IDG
STRATEGIC
MARKETING SERVICES

IBM

IDG Summary | Blockchain

블록체인 기반 프로젝트 시작하기 전, 알아야 할 사항들

블록체인이 IT 세계에 새로운 바람을 일으키면서 대규모 조직을 중심으로 블록체인 도입이 시작됐다. 다양한 산업군에서 블록체인 기술을 접목해, 효과적인 서비스나 기존 문제점을 개선하기 위해 도입을 위한 PoC나 파일럿을 통해 검증을 시도했으며, 블록체인 기술에 대해 명확하게 알지 못하고 시도한 케이스는 실패를 경험했지만, 제대로 된 블록체인 컨설팅을 통해 시작한 블록체인 프로젝트는 정상적인 궤도를 달리고 있다. 블록체인 기반 프로젝트는 기존 IT 시스템 구축 방식과는 큰 차이점이 있다. 여러 조직이 연계하는 영역에서 새로운 비즈니스 프로세스를 구현하는 블록체인을 성공적으로 구현하기 위해서는 무엇보다 철저한 사전 준비가 필요하다. 블록체인 프로젝트의 개념과 프로젝트 수행 전 고려 사항에 대해 알아보자.

블록체인 기반 프로젝트 시작하기 전, 알아야 할 사항들

허강욱 차장 | Blockchain Leader, Client Innovation Lab, CTO Office, IBM Korea

인터넷 시대가 열린 이후, 가장 유망한 기술로 각광받고 있는 블록체인은 간단히 말해, P2P(peer-to-peer) 네트워크를 통해 복제되는 분산원장 데이터베이스 유형이다. 이런 개념은 중앙 데이터베이스 관리자가 없는 다른 유형의 분산 데이터베이스에도 적용될 수 있다. 하지만 블록체인은 네트워크 내의 모든 참여자가 공동으로 거래 정보를 검증하고 기록, 보관함으로써 공인된 제3자가 없어도 거래 기록의 무결성 및 신뢰성을 확보하는 기술이라는 점에서 다른 분산 데이터베이스와 차이가 있다.

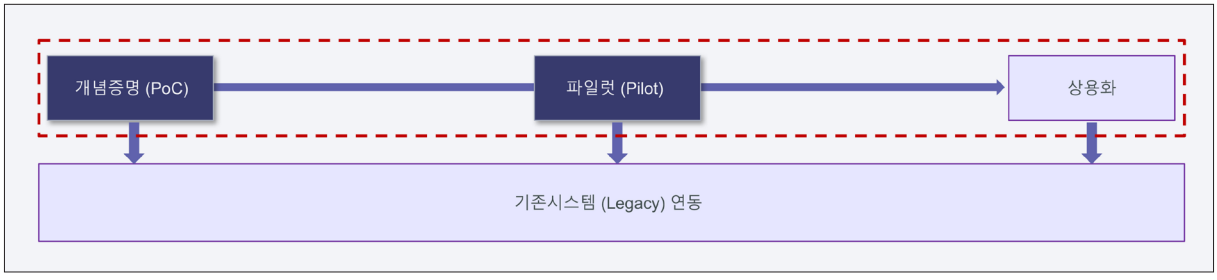
사전 검증이 성패를 가르는 블록체인 기반 프로젝트

블록체인 기술은 암호화, P2P, 합의 알고리즘 등 기존 기술과의 조합으로 공급망이나 추적 등과 같이 여러 조직이 연계하는 영역에서 새로운 비즈니스 프로세스를 구현한다.

블록체인 기반 프로젝트는 기존 IT 시스템의 구축 방식과는 큰 차이가 있다. 블록체인 기반 프로젝트의 경우, 기본적으로 개념 증명, 파일럿, 상용화 과정을 거치게 된다. 우선 블록체인 기반 사용사례를 선정하고 이 사용사례가 기능적으로 구현 가능 여부를 판단하기 위해 개념증명(PoC) 프로젝트를 수행한다. 기능 검증이 확인되면 파일럿 프로젝트를 진행하면서 상용화 이전에 고려해야 할 모든 상황에 대해 검토한다. 파일럿을 통해 검토가 완료되면 상용화 서비스를 구축하고 오픈한다.

이런 단계를 거치기 전에 기업은 블록체인 사용사례를 선정해야 하는데, 사실 이 과정이 가장 어려운 부분이다. 대부분의 기업이 이 단계에서 어려움을 호소하고 있으며, 상당히 많은 프로젝트가 여기서부터 실패했다.

그림 1 | 블록체인 기반 프로젝트 진행 프로세스



지난해 중국에서 블록체인 기술을 기반으로 한 8만 개 프로젝트 가운데 겨우 8%만이 활동적이며, 92%는 이미 실패했다. 그 이유는 블록체인 기술과 적용 서비스를 사전에 제대로 파악하지 않고 무턱대고 도입했기 때문이다. 신기술의 경우, 실패가 좋은 밑거름이 될 수도 있지만, 굳이 일부러 실패를 경험할 필요는 없다.

최근 기업들은 자사의 블록체인 프로젝트가 블록체인에 적합한지 여부를 제3자에게 검증받길 원하며 상당한 논의를 거친 이후에야 POC를 진행하게 된다.

