 및 유통업체와 함께 파일럿 프로그램을 진행했다. <이미지 : IBM>

현재 이 수십 억 달러 규모의 유통업체는 데이터 수집 범위를 확대해 공장에서의 이벤트 그리고 과일이 유통 센터를 떠나 고객 및 소비자 수준에 도달할 때까지 발생하는 이벤트 등도 포함하고 싶어한다. 목표는 식품 안전성에 대한 투명성을 확보하고 개선하는 것이다. 쿨렌은 “업계의 그 누구도 이 문제를 완벽히 해결하지 못했다”라고 말했다.

식품 외에도 추적할 것들이 있다. 10월, 일본에서 3번째로 큰 제철 기업 고베 스틸(Kobe Steel)은 제조한 알루미늄 및 구리의 품질에 대한 생산 기록을 위조했다고 인정했다. 200개의 다른 기업에서 기준 이하의 재료로 제품을 만드는 상황이 발생한

것이다.

IBM의 엔지니어 엘리자베스 스탈은 “블록체인은 원본 검사 인증서가 가짜가 아닌지 확인하고 동의를 통해 승인을 가능하게 한다. 문제가 발생할 경우 블록체인은 자동차, 항공기, 기차 제조업체가 사용한 재료의 출처를 확인하도록 할 수 있다”라고 밝혔다.

하지만 다양한 산업에서 블록체인을 의미있게 배치할 수 있으려면 거쳐야 할 중요한 단계가 있다. 표준 합의가 그것이다. IBM의 블록체인 비즈니스 개발 부사장 브리지드 맥더못은 “블록체인이 새로운 기술이기는 하다. 그렇다고 불필요한 일을 반복할 필요는 없다. 가능한 경우 기존의 표준을 취해야 한다고 생각한다”라고 말했다. 예를 들면, 식품 산업에서 기업들은 포장지의 바코드에 이미 GS1 표준을 사용하고 있기 때문에, 이를 블록체인 프로젝트의 일환으로 수용하는 것이 당연하다는 설명이다.

한편, 블록체인이 낯선 기술이라는 점에서 2015년에 블록체인을 전략적인 우선순위로 설정한 IBM과 그 블록체인 플랫폼은 초기 진입자로서의 이점이 있다. 하지만 마이크로소프트, HPE, AWS, SAP 등 다른 업체들도 스스로 자리를 잡고 있다.

2가지 중요한 문제 “소비 전력과 보안”

모든 상업 거래의 기본은 신뢰이며, 이 신뢰는 제 3자를 통해 수립되는 경우가 많다. 예를 들어, 부동산 업계에서는 중개인이 일반적으로 구매자와 판매자 사이의 신뢰 받는 중개자다.

하지만 블록체인 거래는 합의(consensus)라는 프로세스를 이용해 이뤄진다는 점에서 전통적인 거래와 다르다. 인텔의 플랫폼 보안 사업부 부사장 겸 책임자인 릭 에쉐바리아는 “합의는 블록체인이 주문과 거래의 유효성에 대한 동의에 도달하기 위해 사용하는 프로세스다. 이를 통해 거래하는 당사자들이 신뢰 받는 중개자 없이 동의할 수 있게 된다”고 설명했다.

실제로 추가만 가능하도록 설계된 블록체인 분산형 원장 아키텍처 덕분에 해커는 데이터를 삭제하거나 변경할 수 없다. 그리고 노드(Node)에서 데이터가 삭제된다 하더라도 여전히 백업에 존재하기 때문에 해커의 접근이 매우 어렵다.

하지만 데이터가 작성자의 방화벽 밖에 존재하기 때문에 일부 민감한 용도에는 보안이 부족할 수 있다. 인텔의 의료 프라이버시 및 보안 책임자인 데이비드 호울딩은 “프라이빗 및 허가된 블록체인의 경우라도 블록체인에 입력된 민감한 데이터가 참여 조직의 방화벽과 경계를 실제적으로 벗어날 수 있다”고 밝혔다.

리눅스 재단의 하이퍼레저(Hyperledger) 프로젝트 책임자인 브라이언 벨렌도르프는 하이퍼레저 업계와 참여자들이 “자주적 신원(self-sovereign)”부터 “영지식증명(Zero Knowledge Proofs)”까지 더욱 발전된 보안 방법을 개발하고 있다고 전했다. 하지만 규제 당국 및 네트워크 보안 담당자들은 이 새로운 기술이 민감한 데이터와 관련해 충분히 신뢰할 수 있다는 확신이 필요하다고 지적한다.


보안 우려와 함께 인텔 및 기타 기업들은 소비전력 문제도 제기한다. 에쉐베리아에 따르면 인텔이 블록체인을 연구하려는 시도가 시작된 계기가 네트워크에 끼치는 영향에 대한 우려였다. 이런 우려는 최초의 주요 블록체인 애플리케이션인 비트코인과도 직결되어 있다.

피터 페얼리가 지난 9월 IEEE 스펙트럼(IEEE Spectrum)에서 밝힌 내용에 따르면, 비트코인은 이미 엄청난 양의 전력을 소모하고 있다. 비트코인 채굴자들이 사용하는 컴퓨팅 서버 랙이 소규모 도시 정도의 전력을 소모하고 있기도 하다. 블록체인의 다른 장점과 별개로 전력과 연산 자원의 고갈이라는 단점에도 이목이 쏠리고 있는 것이다.

뜨거운 인력 시장?

업계 전반에 걸쳐 실질적인 관심이 증가하는 조짐은 보이지만 블록체인 기술을 보유한 IT 전문가에 대한 시장의 강도를 구체적으로 측정하기란 쉽지 않다. IDC의 페언리는 “기업과 업체들이 채용문을 열고 있고 각종 컨퍼런스 참석률도 높다. 컨소시엄과 협업이 가속도를 얻고 있다”고 전했다.

고용주들은 블록체인 기술에 대한 프리미엄을 지불하기 시작했다. 약 5,500개 기업 고용주들이 제공하는 임금 프리미엄을 추적하는 컨설팅 업체의 데이비드 푸트는 “현재 블록체인 임금에서 프리미엄이 발견된다. 기본급의 12%부터 17%까지 범위다”라고 말했다. 푸트는 이 프리미엄이 향후 6개월 동안 증가할 것으로 보고 있다.

그러나 블록체인 기술이 많은 사람들이 원하는 기술 목록의 상위를 차지하진 않으며, 갑작스러운 수요 증가를 기대해서는 안 된다고 경고한다. 푸트는 많은 블록체인 노력이 여전히 개념 증명 및 파일럿 단계인 상황에서 이 기술이 그 가능성과 장밋빛 전망에 부응할지는 아직 확실하지 않다고 지적했다. 

블록체인에 뛰어들기 전 고려해야 할 사항

Lucas Mearian | Computerworld

비트코인의 기반을 잘 알려진 블록체인은 IT 부서와 경영진 모두에게 여전히 수수께끼에 가까운, 빠르게 진화하는 기술이다. 분산 원장 기술인 블록체인은 2017년 본격적으로 부상하기 시작했다. IBM부터 JP 모건까지, 그 외에도 수많은 소규모 기업들이 앞다퉀 블록체인을 채택했다. IT 업체에는 블록체인 기술과 이 기술을 사용하는 방법에 대한 기업들의 질문이 쏟아졌다.

블록체인 거래 원장을 구현할 시기와 그 이유에 대한 의사 결정에는 여전히 위험성이 내포되어 있다. 에베레스트 그룹(Everest Group)이 발행한 새로운 보고서 “블록체인 도입 장벽 없애기 - 비즈니스 프로세스를 위한 우선순위 프레임워크(Unblocking Blockchain Adoption- a Prioritization Framework for Business Processes)”에 따르면, 많은 초기 도입 기업들이 궁극적으로 거의 아무런 혜택도 제공하지 않는 기술에 많은 시간과 돈을 투자한 결과를 맞이하게 될 위험이 있다.

은행 및 금융 서비스는 가장 먼저 블록체인 원장을 도입했다. 이들 기업의 핵심 비즈니스 기능이 기록 시스템으로서의 블록체인이 가진 분산, 투명성, 불변성이라는 속성과 잘 맞아 떨어진다는 점을 감안하면 당연한 흐름이다.

또한, 이 업계는 거래 참가자 간 신뢰 구축에 의존해야 하는데 이는 중앙 관리, 많은 수의 중

※ 블록체인 도입에 영향을 미치는 주 요소

(출처 : 에베레스트 그룹, 2017)



개자, 때로는 여러 대륙을 포괄하는 규제 기관의 감독으로 인해 많은 시간이 소비되는 비효율적인 프로세스다.

에베레스트 그룹은 보고서에서 그럼에도 비교적 단순하고 비파괴적인 블록체인 구현을 통해 상당한 비즈니스 혜택을 달성할 수 있다고 밝혔다. 기업에서 블록체인을 평가할 때 고려해야 할 에베레스트 그룹이 제안한 몇 가지 요소는 다음과 같다.

