KORBIT

Block Chain Primer

블록체인의 기술적 이해 및 도입을 위한 첫걸음

블록체인에 대한 관심이 뜨겁다. 국내외를 막론하고 각종 금융기관 및 미디어의 신년 계획과 전망에 빠지지 않고 등장했다. 핀테크나 빅데이터 같은 산업적 개념이 아닌, 언뜻 난해해 보이는 기반 기술을 통칭하는 용어가 이토록 빠르게 확산되고 회자되었던 사례가 있었나 궁금할 정도다. 다만 커진 관심만큼 그것에 대한 오해 내지는 모호한 이해 또한 확대재생산되고 있는 실정이다. 대표적인 게 블록체인이 위변조를 '원천봉쇄'할 수 있는 분산장부(기술)라는 인식이다. 위변조 시도를 애초에 불가능하게 만드는 시스템은 이론적으로 불가능에 가깝다. 다만 블록체인은 위변조 시도를 무의미하게 만들거나 증거가 남게 해 사전 혹은 사후 대응을 용이하게 한다는 점에서 차별화된다. 퍼블릭 블록체인과 프라이빗 블록체인을 구분하지 않고 어느 한 쪽의 문제점을 전체의 것으로 확대하거나, 반대로 모든 기능이 다 구현가능한 것처럼 과장하는 경우도 눈에 띈다.

블록체인에 대한 평가도 엇갈린다. 한편으론 인터넷에 비견될 정도로 엄청난 잠재력을 지닌 기술로 각광을 받지만, 다른 한편에선 비트코인의 화폐적 실험에서 드러난 문제점들까지 고스란히 떠안으며 (부당하게) 평가절하되기 일쑤다.

블록체인으로 무엇을 할 수 있을 지, 어떤 분야에서 어떤 효익을 가져올 수 있을지, 비트코인이라는 역사적 실험의 한계와 성과는 기술로서 블록체인에 어떠한 함의를 지니는 지 등. 중요한 쟁점들은 대부분 흐릿하게 아웃포커스 된 채 성급하게 큰 그림부터 그려지고 있는 건 아닌지 차분하게 되돌아 볼 시점이다.

코빗은 지난 2013년 국내 최초로 비트코인 거래소를 설립하며 한국에 비트코인과 블록체인 기술을 널리 알리고 보급해 왔다. 한국은행, 국세청, 금융위 등 금융당국은 물론 각급 금융기관과 대학 강연을 통해 비트코인의 화폐적 가치 자체 보다는 그것을 가능케 한 기반기술인 블록체인에 주목할 것을 역설해왔다. 아울러 서울디지털포럼(2014년) 강연 및 각종 컨퍼런스와 세미나, 동아비즈니스리뷰 블록체인 스페셜 리포트(2015. 10) 등 여러 매체 기고 활동을 통해 블록체인 기술의 올바른 안내에 앞장 서 왔다. 나아가 블록체인에 대한 연구와 협업을 본격화 하기 위해 지난 가을 블록체인랩(https://blockchain.korbit.co.kr)을 설립, 여러 금융기관 및 기업, 공공기관 등에 기술적 핵심과 비즈니스적 전망을 공유해왔고, 나아가 블록체인 도입을 통한 혁신 모델을 공동 연구, 모색하고 있다.

코빗은 본 보고서를 시작으로 블록체인에 대한 내부 연구 성과를 한국 사회와 활발하게 공유, 블록체인에 대한 실험이 한국에서 본격화되는데 미력하게나마 기여하고자 한다.

블록체인이란 무엇인가

블록체인은 비트코인 시스템을 구동하기 위해 고안된 기반 기술이다. 비트코인이 등장하기 이전에는 P2P(peer-to-peer) 네트워크 상에서 구동되는 분권적 화폐 시스템이 불가능하다는 게 정설이었다. 신뢰성을 담보하는 중앙기관 없이는 이중지불을 막고 장부의 무결성을 유지할 수 없었기 때문이다. 비트코인은 작업증명(proof-of-work)이라는 참여적 컨센서스 방식과 블록체인이라는 분산장부 기술을 토대로 이 한계를 뛰어넘었다.

위키피디아에 따르면, 블록체인은 승인 없는 분산 데이터베이스(permissionless distributed database)로 정의될 수 있다. 옥스포드 사전에는, 비트코인 혹은 다른 암호화화폐의 거래가 순차적이고 공개적으로 기록되는 디지털 장부라고 기술 되어있다(A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly). 뒤에서 더 자세히 살펴 볼 것이지만 위의 두 정의는 모두 비트코인에 특화된 블록체인, 즉 퍼블릭 블록체인의 특성만을 반영하는 뚜렷한 한계를 지닌다.

얼마 전 발간된 영국정부의 블록체인 보고서는 이보다 진전된 정의와 함께 블록체인의 기본 메커니즘을 아래와 같이 간명하게 설명하고 있다.