블록체인 기반의 프로젝트는 기존 시스템 중에서 다른 업체나 계열사와 연관성이 있거나, 협력업체나 비즈니스 파트너 간 프로세스가 있는 부분에서 문제가 있는 사항들을 자동화하거나 개선하는 것으로 블록체인 프로젝트의 80% 이상이 기존 시스템과 연동되는 케이스이다. 특히 국내 기업의 경우, 기존 시스템이 잘 구축되어 있어 블록체인 기술 기반으로만 구축되는 프로젝트는 사실상 거의 없다.

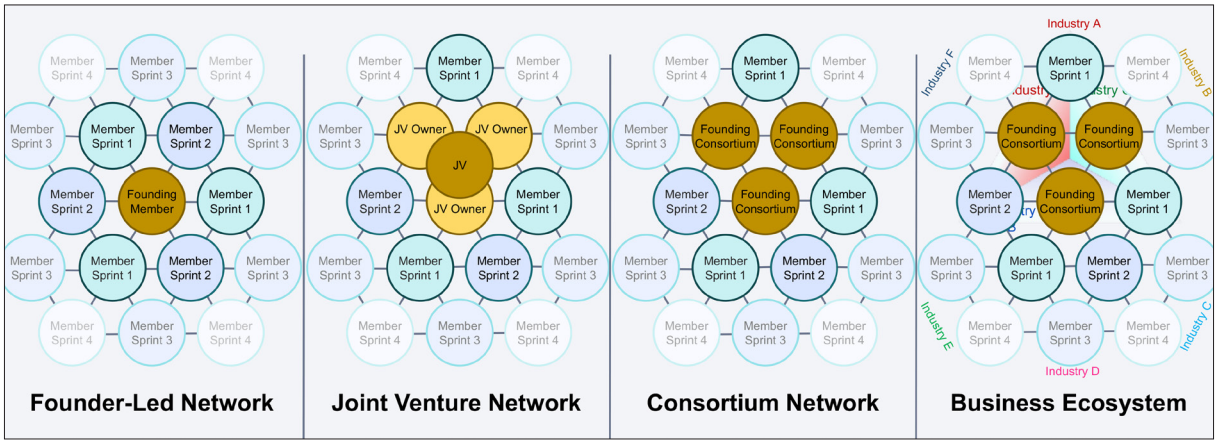
네트워크 기준의 블록체인 분류와 사례

블록체인 프로젝트는 크게 퍼블릭 블록체인과 프라이빗 블록체인으로 나누는 것이 일반적이며, 구현 형태는 네트워크 형태 또는 프로젝트 규모 기준으로 상당히 다양한 형태로 나눠진다. 블록체인 프로젝트는 네트워크 기준으로 (그림 2)와 같이 파운더 리드 네트워크(Founder-Led Network), 조인트 벤처 네트워크(Joint Venture Network), 컨소시엄 네트워크(Consortium Network), 비즈니스 에코시스템(Business Ecosystem) 등으로 나눌 수 있다.

파운더 리드 네트워크는 초기 블록체인 네트워크를 구축할 때 파운더가 주도하는 형태로, 소규모 업체나 대기업과 같은 계열사나 내부 시스템 간 연동 시 많이 나타난다.

조인트 벤처 네트워크는 대기업에서 그룹사와 연관되는 기업이나 협력 기업 간 블록체인 네트워크를 구축하는 형태다. 어느 정도 규모가 있는 기업 간 협력을 통해 특정 비즈니스나 협력 관계에서 블록체인 네트워크를 구축하는 것이다.

그림 2 | 네트워크 기준의 블록체인 분류



IBM의 경우, 머스크 사례가 있는데, 올해 1월 IBM과 머스크가 조인트 벤처를 설립해 함께 물류 관련 플랫폼을 만들고 있다.

컨소시엄 네트워크는 특정 산업 분야나 서비스를 중심으로 블록체인 네트워크를 구축하는 형태다. 이는 소규모 업체가 주도하기엔 어려운 점이 있어 일반적으로 대기업이 주도하고 중소기업이 참여하는 구조다. 특정 목적이나 산업분야, 특히 금융에서 컨소시엄 형태가 많은데, 국내에서는 은행연합회 사례가 대표적이다. 암호화폐에서는 리플(Ripple)이라는 특이한 가상화폐가 컨소시엄 네트워크이며, 코다(Corda)나 이더리움(Ethereum) 역시 컨소시엄 네트워크 형태다.

비즈니스 에코시스템은 좀 더 큰 네트워크 형태로, 여러 산업분야와 연계한 대규모 블록체인 네트워크다. 비즈니스 에코시스템은 컨소시엄도 있고, 조인트 벤처 등 여러 블록체인 서비스나 네트워크가 결합한 혼합된 형태다.

지금까지 블록체인 네트워크는 자금과 규모의 문제로 대기업 위주로 형성되어 왔다. 특히 컨소시엄 네트워크의 경우, 회원 가입을 제한하는 경우도 있으며 상당한 비용이 청구되기도 한다.