파일럿 프로그램부터 시작하기

블록체인 파일럿 프로그램은 많은 비용을 들이지 않고 손쉽게 시작할 수 있다. 에베레스트 그룹의 영업 책임자 로낙 도시는 특히 클라우드 기반 인프라와 통합이 용이한 API를 통한 블록체인 패브릭이 포함된 블록체인 서비스(Blockchain-as-a-Service, 이하 BaaS)가 증가하고 있다고 지적했다.

그러나 유능한 블록체인 개발자 및 모범 사례의 부족, IT 인프라 비용(서버 노드), 재사용 가능한 구성 요소의 부족, 비즈니스 사례 구축 비용으로 인해 초기 비용이 높아질 수 있다. 특히, 여러 당사자가 참여하는 경우 더욱 그렇다.

지금은 시장의 과열된 분위기가 기업들을 끌어들이고 있지만, 에베레스트 그룹에 따르면 “부족한 정보를 근거로 내린 의사 결정은 많은 비용을 초래하는 실수로 이어지고, 이로 인해 강력한 블록체인 기술에 대한 조직의 의욕이 파괴될 수 있으므로” 막무가내로 블록체인을 구현해서는 안 된다.

그렇다고 너무 오래 구경만 하면서 행동에 착수하지 않으면 블록체인이 제공하는 경쟁 우위를 놓칠 수 있다. 도시는 “엔터프라이즈 이더리움(Enterprise Ethereum), 하이퍼레저(Hyperledger), 코다(Corda)와 같은 오픈소스 프로젝트 또는 컨소시엄이 출범하는 여러 엔터프라이즈급 블록체인 플랫폼이 있다”라면서, “그러나 실제 구축사례가 제한적인 현재는 그 실용성이 아직 입증되지 않았다. 2018년 여러 구축 사례가 추가되면 상황이 달라지기 시작할 것”이라고 말했다.

도시는 블록체인 파일럿 프로젝트를 추진하기 전에 블록체인이 무엇을 할 수 있고 어떤 점에서 부족한지 정확히 이해할 수 있도록 CIO 또는 CTO가 이사회를 대상으로 교육을 해야 한다고 말했다. 이는 현재의 과제와 이를 해결하기 위해 기존 프로젝트의 로드맵을 어떻게 만들 것인지에 대한 이해를 의미한다.

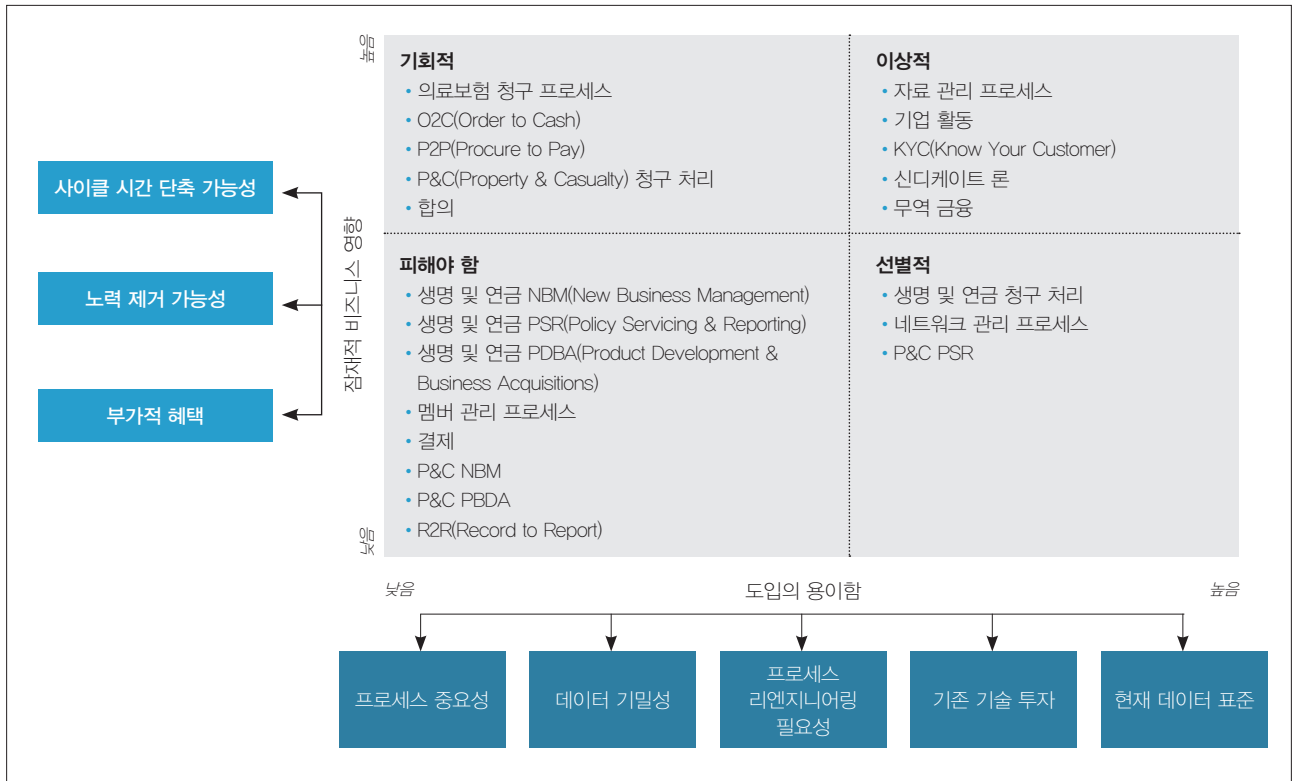
또한, 기업은 시장 정보 팀을 육성해서 블록체인 생태계의 혁신을 살피고 업계의 트렌드에 따라야 한다. 이러한 구성 요소를 갖추면 비로소 기업은 개념 증명과 실제 파일럿에 착수해 블록체인의 잠재력을 탐색하고 이 기술에 대한 내부 전문 지식을 쌓아갈 수 있다.

블록체인에 가장 적합한 기업은?

에베레스트 그룹은 블록체인 프로젝트를 추진하기에 가장 적합한 4개의 비즈니스별 영역과 직무 사용 사례를 구분하는 블록체인 우선 순위 프레임워크를 만들었다. 프로젝트의 범주는 회계, 은행 및 금융 서비스, 보건 및 보험 업계를 포함한다. 에베레스트는 각 비즈니스 프로세스를

블록체인 우선 순위 프레임워크를 사용해 범주화한 비즈니스 프로세스

(출처 : 에베레스트 그룹, 2017)



‘이상적인’ 사용 사례, ‘기회적’ 사용 사례, ‘선별적인’ 사용 사례, 그리고 블록체인 기술을 ‘피해야 할’ 사용 사례로 구분했다. 마지막 범주는 분산 원장이 변화에 대한 강한 저항을 유발하는 반면 큰 이점은 없는 분야를 의미한다.

블록체인 성장은 2018년에도 지속

도시의 올해 확장성과 거버넌스에 관한 문제를 해결할 수 있다면 블록체인의 실제 구현 사례가 폭발적으로 증가하고 그로 인해 “구인 전쟁”이 일어날 것이라고 말했다.

카네기 멜론 대학의 컴퓨터 과학 학부 부교수 비폴 고얄은 많은 기업이 엔터프라이즈 블록체인에 관심이 있으며 “대규모 킬러 앱” 중 하나로 공급망 관리와 관련된 앱을 언급했다. 예를 들어, 고얄은 상품이 한 장소에서 다른 장소로 이동하거나 회사의 한 부서에서 다른 부서로 이동할 때 “기업들은 블록체인을 사용해서 상품의 이동을 추적하는 데 관심이 있다”고 말했다.

보험 업체들은 국가간 수송되는 화물 컨테이너의 상품을 블록체인 분산 원장을 사용해서 추적하는 데 관심을 갖고 있다. 또한, 국경을 넘나들며 실행되는 금융 거래의 경우 블록체인은 거래 투명성, 효율성, 규제 기관 감시로부터의 자유라는 뚜렷한 이점을 제공한다.

고얄은 “중앙 통제 기관이 없다. 현재 비트코인은 법적 회색 지대다. 정부에는 이러한 거래를 차단하거나 규정을 강제할 기술적 역량이 없다”고 말했다.