"분산장부는 기본적으로 자산의 데이터베이스이다. 이 데이터베이스는 여러 시스템, 구성원 그리고 기관들로 구성된 하나의 네트워크 상에서 공유될 수 있다. 네트워크의 모든 참여자들은 각자 자기 고유의 장부 복사본을 가질 수 있다. 공유된 장부에 어떤 변경이 발생하면 그 내용은 모든 장부에 몇 분 내지는 몇 초만에 반영된다. 장부에 기재된 에셋은 금융적, 법적, 물리적 또는 전자적일 수 있다. 장부에 기재된 에셋의 보안성과 엄밀성은 전자키와 전자서명에 의해 암호학적으로 유지되는데, 이것들은 공유된 장부 내에서 누가 무엇을 할 수 있는 지를 통제하는 수단이 된다. 새로운 등재 내용은 하나, 여럿 또는 모든 참여자들에 의해서, 네트워크에 의해 동의된 규칙에 준거해 업데이트 될 수 있다."[1]

한국은행은 최근 발간한 보고서에서 블록체인을 분산원장(distributed ledger) 기술로 규정하면서, "거래정보를 기록한 원장을 특정 기관의 중앙 서버가 아닌 P2P 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하는 기술을 의미"한다고 포괄적으로 설명했다. 세계적인 컨설팅 회사 딜로이트는 좀 더 광범위한 시각에서 "서로 알지 못하는 사람들이 공유된 거래 기록을 믿을 수 있게 해주는 기술"로 정의한다. 아울러 기술의 총합이면서 공유된 기록 그 자체 또는 장부인 블록체인은, 특정한 네트워크 상에서 모든 참여자들에게 분산되어 있으며 참여자들은 자신들의 컴퓨팅 자원을 이용해 거래기록을 유효화하고, 이를 통해 제3기관의 개입을 불필요하게 만든다.[2]

국내외 여러 기관에서 블록체인에 대한 연구작업 성과를 속속 내놓고 있지만 여전히 그 실체적 정의에 대한 엄밀하고 일관된 합의는 이뤄지지 못하는 것처럼 보인다. 블록체인 기술을 보다 네트워크 친화적으로 진화된 데이터베이스로 보는 견해서부터 금융에 특화된 새로운 프로토콜로 사고하는 경향에 이르기까지 다양한 시각들이 혼재되어 있다. 새롭게 부상한 기술을 규정하는 단계서부터 합의가 이뤄지지 않고 있다 보니, 기술 활용을 위한 논의 역시 지지부진해지기 마련이다. 블록체인에 대한 보다 엄밀하면서도 보편적인 정의가 필요한 이유다.

우리는 블록체인을 "Tamper-evident distributed data structure(위변조 증거가 남는 분산 데이터 구조)"로 정의할 것을 제안 한다. 물론 블록체인의 용례가 풍부해짐에

1 Government Office for Science, "Distributed ledger technology: beyond block chain" (2016. 1. 19)
2 딜로이트, Blockchain Enigma. Paradox. Opportunity

따라 이 같은 기술 또한 유효성을 상실할 수 있을 것이다. 그럼에도 불구하고 현 시점에서 블록체인의 특징과 구조를 가장 적절하게 반영하며 논의를 시작하기 위한 토대로서 기능하기에는 충분한 설명이라 판단한다.

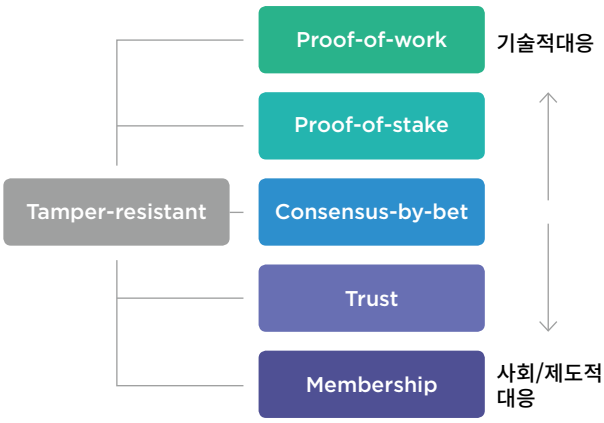
우선 위변조 가능성부터 살펴보자. 일반적인 통념과 달리 블록체인은 위변조가 불가능한 구조가 아니라 위변조를 쉽게 적발할 수 있도록 구조화된 시스템이라고 보는 것이 더 적절할 것이다. 단순히 분산되어 통신하며 업데이트되는 장부라기 보다는 위변조에 대한 대응을 어떻게 하느냐가 더 본질적이기 때문이다. 블록체인은 위변조 행위를 적발하고 그러한 시도에 대응하는 조치에 따라 그림1에서와 같이 크게 다섯 가지로 구분할 수 있다. 이 같은 구분을 통해 우리는 블록체인 내부 구조에 대한 정확한 이해에 한 걸음 더 가까이 다가갈 것이라 생각한다.

또한 블록체인을 분산 장부(ledger)나 데이터베이스(database)라 규정하는 것 보다는 데이터구조(data structure)로 이해하는 것이 보다 유연하면서도 정확한 규정일 것이다. 분산장부 혹은 원장이라는 기술은 금융권에서만 통용될 수 있는 수평적 제한성을 지니며, 데이터베이스라는 규정은 수직적 경직성을 초래한다. 금융이외의 산업에 적용될 때 블록체인은 단순한 원장 이상의 데이터 구조로 기능할 수 있으며, 단순한 데이터베이스 시스템 이상의 구조적 확장성을 담보할 수 있기 때문이다. 분산된 데이터의 무결성 저장 기능뿐만 아니라 디지털 에셋과 자료의 분배 및 공유, 메시징, 암호학, 컨센서스 등의 다종 기술이 집약된 구조로 이해해야 할 것이다.