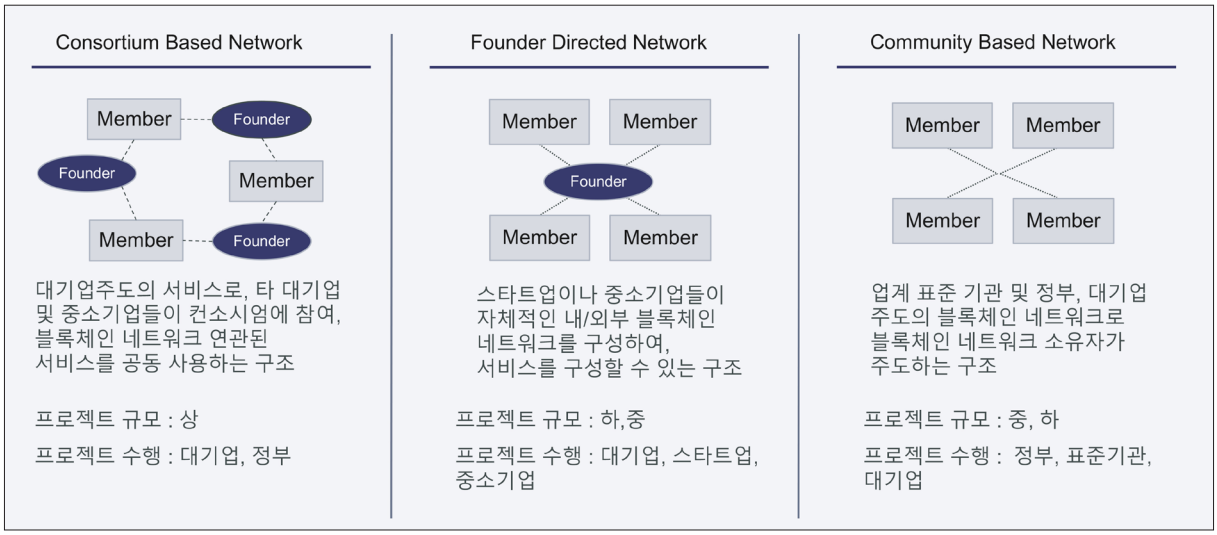
프로젝트 규모로 나눈 블록체인 분류와 사례

프로젝트 규모 기준으로 블록체인을 분류하면, (그림 3)과 같이 컨소시엄 기반의 네트워크(Consortium Based Network), 파운더 감독 기반의 네트워크(Founder Directed Network), 커뮤니티 기반의 네트워크(Community Based Network) 등 세 가지 형태로 나눌 수 있다.

컨소시엄 기반의 네트워크는 대기업 주도의 서비스로, 타 대기업과 중소기업을 컨소시엄으로 묶어 블록체인 네트워크를 공동으로 사용하는 구조다. 파운더가 여러 개로 규모가 크기 때문에 프로젝트 수행은 대기업이나 정부가 주도한다.

올해 초 발표한 관세청의 수출통관 물류 서비스가 컨소시엄 네트워크 구조와 비슷하다. 관세청은 수출화물에 대한 수출신고와 적하목록 제출절차에 블록체인

그림 3 | 프로젝트 규모 기준의 블록체인 분류



기술을 적용하는 것이 가능하다는 것을 검증하고 5월 시범 사업을 위해 총 60개 사를 모집했다. 이에 수출입자, 물류창고업자, 화물운송주선업자 등도 시범 사업에 신청해 충분한 사업자를 확보했다. 이 프로젝트는 해외 관세청과의 공동 투자를 통해 보다 큰 규모의 블록체인 네트워크를 형성할 수도 있다.

파운더 감독 기반의 네트워크는 파운더가 하나로 스타트업이나 중소기업들이 자체적인 내외부 블록체인을 구성해 서비스하는 구조다. 개인이 자신만의 가상화폐를 만들어 블록체인 네트워크를 구축할 수도 있다. 초기에는 내부 서비스로만 사용하다가 외부 업체를 참여시키거나 내부에서도 확대해나가는 구조라고 볼 수 있다. 프로젝트 규모는 하, 중 규모로 상대적으로 작다.

커뮤니티 기반의 네트워크는 업계 표준기관, 정부, 네트워크 서비스를 직접 제공하는 대기업이 주도하는 블록체인 네트워크로, 파운더는 없지만 참여자간 합의를 통해 네트워크 서비스 소유자가 주도로 구성된다.

일반적으로 생각하는 블록체인 네트워크는 모든 업데이트되는 데이터를 공유한다는 개념이지만 최근에는 당사자 간 거래는 당사자끼리만 저장하는 개념도 있다. 이렇게 공유는 하지만, 데이터는 당사자간이나 자체적인 데이터를 소유하는 개념으로 공유하고 싶지 않은 정보나 데이터를 참여자 자체적으로 원장에 보유 하는 것이다.

예를 들어, 은행연합회의 경우, 은행들이 별도의 노드를 다 구성했는데, 목적은 두 가지다. 하나는 뱅크 사인이라는 블록체인 네트워크의 한 참여자로 서비스를 받기 위함이고, 하나는 은행 내부의 시스템에서 블록체인 네트워크를 갖고자 하는 것이다.