에베레스트 그룹의 보고서는 기업이 블록체인 개념 증명을 진행할지, 기술이 더 성숙해질 때까지 기다릴지, 또는 핵심 비즈니스 애플리케이션 측면에서 이점이 없으므로 피해야 하는지 여

블록체인 도입 여부 결정을 위한 방법론

(출처 : 에베레스트 그룹, 2017)

잠재적 비즈니스 영향		도입의 용이함	점수가 높을수록 블록체인 도입이 적합함
사이클 시간 단축 가능성 	블록체인 도입의 결과로 부가적 혜택을 얻을 가능성이 낮음		높은 사이클 시간 단축 및/또는 그 결과로 얻는 비즈니스 혜택이 많음
노력 제거 가능성 	블록체인 도입의 결과로 노력을 제거할 가능성 낮음		부가적인 혜택을 얻을 가능성 높음
부가적인 혜택 	블록체인 도입의 결과로 부가적인 혜택을 얻을 가능성이 낮음		부가적인 혜택을 얻을 가능성이 높음
프로세스 중요성 	핵심 프로세스		비핵심 프로세스
데이터 기밀성 	데이터 공유에 대한 큰 장벽		데이터 공유에 대한 낮은 장벽
프로세스 리엔지니어링 필요성 	대대적인 프로세스 재설계 필요		프로세스를 블록체인에 옮겨 넣을 수 있음
기존 기술 투자 	높은 기존 기술 투자		대대적인 기존 기술 투자 없음
현재 데이터 표준 	이질적인 데이터 표준		범용 데이터 표준 유행

부를 결정하기 위한 방법론을 제시한다.

고려해야 할 핵심 요소

도입을 위해 유의해야 할 핵심 요소에는 ‘프로세스 중요성’ 즉, 비즈니스 프로세스가 얼마나 중요한지, 문제가 발생할 경우 관련된 위험이 어느 정도인지 포함된다.

도시는 프로세스 중요성은 프로세스를 현재 시스템(예를 들어, 중앙 관리 관계형 데이터베이스)에서 블록체인 기반 시스템으로 옮기는 것과 관련된 잠재적 위험으로 정의된다고 말했다. 도시는 “많은 양의 고객 상호작용 및/또는 민감한 데이터 사용이 포함되는 프로세스 또는 위험과 금융 비용이 큰 프로세스는 중요한 프로세스로 간주된다”고 말했다.

기업은 다음을 고려해야 한다.

1. 데이터 기밀성 : 퍼블릭 블록체인은 투명하며, 중앙 관리되는 프라이빗 또는 ‘허가형’ 블록

체인이라 해도 그 블록체인의 참가자에게는 투명하다. 도시는 “허가형 원장에 있는 데이터의 기밀성 관리를 약속하는 엔터프라이즈급 블록체인이 여러 개 있다”면서 “지금으로써는 어떤 솔루션도 기밀성과 데이터 보안에 대한 철저한 검증을 받지 않았다. 이 우려는 2018년에 여러 프로젝트가 구축되면서 차차 완화될 것”이라고 말했다.

2. **프로세스 리엔지니어링** : 기업은 비즈니스 프로세스를 블록체인 기반 환경에 정렬하기 위한 비용을 감안해야 한다.
3. **기술 투자 손실** : 블록체인 시스템으로의 전환에는 비용이 발생하며, 기존 소프트웨어 및 하드웨어에 대한 과거의 투자가 낭비될 수 있다.
4. **블록체인을 도입하기 위해서는 새로운 기술 파트너가 필요할 수 있으며, 이는 기업에서 각자의 상황에 가장 잘 맞는 기술 공급업체와 서비스 제공업체를 파악해야 함을 의미한다.**

도시는 대부분의 경우 현재 기업 프로세스는 신뢰 보장 중앙 기관이 포함된 워크플로우를 중심으로 설계됐다고 지적한다. “그러한 워크플로우는 블록체인을 구현할 수 있도록 다시 설계해야 한다. 특정 단계가 중복되기도 하고 새로운 기술에 맞게 재구성해야 할 필요성도 발생할 수 있다”면서, “현재 워크플로우가 분산된 정보 흐름(예를 들어, 무역 금융)에 맞게 설계된 사용 사례의 경우 프로세스를 약간만 변경하면서 블록체인 기술을 적용할 수 있다”고 말했다.

마지막으로, 기업은 공통 데이터 표준을 사용해 블록체인에서 어느 정도 범위의 정보를 공유할지를 결정해야 한다. 예를 들어, 스탠포드 아일랜드 MLS(Staten Island Multiple Listing Service)는 프로세스 투명성 및 기타 기존 부동산 거래에 만연한 비효율성을 해결하기 위해 부동산 등재용 블록체인 개념 증명을 3개월 전에 개발했다.

이 회사의 기술 책임자인 리차드 모어에 따르면, 온라인 목록 웹사이트를 위한 일련의 API를 채택하는 것만으로 간단히 플랫폼을 구축할 수 있었다. 셸터Zoom(ShelterZoom)의 온라인 플랫폼을 기반으로 한 이 블록체인 원장이 부동산 표준 기구 데이터 사전에 준수한다는 점도 현재 스탠포드 아일랜드 MLS 시스템과의 통합을 간소화하는 데 도움이 됐다.

도시는 블록체인이 새 시스템에서 프로세스의 모든 당사자 간에 거버넌스와 계약 강제 매커니즘을 보장할 수 있는 영역에서 신뢰를 구축하는 용도로 가장 적합하다고 말했다.

조직 내부 프로세스의 경우 기업은 블록체인 기능을 사용해 분산 애플리케이션을 만들 수 있다. 도시는 이러한 점이 고도의 연합체인 기업에 잘 맞다고 덧붙였다. 연합된 엔터프라이즈 아키텍처는 분산된 사업부 간의 정보 공유를 가능하게 하지만 시스템에서 무엇을 통합하고 표준화해야 하는지에 따라 관리하기가 어려울 수 있다.

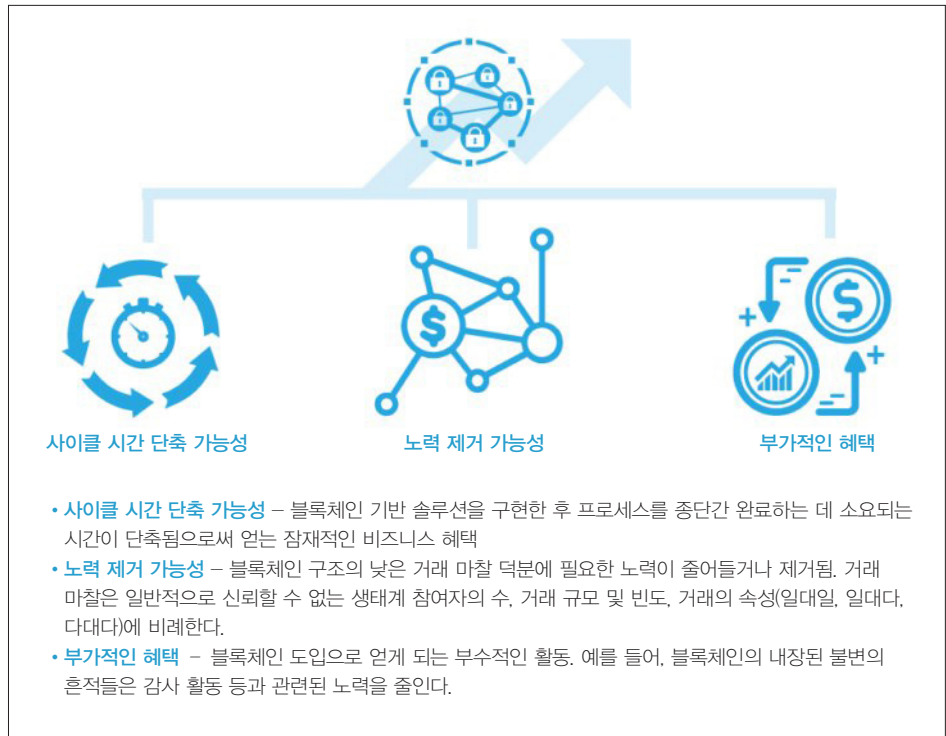
연합된 아키텍처와 마찬가지로 블록체인을 사용해서 정보를 교환하고 네트워크에서 신뢰를 생성하기 위한 목적으로 분산된 기업을 연합할 수 있다. 도시는 “이로써 블록체인은 특정 프로세스 단계를 제거하거나 자동화한다”고 말했다.

비관론자 또는 맹목적 신봉자?

기존 기술 솔루션으로는 현재의 과제를 해결할 수 있는 프로세스 또는 비즈니스 사용 사례가 이미 있고 그 효율성이 블록체인과 거의 동일하다면 그 기업은 블록체인을 구축할 필요가 없다.

❖ **블록체인 도입시 고려해야 할 잠재적 비즈니스 영향**

(출처 : 에베레스트 그룹, 2017)



현재 많은 기업이 두 그룹 중 하나에 속한다. 하나는 블록체인 기술이 성숙함에 따라 그 수가 줄어들고 있는 비관론자, 다른 하나는 맹목적 신봉자다. 비관론자는 뒤처질 위험을 안고 있지만, 맹목적 신봉자는 데이터베이스가 필요하다면 닥치는 대로 블록체인 개념 증명을 구현할 위험을 안고 있다. 후자의 기업은 거의 아무런 혜택도 얻지 못하면서 상당한 리소스를 낭비할 위험이 크다.