뒤에서 살펴볼 것이지만 블록체인은 목적과 특성에 따라 세분화될 수 있다. 이런 구분과 상관없이 모든 블록체인은 아래와 같은 본원적 공통 요소를 지닌다.

- 분산구조
- 참여자 네트워크와 참여자 스스로 제공하는 컴퓨터를 활용
- 암호학과 디지털서명으로 이용자식별
- 기록 조작/변경을 어렵게 만드는 메커니즘
- 타임스탬핑
- 개별 거래를 프로그램화 (programmable transaction)

그림1. 위변조에 대응하는 블록체인 메커니즘 분류



위변조에 대응하는 방식은 블록체인의 목적과 그에 연동하는 설계 방향에 따라 여러 방식이 있을 수 있지만 현재 등장한 방식은 위의 다섯 가지 정도로 나눠볼 수 있다. 맨 왼쪽의 작업증명(proof-of-work) 방식의 경우 가장 기술적인 접근 방법으로 비트코인을 통해 그 효용성이 입증돼 왔다. 불특정 다수가 참여하기 때문에 마이닝 과정에 많은 컴퓨팅 자원을 들이게 하는 방식으로 보안장벽을 높이는 한편, 참여에 따른 인센티브를 지급해 네트워크에 반하지 않게끔 만들었다. 이런 접근은 보안성이 매우 뛰어나지만, 많은 전기와 컴퓨팅자원이 소모되고 거래가 확정되는 주기가 다소 길다는 점 등의 한계를 갖고 있다. 이같은 문제점 극복을 위해, 우측으로 갈수록 기술적/암호학적 요소 뿐만 아니라 사회/제도적 요소들을 적절히 융합, 위변조에 대응하는 다양한 방식이 고안되고 있다. 비트코인처럼 누구나 참여하는 네트워크가 아니라 사전 승인 방식으로 참여를 제한하는 경우 고도의 기술적 방식 보다는 사회/제도적 장벽이 보다 효과적이기 때문이다.

왜 블록체인을 도입하는가?

블록체인은 물론 만능 열쇠가 아니다. 모든 문제의 해결책이 될 수는 없다. 다만 제대로, 정확한 목적하에 도입, 적용한다면 다음과 같은 이점을 누릴 수 있다.

1. 향상된 보안성

블록체인을 도입하면 중앙 데이터베이스에 모든 자료를 저장하는 것보다 상대적으로 높은 보안성을 가져다준다. 모든 데이터베이스를 한 곳에 보관/관리 한다면 해커들이 단 하나의 데이터베이스만 침입하는 것으로 치명적인 피해를 유발할 수 있다. 하지만 블록체인처럼 분산된 데이터 구조에 침입하는 것은 현실적으로 매우 어렵다. 위에서 언급한 다양한 방법들로 위변조를 막고 있을뿐만이 아니라 수십, 수백, 수천개의 컴퓨터를 동시에 해킹하는 것은 매우 많은 비용을 들여야 하므로 사실상 불가능에 가까운 일이 된다. 아울러 중앙집중적인 관리가 불필요해지므로 내부자에 의한 조작 또는 정보유출 위험 또한 크게 감소한다.

2. 향상된 투명성

블록체인은 기본적으로 공개성이라는 특징을 가지고 있다. 각종 금융거래, 회계관리와 같은 투명성이 중요한 곳에서 블록체인의 활용에 대한 연구가 활발한 건 그 때문이다. 최근 R3CEV와 11개 은행의 블록체인을 활용한 실험, 나스닥의 블록체인을 활용한 주식발행과 같은 사례들은 왜 블록체인이 가지는 투명성과 공개성에 선도기업들이 눈독들이는지를 보여주는 좋은 사례라고 할 수 있다. 모든 참여자들이 장부를 공유하고 있기 때문에 기본적으로 모든 거래기록이 투명하게 공개된다.

3. 안정성

블록체인의 분산 구조는 기업이나 공공기관이 기존과 같이 한 곳에 모든 데이터를 보관해야 하는 잠재적 위험성을 피할 수 있게 해준다. 즉, 단일 실패점(single point of failure)이 존재하지 않기 때문에 일부 시스템에 오류 또는 성능저하가 발생하더라도 전체 네트워크가 타격을 입을 가능성의 희박하며 쉽게 복구가 가능하다.

4. 효율성

블록체인은 복잡한 거래 기록 관리 및 추적에 용이한 장점을 지닌다. 아울러 여러 기관이 참여하는 경우에도 시스템 통합에 따른 복잡한 프로세스와 그에 수반하는 고비용 구조를 우회하게 해준다.

블록체인을 통해 2022년까지 은행의 인프라 비용을 150~200억 달러를 절감할 수 있을 것이라는 예측(Santander InnoVentures) 등이 나오는 것은 이런 특성 때문이다. 아울러 개별 트랜잭션에 프로그램을 입힐 수 있어 스마트 컨트랙트 등 복잡하고 지능적인 거래를 가능케 하고 이를 통해 많은 효율성을 기대케 한다.