블록체인 기반 프로젝트 수행 시 고려 사항

블록체인 기반 프로젝트를 수행하기 위해 알아야 할 사항 가운데 대표적인 4가지는 다음과 같다.

1. 블록체인은 모든 데이터를 저장, 처리하는 분산 저장 데이터베이스가 아니다.
2. 블록체인 기술 도입시, 효과 여부를 사전에 파악해야 한다.
3. 블록체인 프로젝트 수행 범위 중, 비용 절감 영역과 비용 증대 영역을 사전에 검토해야 한다.
4. 감사(Audit) 및 중앙에서 데이터 관리가 필요한 체계가 필요한 지 여부를 검토해야 한다.

블록체인은 모든 데이터를 저장, 처리하는 분산 저장 데이터베이스가 아니다. 많은 사람이 블록체인 자체를 데이터베이스라 생각하는데, 블록체인은 일반적으로 알고 있는 RDBMS 방식이 아니라 NoSQL 방식이다. RDBMS 방식에서 NoSQL 방식으로의 전환은 어려우며, 그룹핑하기도 어렵다. 또한 블록체인은 모든 데이터를 저장, 처리하는 분산 저장 데이터베이스가 아니다. 물론 모든 데이터를 저장할 수 있긴 하지만 불필요한 데이터를 굳이 저장할 이유는 없다.

앞서 설명한 대로 레거시 시스템과 연동한다면 NoSQL에 분산 원장 데이터,

즉 필요한 데이터만 저장하고 나머지는 RDBMS에 저장하는 등의 하이브리드 방식으로 구성하게 된다.

또한 기업은 기존 업무 시스템 개선 및 확장, 혹은 신규 서비스를 구축하는데 블록체인 기술을 도입해 얻을 수 있는 효과를 사전에 확인해야 한다. 무작정 블록체인 프로젝트를 구현한다고 해서 효과를 얻을 수 없다. 중요한 것은 어떤 문제가 있는지, 이를 해결하는 것인지, 개선하는 것인지, 또는 확장하는 것인지 도입 이유가 명확해야 한다는 점이다.

비용절감효과, 비용증대영역, 사전 검토, 그리고 감사와 관련된 부분, 중앙에서 데이터 관리가 필요한 부분에서도 블록체인 효과가 있는지 확인해야 한다. 특히 금융권에서 블록체인 프로젝트에는 감사 기관이 일부로 참여하게 된다. 이 감사 기관은 데이터를 지켜보는 역할만 한다. 실제 2개 이상의 업체나 은행들이 블록체인을 통해 서로 데이터를 주고받을 때, 감사기관은 해당 데이터를 계속 지켜보는 것이다. 모니터링 중에 애매한 것이나 문제가 되는 것이 있다면 바로 확인한다는 개념이다. 현재까지는 금융 분야에서만 감사 기관이 참여하는 경향이 있지만 제조 등 다른 분야에서도 참여하려는 움직임을 보이고 있다.

사용사례 선정을 위한 고려 사항들

사용사례를 선정하기 위해서는 먼저 비즈니스적, 기술적, 법률적 고려 사항을 살펴봐야 한다. 우선 블록체인 프로젝트에서 비즈니스 적합 여부를 파악하는 요소는 다음과 같다.

1) 디지털 기반의, 혹은 디지털화된 자산에 적합한가
2) 당사자간에 신뢰가 필요한가
3) 실시간 처리 기반의 결제 시스템이 필요한가
4) 현재 서비스 아키텍처에 수작업이 다수 포함되어 있는가
5) 결제 관련 서비스가 운영상의 이유로 프로세스 처리에 많은 시간이 걸리는가
6) 고객, 참여기관, 규제 당국에 자료의 투명성 및 보고가 필요한가

기업 시스템 상 데이터 흐름에는 빌링 시스템이 함께 할 수 있다. 예를 들어, 주문이 내려오면 내부적으로 빌링 시스템에 주문하고 돈이 오고갈때 실시간 처리가 필요한 상황인지 판단한다. 또한 현재 서비스가 수작업, 즉 비자동화된 작업이 어느 정도 포함되어 있는지 파악한다. 이미 자동화되어 있는 시스템을 굳이 블록체인으로 전환할 필요는 없으며, 수작업이 많을수록 블록체인 프로젝트 효과는 올라간다. 블록체인은 인터페이스나 네트워크를 만드는 것으로, 블록체인 네트워크에 참여하는 기업이나 기관은 데이터를 함께 받을 수 있는 것이다.

"지속적으로 발전하는" 기술적 고려 사항

프라이빗 블록체인은 퍼블릭 블록체인과 달리, 참여자가 원하는 대로 블록 생성주기와 데이터 크기, 블록 크기를 지정할 수 있는 점이 가장 큰 장점이다. 프

라이빗 블록체인 프로젝트에서 기술적으로 고려해야 할 사항은 다음과 같다.

