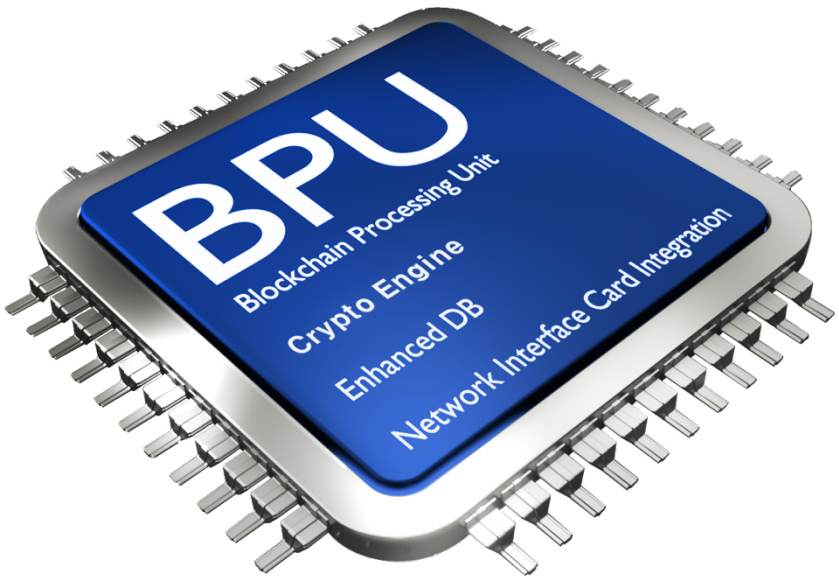
MEDIUM

MEDIUM

4th GENERATION BLOCKCHAIN

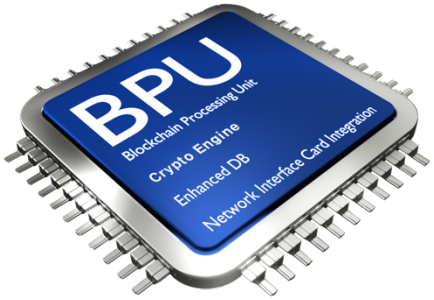
H/W BLOCKCHAIN PLATFORM & BPU TECHNOLOGY

POSITION PAPER | VERSION 1.0



Contents

Abstract



4th GENERATION BLOCKCHAIN

H/W BLOCKCHAIN PLATFORM & BPU TECHNOLOGY

2008년 사토시 나카모토의 논문을 통해 처음 세상에 공개된 비트코인은 현재 중앙은행이 존재하지 않는 탈중앙화 된 "법정 통화 대체수단"이라는 기대감으로 세계적인 관심을 받았다. 이러한 탈중앙화의 성립요건에는 핵심기술인 "블록체인"이 존재하며 블록체인은 비트코인에 대한 경제적가치와 더불어 4차 산업을 선도하는 기술이라는 인식이 지배적이다. 이에 따라 전 세계적으로 다양한 국가와 기업들이 기존의 산업과 블록체인을 융합하려는 시도가 증가하고 있다.

하지만 현실적으로 현재의 블록체인기술은 엔터프라이즈 시스템에서 필요한 초당처리속도 즉, TPS (Transaction Per Second)를 충족하지 못하는 수준으로 기존의 네트워크 서비스에 비해 낮은 데이터 처리속도를 기록하고 있다. 따라서 지금의 블록체인 기술은 높은 사회적 기대감과 요구에 비해 거둬들인 성과는 매우 미진한 상황이라 할 수 있다.

우리는 블록체인이 가지고 있는 성능적 한계를 극복하고자 지금까지의 블록체인 플랫폼을 지향하는 많은 연구들이 소프트웨어 아키텍처와 알고리즘 개선을 통한 성능향상을 추구하는 일반적인 방법이 아닌 블록체인 전용의 독자적인 H/W를 설계하고 핵심적인 기능을 수행하는 BPU(Blockchain Processing Unit)를 자체적으로 개발하여 상용화 수준의 엔터프라이즈 전용 블록체인 플랫폼을 구축하고자 한다. 이와 같은 접근방법을 통해 구현된 MEDIUM 블록체인 플랫폼 상에서 구동되는 서비스는 초당 수 십만 건 이상의 트랜잭션의 처리속도를 보장받게 될 것이다. 이 문서를 배포하는 2019년 7월 현재 자체적인 개발 환경을 통해 100,000 TPS를 구현하였으며 그 수치는 지속적으로 발전하고 있다.

MEDIUM은 상용화 수준의 엔터프라이즈 서비스를 위한 블록체인 플랫폼을 구축하기 위해 기존 엔터프라이즈 시장의 De Facto Standard인 Hyperledger Fabric과 상호운용성(Interoperability)을 보장한다. 이를 통해 글로벌 엔터프라이즈 시장의 접근성을 용이하게함과 동시에 Hyperledger의 검증된 소프트웨어 사양과 다양한 라이브러리를 함께 제공함으로서 전세계의 다양한 블록체인 서비스를 개발하고 있는 개발자들에게 안정성과 편의성을 보장하고자 한다.

이와 함께 MEDIUM 코인을 한정 개수로 발행하여 향후 여러 서비스와 솔루션들이 MEDIUM 블록체인 플랫폼을 이용함에 따라 발생할 수 있는 플랫폼 이용 수수료로 사용할 수 있다. 또한, MEDIUM 블록체인 네트워크 안에서의 소비, 마켓플레이스의 등록 보상비, 솔루션의 거래 등 MEDIUM Token Economics 전반에 활용될 예정이다.

우리는 비트코인, 이더리움, 이오스 등을 비롯한 전세계의 다양한 블록체인 연구 과제들이 소프트웨어의 성능개선에만 몰두하는것과 근본적으로 다른 방식으로 접근하여 새로운 혁신과 획기적인 성과를 낼 수 있다고 확신한다. 이를 통해 기존에는 불가능했던 엔터프라이즈 기반 블록체인 서비스 모델의 성공사례들이 MEDIUM을 통해 실현되기를 희망한다.

01 Introductions

1) 블록체인의 등장과 엔터프라이즈 적용 가능성

2008년 세상에 비트코인이 공개된 이래로 전세계 다양한 국가와 기업들이 비트코인의 핵심기술인 블록체인을 다양한 산업영역에 적용해보고자 하는 연구와 노력을 지속하고 있다. 중앙시스템이 존재하지 않는 화폐 거래의 가능성을 확인한 글로벌 ICT 산업계는 이른바 "탈중앙화"의 기술적, 산업적 가치에 열광하였고, 거래정보 뿐만 아닌 데이터를 저장하고 전달하는 모든 방식에 있어 블록체인 기술을 활용하고자 하는 시도가 이어지고 있다. 가용성(Availability)과 기밀성(Confidentiality)이 강화된 정보시스템환경에서 정보주권의 탈중앙화 (Decentralization)가 이루어지며 분산 기록된 데이터가 무결성(Integrity)까지 보장받을 수 있다면 곧 현실화될 4차산업혁명에 있어 블록체인 기술은 모든 산업분야에 반드시 필요한 필수 기술이 될 것이다.

현재 기업의 IT 환경은 여러 기준에 따라 나누어져 있는 경우가 대부분이다. 기업 내에서도 계열사 혹은 사업본부, 부서에 따라 시스템을 별도로 구축하는 경우도 있다. 여기에 보안절차를 더하면 부처 간 데이터를 주고받는 과정에 수 많은 절차가 생성되며 기업 내·외부적으로 데이터를 교환할 때 신뢰 가능한 제3의 주체가 필요하다. 이러한 예시를 통해 데이터 교환의 측면에서 기업 시스템과 금융 시스템은 유사한 구성을 가지고 있는 것을 확인할 수 있으며 금융시스템이 비트코인의 등장으로 "탈중앙화"의 가능성을 확인한 것과 같이 기업 시스템 즉, 데이터 이동 또한 "탈중앙화"의 적용 가능성을 확인할 수 있다.