세계적인 컨설팅회사 맥킨지는 블록체인 기술이 “속도, 보안성, 투명성, 편의성과 비용 측면에서 상당한 혜택을 가져다 줄 것"이라고 분석했다. 아울러 빠른 속도와 영구적인 타임스탬핑을 필요로 하는 다음과 같은 서비스에 매우 적합할 것이라 덧붙였다.

- 페이먼트
- 금융자산 이전
- 스마트 컨트랙트
- 소유권 분할 및 공증 서비스

블록체인의 종류와 구분

블록체인은 크게 퍼블릭(public) 블록체인과 프라이빗(private) 블록체인으로 나눌 수 있다. 흔히들 언급하는 블록체인은 대부분 퍼블릭 블록체인이다. 비트코인, 이더리움, 라이트코인이 작동하는 블록체인은 모두 퍼블릭 블록체인을 활용한 가상화폐/스마트금융플랫폼이다. 그렇기에 퍼블릭 블록체인은 공개성, 분산성과 같이 흔히 블록체인에 대해 이야기 할 때 언급하는 특성들을 모두 가지고 있다. 반면 프라이빗 블록체인은 특정한 기관, 업체들이 자신들의 목적과 특성에 맞게 설계한 블록체인이다. 그렇기 때문에 블록체인이 가지는 공개성, 분산성과 같은 특성을 모두 다 구현하지 않을 수 있다. 또한 프라이빗 블록체인은 정보의 흐름을 확인하는 방법 역시 다를 수밖에 없으며 활용방식 역시 상이할 수 있다.

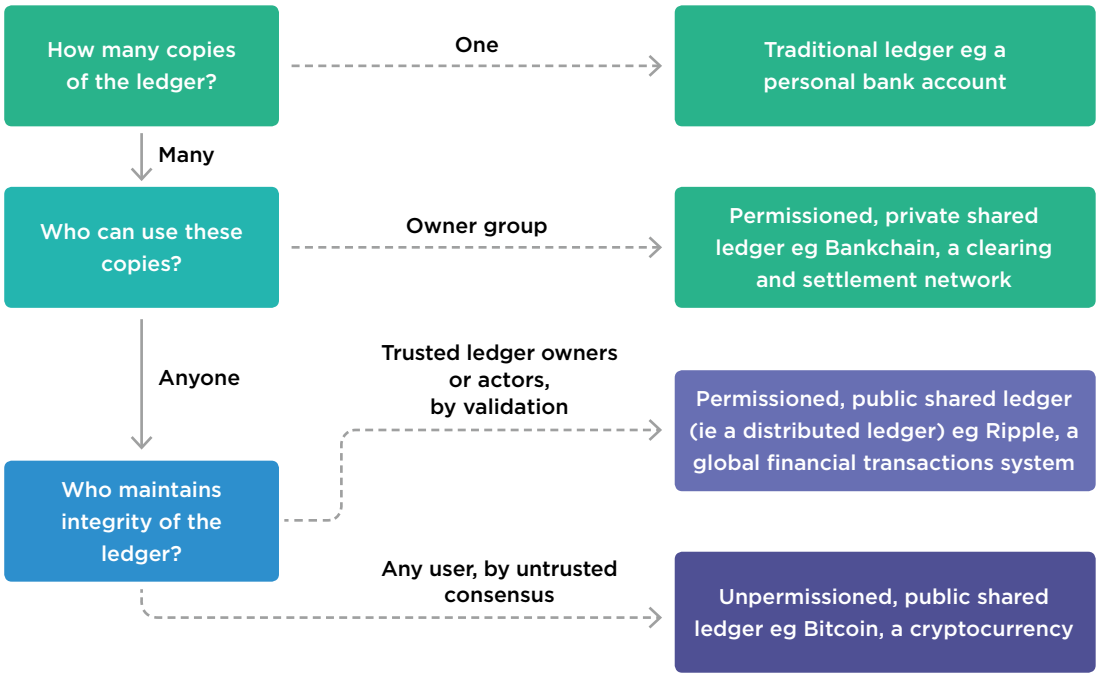
Blockchain types

	No Native Currency	Native Currency
Closed Membership	**공유장부: 데이터관리 최적화** (은행간 블록체인)	혼합 시스템 (리플, 사이드체인...)
Open Membership	불가능?	**암호화 화폐: 결제 최적화** (비트코인, 이더리움)

프라이빗과 퍼블릭으로 구분했을 때 블록체인이 활용되는 양상 역시 달라진다. 비트코인, 이더리움과 같은 퍼블릭 블록체인은 공개 네트워크를 운용하기 위해 고유한 화폐(native currency)를 발행하는 것이 일반적이다. 퍼블릭 블록체인은 블특정 다수의 참여를 통해서 운용되어야 하기 때문에 참여와 충성도를 유도하기 위한 경제적 인센티브가 필요하기 때문이다. 이를 위해 비트코인, 이더리움과 같은 공개 블록체인은 참여자(채굴자)들에게 블록체인 상에서 발행된 코인을 지불한다.