1) 가상 암호화폐나 자체적인 코인 또는 토큰 처리기반 프로세스가 핵심요소인가
2) 블록체인을 통해 전자화된 자산의 결정적 결제 완결성(deterministic settlement finality)을 보장할 수 있는가
3) 결제(settlement)가 블록체인을 통해 청산되는가, 블록체인을 기반으로 청산되는가
4) 자산 생애주기 추적, 결제보고, 아이덴티티 관리, 담보 자산 관리 등의 다양한 필요요건을 충족시키는 시스템을 가지고 있는가
5) 기존 시스템과 통합될 수 있는가
6) 기관 간의 네트워크 동의가 이뤄지는 동시에 데이터 정보가 공유되지 않게 프라이버시를 보장하는가
7) 규제기관이 관찰자(observer)로서 참여할 수 있는가

사실 이전에는 디지털화된 자산, 즉 가상화폐(Crypto currency) 부분에서 '퍼블릭 블록체인에 있는 코인이 왜 프라이빗 블록체인에는 없냐'는 질문에 대해 대답하기 어려웠다.

IBM 사용사례 가운데 위트레이드(we.trade)는 중소기업들이 믿고 거래할 수 있는 환경을 만들기 위해 유럽 9대 은행이 구축한 블록체인 기반의 국제 금융 거래 플랫폼이다. 위트레이드 플랫폼은 무역을 위한 디지털 원스톱 쇼핑몰로, IBM의 블록체인 플랫폼과 하이퍼레져 패브릭(Hyperledger Fabric) 기술을 사용해 중소기업들이 간단한 사용자 인터페이스에 접속해 혁신적인 스마트 컨트랙트(Smart Contract)를 활용해 거래를 한다.

기업 간 거래 서비스인 이 플랫폼에서 돈이 오가는 것은 당연한 프로세스였지만, 프라이빗 블록체인 네트워크에서는 코인이 없기 때문에 데이터만 이동하고 돈은 별도로 보내야 하는 비효율적인 구조였다. 그래서 최근에 패브릭 코인(Fabric coin)이라는 실물 자산 기반의 토큰이 탄생했다. 이 토큰은 자산 평가 당시 가치를 기반으로 토큰을 발행하게 된다. 하지만 발행한 조직 또는 기관의 자산 가치가 떨어지면 해당 토큰의 가치도 떨어져야 하는데 그렇지 않다는 것이 문제가 된다. 또한 해당 자산을 폐기처분했을 시 이를 기반으로 한 토큰을 어떻게 처리할 것이냐는 문제도 발생한다.

최근 IBM은 스텔라 기반의 스테이블 코인 '스트롱홀드 USD(Stronghold USD)'를 준비하고 있다고 발표했다. '스테이블 코인'이란 가상화폐의 단점인 가치 변동성을 줄이기 위해 기존 정부 발행 화폐와 연동시킨 안전한 암호화폐를 의미한다.

이처럼 블록체인을 통해 전자화된 자산에 대해 결제 완결성 보장 여부와 전자화된 자산의 실물 자산 유효 여부도 판단해야 한다. 결제 완결성이란 참여자들의 지급 지시에 따라 지급 시스템을 통해 이뤄진 결제는 어떠한 상황에서도 취소(revocable)되거나 재지급(repaid)되지 않고 지급결제 시스템의 운영규칙에 의거해 무조건적(unconditional)으로 성사되는 것을 의미한다. 여기에는 해당 자

산에 참여하는 기관이나 업체간 공동 합의가 있어야 하는데, 서로간 보내는 데이터에 대해 동일한 자산으로 판단하겠다는 법률적 검토가 내재되어야 한다.

이와 함께 기술적으로 중요한 것은 기존 시스템과 통합 가능 여부다. 기존 시스템이 제공하는 인터페이스나 API, 관리하는 데이터에 따라 어떤 방식으로 통합할 것인지 사전에 고려해야 한다. 블록체인에서 제공하는 기능들이 제한적이기 때문에 기본적으로 중간에 에이전트를 만들어 공유하는 사례가 많다.

또한 기관 간 네트워크 동의가 이뤄지긴 했지만, 동시에 데이터가 공유되지 않도록 하는 것도 중요하다. 앞서 설명한 대로 블록체인 기반 프로젝트는 상당히 다양한 형태로 구축할 수 있기 때문에 필요한 데이터만 공유하거나 3, 4개의 네트워크 구조로 만들 수 있다. 전체 공유 데이터, 당사자 간 공유 데이터, 컨소시엄 형태에서의 내부적 그룹핑, 그룹 간 공유 데이터, 자체적으로 저장하는 데이터 등은 기술적으로 처리하는 방식이 다르기 때문에 확인이 필요한 사항이다.

갈 길이 먼 법률적 고려 사항

현재 법률적 고려 사항에 대해서는 아직 정의가 명확하게 규정되지 않아 상당히 많은 논의를 하고 있다. 특히 국내에서는 법률적 논의 자체가 많이 늦은 상황이며 최근 문제가 되고 있는 부분은 스마트 컨트랙트(Smart Contract)다.