데이터를 교환하고자 하는 주체들에게 데이터가 암호화되어 분산 저장되고, 누가 어떠한 목적으로 데이터를 가져갔고 어디에 사용했는지를 분산 원장에 기록한다면 기존과 같이 제3자 시스템의 개입 없이 통합 시스템을 구축할 수 있다. 이는 현재 조직 간의 신뢰 문제로 인해 분산된 여러 시스템을 효과적으로 통합하여 비용을 절감할 수 있도록 해줄 것이며, 나아가 데이터가 중복되는 문제와 데이터를 요청하고 전달받는 과정에서 발생하는 시간을 혁신적으로 단축할 것이다.

더 나아가 이러한 데이터들이 저장된 블록체인을 하나의 엔터프라이즈형 데이터 플랫폼으로 구성한다면, 기존 솔루션의 통합하는 과정의 호환성 문제도 해소할 수 있다. 해당 플랫폼 위의 솔루션들이 참조하고자 하는 데이터는 아래 데이터 플랫폼 계층에 블록체인으로 저장되어 있고, 솔루션은 해당 데이터를 요청함으로써 읽기/쓰기 작업을 수행할 수 있게 구현된다. 그렇다면 데이터의 중복 문제가 원천적으로 사라지게 되며, 나아가 데이터를 솔루션 상에서 교환할 필요마저 없어지기 때문에 기존의 통합 프로젝트 자체를 대신할 것으로 전망된다.

이러한 기대감에 기반하여 기존 기업형 솔루션을 제공하는 업체들 중 IBM이 가장 먼저 블록체인에 관심을 보였으며 아파치 재단과 함께 하이퍼레저 재단을 공동 설립하고 하이퍼레저 패브릭을 공개했다. 연달아 Microsoft, Oracle, SAP 등도 블록체인 관련 기술개발에 착수하였고 서비스를 출시하였다.

2) 블록체인 플랫폼은 누구를 위한 것인가?

대표적인 암호화폐 정보포털 Coinmarketcap.com에 따르면 현재 약 2500여개의 블록체인 프로젝트가 등록되어 있으며 전체 약320억 달러의 시가총액을 집계하여 보여주고 있다. 블록체인 기술에 기반하여 독자적인 암호화폐 생태계를 구축하고자 하는 플랫폼 프로젝트도 수백여 가지에 이르지만 독자적인 플랫폼을 지향하는 것이 아닌 독창적인 암호화폐 비즈니스 모델을 블록체인 기술로 구현하고 있는 수천 여개의 분산화 앱 서비스 프로젝트들도 어렵지 않게 찾아볼 수 있다. 이는 전세계 각국에서 진행중인 다수의 블록체인 관련 프로젝트 중 극히 일부를 대표하고 있을 뿐이며 지금 이 시간에도 각자의 영역에서 새로운 가치를 창출하고자 수많은 연구들이 진행되고 출시되고 있다.

그렇다면, 이와 같이 새로운 IT 빅뱅과도 같은 블록체인 산업에서 진정한 의미의 플랫폼은 누구를 위하여 연구되고 천문학적인 투자가 진행되고 있는가?

플랫폼은 독립적으로 존재할 수 없으며 누군가 플랫폼위에서 기능을 제공하는 시스템을 제공할 때야 비로소 플랫폼으로서 가치를 실현할 수 있다. 블록체인 플랫폼이란 초고속 통신이 가능한 인터넷 네트워크 망 위에서 서비스될 수 있는 모든 형태의 시스템이 적용될 수 있어야 하며 어떤 형태의 서비스라도 블록체인의 특성을 활용하여 서비스를 구현하고자 한다면 서비스 제공자가 블록체인 시스템을 구현하기 위해 필요한 모든 기술을 개발하고 연구할 수고로움과 시간, 비용을 줄여줄 수 있어야 한다는 것이다.

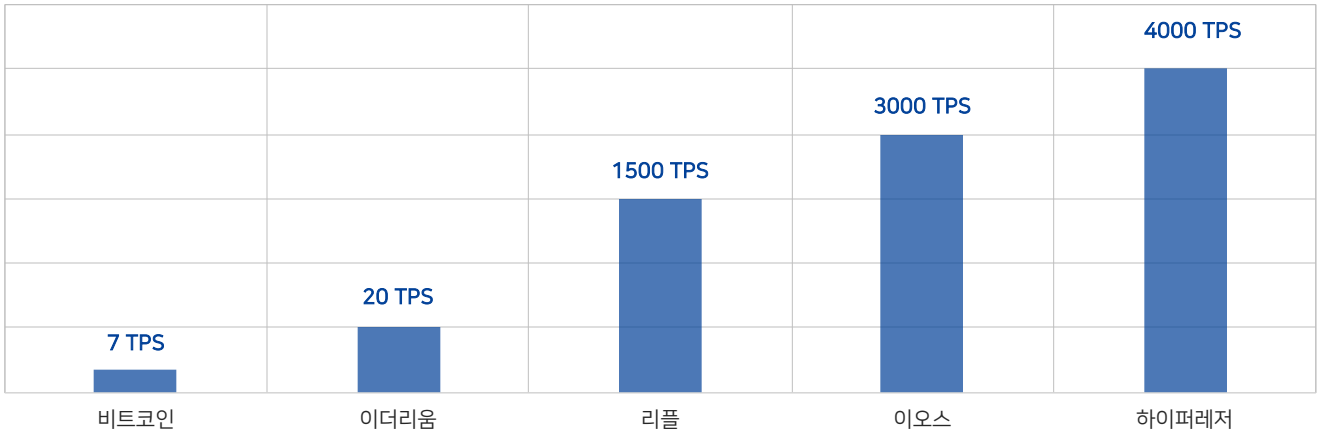
3) 현재까지의 블록체인 문제점

(1) 블록체인의 성능 문제

앞서 기술한 블록체인의 엔터프라이즈 적용가능성으로 전세계의 사람들에게 블록체인은 “The Next Cloud” 또는 “4차 산업혁명의 핵심기술”이라는 인식을 주었지만 실제 산업분야에서 완벽하게 적용되는 사례를 찾기는 아직 힘들다고 할 수 있다. 데이터를 분산 원장에 기록하기 위하여 높은 컴퓨팅 파워와 네트워크 트래픽을 기존 시스템보다 훨씬 많이 사용함에도 불구하고 엔터프라이즈 시스템에 적용하기에는 여러 제한적인 요소들이 있기 때문이다. 그중 가장 큰 원인은 바로 현저하게 느린 블록체인의 데이터 처리 성능에 있다.

시스템의 중단이나 속도 저하 현상이 비즈니스에 크게 영향을 줄 수 있는 기업 환경의 특성상, 기업들은 통상 일정 수준의 SLA(Service Level Agreement)를 요구한다. 그 중 대표적인 지표가 TPS(Transaction Per Second)이고, 이는 기업 내의 특정 시스템이 여러 사용자들로부터 대량의 작업을 동시적으로 요청할 때에도 속도 저하 없이 안정적인 응답시간을 보장하기 위한 기본적인 측정 지표가 된다.

이오스를 제외한 비트코인과 이더리움의 TPS는 100에도 미치지 못하는 반면, 기업들이 원하는 TPS 수준은 이에 비해 상당히 높은 편이다. VisaNet의 경우 평균 2,000TPS 정도가 사용되고 있지만, 사용자가 급속도로 증가하는 경우를 대비하여 56,000TPS를 요구하고 있으며[1], 중국 내 사실상 표준 결제시스템으로 자리 잡은 알리바바는 이미 수십만의 TPS를 수용하기 위한 프로젝트를 진행중에 있다[2].



[그림01] 비트코인, 이더리움, 리플, 이오스 TPS

1) visa-fact-sheet-Jun2015 at https://usa.visa.com

2) https://www.alibabacloud.com/blog/when-databases-meet-fpga-achieving-1-million-tps-with-x-db-heterogeneous-computing_594147

위의 사례만 보더라도 현재의 블록체인은 기업의 TPS 요구사항에 현저히 미치지 못하고 있으며 블록체인을 기술산업 현장에 적용하려는 연구기관과 기업에서는 이를 개선하기 위해 다양한 방법론들을 연구하고 있지만 뚜렷한 방안을 찾지 못하고 있다.