반면 프라이빗 블록체인의 경우 네트워크 상의 운용 노드가 제한되어 있다. 그렇기 때문에 코인을 발행할 이유가 비교적 명확치 않고, 발행한다고 해도 이를 통용 할 수 있는 경제적 토대가 마련되기 어렵다. 그래서 프라이빗 블록체인의 경우 고유 화폐를 통한 네트워크 유지나 지불/결제와 같은 용도로 사용되기 보다는 데이터를 분산 관리하는데 더 적합할 것으로 점쳐진다.

그림2. 어떤 블록체인을 선택할 것인가?



<Government Office for Science, "Distributed ledger technology: beyond block chain" (2016. 1. 19) >

기업의 특성, 산업 그리고 이를 운용하고자 하는 목적에 따라 퍼블릭 블록체인을 도입할지 프라이빗 블록체인을 도입할지에 대해 고려해보아야 한다. 각각의 블록체인이 가지는 특성과 기업이 원하는 특성간에 무엇이 일치하는지 다음과 같은 질문들을 통해 기본적인 사항들을 확인해 볼 수 있다.

1. 자료를 나누어 저장할 것인가?

a. 블록체인은 기본적으로 자료를 분산해서 저장하는 특성을 가진다. 만약 자료를 분산해서 저장할 필요가 없거나 분산해서 저장하는 것보다 한곳에 모아서 저장하는 것이 효율적이라고 생각된다면 블록체인을 도입하기보다 기존 기술을 도입하는 것이 더 좋다. →기존 기술 활용

2. 누가 이 블록체인을 쓸 것인가?

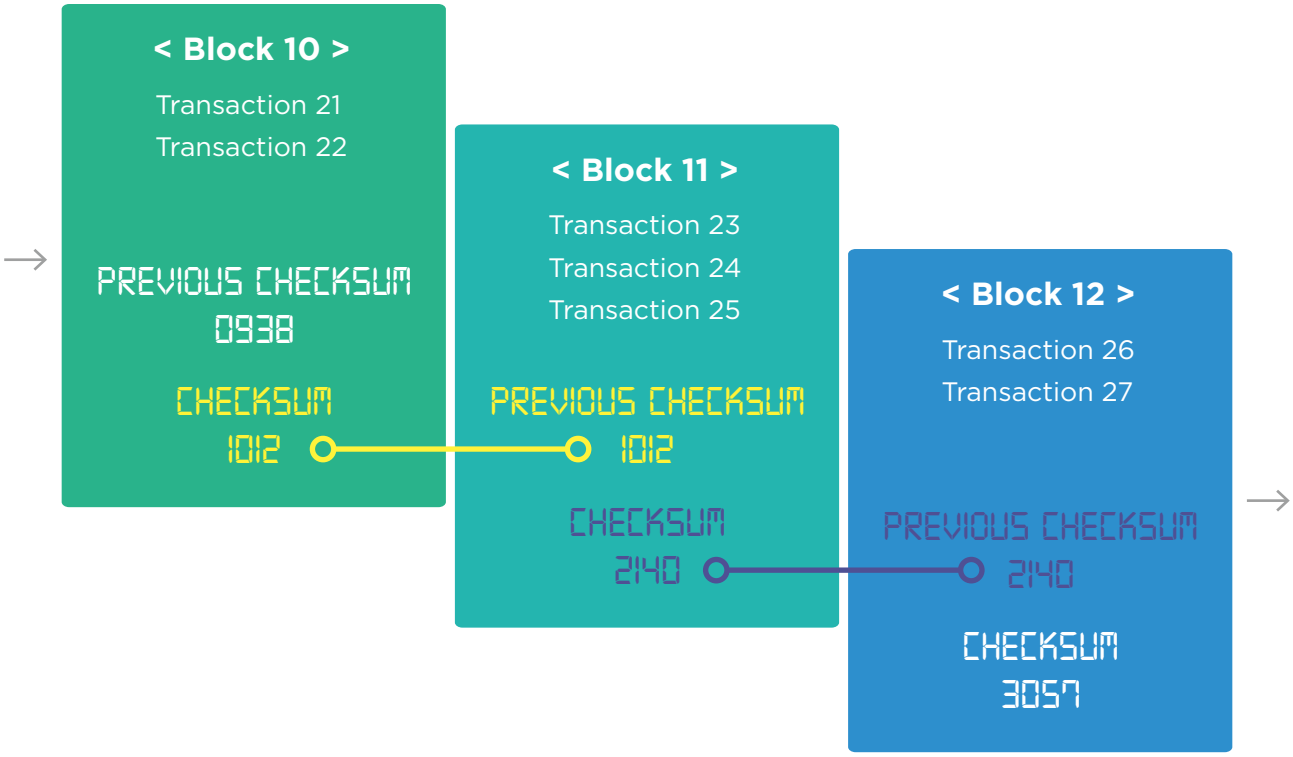
a. 만약 누구나 블록체인을 쓸 수 있게 만들 예정이라면 퍼블릭 블록체인을, 허가된 사람만 쓸 수 있게 만들 예정이라면 프라이빗 블록체인을 사용하는 것이 좋다. →프라이빗 블록체인 활용

3. 누가 이 블록체인을 관리할 것인가?