에베레스트 그룹은 보고서에서 “기업은 체계적인 우선 순위 프레임워크를 블록체인 도입을 향한 여정의 시작 지점으로 사용해야 한다”고 조언했다. ITWORLD

‘BaaS’ 쏟아진다... 위험부담 없이 기술 테스트 가능

Lucas Mearian | Computerworld

마은 기업이 블록체인 도입을 검토하는 가운데, IT 업체가 잇달아 블록체인 서비스 (Blockchain-as-a-Service, 이하 BaaS)를 내놓고 있다. BaaS의 가장 큰 특징은 온프레미스 배치에 따르는 비용이나 위험 부담 없이 블록체인 기술을 테스트할 수 있다는 것이다. 새로 인프라를 구축하기 부담스럽거나 기존 개발자를 교육하려는 기업이 큰 관심을 보인다. IDC의 블록체인 담당 애널리스트 빌 피언리 주니어는 “블록체인 물결은 아직 초기여서 수년간 많은 실전 경험을 갖춘 인력이 매우 드물다”라고 말했다.

블록체인 기술은 비트코인 암호화폐 때문에 널리 알려졌다. 일부 부풀려진 측면이 있지만 정보 공유 방식에 새로운 패러다임을 제공할 것으로 기대를 모으고 있다. IT 업체는 물론 많은 기업이 이 기술을 이용해 시간과 관리 비용을 절감하는 방법을 경쟁적으로 찾고 있다.

이런 가운데 BaaS 제품은 꽤 매력적이다. 많은 기업이 이미 사용 중인 클라우드 서비스를 통해 블록체인을 미리 경험할 수 있기 때문이다. 피언리는 “신기술이다 그렇듯 기업이 이를 활용하려면 일정한 학습 곡선이 필요하다. 이때 BaaS 제공업체와 제휴하면 업체가 가진 기본적인 노하우를 활용해 사용자가 시스템을 더 안전하게 보호할 수 있다”라고 말했다.

지난 2015년 마이크로소프트는 업계 최초로 애저(Azure) 클라우드 플랫폼에 BaaS를 추가했다. 애저 클라우드 서비스는 다양한 블록체인 프로토콜을 지원한다. 하이퍼레저와 같은 간단한 UTXO(Unspent Transaction Output) 기반 프로토콜은 물론, 이더리움과 같이 더 복잡한 스마트 계약(Smart Contract) 기반 프로토콜과 그 밖에 개발 중인 프로토콜 등을 포함한다. 구체적으로는 이더리움, 하이퍼레저, 패브릭(Fabric), R3 코다(R3 Corda), 퀴럼(Quorum), 체인 코어(Chain Core), 블록앱(BlockApps) 등이다.

HPE도 2017년 BaaS 지원 대열에 합류했다. 주로 금융 서비스 기업을 대상으로 하며 다른 BaaS 제품과 마찬가지로 유연한 과금 모델을 제공한다. 가격은 서버 노드와 CPU 또는 코어 기준으로 책정된다. HPE의 신규 블록체인 SaaS 제품은 코다를 기반으로 한다. 코다는 뉴욕 기반 뱅킹 컨소시엄 R3가 개발한 블록체인 플랫폼이다. 포레스터 리서치의 수석 애널리스트 마르다 베넷에 따르면, R3 코다는 블록체인 환경을 지원하는 은행, 보험회사 등으로 구성된 최대 규모의 상업 컨소시엄이다.

핀테크 업체도 블록체인을 가장 먼저 받아들인 주체에 속한다. 코다는 R3가 리눅스 재단의 하이퍼레저 개발 프로젝트에 코드를 넘겨주면서 오픈소스 분산 원장으로 전환했다. 이밖에 오라클이 리눅스 재단의 하이퍼레저 프로젝트에 기반을 둔 BaaS를 공개했고, IBM도 뒤를 따랐다. IBM BaaS 제품은 국경을 넘는 환전을 지원하는 것이 특징이다.

2017년 초 하이퍼레저 프로젝트는 패브릭 1.0을 공개했다. 블록체인 기반 비즈니스 네트워크를 구축하는 협업 툴이다. SAP 역시 올해 초 자체 레오나르도(Leonardo) 디지털 소프트웨어 플랫폼에 BaaS 제품을 추가했다.


BaaS 플랫폼을 이용하면 기업의 분산 원장 테스트와 배치 작업이 수월해진다. 언스트 앤 영(Ernst & Young)의 블록체인 기술 글로벌 혁신 책임자 폴 브로디는 “우리는 여러 클라우드의 제품을 모두 테스트했고, 그 결과 SAP의 클라우드 플랫폼과 SAP 레오나르도에 적합한 오픈체인(OpsChain, 운영 및 공급망) 제품을 출시했다. BaaS는 매우 유용하고 관리와 배치 작업을 간단하게 해 주지만 ERP에 통합해야만 블록체인의 가치를 충분히 활용할 수 있다”라고 말했다.

단, ERP 시스템은 기업을 운영하는 핵심이다.여기로 블록체인 관련 프로세스를 이전해야 한다면 위험부담 때문에 블록체인의 매력력이 떨어질 수 있다. 예컨대, 블록체인 기반 조달 시스템을 구축하는 기업이라면 이미 SAP와 같은 업체가 제공하는 ERP 시스템을 신중하게 맞춤형으로 갖춰야 한다. 승인된 업체로부터만 구매하고 허가 받은 사용자만 구매 및 결제를 승인할 수 있어야 하기 때문이다.

브로디는 “언스트 앤 영의 오픈체인 시스템을 활용하는 기업은 복잡한 다자간 조달 방식을 블록체인을 통해 관리할 수 있다. 또한, 공급망을 통해 들어오는 자재를 추적하고 이용 가능한 수량 할인을 확인하는 등의 업무를 처리할 수 있다. 그러나 만약 블록체인 시스템에서 조달 규칙을 전부 다시 설정해야 한다면 솔루션 가치가 반감될 것이다”라고 말했다.

오픈체인 시스템을 SAP의 BaaS에 통합하면 기존 업무 규칙과 시스템 내에서 조달 활동을 확인, 승인, 결제할 수 있다. 이 과정에서 블록체인의 모든 장점, 즉, 보안과 분산 특성을 누릴 수 있다. 블록체인은 안전하다고 알려졌지만 허점이 없는 것은 아니다. 모바일 결제, 의료 기록 교환, 화물 선전량에 대한 증권 등 특정 목적을 위한 소프트웨어 위에 구축돼 있기 때문이다. 그 결과 블록체인은 응용프로그램 소프트웨어와 암호 기술에 의존한다.

문제는 블록체인 기술을 개발하는 신생 업체가 수백 곳에 달하고 이들이 검증된 알고리즘을 사용한다는 보장을 할 수 없다는 점이다. 실제로 최근 이더(Ether)라는 암호화폐 수억 달러의 거래가 중단됐다. 한 사용자가 다른 사람의 자산을 최대 3억 달러로 묶어 놓을 수 있는 코딩 취약성이 발견됐기 때문이다. 이 때문에 실제 데이터에 블록체인을 결합했을 때 어떤 일이 일어날지 알아보기 위한 테스트가 점점 중요해지고 있다.

피어리는 “기업 대부분은 블록체인을 스스로 구축하기 힘들 것이다. 분산 원장에 흥미롭고 강력한 혁신이 수반되는 것은 사실이지만, 관련 네트워크를 구성하고 관리할 인력을 확보하는 것이 숙제다”라고 말했다. 

우후죽순 속 옥석은?... 검토할 만한 블록체인 분야 스타트업 10곳

Peter Sayer | IDG News Service

하루가 멀다 하고 블록체인 부문의 창업회사 관련 소식이 들려오고 있다. 벤처 자본 투자 유치를 발표하거나 블록체인 부문의 IPO라 할 수 있는 ICO(Initial Coin Offering)를 진행하고 있다. 이렇게 급변하는 시장에서는 각 기업에 대한 정보를 확인하기 어렵다. 기업들이 검토할 만한 블록체인 사업체 10곳을 골라봤다.

비트고(Bitgo)

비트코인은 첫 번째 블록체인 활용처다. 서로를 모르는 당사자 간 지불을 보증할 수 있는 암호 통화 시스템이다. 비트코인 지불을 처리하고 싶은 기업들이 직면하는 주요 과제 중 하나는 비트코인을 기존 체계와 통합하는 것이다. 기존의 장부 관리에서는 기존의 여러 통화로 구성된 시스템으로 충분했지만, 비트코인은 이를 넘어선다. 또한, 지불을 누가, 누구를, 누구에게 승인 할지에 대한 액세스 제어와 지불 이유와 주체를 확인하기 위한 로그인 등이 필요하다.