더욱이 블록체인은 단순한 분산 원장의 개념을 넘어서 스마트 컨트랙트 등의 응용 분야가 넓어지면서 TPS의 개선에 대한 관심은 더욱 커지고 있다. EOS와 같은 일부 프로젝트는 기존 이더리움보다 최소 28배 빠를 뿐 아니라 100만 TPS를 목표로 추가 개발할 것이라고는 하나, 아직 수천 TPS수준이고, 기업에서 필요한 Private망 등 데이터 Ownership에 대한 제어가 근본적으로 어렵기 때문에 엔터프라이즈용 플랫폼으로는 적합하지는 않다.

그렇다면 과연 블록체인 플랫폼의 구체적으로 어떤 부분이 얼마만큼의 지표에 도달해야 고성능의 플랫폼으로 평가될 수 있는 것인지에 대해서 우리 MEDIUM은 많은 사례 조사와 분석을 통해 다음과 같은 항목들을 제시하게 되었다.

(2) 블록체인 플랫폼의 성능 평가기준

블록체인 플랫폼의 성능을 표현하는 대표적인 정량 지표로 TPS(Transaction per Second)를 대표적으로 거론하는데 이는 초당 처리되는 트랜잭션의 수치를 집계한 지표이다. 하지만 최근 이는 블록체인 플랫폼이 처리해야하는 다양한 기능에 비해 단편적으로만 평가되는 지표라는 관점이 지배적이다. 따라서 다양한 측면에서 성능을 측정할 때 분석해야 하는 항목을 다음과 같이 제시한다.

구분	항목	설명
트랜잭션	초당 트랜잭션 처리 개수 - TPS	1초 동안 실행을 완료하여 기록되는 트랜잭션의 개수
스마트 컨트랙트	초당 스마트 컨트랙트 체결 개수	1초 동안 스마트 컨트랙트를 실행을 완료하여 블록에 기록하는 개수
	초당 병렬적으로 처리 가능한 스마트 컨트랙트 체결 개수	병렬적으로 각기 다른 스마트 컨트랙트 실행을 요청하였을 때 1초 동안 동시에 실행할 수 있는 스마트 컨트랙트의 개수
확장성	노드의 최대 증가분(Target TPS Fixed)	요구되는 TPS가 Fix된 상황에서 노드의 개수를 얼마만큼 증가시킬 수 있는지를 측정
	노드 증가분에 따른 합의 알고리즘 처리 개수	노드의 물리적 수가 증가함에 따라 단위 시간 동안 최종적으로 합의알고리즘이 체결되는 전체(Throughput) 수치를 측정
	노드 증가분에 따른 합의 알고리즘 처리 속도	노드의 물리적 수가 증가함에 따라 요청된 합의 알고리즘 별 처리 속도를 측정
응답시간	트랜잭션 응답시간	End-point(Web, App I/F)에서 트랜잭션을 요청하여 처리 완료되는 응답시간을 측정

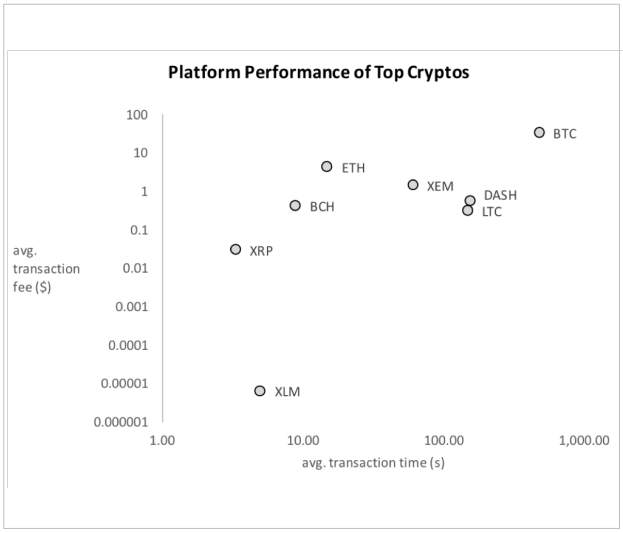
[표01] 블록체인 플랫폼 성능분석 평가기준 by MEDIUM

(3) 블록체인 플랫폼의 비용문제

블록체인 성능의 문제와 함께 쉽게 거론되는 쟁점이 바로 블록체인 플랫폼의 이용에 따른 비용문제가 있다. 전세계적으로 사용되어 왔던 해외 송금의 비싼 수수료의 문제의식에서부터 고안된 비트코인 시스템이지만 아이러니하게도 비트코인 네트워크를 활용하여 개발된 송금시스템은 비트코인 네트워크의 과부하와 병목구간에서 기존 중앙화 시스템을 이용할 때보다 훨씬 더 비싼 수수료를 부담해야하는 상황이 직면하게 된다.

이는 비단 비트코인에만 해당되는 문제는 아니며 이더리움, NEM, DASH 등 비교적 초창기에 등장한 블록체인 플랫폼들은 높은 네트워크 수수료 정책으로 생태계 확장에 어려움을 겪고있는 것이 사실이다.

비싼 네트워크 수수료 정책은 일차적으로 플랫폼을 활용하여 서비스를 개발하고자 하는 개발자에게 부담을 주는 것은 물론이고 비용을 줄이기 위해 별도의 미들웨어를 두거나 복잡한 UX를 설계하게 되는데 이는 고스란히 사용자의 불편함과 시간을 소비하게 함으로 새로운 문제점을 야기하는 것에 봉착하게 된다. 이러한 문제를 해결하기 위해 네트워크 병목현상을 개선하고자 추가적으로 노드를 증설하고 합의알고리즘을 개선하는 노력이 이루어 졌지만 그에 따른 총 비용의 투입은 획기적인 총 비용 절감으로 연결 되지는 못했다.



[그림02] Transaction fee by avg. TPS of Top Cryptos[3)]

비교적 진보된 형태의 블록체인 플랫폼을 지향하면서 등장한 EOS, Tron 등에서는 “수수료가 없는 모델”을 지향하면서 시스템을 개발하였지만 각각의 플랫폼 기반의 상용서비스가 수 천 ~ 수 만명의 사용자에게 트래픽을 제공하기 위하여 원활한 트랜잭션 처리 대역폭을 확보하여야 하고 그 과정에서 많은 양의 플랫폼 토큰을 홀드하고 있어야 한다.

전화선을 기반으로 데이터 통신이 도입되었을 당시 음성 통화만 가능하던 시대를 PC가 연결되는 시대로 변화를 가져왔고 문자로 통신하는 혁신을 이루었지만 비싼 통신요금으로 일반인들은 인터넷 서비스라는 것을 경험할 수 없었다.

하지만, 초고속 통신망 기술이 빠르게 도입되고 보편화되면서 이제 더이상 인터넷 자체를 비싼 유료서비스라 인식하지 못한다. 때문에 초고화질의 실시간 중계, 개인방송, 멀티채널 등의 다양한 콘텐츠 서비스가 시대흐름을 바꾸고 있는 것이다. 블록체인 또한 플랫폼으로서 자리매김하기 위하여 높은 처리 성능을 보장하고 공공재에 가까운 비용수준을 달성한다면 트랜드를 이끌고 시대를 주도하는 신개념의 분산화 서비스들이 보편화 될 것이라 본다.

4) 왜 블록체인 플랫폼은 고성능 이어야 하는가?

MEDIUM은 블록체인 플랫폼이 가져야 할 여러 특징 중 무엇보다도 성능을 우선시하고 강조하고 있다. 네트워크 리소스를 특정 기관의 정책과 제한없이 자유롭게 전세계 어느 곳에서든 언제든지 자유롭게 이용하고 확인할 수 있는 탈중앙화의 가치가 극대화 되기 위해서는 동시에 여러 서비스가 원활히 동작할 수 있어야 하며 수 백, 수 천명 만을 위한 국지적 서비스가 아닌 수백만 수천만 명 이상의 사용자들이 국경과 시공간의 제약 없이 사용할 수 있는 글로벌 스케일의 서비스여야 하기 때문이다.