a. 만약 지정된 사람만이 블록체인을 관리하게 만든다면 현재 리플과 같이 본인들이 블록체인을 관리해야 한다. 이 경우 블록체인을 운용하는데 드는 모든 비용과 이에 따른 리스크를 부담해야 한다. →혼합 블록체인

b. 만약 모든 사람이 블록체인을 관리할 수 있게 만들 것이라면 퍼블릭 블록체인으로 이를 설계하는 것이 좋다. 이 때는 어떤 식으로 위변조를 방지할 것인지, 어떤 방식으로 네트워크를 운용하는 사람들에게 보상할 것인지를 잘 고려해서 개발해야 한다. →퍼블릭 블록체인

블록체인상의 거래 기록 및 확정 메커니즘



여러 블록체인들 중 가장 기본적인 비트코인 블록체인에서 어떻게 거래가 기록되는지 알아보자. 비트코인 블록체인은 앞에서 언급했듯이 작업증명(proof-of-work) 과정을 거쳐서 거래 기록이 확정된다. 채굴자(miner)는 네트워크상에 방송된 여러 거래들을 모아서 하나의 블록을 형성한다. 이를 증명(proof)하고 이전 블록에 연결하기 위해 채굴자는 블록의 내용을 특정값(nonce) 을 이용하여 SHA 256(Secure Hash Algorithm 256) 해시값으로 만들어 내는 과정을 거친다. 이 때 만들어지는 해시값을 시스템이 허락할 정도로 작게 만들어내는 특정값(nonce)을 찾은 경우 블록이 하나 생성되어 체인에 연결된다. 이 과정을 사용자 입장에서는 컨펌(confirmation)이라고 하며 채굴자 입장에서는 채굴(mining)이라고 부른다.

이렇게 작업증명 과정을 거쳐 체인으로 연결되어 구조화된 거래기록은 위변조하기 매우 어렵다. 이런 메커니즘에 대해 금융보안원은 다음과 같이 분석한다.

- 각 노드들에 저장된 해쉬 값은 이전 블록들의 값에 영향을 받아 생성되므로 등록된 내용을 위·변조하는 행위가 매우 어려움
- 다만, 노드의 과반수를 동시에 해킹한다면 데이터 변조가 가능하지만 현실적으로 어려움[3]

3 금융보안원, 보안연구부, '블록체인 및 비트코인 보안기술'(2015. 11. 23) 2p

위에서 설명했듯이, 거래 기록 과정에서 위변조에 대응하는 방식은 비트코인이 채택하고 있는 작업증명 외에 여러 가지 방식이 존재할 수 있다. 작업증명을 포함해 현재 실험 중인 컨센서스 및 위변조 대응방식을 5가지 정도로 추려보았다.

첫번째: Proof-of-work

이는 비트코인과 같은 공개 블록체인에서 많이 쓰이는 구조이다. 여러 거래들을 하나의 블록으로 모은다. 이 블록을 만들기위해 채굴자가 해쉬 알고리즘을 풀어서 이를 증명한다(이를 채굴이라고 한다). 증명에 성공한 채굴자는 이를 전체 블록체인 노드에 이를 중계하고 블록체인의 가장 마지막 블록에 자신이 채굴한 블록을 연결한다. 이와 같은 과정이 반복되면 여러 블록이 하나의 체인을 이루기 때문에 이를 블록체인이라고 한다. 이를 위변조하기 위해서는 proof-of-work의 과정을 한번 더 거쳐야하는데 이는 사실상 불가능하다고 볼 수 있다. 즉, 위변조를 시도하는 사람은 엄청난 컴퓨터 파워를 사용하면서도 이에 대한 혜택을 얻을 수 없기 때문에 위변조에 대한 시도를 방지하는 시스템이다.

두번째: Proof-of-stake

Proof-of-stake는 proof-of-work의 단점을 보완하기 위해 등장한 시스템이다. Proof-of-work는 전체 네트워크의 채굴을 50% 이상 독점하는 사람 혹은 단체가 있을 경우 다양한 문제들이 등장할 수 있는 구조이다. 독점한 채굴자가 수수료 상승, 고의적인 거래기록 누락등을 통해 자신의 수익을 극대화 할 수도 있는 시스템이다. 이를 극복하기 위해 proof-of-stake 구조가 제안되었다. Proof-of-stake는 소유자가 자신이 가진 자산(stake)을 스스로 증명해야 한다. 다만 proof-of-stake의 경우 nothing at stake[4]나 stake grinding[5]과 같은 공격을 받을 수 있다. 그래서 이 구조를 사용하는 Blackcoin이나 Peercoin 같은 경우 블록체인 전체를 컨트롤하는 마스터 퍼블릭키를 두어 이런 공격을 대비하고 있다.

세번째: Consensus-by-bet

Consensus-by-bet에는 Tendermint와 이더리움에서 개발중인 CASPER 등이 있다. Tendermint는 채굴 없는 방법을 지향한다. 기존의 proof-of-work, proof-of-stake가 컴퓨터파워를 활용하여 수학적으로 문제를 품으로써 거래를 승인하고 이를 통해 위변조를 방지하는 방법을 사용했다면 Tendermint는 네트워크에 참여하는 사람들의 동의를 통해서 블록체인의 거래를 승인하는 방법을 사용한다. 승인이란 제도는 어느 한 사람이나 단체가 네트워크를 독점하기 어렵기 때문에 다른 방법들에 비해 네트워크 독점에 대한 우려가 줄어들 수 있는 구조이다. 이 때 승인에 참여하는 노드들은 보증금을 걸고 승인에 참여한다. 만약 이중결제와 같이 잘못된 곳에 승인을 해줄 경우 보증금을 돌려받을 권한을 잃게 된다. 이를 통해 승인에 참여하는 사람들이 올바른 거래만 승인할 수 있도록 인센티브/처벌 시스템을 가동한다.