기본적인 비트코인 지갑은 소유주가 액세스 감사 체계를 구축하지 않고 비트코인 지불을 처리할 수 있는 프라이빗 키를 저장하는 정도다.

비트고는 거래에 공동 서명과 승인을 사용할 수 있고, 한도를 정하고, 화이트리스트로 잘못된 지불을 줄이고, 다른 엔터프라이즈 애플리케이션과 통합할 수 있는 API를 탑재한 기업 친화형 비트코인 지갑을 개발했다.

비트고는 여기에 더해, 영국 로얄 민트(Royal Mint) 순금 거래 온라인 시장의 거래 기록용 시스템 등 프라이빗 블록체인 시스템을 개발하고 있기도 하다.

체인(Chain)

비트코인이 누구나 액세스할 수 있는 무승인 블록체인을 기반으로 운영되는 반면, 체인은 기업에 승인형 블록체인을 제공한다. 체인의 서비스 또한 다른 모든 블록체인처럼, 시퀀스로 데이터의 불변성을 보장한다. 그러나 이와 동시에 필요한 암호 키가 있는 시큐어 엔클레이브(Secure Enclaves)를 관리, 레코드에 데이터를 추가할 수 있는 사람을 제한한다.

체인은 자동차 공유 지불 관리, 대출, 암호 통화 교환소 생성, 모바일 지갑 보안 등에 사용할 수 있는 기술이라고 주장한다. 기타 계정에 대차대조표를 기록하는 모든 시스템에 사용할 수 있



SETL OpenCSD

다는 설명이다.

이와 관련해 '키 투 시퀀스(Key to Sequence)'가 특정 역할, 레저(장부) 액세스 권한을 갖고 있거나 갖고 있지 않은 사람과 시스템으로 구성된 팀에 적용되는 핵심 개념이다. 관련된 자산이나 계정에 대한 권한을 갖고 있는 사람이나 시스템이 레저의 각 각 트랜잭션을 승인해야 한다.

SETL

SETL은 소유권 등록부, 유가 증권과 뮤추얼 펀드, 사모 펀드 등의 거래소를 구축할 수 있는 실시간

블록체인 청산 플랫폼을 공급하고 있다. SETL에 따르면, OpenCSD로 불리는 이 플랫폼은 팩토링과 할인을 통해 상업 인보이스 시장의 유동성을 높일 수 있다.

현재 그루파나 AM(Groupana AM)과 아키아 인베스트먼트 서비스(Arkea Investment Services) 등 4개 프랑스 자산 관리 회사가 범유럽 펀드 기록 유지 플랫폼인 IZNES 구축에 OpenCSD를 사용하고 있다. 또, 영국 메트로 은행(Metro Bank)가 고객 결제(신용 및 현금) 카드 기록 및 처리에 OpenCSD를 테스트했다.

블록스트림(Blockstream)

블록스트림은 비트코인 지불 시스템과 같은 블록체인을 기반으로 한다. 비트코인 블록체인에 사이드체인을 추가, 시스템의 불변성과 글로벌 범용성이라는 이점을 제공한다. 여기에 더해, 공유 프로토콜로 이질적인 시장을 연결하는 방식으로 특정한 사이클을 넘어 블록체인 간 자산을 이동할 수 있게 지원한다. 이 회사는 기업들이 이런 기능을 용이하게 활용할 수 있도록 도움을 주는 오픈소스 소프트웨어 플랫폼인 엘리먼트 프로젝트(Elements Project)를 제공하고 있다.

블록스트림은 비트코인을 '우주'에 구현할 계획도 가지고 있다. 비트코인이 글로벌 지불 시스템이 되지 못하도록 가로막는 장애물 중 하나는 '이를 활용할 수 있도록 연결을 해야 하는 것'이다. 다시 말해, 글로벌 트랜잭션 레저에 액세스 해야 비트코인을 지불하는 사람이 실제 비트코인을 가지고 있는지, 아니면 비트코인을 이미 다 써버렸는지 알 수 있다.

블록스트림은 비트코인 블록체인의 '업데이트' 내용을 지속적으로 브로드캐스팅해 인터넷을 이용할 수 없는 지역의 사용자도 트랜잭션 데이터베이스를 최신 상태로 유지할 수 있도록 위성들을 발사할 계획이다. 처리 트랜잭션의 세부 정보를 나머지 세상에 제공하는 것 또한 도전과제다. 그러나 일부 데이터만 이동하면 된다.

엘립틱(Elliptic)

비트코인과 관련된 흥미로운 이야기 중 하나는 "규제 당국이 비트코인 투자자를 미래의 기소 대상으로 본다는 것"이다. 블록체인의 경우, 그동안의 모든 비트코인 트랜잭션 기록이 불변한다. 또 트랜잭션과 관련된 계정에 대한 정보도 계속 유지된다. 특정 트랜잭션이 불법 행위와 연

결된 것으로 드러날 경우, 몇 년이 지난 후에도 검사가 관련자와 활동을 추적할 수 있다.

또 비트코인 사용자 중에 ‘평판이 좋지 않은 사용자’들이 있다. 랜섬웨어와 불법 암시장 등 범죄 활동에 관여하는 사용자를 말하는 것이다. 이런 불법 행위를 하는 사람들과 거래를 하면, 평판에 큰 피해가 초래될 수도 있다. 처음 시작한 비트코인 거래에서 이런 불법 행위자들과 연결되고 싶지는 않을 것이다.

엘립틱이 여기에 도움을 준다. 엘립틱을 이용하면 비트코인 블록체인의 불법 행위를 식별할 수 있고, 법 집행 기관이나 금융 기관에 이를 경고할 수 있다. 기업은 블록체인과 증거 데이터베이스를 이용, 잠재 고객을 대상으로 감사가 가능한 위험 프로필을 만들 수 있다.

엘립틱은 랜섬웨어 극복에 도움을 줄 수 있는 2가지 방법도 제공한다. 이 회사에 따르면, 공격자의 지불 주소와 과거 트랜잭션을 이용해, 사이버 몸값을 지불했을 때 ‘인질’이 된 데이터 암호가 풀릴지 판단할 수 있다. 피해자가 사이버 몸값을 지불한 경우, 이 ‘돈’을 추적해 범죄자의 신원을 식별해 법 집행기관에 알릴 수 있다.



이더리움 홈스테드

웨이브 플랫폼(Waves Platform)

블록체인 기반의 로열티 프로그램이나 투표 시스템이 필요하지만, 이를 직접 구축하고 싶지 않다면 웨이브 플랫폼을 활용할 수 있다. 이 회사는 이미 모바일 게임 회사 한 곳, 공동 사무 작업공간 관련 개발사 등을 대상으로 총 5,000여 토큰을 제공하고 있다. 또한 비트코인 시스템을 향상시키는 여러 기술 중 하나에 기반을 둔 새로운 블록체인 기술을 이용, 트랜잭션 속도를 높이는 방법을 테스트하고 있다.

웨이브-NG 시스템은 긴 시간 간격으로 정기적으로 수 많은 트랜잭션이 승인되도록 전송하는 대신, 여러 트랜잭션을 작은 마이크로 블록들로 통합하고, 이후 특정 통합 블록을 핵심 블록으로 지정하는 방식으로 트랜잭션이 도착하는 즉시 처리한다. 핵심 프레임 전송 후, 다음 핵심 프레임까지 변경 사항만 전송하는 디지털 비디오 스트림 압축 방식과 유사한 방식이다.

이더리움(Ethereum)

비트코인은 지불 처리용이다. 그러나 이더리움은 더 큰 계획을 갖고 있는 블록체인 기술이다. 처음부터 트랜잭션 기록은 물론 코드를 실행할 수 있도록 개발됐다. 즉 스스로 이행 시기를 판단하는 트랜잭션인 ‘스마트 계약’ 기능이 구현되어 있다.

이더리움의 스마트 계약에는 새로운 프로그래밍 언어인 솔리디티(Solidity)가 사용됐다. 코드를 개발, 홈스테드(Homestead)로 불리는 이더리움의 글로벌 분산형 소프트웨어 플랫폼에서 실행한다. 스마트 계약으로 프라이빗 암호 통화를 생성하고, 클라우드펀딩 거래를 관리하고, 자율 조직(시스템)을 구현할 수 있다. 이 밖에도 많은 일을 할 수 있다.

이더리움은 ‘코드는 법’이라는 원칙에 토대를 두고 있다. 따라서 누군가 코드를 조작하는 경우 문제가 될 수 있다. 이로 인해, 몇 차례 사람이 직접 개입을 해야만 했다. 첫 번째는 2016년 6월이었다. 누군가 DAO로 불리는 벤처 자본 기금과 관련된 스마트 계약의 취약점을 공격, 가치의 1/3을 증발시켰다. 이 DAO 취약점 공격을 원상태로 복구하기 위해 모든 이더리움 사용자에게 공유 레저 수동 변경을 승인 받아야 했다.