3) https://www.stellar.org/blog/Q1-2018-stellar-and-state-of-crypto/

5) 블록체인 플랫폼 성능 향상을 위한 업계의 노력

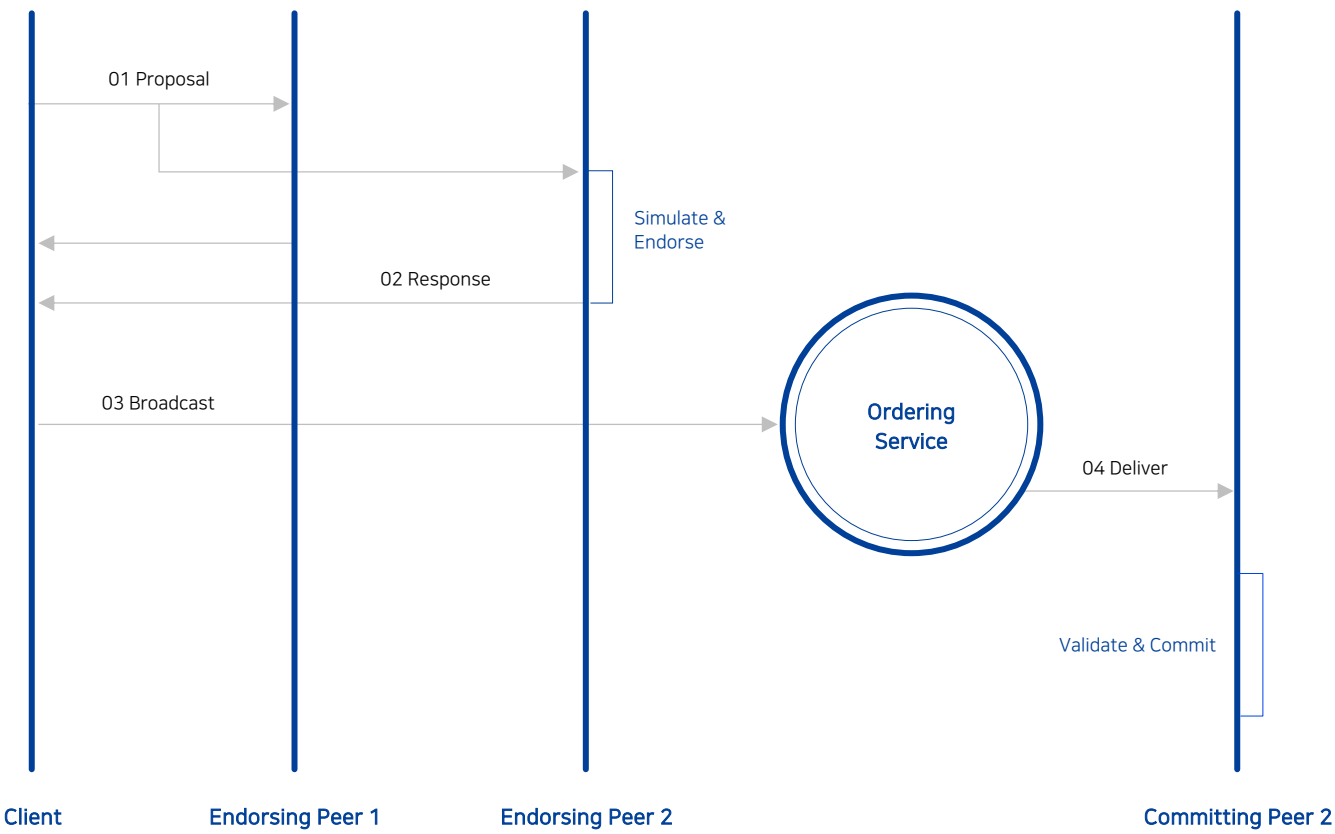
(1) 허가형(Permissioned) 블록체인 플랫폼

블록체인의 성능을 고도화 함에 있어 가장 첫번째로 언급되는 요소중의 하나가 블록체인의 제공 형태이며 퍼블릭, 프라이빗, 하이브리드, 사이드체인등의 다양한 제공 방식이 제안되고 있지만 플랫폼의 노드 참여 기준이 명확하고 일관된 허가형(Permissioned) 블록체인이 성능 제고 측면에서 가장 효율성이 높다는 연구들이 여러 블록체인 연구기관의 논문으로 발표되었다[1].

이와 같은 연구는 기업 또는 기관 등 특정 독립된 기관 전용의 특수목적의 블록체인 플랫폼 개발을 위하여 설계되고 있으며 Hyperledger, EEA, JP Morgan Quorum, R3 등이 있다. 이중 IBM에서 Apache 재단을 통해 연구를 주도하고 있는 Hyperledger Fabric은 현재 사실상의 엔터프라이즈 시장의 De Facto Standard로 자리매김하고 있다.

(2) Hyperledger 기반의 성능개선 연구사례 - Fast Fabric

Hyperledger Fabric를 기반으로 상용화 플랫폼을 구축하는 사례가 잇따르면서 트랜잭션 처리량 및 확장성에 있어서 제한이 있다는 점이 쟁점화 되었고 Hyperledger Fabric 기반의 플랫폼의 성능을 개선하고자 여러 연구가 진행되는 가운데 기존 Transaction Flow에서 핵심적으로 언급되는 성능 제한 원인을 토대로 4가지의 성능개선 방안으로 수렴하는 연구사례[4]를 확인할 수 있었다.



[그림03] Hyperledger Fabric의 Transaction Flow [2]

4) Fast Fabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second

성능향상 제한 요소	해결방안
데이터와 메타 데이터의 분리	Transaction Ordering 프로세스 재설계를 통해 Tx ID만으로 처리하여 처리량 증가
병렬 처리 및 캐싱	Transactions 유효성 검사를 일부 병렬처리하거나 데이터 캐싱을 통해 전체 처리량 증가
계층적 메모리 구조를 활용한 데이터 엑세스 방식 개선	더 중요한 트랜잭션 데이터에 빨리 액세스가 가능하도록 데이터 관리 레이어를 재설계하여 최적화
자원관리 아키텍처의 변형	Committing Peer와 Endorsing Peer 간의 역할을 분리하는 아키텍처의 변형을 통해 성능 개선

[표02] Diagnostics Cases of Fast Fabric Study

6) MEDIUM의 제안

MEDIUM은 상용 엔터프라이즈 시장의 요구사항에 대응하기 위한 블록체인 플랫폼으로, 상용 엔터프라이즈 수준의 고성능 및 초고속의 블록체인 시스템을 보장할 것이며 또한 그에 적합한 솔루션과 더불어 기존 블록체인 시장과의 통합성을 동시에 제공하고자 한다.

이를 위해 MEDIUM은 트랜잭션 처리를 위한 명령어 수행과 블록 생성을 위한 스레드를 동시 처리하기 위한 병렬화 기술이 적용된 블록체인 컴퓨팅 전용 하드웨어 BPU(Blockchain Processing Unit)를 개발했다. BPU는 블록체인의 주요 기능들을 독립적으로 수행하기 위하여 하드웨어가 모듈별로 구성되어 있으며, 블록체인 플랫폼의 처리 성능을 혁신적으로 올려주는 MEDIUM의 기술이 집약된 결과물이라 할 수 있다.

BPU는 블록체인에서 속도 지연 현상의 주요 원인이 되는 병목 구간과 복잡한 구조의 처리방식을 모듈화하고 효율적으로 처리하도록 설계되었다. 또한, MEDIUM 블록체인은 현재 프라이빗 블록체인 시장의 De Facto Standard인 Hyperledger Fabric의 아키텍처를 벤치마킹하여 새롭게 설계하였으며, H/W와 CPU를 가장효율적으로 사용하는 언어인 C++로 Hyperledger Fabric을 BPU 상에서 처리할 수 있도록 완전 재구성함으로써 이론상 구현 가능한 가장 빠른 속도를 MEDIUM BPU로 실현시키고자 한다.