1) 블록체인을 통해 전자화된 자산의 결제완결성이 '법적으로' 보장될 수 있는가
2) 전자화된 현물 자산의 법적 보증을 누가 할 것인가
3) 법률적으로 정해진 예탁 또는 청산기관의 역할은 무엇인가
4) 스마트 컨트랙트가 법률적 효력을 가지는가
5) 한 예로 외환 송금시, 외환법에 위배되지 않고 서비스가 가능한가
6) 고객 정보를 블록체인 분산원장에 저장, 공유할 경우 법적으로 보장받을 수 있는가

스마트 컨트랙트는 계약 정책이나 처리 프로세스를 작성한 후, 조건에 따라 계약 내용을 자동으로 실행할 수 있는 디지털 계약서다. 기존 서면 계약서에서는 계약 조건을 실제 사람이 계약서 내용대로 수행해야 하지만, 스마트 컨트랙트는 계약 조건이 갖춰지면 자동적으로 계약이 체결되고 동시에 이행된다. 이런 스마트 컨트랙트의 거래 방식은 민법에서부터 전자거래기본법에 이르기까지 총 5개 법에 적용되는데, 법마다 해석이 제각기 다르다. 예를 들어, 스마트 컨트랙트는 계약 성립과 이행을 구분하도록 한 민법과 개념이 정면으로 대치되기 때문에 법 개정없이는 활용하기 어려운 상황이다.

또한 ▲스마트 컨트랙트의 주체를 결정하는 문제 ▲계약 내용 로직에 대한 당

사자간 합의 여부 문제 ▲계약 유효 및 성립 시기 문제 ▲계약 보증과 실수로 인한 책임 소재 및 보상 문제 등 해결해야 할 사안들이 복잡하고 다난한다. 특히 국내에서는 ▲스마트 컨트랙트를 실제 전자문서로 인식할 것이냐는 사안조차 정확히 정의되지 않았다.

이와 함께 실제 송금시 블록체인 네트워크를 통하면 국가와는 관계없이 큰 돈이 거래될 수 있는데, 이로 인해 외화 송금시 외환법에 위배되는 경우가 발생한다. 국내에서는 지난해 말부터 외화 송금 금액을 제한하고 있다.

그리고 고객 정보 관련 문제도 사전에 고려해야 할 사안이다. 최근 EU에서 시행한 GDPR이나 국내 클라우드 법에서 개인정보는 해당 국가 위치에 저장되어야 하는데, 블록체인 네트워크에서의 저장 위치는 특정되지 않기 때문에 위배될 소지가 있다. 최근 국내에서는 개인정보를 국내뿐만 아니라 국외 클라우드에도 저장할 수 있도록 법안을 개정하려는 시도가 있다. 하지만 개인정보 저장 문제는 생각보다 간단치 않다. 개인정보 저장 방법에서부터 관리 방식, 그리고 GDPR과 같은 각국의 컴플라이언스를 피하기 위한 방법 등 많은 사안이 논의되고 있다.

"키를 잃으면 전부를 잃는다" 퍼블릭 블록체인 프로젝트 고려 사항

퍼블릭 블록체인 프로젝트를 진행하기 위해서는 키 관리, 참여자 권한 관리, 거래 검증 및 합의, 블록체인 소프트웨어 보안, 서비스 보안 등 총 5가지 항목에서 사전 검토가 필요하다.

퍼블릭 블록체인에서 가장 중요한 문제는 키(Key)다. 자신이 보유한 키를 분실 혹은 도난당하는 순간, 모든 것을 잃게 된다. 그래서 보유키가 유출되지 않도록 안전하게 보관할 필요가 있는데, 최근 월렛 기반의 USB 스틱이나 월렛 기능을 탑재한 스마트폰을 사용하는 이들이 많아졌다. 또한 키 도난 및 분실시, 다중 서명 방식의 복구 절차가 필요하다.

퍼블릭 블록체인은 불특정 다수가 참여자이기 때문에 당사자가 해당 서비스를 이용할 때는 상당히 제한적이다. 블록체인에서 51% 공격은 전체 네트워크의 해시파워를 절반이상 보유한 경우 데이터를 변조할 수 있다는 구조적 약점으로 알려져 있지만, 사실 변조할 수 있는 데이터는 자신이 올린 데이터만 가능하다. 그런 의미에서 거래와 무관한 제 3자 접근 통제가 필요하다. 불특정 참여자들로 구성되다보니, 자기가 원하는 거래자와 거래할 수 있는 사례는 드물다. 그래서 블록체인의 참여자 권한은 사실상 제한적인 셈이다. 또한 거래무결성 확인을 위한 정보 외에 개인정보 침해가 우려되는 정보를 관리할 필요가 있다.

블록체인의 거래 검증 및 합의는 대부분 마이닝 방식으로 되어 있기 때문에 실제로 리스크가 많으며, 내외부 사이버공격으로부터 노드 유효성 조작에 대한 방지책이 필요하다. 많은 참여자가 거래 검증에 합의하는 구조 검토가 필요한데, 합의에 대한 이중지불이나 긴 블록 우선권 문제를 해결하기 위해 이더리움은 POW(Proof Of Work) 방식에서 POS(Proof Of Stake) 방식으로 바꾸려고 한다.