이때 승인을 한 사람들이 현재 사용하고 있는 블록체인이 ‘이더리움’, 승인을 거부한 사람들이 사용하고 있는 블록체인이 ‘이더리움 클래식’이다. 이렇게 분기됨에 따라 다른 ‘진영’에 기반을 둔 사람들과는 더 이상 거래할 수 없다.

두 번째는 2017년 11월이었다. 누군가 패리티(Parity)가 만든 수백 스마트 지갑의 버그를 잘못 건드려 그 안의 기금이 돌이킬 수 없는 상태로 잠기는 문제가 발생했다. 영향이 초래된 암호 통화의 가치는 미화 1억 6,000만 달러에 달했다. 문제 해결을 위해 ‘하드 포크(Hard Fork, 블록체인을 기존 버전과 호환되지 않게 업데이트하는 것)’가 요구될 수도 있다.

이더리움에 기반을 둔 기업들은 향후 문제가 해결될지라도 다른 비즈니스가 이 플랫폼에서 빠져나가는 경우 혼란이 나타날 수 있다는 점을 인식해야 한다.

R3

R3는 마이크로소프트 애저를 지원하는 코다(Corda) 분산형 원장을 운영하고 있다. 100개 금융 기관이 코다를 후원하고 있다. 또한, 코다는 애초 이 시장을 겨냥해 개발된 기술이다. 이더리움과 마찬가지로 스마트 계약을 지원한다. 그러나 이더리움과 다르게, 금융 관련 트랜잭션만 처리할 수 있는 스마트 계약이다. 예를 들어, 가상 투표를 지원하지 않는다.

모든 참여자가 원장 자체를 공유할 수 있지만, 특정 쌍방만 비밀리에 메시지를 교환할 수 있다. 금융 관련 서비스에 유용하다. 예를 들어, X의 100만 달러 지불이라는 ‘팩트’ 자체에는 모든 이들이 동의 및 승인을 해야 하지만, 다른 관계자가 거래 내용을 몰라야 하기 때문이다.

코다는 사용자가 거래 대상을 확인하고, 분쟁 발생 때 스마트 계약의 목적을 판단하는 데 사용할 수 있는 실제 법정 계약의 지원을 받을 수 있는 승인형 시스템이다.

젬(Gem)

젬은 블록체인을 사용, 특정 시장이나 산업의 정보에 대한 액세스를 관리할 수 있는 공유 ID(신원) 시스템을 구축하려 한다. 의료와 공급망 관리, 사용 기반 자동차 보험과 관련된 애플리케이션이 초기 ‘타깃’이다. 모두 정보를 공유해야 하지만, 신뢰 문제가 많은 분야들이다.

젬 측은 기업들이 GemOS를 사용해 어떤 데이터 저장소나 블록체인 네트워크에도 액세스할 수 있다고 강조하고 있다. 단, 초기인 현재 단계에서는 이더리움과 하이퍼레저에 기반을 둔 블록체인들을 ‘타깃’으로 삼고 있다.


자동차 보험 산업을 예로 들면, 젬은 보험 회사들이 더 많은 정보에 액세스할 수 있을 때 고객들에게 더 나은 ‘거래 조건’을 제시할 수 있다고 믿는다. 그러나 고객들은 차량 구매, 운행, 응급실 방문 등에 대한 데이터 액세스 승인을 꺼리는 경향이 있다.

점은 이런 데이터를 암호화 하고, (블록체인이라는)증앙화 된 저장소와 연결해 승인을 받은 사람만 여기에 접근하게 만드는 방법으로 이 문제를 해결할 수 있다고 강조하고 있다.

빅체인DB(BigchainDB)

블록체인은 일종의 데이터베이스가 되었다. 그러나 쿼리가 쉽지 않은 데이터베이스이다. 빅체인DB는 불변성과 분산이라는 기존 블록체인의 특성을 유지하면서 확장과 검색이 가능한 데이터베이스를 제공하고자 한다.

빅체인 DB 시스템은 노드 ‘페더레이션’으로 운영된다. 각 노드가 몽고DB나 리싱크DB 같은 기존 데이터 베이스 위에 위치한 빅체인DB 블록체인 계층을 실행시키는 방식이다. 이 회사는 서버 클러스터에 이런 페더레이션을 구축하는 방법을 권장하고 있다. 여러 장소와 여러 사람들이 관리하는 노드들로 구성된 페더레이션이다.

공개된 빅체인DB 인스턴스도 있다. ipdb.io에서 테스트 할 수 있는 인터플래네티리 데이터베이스(Interplanetary Database)다. 빅체인DB는 자동차, 에너지, 공급망(물류) 산업을 대상으로 블록체인 애플리케이션을 배포하기 위해 파트너들과 협력을 시작한 상태다. 



IT 트렌드 종합 정보센터 IDG Tech Library

IDG Tech Library는 IDG 글로벌 네트워크를 통해 축적된 전문 정보를 재구성하여 최신 기술의 기본 개념부터 현황, 전략 및 도입 가이드까지 다양한 프리미엄 IT 정보를 제공합니다. Computer World, Info World, CIO, Network World 등의 세계적 IT 유명 매체의 심도 깊은 정보를 무료로 만나보세요

IDG Deep Dive, Tech Focus, Summary, World Update 등의 다양한 콘텐츠를 제공 받을 수 있습니다.



한국IDG(주) 서울시 중구 봉래동 1가 108번지 창화빌딩 4층 100-161 Tel : 02-558-6950 Fax : 02-558-6955
www.itworld.co.kr www.twitter.com/ITWorldKR www.facebook.com/ITworld.Korea

블록체인의 5가지 문제점

Lucas Mearian | Computerworld

블록체인 기술은 여러 산업 분야에서 신뢰 모델과 비즈니스 프로세스를 혁신적으로 바꾸어 놓을 수 있는 잠재력을 지니고 있다. 그러나 이 기술은 아직까지 초기 단계에 있으며, 블록체인 기술에 사용되는 분산 원장 기술 역시 적절한 모니터링이나 점검을 받지 않고 있다.

이처럼 잠재력이 큰 기술임에도 불구하고 CIO 및 비즈니스 리더들은 블록체인 기술을 도입할 때 발생할 수 있는 소프트웨어 버그나 양자 컴퓨팅 기술로 인한 리스크 등 다양한 위험 요소들을 생각해봐야만 한다고 포레스터 리서치가 최근 보고서를 통해 지적했다.

또한, 블록체인 기술이 일부 비즈니스 프로세스에는 적합하지 않을 수 있다는 전문가와 애널리스트들의 지적도 있다. 예를 들어, 이더리움 환전소인 레브라이(Lever)의 창립자인 바라스 라오는 암호화 화폐 이외 분야에 블록체인 활용 가능성에 대해 회의적인 태도를 보였다. 그는 블록체인 기술이 중앙집권화된 관계형 데이터베이스와 같은 기존의 거래 기술에 비해 더 비싸고 도입 시간도 오래 걸린다고 말한다.

그는 “블록체인은 효율성을 버리고 자율성을 얻는 시스템”이라고 지적했다. 새로운 블록이 블록체인에 추가되기 위해서는 모든 블록의 암호화 확인 절차가 요구된다. 이 때문에 빠른 거래가 필수인 비즈니스 분야에 적용되기에는 효율적이지 못하다는 것이다.

둘째로 “블록체인은 말 그대로 ‘체인’ 형태이기 때문에 블록 삽입이 직렬화되어야 한다. 때문에 업데이트 속도가 병렬적인 업데이트를 하는 전통적인 데이터베이스보다 느리다”고 말했다.

블록체인에 회의적인 것은 라오 뿐만이 아니다. 포레스터 리서치 역시 블록체인을 둘러싼 열풍과 이 기술의 현주소에 초점을 맞췄다. ‘세계경제포럼의 글로벌 리스크 평가단이 정확히 지적했다, 이처럼 많은 사람들이, 이처럼 소수의 사람들만이 제대로 이해하고 있는 기술로부터 이만큼이나 많은 것을 기대한 것은 전혀 없는 일이다.”

포레스터는 2018년에도 블록체인 열풍이 계속될 것이라고 예측한다. 그러나 포레스터의 수석 애널리스트인 마사 베넷은 현실에서 블록체인 기술의 확산은 느리고 꾸준한 페이스로 이어질 것이며, 대기업보다는 틈새시장에서 훨씬 많이 활용될 것이라고 전망했다.

포레스터가 지적하는, 오늘날 블록체인이 지닌 5가지 문제점에 대해 알아보자.