본 문서를 배포하는 시점인 '19년 7월 현재 측정 결과 약 100,000 TPS를 확인했으며 이러한 성능 측정 결과를 연구개발 분야에서 MEDIUM과 협업중인 인증 전문기관에서 공식적인 성능수치를 측정하여 그 결과를 공시할 예정이다.

7) MEDIUM 블록체인의 정책과 방향성

MEDIUM 블록체인 플랫폼은 초고속의 성능을 보장하기 위하여 다음과 같은 정책과 방향성을 기반으로 기술을 구현해 나가고자 한다.

(1) H/W Oriented Improvement with BPU Enhancement

블록체인 플랫폼이 구동되면서 트랜잭션을 생성하고 처리하는 과정 및 스마트 컨트랙트가 생성하고 처리하는 과정에서

많은 병목현상과 처리지연 현상이 발생한다. 이러한 현상은 요청된 프로그램의 명령을 처리하는 소프트웨어의 구조적인 부분도 있지만 범용 목적으로 설계된 일반 컴퓨터의 CPU 및 메모리 구조에서 처리하는 방식은 당연히 발생할 수 밖에 없는 속도 지연 현상의 근본 원인이라 할 수 있으며 현재 이와 같은 현상은 모든 블록체인 플랫폼 제공자가 동일하게 직면하는 문제이다. MEDIUM은 이에 블록체인 플랫폼에 특화된 기능과 명령 처리 구조에 최적화된 형태의 BPU를 직접 독자적으로 설계, 개발하여 전체적인 플랫폼의 처리 성능향상을 구현해 나가고자 한다.

(2) Permissioned Blockchain: Consortium Blockchain

MEDIUM 블록체인은 초고속의 처리성능을 보장하기 위하여 블록체인 노드 참여에 특정한 기준을 제시하고 일부에게만 노드를 참여할 수 있는 권한이 부여되는 허가형(Permissioned) 블록체인 네트워크를 구축하고자 한다. MEDIUM이 제시하는 기준에 부합하고 전세계 각 대륙을 대표할 수 있는 노드 운영 기관이 선정될 것이며, 각 대륙 별 대표 기관들의 Consortium이 구성되어 MEDIUM 블록체인 플랫폼이 구축될 것이다.

(3) MEDIUM Appliance® use exclusively

MEDIUM 블록체인 플랫폼에 노드로서 참여하거나 MEDIUM 기반으로 별도의 플랫폼을 구축하고자 할 경우 MEDIUM에서 자체적으로 개발한 MEDIUM 전용 H/W 장비를 반드시 사용하는 것을 원칙으로 한다. MEDIUM H/W 장비는 MEDIUM BPU의 성능을 극대화 시키도록 별도 설계/개발된 전용 Chipset, Board가 종합되어 만들어진 하드웨어 장비이며 MEDIUM 블록체인의 운영체제와 소프트웨어 아키텍처가 실행될 수 있는 최적의 환경을 보장한다. 만약 MEDIUM 블록체인 플랫폼의 소프트웨어 패키지만을 일반 Intel 계열의 PC나 서버 또는 기타 머신에 적용했을 경우는 정상동작하지 않을 수 있으며 원활한 성능을 보장받지 못하게 될 것이다.

(4) Large Bandwidth permissioned Network Environment: Co-location Service

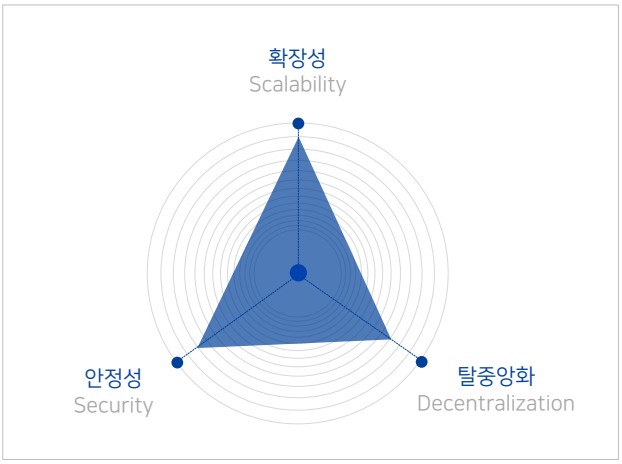
MEDIUM Consortium Network에 참여한 노드 장치들은 모두 백본망(Backbone network)에 최대한 근접해 있고 초고속 인터넷 망을 항시 쾌적하게 이용할 수 있는 데이터센터에 입고되어 운용될 예정이다.

최근의 국내를 비롯한 전세계 각국의 데이터 센터는 하루 24시간 1년 365일 무중단, 무정전, 항온, 항습은 물론 고품질의 장애 대응 및 모니터링 시스템을 갖추고 있고 매우 엄격한 조건하에 관리되고 있다. 엔터프라이즈급의 성능을 보장하기 위한 플랫폼의 성능을 제공하기 위해 고대역폭의 네트워크 환경을 보장하는 것은 매우 필수적이며 초고속 블록체인 플랫폼의 필요충분 조건이라 판단하고 있다.

8) MEDIUM 블록체인의 아이덴티티

앞서 언급했던 바와 같이 우리는 블록체인 플랫폼을 상용화 수준의 엔터프라이즈 시스템으로 구현하고자 플랫폼 구현에 필요한 모든 시스템을 H/W 단계에서부터 Backbone 연동 구조에 이르기까지 직접 재설계하고 최적화하여 플랫폼의 성능을 극대화 시키는데 집중한다.

MEDIUM 블록체인은 TPS로 단편화된 처리능력과 확장성(Scalability)의 향상만을 추구하는 것이 아닌 탈중앙화(Decentralization), 안정성(Security) 또한 보장될 수 있는 통합적 기술 구현을 목표로 한다.



[그림04] MEDIUM Blockchain Trilemma Goal

9) MEDIUM 블록체인의 최종목표

MEDIUM Blockchain은 앞서 블록체인 플랫폼의 본질에 대해서 깊게 고찰하면서 누구를 위하여 플랫폼을 상용화하는지, 누구를 위하여 기술을 고도화 해야 하는지에 대해 이미 잘 알고있다.

본 문서가 작성중인 2019년 상반기에는 아직 일반 대중에게 보편화된 블록체인 기반의 분산화 서비스는 없다고 하지만, 앞으로 블록체인 기술과 네트워크 기술이 진화를 거듭하게 될 것이고 탈중앙화 네트워크 서비스가 보편화(Generalization) 된다면, 또한 암호화폐가 생활 밀착 서비스에 범용화(Commoditization) 된다면, 그것은 우리 MEDIUM과 같은 발상과 접근방법의 전환을 통하여 진화를 거듭한 기술들이 가져온 결과일 것이라 생각한다.

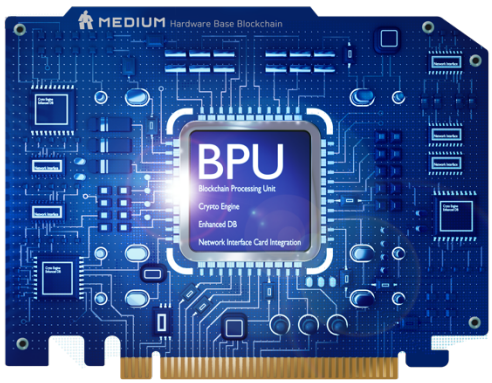
앞으로 보편화될 전세계의 수 천, 수 만의 블록체인 서비스 개발 프로젝트를 위하여 MEDIUM은 최종적으로 1Million TPS를 구현하는 것에 목표를 두고있으며 이는 가장 빠른 플랫폼의 성능과 가장 저렴한 비용을 보장하는 것을 상징하는 대표적인 지표가 될 것이다.

또한, 전세계의 개발자들이 쉽고 빠르게 MEDIUM 네트워크에 접근하여 자신들의 아이디어를 실현시키는데 최적화된 도구를 제공할 것이고 원하는 목표를 달성하기 위한 최적의 환경을 제공할 것이다. 그로 인하여 진정한 의미의 탈중앙화 가치를 전세계 IT 산업에 뿌리내릴 수 있게 하는데 공헌하고자 한다.