4 공격자가 다수의 충돌되는 블록에 투표를 하여도 처벌이 없는 경우.

5 자신의 자산을 블록체인을 거슬러 올라가 자산이 블록을 이기는 지점을 찾는다. 그 이후 그 지점 다음 블록의 헤더를 변경해서 지속적으로 자신의 블록이 이기게 조정한다. 이에는 약간의 컴퓨팅 파워가 필요하지만 꽤나 실용적인 편이다.

네번째: Trust

Trust 기반의 consensus를 활용하는 블록체인으로 Ripple, Stellar와 같은 가상화폐시스템에서 주로 사용되는 방법이다. 위에서 언급한 세가지 컨센서스 방식이 네트워크에 참여한 각 노드들이 사기, 위변조 시도를 할 수 있다는 것을 전제한 상태에서 만들어진 방법들인데 비해서 Trust를 활용한 방법은 기본적으로 네트워크에 신뢰할 수 있는 사람들이 참여한다고 전제한다. 물론 참여자들은 전체 네트워크를 믿을 필요는 없다. 다만 네트워크 상에서 참여자들은 스스로 믿을 수 있다고 판단하는 노드를 선택적으로 신뢰하면 된다. 여기서 적용되는 consensus 방식은 byzantine agreement protocol[6]을 기반으로 하고 있으며, 이는 네트워크에 참여하는 노드들의 투표와 동의를 통해서 블록체인의 거래를 승인하는 방법을 사용한다. 참여자들은 네트워크가 정상적으로 작동되기를 바라기 때문에 위변조를 시도하는 공격자의 신호를 무시하게 될 것이고 공격자는 궁극적으로 신뢰 시스템에 의해 네트워크에서 배제될 것이다. 이를 통해 네트워크에 신뢰할 수 있는 노드들만 남고 위변조를 시도하는 이용자는 지속적으로 걸러짐으로써 전체 네트워크를 튼튼하게 만들 수 있다는 가설이다. 사실상 세번째 방식인 Tendermint도 byzantine agreement protocol의 변형이라고 볼 수 있다.

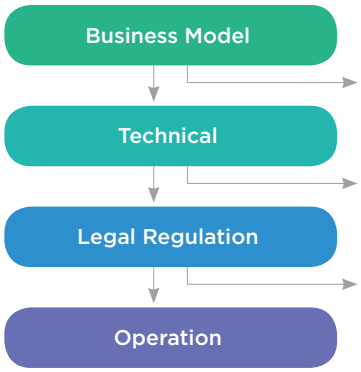
다섯번째: Membership

Membership을 활용하는 블록체인은 프라이빗 또는 컨소시움 블록체인과 같이 네트워크를 관장하는 (단수 혹은 복수의)주체가 명확할 때 사용 가능한 방법이다. 아울러 퍼블릭 블록체인과 달리 불특정 다수가 아닌 기본적으로 허가를 얻은 노드들만 승인 작업에 참여하기 때문에 이들의 행위를 계약관계 등으로 제약하는 것이 가능하다. 또한 블록체인에 접근해 공격하는 시도가 있더라도 기존처럼 데이터베이스에 침입해서 공격을 시도하는 해커를 처벌하듯 민형사상의 처벌 또한 가능하다.

6 Byzantine agreement protocol와 관련된 정보는 다음 백서를 참조
https://www.stellar.org/papers/stellar-consensus-protocol.pdf

블록체인 도입을 위한 사전 검토와 설계 체크리스트[7]

기업 및 기관들은 블록체인 도입을 결정하기 앞서서 과연 도입이 필요한지, 많은 효익을 가져다 줄 수 있는 지 자기진단 과정을 거쳐 확인할 필요가 있다. 여러 방법이 있겠지만 다음과 같은 4가지 Filter를 활용할 수 있다. 그것들은 Business Model, Technical, Legal Regulatory, Operational(BTFO)[7]의 네 영역으로 구성된다. 순서대로 네 영역의 질문들을 확인하는 비교적 간단한 방식이다.



Business Model

a. 디지털 기반인가?

i. 디지털 기반의 혹은 디지털화 된 자산에 적합하다.

b. 중개자가 끼어 있는가?

i. 당사자간에 신뢰가 필요없어도 되는 사업 모델에 적합하다.

c. 사업이 성공가능해 보이는가?

i. 이런 새로운 가치가 제안되었을때 고객들이 충분한 수수료를 낼 것으로 보이는가?

d. 거의 실시간 결제가 필요한가?

i. 지금 결제 시스템이 몇일이 걸리지만 고객, 규제당국이나 자본상의 이유로 실시간에 가까운 결제 시스템이 필요할 때 적합하다.

ii. 블록체인이 가지는 자동화 특성과 분단위의 글로벌 원장 동기화는 거의 실시간으로 결제를 할 수 있게 도와준다.

e. 투명성이 필요한가?

i. 고객이나 규제 당국이 자료의 투명성을 요구하는가?

ii. 블록체인의 분산성은 낮은 비용에 데이터를 보여주는데 적합하다.

f. 보고가 필요한가?

i. 고객, 파트너, 규제 당국에 보고를 강화할 필요가 있는가?

ii. 블록체인의 분산성은 데이터의 동기화를 값싼 비용에 가능하게 해준다.

g. 노동집약적인가?

i. 현재 자사의 프로세스가 수동이거나 반자동이여서 비싼가?

ii. 블록체인은 완전한 자동화를 가져오기 때문에 장기적으로 비용을 절감하는 효과가 있으며, 만약 언젠가 자동화를 도입할 예정이라면 블록체인을 통한 자동화가 더 저렴하다.