블록체인 소프트웨어는 보안 취약점에 대한 검토가 필요하다. 시큐어 코딩, 코

드 검토, 보안 테스팅 등 보안 사항 검토가 필요하며 DDoS 공격과 같은 대량의 트랜잭션 공격에 대응 가용성 문제를 검토할 필요가 있다. 그리고 상호운용성을 위해 비정상거래 탐지 및 차단 방안이 검토해야 한다.

"인증서 관리가 중요한" 프라이빗 블록체인 프로젝트 고려사항

프라이빗 블록체인은 퍼블릭 블록체인과는 달리 허가받은 특정 노드만 참여할 수 있는 블록체인 네트워크로, 프로젝트 진행시 총 5가지 항목에 대해 사전 검토해야 한다.

- **인프라** : 사용사례를 기준으로, 참여 노드의 환경 및 분산원장 저장 데이터 형태, 자체 시스템 구성 여부에 따른 인프라 환경 구성이 필요하다. IBM 블록체인 플랫폼의 경우, 기업이 사용사례를 선정하면 그에 따른 시스템 환경이 결정하고 제공하기 때문에 기업은 인프라와 관련한 여러 가지 고려 사항들을 신경쓰지 않아도 된다.
- **네트워크** : 시스템 및 노드 간의 복잡한 네트워크 구간의 암호화 및 전송 데이터 암호화가 필요하다.
- **인증서 관리** : 프라이빗 블록체인은 폐쇄형으로 네트워크에 접속, 참여하는 노드와 클라이언트의 인증 절차는 필수적이다. 또한 인증서를 발급받은 참여자만이 조인할 수 있기 때문에 인증서 관리는 무엇보다 중요하다. 신뢰할 수 있는 당사자가 해킹당하면 블록체인 보안은 사라지기 때문이다. 그래서 인증서가 유출되지 않도록 별도의 HSM(Host Security Module) 장비에 저장하거나, 좀더 안전한 환경에서 인증서를 저장하는 사례도 있다.
- **스마트 컨트랙트** : 스마트 컨트랙트는 조건이 충족되면 자동으로 실행되고 이는 되돌릴 수 없다. 즉, 문제를 실행 취소하고 실수를 수정하거나 사기(frauds)를 되돌리기가 매우 어렵다는 걸 의미한다. 지난해 가을 누군가의 실수로 멀티파티 이더리움 계약을 잠궜는데, 그 결과 3억 달러 상당의 통화가 손실된 적이 있다. 그래서 비즈니스와 연관된 참여자간의 협의된 로직 구성 및 디버깅을 통한 코드 오류 항목에 대한 사전 검토가 필요하다.
- **데이터(분산원장)** : 분산원장에 개인정보 및 공유불가 데이터에 대한 저장 및 처리방식을 사전에 검토할 필요가 있다.

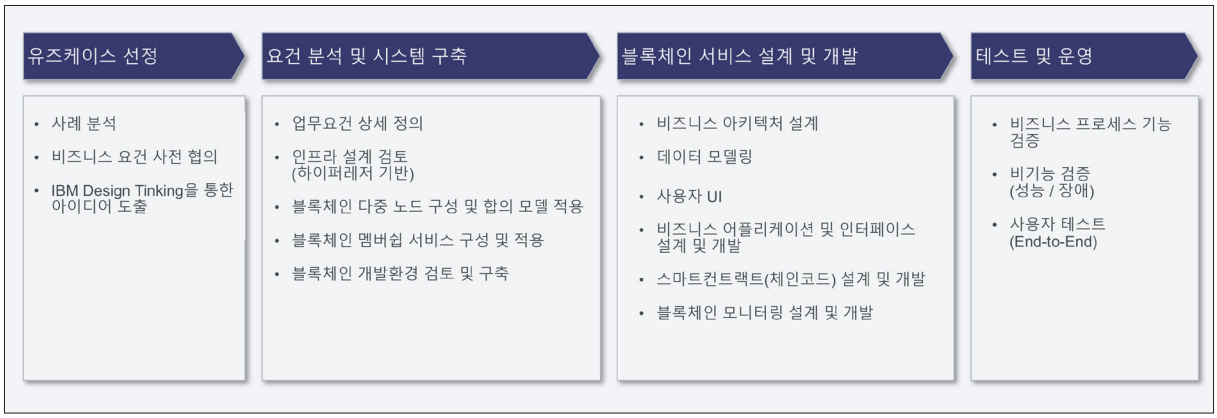
블록체인 기반 프로젝트 4단계 수행 방법론

블록체인 기반 프로젝트는 1단계 사용사례 선정, 2단계 요건 정의 및 시스템 구축, 3단계 블록체인 서비스 설계 및 개발, 4단계 테스트 및 운영으로 구성된다.

이 가운데 가장 중요한 단계는 1단계인 사용사례 선정이다. 사용사례 목적에 따라 퍼블릭 블록체인이나 프라이빗 블록체인 적용 여부를 판단하게 되는데, 사용사례 도출을 위한 시간적인 투자가 필요하다. 퍼블릭 블록체인과 프라이빗 블록체인 선택에 따라 전체 블록체인 구성 방안이 달라진다.