미숙한 기술과 더 미흡한 소프트웨어

2008년 블록체인의 개념을 처음 제시한 것은 ‘사토시 나카모토’라는 사람이었지만(이것은 개인의 이름일 수도 있고, 개발자 모임의 필명일 수도 있다), 이 기술이 실제 사례에 적용되기 시작한 것은 불과 몇 년 전이다. 오늘날 블록체인 기술은 주로 암호화 화폐나 가상 금융 거래에서 분산 원장을 만드는 데 사용된다.

가장 잘 알려진 블록체인 플랫폼인 하이퍼레저와 이더리움마저도 아직까지 미숙한 단계이기 때문에, 이 기술의 도입 과정에는 예기치 못한 문제가 발생할 수 있다. 따라서 CIO는 블록체인 기술 도입 과정에서 심각한 소프트웨어 버그가 발견되거나, 심지어는 프로젝트를 엮고 처음부터 다시 시작할 리스크도 있음을 알아야 한다고 포레스터는 지적했다.

베넷은 “블록체인 커뮤니티뿐만 아니라, 프로젝트를 본격적으로 진행하지 않은 기업들은 버그 없는 소프트웨어가 어디 있느냐며 가볍게 이야기한다. 그리고 몇몇은 버그가 아닐 수도 있다고까지 이야기한다”고 지적했다.

예를 들어, 스마트 계약을 이행하는 이더리움 스크립트인 솔리디티(Solidity)는 소수점 사용을 지원하지 않는데, 이를 위해서는 우회로를 만들거나 모든 것을 다시 시작해야 하기 때문이다.

베넷은 “실제로 이런 경우를 많이 봤다. 프로젝트, 그것도 아주 규모가 크고 책임감이 막중한 프로젝트에 참여하는 이들과 블록체인에 대해 이야기를 나누어 보면, 블록체인 기술을 오래 접한 이들일수록 이 기술이 아직 미흡한 부분이 많다는 점에 동의한다”고 말했다.

얼마 전에는 코딩 취약성으로 인해 한 사용자가 수억 달러에 달하는 이더리움 암호화 화폐인 이더(Ether)를 동결시키고 최대 3억 달러에 이르는 타 사용자들의 화폐 유동성을 제한하는 사건이 발생했다.

패리티 테크놀로지(Parity Technologies)가 관리하는 이더리움 블록체인이 공공 거래장부 변경을 위한 사용자들의 동의를 얻어야 하는데, 코딩 상의 문제로 인해 한 개인 사용자가 ‘우연히’ 체인 상의 모든 암호화 화폐 지갑에 대한 통제권을 갖게 된 것이다.

블록체인, 데이터 저장에 적합하지 않을 때도 있다

블록체인 기술의 최대 장점은 한 번의 데이터 생성으로 많은 이들에게 이를 공유할 수 있다는 것이다. 웹의 각기 다른 노드에 손쉽게 도입할 수 있으면서도 각 기록이 자체적인 해시를 간직하고 있기 때문에 조작이 불가능하다.

블록체인 기반 네트워크를 통한 분산 원장은 그래서 내부 시스템과 블랙리스트에 기반한 선택적 기록보다 훨씬 더 풍부하고 포괄적인 거래 기록을 남길 수 있다. 하지만 그렇다고 해서 거래 관련 데이터가 반드시 블록체인의 일부가 되어야 하는 것은 아니다.

예를 들어, 블록체인 사용자가 거래 기록의 일부로 이미지를 첨부할 경우, 데이터 용량은 급증하고, 시간이 흐르며 일방적인 추가만 가능한 상황에서 데이터 용량이 커짐에 따라, 이는 곧 네트워크 오버헤드로 이어지게 될 것이다. 이 경우 데이터를 분산하는 블록체인의 특성으로 인

해 모든 데이터가 체인 상의 모든 노드에 복제되어야 한다.

따라서 일부 거래에 대해서는 통제가 어려운 블록체인보다는 별개의 네트워크 스토리지로 운영되는 관계형 데이터베이스를 사용하는 것이 더 낫다. 베넷은 “반드시 기억해야 할 것은 관계형 데이터베이스만으로도 충분한 상황에서 굳이 블록체인 기반 아키텍처를 도입할 이유는 절대 없다는 사실이다”고 말했다.

블록체인은 생각만큼 안전하지 않을 수도 있다

블록체인에는 크게 2종류가 있다. 퍼블릭 블록체인과 프라이빗 블록체인이다. 퍼블릭 블록체인은 누구나 가담할 수 있다. 화폐 구입을 원하는 누구나 체인에 가담할 수 있게 열어 놓은 비트코인이 바로 퍼블릭 블록체인의 대표적인 예다. 퍼블릭 블록체인은 개방되어 있고 투명하기 때문에, 체인 상의 모든 사용자가 모든 거래 내역을 투명하게 볼 수 있다.

반면, 프라이빗 블록체인은 중앙권위체에서 단독으로 관리하며 가입을 위해서는 승인이 필요하다. 단일 기업이나 파트너 기업들간에 주로 사용되는 형태로, 승인된 사용자들만이 체인에 가담할 수 있다.

퍼블릭이건 프라이빗이건 블록체인은 기본적으로 조작이 불가능하다. 각 거래 기록 또는 블록을 임의로 변경할 수 없고 다른 모든 블록들과 연결되어 있기 때문이다. 따라서 보안을 보장 받는다. 이러한 블록체인에 새로운 블록을 추가하려면 다른 사용자들의 동의가 있어야 한다.

얼마만큼의 사용자 동의가 필요한가는 사용되는 블록체인에 따라 다르다. 일부 블록체인의 경우 50%의 동의를, 또 어떤 블록체인은 그보다 더 많은 사용자들의 동의가 필요하다. 이처럼 약간의 차이는 있지만, 기본적으로 블록체인은 거래 장부 변경이 불가능하고, 사용자들의 동의를 기반으로 거래가 이루어지기 때문에 그 어떤 네트워킹 기술보다 더 안전하다.

그렇지만 블록체인 기술이 애플리케이션 소프트웨어 및 암호화 기술에 의존하고 있는 것도 사실이며, 오늘날 블록체인 기술을 개발, 제공하는 수백 개의 스타트업들 중에는 아직 검증되지 않은 알고리즘을 사용하는 곳들이 적지 않다.

예를 들어, 비트코인의 경우 이미 검증된 알고리즘인 SHA-256을 해시에 사용한다. 그러나 여러 연구 결과에 의하면, 양자 컴퓨팅으로 인해 궁극적으로 이러한 알고리즘이 깨질 것이다. 그나마 다른 블록체인들은 그저 개발자가 안전을 ‘보장’했기 때문에 믿을 수밖에 없는 알고리즘을 사용하기도 한다.

베넷은 “그 어떤 암호화 전문가에게 물어 보더라도, 새로운 암호화 알고리즘이 안전한 것으로 수용되기 위해서는 수년의 시간이 걸린다는 점에 동의할 것이다. 이런 상황에서, 어느 스타트업 기업이 보지도 듣지도 못한 알고리즘을 가지고 나타난다면, 그런 블록체인 시스템에 도박을 해서야 되겠는가? 실제로 많은 스타트업들이 새로운 해시 알고리즘을 도입하려 했지만, 이런 시도들은 모두 처참한 실패로 돌아갔다”고 지적했다.

암호화 및 보안 전문가인 브루스 슈나이어는 현재까지 블록체인 네트워크가 해킹당한 적은 없으며, 이는 미래에도 마찬가지일 것이라고 말했다. 그는 “블록체인 같은 기술은 해킹으로 깨



지지 않는다. 그보다는 소프트웨어상의 취약점으로 인해 깨질 확률이 더 높다”고 지적했다.

예를 들어, 2016년 분권화된 블록체인 기술을 도입한 벤처 캐피탈 다오(The Dao)는 코드 문제로 6,000만 달러 가량의 디지털 화폐 이더를 도둑맞았다. 같은 해 홍콩 기반 암호화 화폐 거래소인 비트피넥스(Bitfinex) 역시 6,800만 달러에 달하는 12만 비트코인을 도둑맞았다. 조사 결과에 따르면, 비트피넥스의 비트코인 지갑 업체인 비트고가 지닌 소프트

웨어상의 취약성으로 인해 생긴 문제였다.

가장 큰 두 가지 과제 : 확장성과 신뢰성 확보

블록체인 기술은 기본적으로 두 개인, 기업, 단체 간의 신뢰를 수학적 원리로 대체하려는 시도다. 이는 바꿔 말해 블록체인 기술의 수학적 원리에 대한 의존성이 커질수록 더 많은 노드(서버)가 필요하게 되며, 운영 환경이 더욱 연산 집약적이 되고, 그에 따라 비용도 증가하게 됨을 뜻한다고 베넷은 지적했다.