7 Alex Batlin “Crypto 2.0 Musings - Blockchain Disruption Evaluation” (2016. 1. 11)

a. 자본집약적인가?

i . 결제일의 지연, 운영상의 이유로 자본이 묶여있는가?

i . 거의 실시간으로 결제를 가능하게 해주는 블록체인은 이런 자본의 묶임을 줄여줄 수 있다.

b. 레거시 기술이 많은가?

i . 현재의 데이터 저장, 관리, 계산 기술이 복잡하고 오래되었는가?

i . 만약 이 기술들을 업그레이드 할 필요가 있다면 블록체인을 활용하여 더 강하고 저렴한 기술적 효과를 고려해봄직하다.

2.Technical

a. 기술적으로 성공가능해 보이는가?

i . 현재의 시스템 요구사항이 블록체인 기술을 감당할 수 있는가?

b. 거래정보를 얼마나 암호화 할 것인가?

i . 현재 퍼블릭 블록체인은 거래가 일어났음은 확인할 수 있지만 어떤 사람들끼리 했는지는 그 암호화 메커니즘으로 인해 확인할 수 없다.

c. (Public인경우)너무 처리량이 많지는 않는가?

i . 만약 퍼블릭 블록체인을 활용할 예정이라면 현존하는 퍼블릭 블록체인의 처리속도가 아직 충분히 많지 않다는 것을 알아야한다.

d. (Public인 경우)초저지연 처리가 불필요한가?

i . 퍼블릭 블록체인을 활용할 예정이라면 현존하는 퍼블릭 블록체인중에 비트코인의 경우 10분의 딜레이가 있을 수 있음을 알아야한다.

3. Legal Regulatory

a. 법률 규제가 있는가?

i . 법률상의 합의 및 허락을 받을 필요가 있는가?

i . 블록체인의 스마트 계약의 데이터 동기화, 암호화, 순차적인 기입은 회계 추적 및 법률 준수에 적합하다. 만약 이런 사항들을 도입할 필요가 있다면 블록체인을 도입하는 것이 비용적으로 저렴하다.

4. Operational

a. 통합이 잘 되어 있는가?

i . 만약 현존하는 시스템이 잘 통합되어 있다면 그 시스템에는 블록체인을 적용하지 않는 것이 좋다.
우선은 독립되어있고 다른 시스템, 비지니스에 영향을 받지 않는 사업에 우선적으로 블록체인을 도입하는 것이 좋다.

위의 네 가지 렌즈를 통해 블록체인 도입의 필요성을 확인했다면, 다음과 같은 요소들을 고려하여 블록체인 디자인을 시작할 수 있다.

블록체인 설계를 위한 체크리스트[8]

	설명	비트코인의 경우
데이터(블록) 크기	블록 크기 및 컨펌주기는 작고 빠를 수록 이용 환경이 용이한 측면이 있지만, 너무 잦은 주기는 보안상의 문제를 초래할 수 있고, 블록 사이즈가 너무 작아지면 처리량이 제한될 수 있다.	1MB, 초당 7건
거래 참여자	누구에게 거래 기록을 제출(기입)할 수 있도록 권한을 줄 것인가?	모든 사람
거래 기록 열람자	누구에게 거래 기록을 열람할 수 있도록 권한을 줄 것인가?	모든 사람
거래 승인 권한	누가 거래를 승인할 것인가, 누가 네트워크를 운용할 것인가?	채굴자
블록 생선 권한	누가 블록을 생성할 권한을 가지는가, 어떤 원칙으로 기회를 분배하는가?	채굴자 경쟁
승인 방식을 무엇으로	PoW, PoS 등	PoW, 긴 체인 우위
보상	블록 생성, 거래 승인, 블록 데이터 보관	블록내 모든 수수료+25BTC
벌칙	배반 행위 및 실수	사용된 컴퓨팅 파워 및 전력의 낭비
자체 화폐 발행 여부	Native Coin을 발행할 것인가?	비트코인(BTC)
컨센서스 방식	블록이 갈라질 경우 어떤 블록에 정통성을 부여할 것인가?	긴 체인 우위
룰 개정 방식	룰을 개정할 수 있는가? 어떤 과정과 방식을 통해 개정할 것인가?	커뮤니티의 동의

8 http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/ 의 내용을 재가공

Block Chain Primer

블록체인의 기술적 이해 및 도입을 위한 첫걸음

발행일 : 2016년 3월 24일

버젼 : 1.0

발행처 : (주)코빗

집필 : 김진화, 정명호, 김재모, 유영석

문의 : info@korbit.co.kr