02 MEDIUM의 기술 핵심

1) BPU (Blockchain Processing Unit)

BPU는 MEDIUM에서 전세계 최초로 개발한 블록체인 플랫폼을 위한 하드웨어 정보처리장치이다. BPU는 Crypto Engine, Enhanced DB, SC Engine, NIC Engine 모듈로 구성되어 있으며 이는 블록체인 플랫폼에서 반복적으로 수행하는 동작 형태를 묘듈화하였고 각 모듈 파트별로 데이터 처리 패턴의 특징에 맞게 구조가 설계되어 동작된다. 이와 같은 패턴 모듈화 설계 방식은 기존 범용 목적으로 설계된 CPU에서 동작하는 데이터 연산과 메모리 컨트롤 메커니즘 상에서 발생할 수 밖에 없는 병목현상을 근본적으로 개선할 수 있으며, 통상적으로 블록체인 플랫폼에서 발생되는 트랜잭션 데이터와 스마트 컨트랙트 데이터 등의 데이터 패턴에 맞게 최적화되었다.

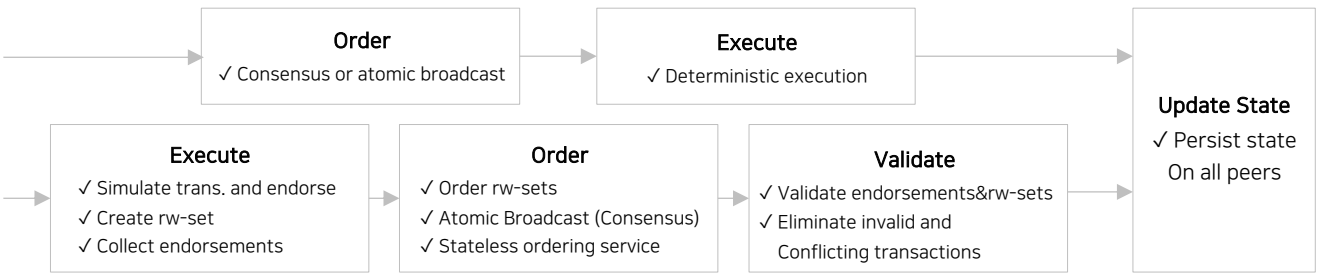


[그림05] MEDIUM BPU (Blockchain Processing Unit)

이러한 BPU는 전세계적으로 처음 시도되었고 수 천개가 넘는 블록체인 연구들과는 근본적으로 다른 방법으로 블록체인 기술을 고도화 하는 연구이다. MEDIUM의 이러한 시도는 이제 시작에 불과하며 앞으로 지속적으로 혁신을 거듭하여 고성능 블록체인 플랫폼의 표준을 제시할 것이다.

2) MEDIUM Architecture

MEDIUM은 Order-Execute를 비롯한 여러 합의 방식과 Architecture에서 드러난 성능 제한 요소들을 개선하기 위하여 고안된 방법 중 Hyperledger Fabric이 고안한 방식을 벤치마크하였다. Fabric의 경우 몇몇 노드들이 먼저 트랜잭션을 실행시킨 후 결과값에 대한 검증을 하는 단계와 모든 노드들 에게 적용하는 단계를 분리하여 처리하는 Execute-Order-Validate Architecture를 지향하고 있다. 이러한 설계는 Fabric이 Order에 대한 최종 합의에 도달하기 전에 트랜잭션을 실행한다는 점에서 Order-Execution 방식과 근본적으로 다른 구조라 할 수 있다.



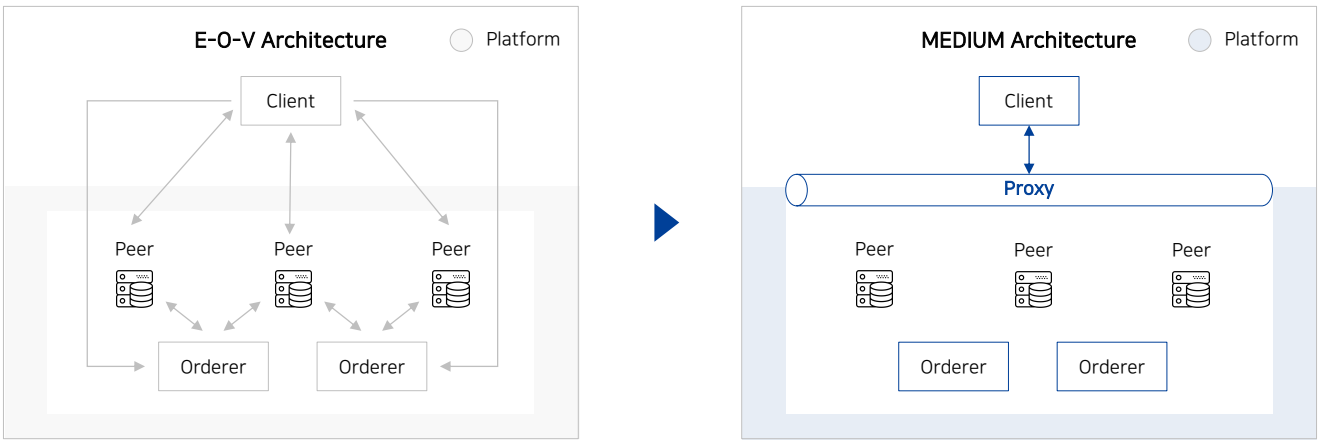
[그림06] Order-Execute and Execute-Order-Validate Architecture Process Comparison

MEDIUM은 하이퍼레저 패브릭의 E-O-V 방식의 아키텍처 메커니즘과 합의방식의 방향성을 벤치마크하여 자체적인 아키텍처를 설계하여 적용하고 있으며 트랜잭션 정보를 확인하고 검증하는 과정을 좀 더 모듈화하고 구조화하여 성능을 극대화시키는 아키텍처를 구현하고 있다.

3) MEDIUM Proxy

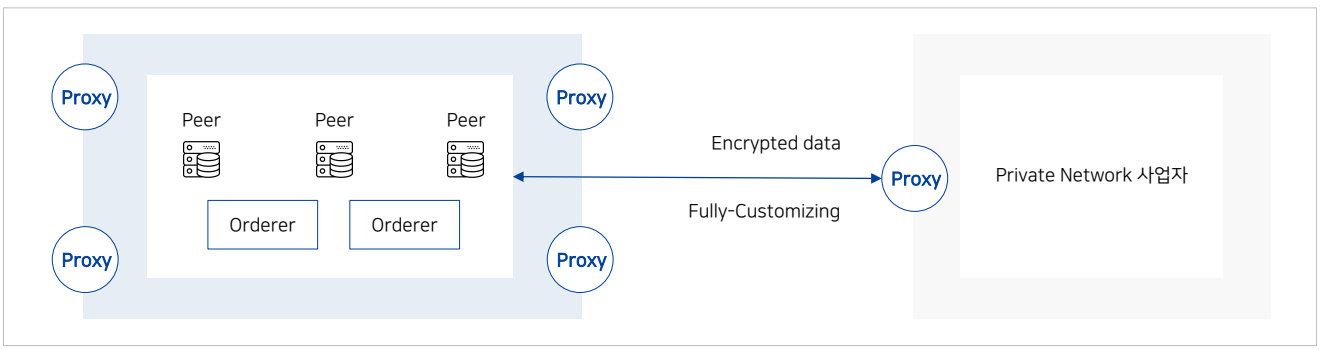
E-O-V Architecture를 이용하여 분산화 서비스를 운영할 때에 플랫폼에 접근하여 리소스를 이용하는 역할을 Client가 담당하게 되며 Client는 플랫폼 내부에서 존재하는 Peer, Orderer와 직접 통신하여 노드에 대한 인증과 데이터의 기록을 수행하게 된다. 이는 Client가 Peer, Orderer의 IP 주소 등 접속과 통신을 위한 정보를 알고있어야 하며 인증 확인, 체결, 요청 등의 여러 단계를 Client가 직접 노드들과 여러 번의 통신 과정을 거치게 된다. 이러한 구조는 Client의 최종적인 정보처리 성능에도 영향을 미칠 수 있으며, Peer와 Orderer의 정보가 모든 클라이언트에게 노출되는 측면에서도 개선이 필요한 구조라 할 수 있다.