이후 선정된 사용사례를 기반으로 효과적인 블록체인 도입을 위한 업무별 IT

표 | 블록체인 기반 프로젝트 수행 단계별 고려 사항



현황과 데이터 처리 현황 파악이 중요한데, 블록체인 적용 범위에 따라 시스템 구축 방식이 달라지기 때문이다. 2단계에서는 주요 IT 영역을 중심으로 시스템 구축 계획을 수립하고 비즈니스 확장성과 구축 자원 등 종합적 상황을 고려해 인프라 구축안을 선정한다. 3단계에서는 도출된 요구사항을 기준으로 체인코드 기능 및 KVS(Key Value Store) 설계 방식에 따라 효율적인 블록체인 처리 방식을 설계, 개발한다. 개발 단계에서 블록체인 모니터링과 체인코드 개발은 아주 중요한 요소다.

블록체인 서비스 테스트는 기능, 비기능 검증으로 구분되며, 기능처리 부분과 성능/장애 항목 검증이 중요하다. 테스트 결과를 기반으로 블록체인 기반의 실제 서비스 운영 가능 여부를 판단한다. 또한 블록체인 성능 및 장애 테스트에 대한 시나리오 준비가 중요하다.

IBM 블록체인 플랫폼을 사용하는 이유

IBM 블록체인 플랫폼은 비즈니스 네트워크 개발 및 거버넌스, 그리고 운영 관리 효율성 증대를 위해 최적화된 기업용 블록체인 플랫폼이다.

이를 통해 기업은 비즈니스 네트워크 활성화 및 참여자 통제 기능을 통한 관리 능력이 향상되고, 상시 비즈니스 네트워크를 구축할 수 있다. 기업이 일반적인 온프레미스 방식으로 도커 이미지를 직접 다운로드 받아 구축하면 많은 어려움을 겪게 된다. 하지만 IBM 블록체인 플랫폼은 기본적으로 5분 내로 원하는 네트워크 환경 구축이 가능하다.

IBM 블록체인 플랫폼은 총 3가지의 특징을 갖고 있다.

첫 번째, 하이퍼레저 기술을 통한 블록체인 애플리케이션 개발 지원이다. 일반적으로 IBM은 하이퍼 레저 패브릭 기술을 주도하고 있으며, 이를 기반으로 한 경험 또한 상당하기 때문에 블록체인 애플리케이션 개발 지원이 가능하다. 이를 통해 비즈니스와 개발 기간을 단축시키고 오픈소스 툴과 언어를 활용해 블록체인 애플리케이션을 빠르게 구축할 수 있으며, 누구나 쉽게 학습하고 개발할 수 있다.

두 번째, 새로운 블록체인 네트워크를 간편하고 빠르게 구축할 수 있다. 기본

정책을 통해 블록체인 네트워크를 효율적으로 관리할 수 있으며, 스마트 컨트렉트, 네트워크 참여자 및 트랜잭션 기반의 채널을 탄력적으로 구성할 수 있다. 또한 기본 구축된 룰 및 정책을 통해 빠른 환경 구성과 커스터마이징이 용이하다.

세 번째, 우수한 보안 및 성능의 블록체인 네트워크 구축 및 확장이다. IBM 블록체인 플랫폼을 통해 기업은 작은 규모로 시작해 참여자가 증가하거나 트랜잭션 볼륨 증가에 맞춰 빠른 네트워크 확장이 가능하다. 또한 IBM 전용 하드웨어 펌웨어, 소프트웨어 기능이 포함된 우수한 보안 환경을 제공하며, 네트워크 확장 및 업그레이드 시에도, 서비스 중단 없이 상시 운영이 가능하다.

블록체인 플랫폼의 2가지 제공 방식

IBM 블록체인 플랫폼을 크게 2가지 방식으로 제안하는데, 스타터 플랜(Starter Plan)과 하이 시큐리티 비즈니스 네트워크(High Security Business Network, HSBN) 기반의 엔터프라이즈 플랜(Enterprise Plan)은 클라우드 상에서 블록체인 플랫폼을 구현하는 방식과 나머지 한가지는 기업 내에 자체적인 시스템 구축을 하는 온프레미스(On-Premise) 구축 방식이다. 스타터 플랜은 개발 부문에서 필요한 사례를 간단히 구축해 테스트하는 환경이며, 엔터프라이즈 플랜은 엔터프라이즈 서비스에 맞는 구조로 선택해 구성할 수 있는 계획을 제공한다. 온프레미스는 도커 이미지를 깔아서 직접 구축하는 방식이다. 현재 IBM 블루믹스(https://console.bluemix.net/catalog/services/blockchain)에서 스타터 플랜을 신규 등록하면 제공되는 500달러 크레딧으로 블록체인을 무료 체험해 볼 수 있다. IBM은 총 600개 이상의 다양한 사용사례와 경험을 토대로 어떤 서비스에 블록체인을 최적화할 수 있는지 컨설팅과 하이퍼레저 패브릭 기술을 토대로 실제 클라우드 기반에 최적화되도록 커스터마이징 한 블록체인 플랫폼을 제공한다.