레브라이의 라오도 이에 동의했다. 블록체인은 ‘체인’ 형태이기 때문에 블록 삽입이 직렬화되어야 한다. 때문에 업데이트 속도가 병렬적인 업데이트를 하는 전통적인 데이터베이스보다 느리다. 라오는 “검증되지 않은 불특정 다수의 사람이 참가할 수 있는 글로벌 규모의 네트워크에서는 이처럼 비싼 비용과 느린 속도가 용납이 될 수 있다. 그렇지만 참가자가 엄격히 통제되는 기업 환경에서 딱히 부가적인 이득이라고 할 것도 없는 블록체인 기술에 그토록 많은 에너지와 시간을 쏟을 필요는 없어 보인다”라고 말했다.

또한, 가장 널리 사용되는 블록체인 형태이기도 한 퍼블릭 블록체인은 불특정 다수에게 투명하게 오픈되어 있기 때문에 누구나 거래장부를 볼 수 있다. 비트코인이 이런 경우다.

그렇지만 상업적 환경에서 이 기술을 사용할 때는 이와 같은 투명성이 반드시 좋은 것이라고 보기 어렵다. 예를 들어, 만약 블록체인 기술이 주식 거래 플랫폼상에서 즉각 합의(instant settlement) 메커니즘으로 사용된다면 어떨까? 각 참여자가 다른 참여자의 모든 의도와 행동을 읽을 수 있게 되므로 결국 메커니즘 자체가 제대로 기능하지 못할 것이다.

또 다른 예로, 만일 제조업에서 공급업체에 대한 공개 거래 장부로서 블록체인 기술을 사용할 경우 일방 계약자가 블록체인상의 다른 모든 하도급 업체들을 볼 수 있게 될 것이다.

베넷은 “블록체인상에서 특정 거래를 원하는 기업이라고 할지라도, 고객이 모든 하도급 업체를 알게 되는 것은 원하지 않을 수 있다. 결국 기업은 이러한 거래 데이터를 어떻게 하면 비공개로 유지할 수 있을지에 대해 고민하지 않을 수 없다”고 말했다.

블록체인에서도 일부 사용자들만이 중요 데이터나 기밀 데이터를 볼 수 있도록 베타성을 도입하는 방법이 없진 않다. 예를 들어, 리눅스 재단의 오픈소스 블록체인 프로젝트인 하이퍼레저의 경우, ‘채널’이라 불리는 서브 체인을 이용해 승인된 일부 사용자들만 중요 정보에 접근할

수 있도록 하고 있다.

블록체인의 스마트 계약, 지나치게 과장됐다

스마트 계약, 또는 자체 이행 계약은 별도의 이행 강제 권위체가 필요 없다는 점에서 블록체인이 가진 가장 매력적인 기능 중 하나라고 할 수 있다. 기본적으로 이는 계약 당사자들이 동의한 거래 조건이 달성될 때 그 대가로 약속된 돈이나 물건이 자동으로 상대방 당사자에게 전달되는 시스템이다. 예를 들어, 보험사에서 허리케인이나 가뭄과 같은 세계 기후 현상에 기반해 보험금을 지불할 수 있을 것이다.

그렇지만 베넷은 이 스마트 계약이라는 것이 사실 스마트하지도 않으며, 법적으로 볼 때 진정한 의미에서의 계약이라고 하기도 어렵다고 말한다. 그는 “개념적으로만 보면 정말 멋진 아이디어다. 이는 일종의 비즈니스 프로세스 자동화라고 할 수 있다. 비즈니스 프로세스 자동화를 위해서는 일단 자동화의 대상이 되는 프로세스가 무엇인가에 동의할 수 있어야 한다. 이 프로세스에 어떤 룰을 적용할 것인지를 합의하고 나서 이를 코드로 옮겨야 한다. 때문에 이러한 프로세스 자동화는 사람들이 생각하는 것보다 훨씬 복잡하고 어렵다”라고 말했다.

그런데 블록체인 스크립팅 언어는 아직까지 이 정도의 자동화가 가능할 만큼 성숙하지 못했으며, 프로그래머들 역시 아직까지 이 언어에 대해 배워가는 단계다. 이러한 이유로 버그나 취약성도 발생할 수 있다.

스마트 거래 당사자들은 또한 거래 운용 방식을 어떻게 준수할 것인가에 대해, 그리고 거래 이행 여부에 대한 분쟁 발생시 이를 어떻게 해결할 것인가에 대해서도 합의를 해야 한다. 베넷은 “코딩에 실수가 있었다든가 하는 식으로 예기치 못한 상황이 발생할 경우에 대비해, 외부 경로를 통해 코딩을 수정할 수 있어야 한다. 아니면 최소한 양 당사자 모두 원하지 않았던 비상 상황에 대비해 최종 ‘오프 스위치(계약 파기 방법)’이 마련되어야 한다”고 말했다.

예를 들어, 지난 2010년 어느 한 자동화 상거래 이행 시스템이 순간적으로 장애를 일으키며 전 세계적인 무역 네트워크에 영향을 미친 일이 있었다. 당시 한 대규모 거래 당사자가 거래 플랫폼 상에 주문 정보를 피딩하기로 프로그램되어 있던 자동화 알고리즘을 통해 판매 프로그램을 실행하려 했다. 이러한 판매 프로그램의 실행은 전례 없는 대규모의 변화를 야기했고, 시스템 충돌과 함께 이례적인 수준의 주가 변동성을 가져왔다.

이러한 시스템 충돌을 겪은 규제 당국은 상기 언급한 것과 같은 ‘오프 스위치’를 만들어 냈다. 5분 내로 10% 이상의 주가 변동이 관찰될 경우 개별 주식 거래를 정지시키는 제도를 도입한 것이다.

베넷은 “이러한 사례를 통해 스마트 계약과 조작 불가능성의 개념이 양립 불가능한 경우도 있음을 알 수 있다. 왜냐하면 스마트 계약에서 ‘조작 불가능’을 인정한다면, 최악의 보안 버그가 존재해도 이를 고칠 수 없게 됨을 뜻하기 때문이다”고 말했다.

블록체인 기술이 발전하면서, 이에 대한 학술 연구도 활발히 진행되고 있다. 특히, 블록체인의 수학적 원리에 대한 연구가 그러하다고 포레스터는 밝혔다. 일부 기업들은 자사 블록체인 솔루션의 수학적 분석을 의뢰하였으며, 이러한 경향은 2018년에 더욱 강해질 전망이다.

베넷을 포함한 많은 이들도 블록체인이 혁명적인 발상의 전환임에는 동의한다. 새로운 비즈니스 및 거래 신뢰 모델을 제공하기 때문이다. 그럼에도 불구하고 이러한 신뢰 모델이 시장에서 어떤 형태가 될 것인가는 아직까지 불분명한 상태로 남아있다.

베넷은 “오늘날 기업들의 블록체인 프로젝트들을 살펴보면, 대부분이 기존 프로젝트를 최적화하는 형태를 띠고 있다. 그렇지만 퍼블릭 프로세스를 포함하여, 프로세스 운용 방식을 진정한 의미에서 재탄생 시키는 작업은 기술이 보다 정교하고 완성된 미래의 과제로 남아 있다”고 말했다.

새로운 비즈니스 프로세스를 만들어 내기 위해서는 개별 사용자들 간의 비즈니스 프로세스 조건에 대한 동의가 선행되어야 한다. 실제로 블록체인 운용 조건에 대해 사용자들 간 합의가 이루어지지 않아 무산된 프로젝트들도 있다. 블록체인은 IT만큼이나 당사 간 합의나 신뢰가 중요한 분야이기도 하다.

베넷은 “최근 한 지인이 나에게 이런 말을 했다. 블록체인은 2할이 기술이고 8할은 비즈니스라고 말이다”라며, 블록체인의 비기술적 측면을 강조했다. **ITWORLD**

ITWORLD

테크놀로지 및 비즈니스 의사 결정을 위한 최적의 미디어 파트너



기업 IT 책임자를 위한 글로벌 IT 트렌드와 깊이 있는 정보

ITWorld의 주 독자층인 기업 IT 책임자들이 원하는 정보는 보다 효과적으로 IT 환경을 구축하고 IT 서비스를 제공하여 기업의 비즈니스 경쟁력을 높일 수 있는 실질적인 정보입니다.

ITWorld는 단편적인 뉴스를 전달하는 데 그치지 않고 업계 전문가들의 분석과 실제 사용자들의 평가를 기반으로 한 깊이 있는 정보를 전달하는 데 주력하고 있습니다. 이를 위해 다양한 설문조사와 사례 분석을 진행하고 있으며, 실무에 활용할 수 있고 자료로서의 가치가 있는 내용과 형식을 지향하고 있습니다.

특히 IDG의 글로벌 네트워크를 통해 확보된 방대한 정보와 전세계 IT 리더들의 경험 및 의견을 통해 글로벌 IT의 표준 패러다임을 제시하고자 합니다.