이를 개선하기 위하여 MEDIUM은 Proxy 개념을 도입하여 Client가 플랫폼에 접속하거나 리소스를 사용하고자 할 때 Proxy를 통해 효율적으로 할 수 있는 구조를 만들었다. MEDIUM Proxy 시스템을 통하면 Client는 개별적으로 Peer, Orderer 등과 같은 개별 노드와 통신할 필요가 없으며 데이터의 요청, 관리를 위한 통신을 Proxy 노드하고만 개별적으로 수행하면 된다. 이는 절차적 효율성 측면에서도 개선된 구조라 할 수 있지만, 서비스를 위해 플랫폼에 접속한 Client가 불필요하게 플랫폼 구성에 대한 민감 정보를 취득하게 되는 정보보안 측면에서도 보안성을 강화시킬 수 있는 구조라 할 수 있다.



[그림07] MEDIUM Proxy System 구조

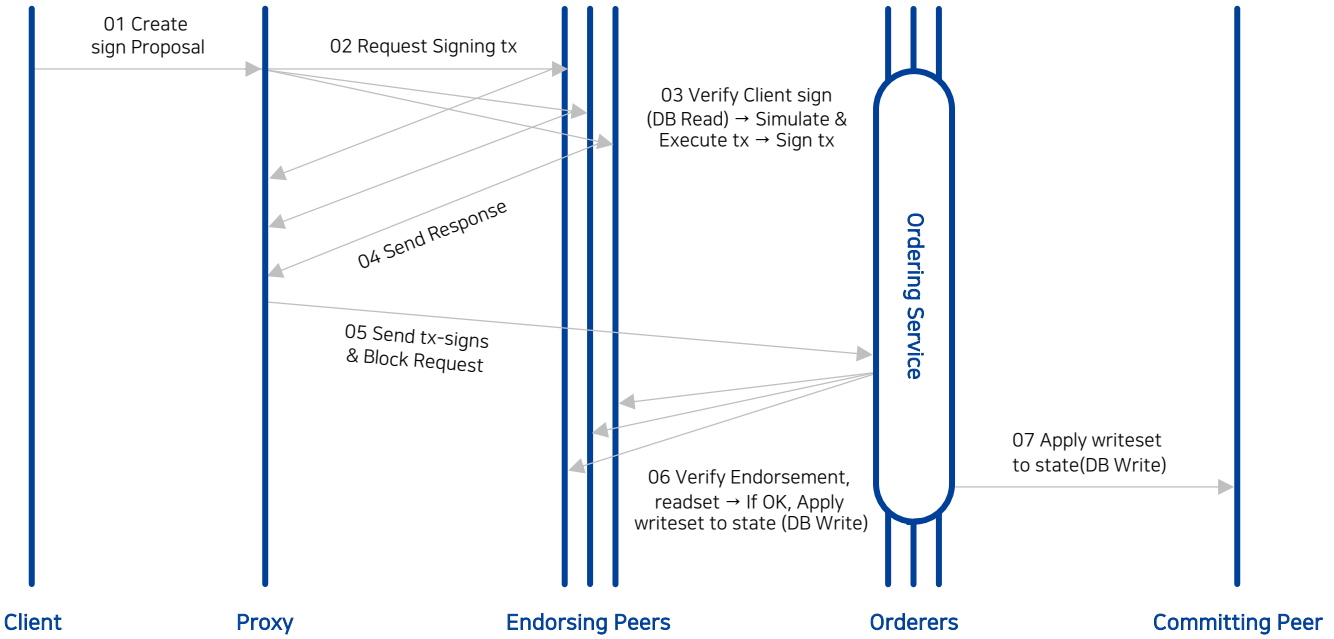
위에서 설명한 경우는 분산화 서비스(DAPP)가 블록체인 플랫폼에 접속하여 리소스를 이용하는 일반적인 경우를 예로 들어 설명했다면 아래의 경우 개별적으로 Private Network를 운영중인 사업자(정부기관, 금융기관, 단체 등)가 초고속의 블록체인 플랫폼 기능만을 별도로 이용하고자 할 때 MEDIUM Proxy 노드를 통해 안전하고 효율적으로 MEDIUM Public 플랫폼을 이용할 수 있는 구조를 설명한다. 이때 제공되는 Proxy 노드는 Private Network 사업자의 요구사항과 특수 환경에 맞게 Fully-Customizing 할 수 있으며 암호화된 데이터 통신 방식을 통해 보안성을 보장한다.



[그림08] Private Network 사업자의 Proxy 노드 이용 구조

4) 플랫폼 성능 향상을 위한 MEDIUM의 진단과 해결책

우리 MEDIUM은 Hyperledger Fabric를 비롯한 엔터프라이즈형 블록체인 플랫폼과 대표적인 퍼블릭 블록체인 플랫폼의 합의 방식 및 트랜잭션 처리방식을 분석하여 성능향상에 제한되는 요소가 공통적으로 도출되는 5가지 쟁점으로 수렴되는 것을 확인할 수 있었으며 MEDIUM BPU를 통하여 직접처리하여 성능을 개선하는 모델을 총 7가지로 제시하고자 한다.



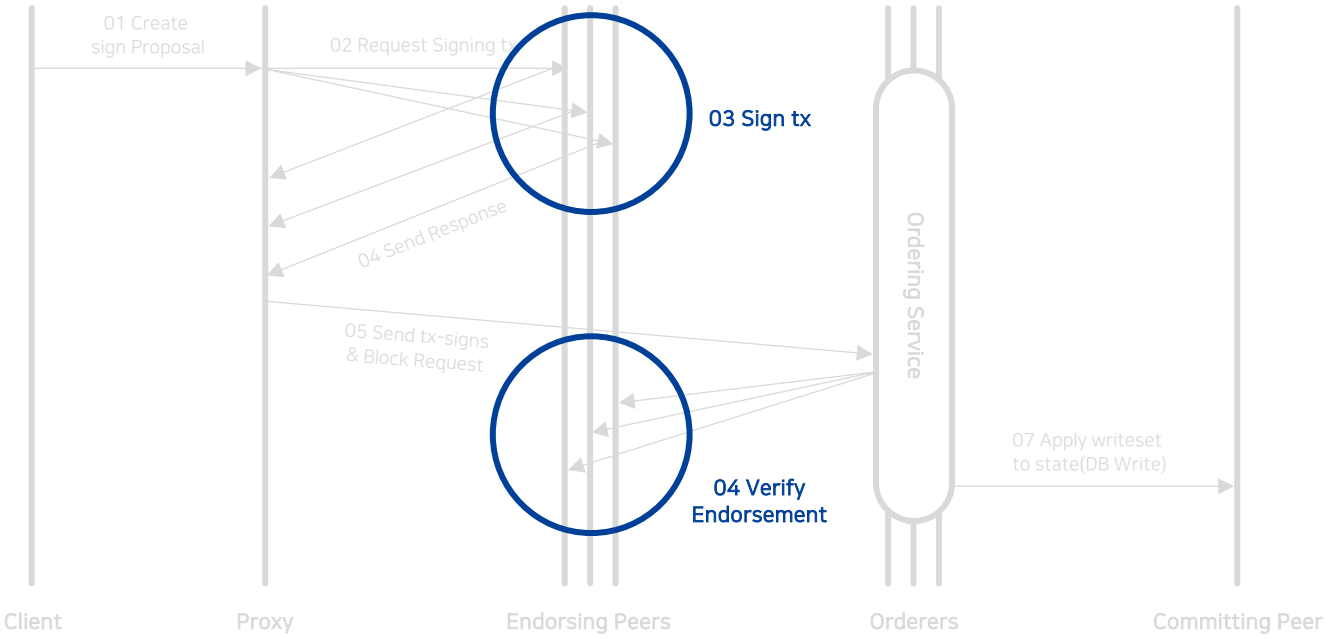
[그림09] MEDIUM Blockchain Transaction Flow

성능향상 제한 요소	해결방안
[Issue1] Sign & Verification Process	[Solution1] Accelerating for Sign & Verification by Crypto Engine
	[Solution2] Sign Algorithm for Peer's Scalability
[Issue2] Data Processing	[Solution3] Data Serialization by Data Processing Engine
	[Solution4] High Performance Key-Value Storage
[Issue3] Operation Process of Smart Contract	[Solution5] Increase Smart Contract Parallelism
[Issue4] Network Overhead	[Solution6] TCP Offload Engine
[Issue5] Ordering Consensus	[Solution7] H/W based Ordering Consensus

[표03] 블록체인 플랫폼 성능향상 제한요소와 해결방안 by MEDIUM

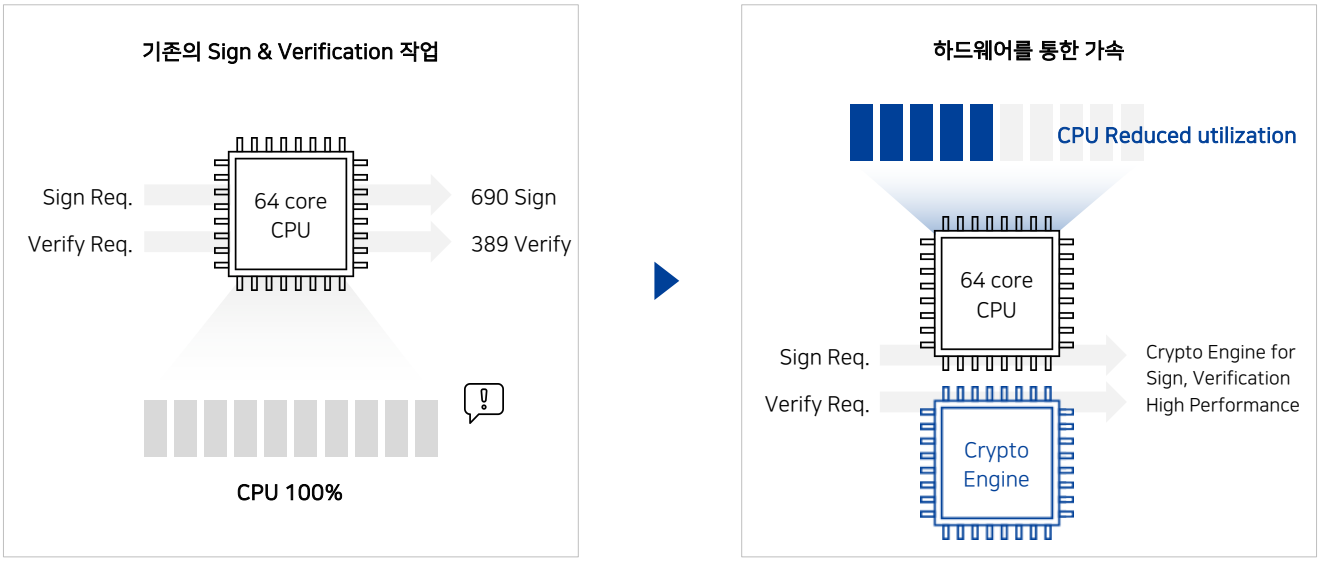
(1) Sign & Verification Process의 이슈와 그 해결방안 2가지

a. 서명(Sign)과 서명확인작업(Verification Process)에서의 속도 저하 원인
- Sign tx와 Verify Endorsement가 수행 되는 과정에서 Tx의 요청이 1M에 가까워질수록 병목 현상 증가와 속도 급감 현상 발생



[그림10] Sing & Verification 처리과정에서의 속도 저하 원인

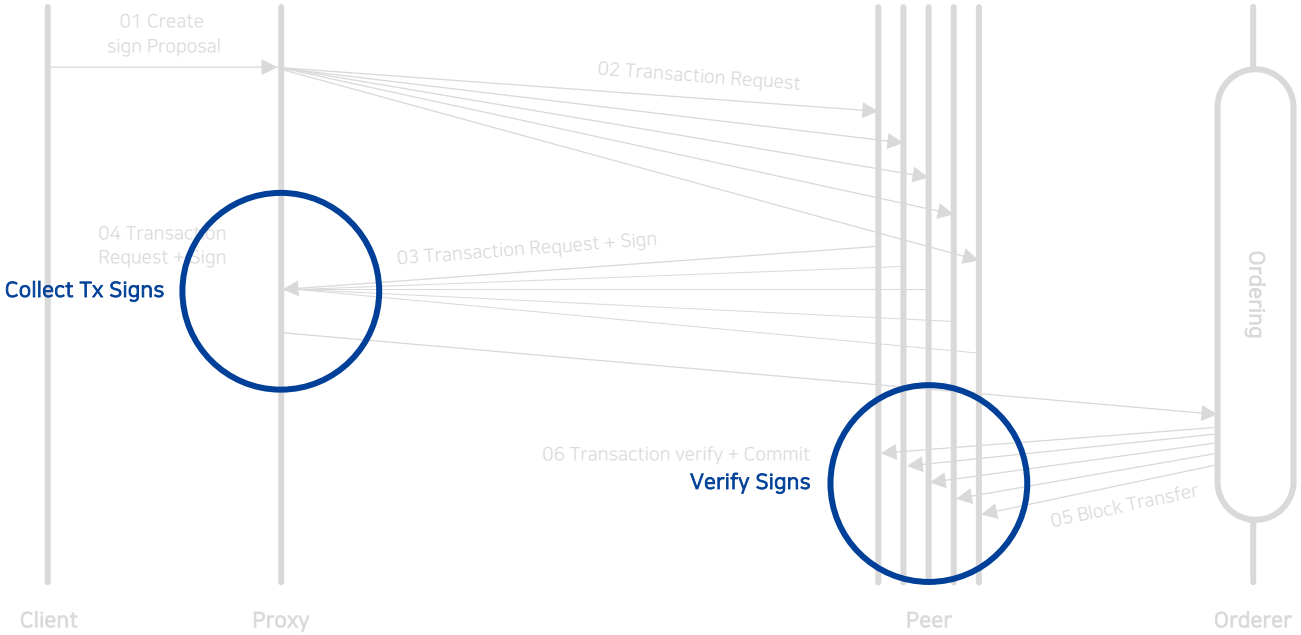
b. Solution1 : Accelerating for Sign & Verification by Crypto Engine
- 기존의 Sign & Verification 작업을 수행함에 있어 CPU 가용율 100% 기준으로 690K Sign요청, 380K Verify 요청의 처리를 확인할 수 있었음(64Core CPU 기준)
- Sign & Verification 기능을 수행하기 위한 전용 H/W – "Crypto Engine Chip"을 이용하여 작업 성능을 향상



[그림11] Accelerating for Sign & Verification by Crypto Engine

c. Peer 개수가 증가함에 따른 속도 저하 원인

- 전체 Node에서 새로운 Node(Peer)가 추가/증설 되었을 경우 Sign tx와 Verify Endorsement가 수행되는 과정의 수가 기하급수적으로 증가됨에 따라 속도 저하의 직접적인 원인이 됨



[그림12] Sing & Verification 처리과정에서의 속도 저하 원인

d. Solution2 : Peer의 확장성을 위한 Verification 전용 알고리즘 적용

- Peer 확장 시 트랜잭션 당 Sign도 동일한 개수대로 증가하여 서명 확인 작업에 대한 CPU 부하가 증가하는데 Peer가 증가해도 Verify 할 서명의 수가 특정 개수로 수렴하는 서명 전용 알고리즘을 적용하여 성능향상

기존의 서명 알고리즘

	Peer 1	Peer 2	Peer 3	Peer 4	Peer 5	···	···	···	···	Peer N
Tx 1	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	···	···	···	···	Sign N
Tx 2	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	···	···	···	···	Sign N
Tx 3	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	···	···	···	···	Sign N
⋮	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	···	···	···	···	Sign N
Tx 300,000	Sign 1	Sign 2	Sign 3	Sign 4	Sign 5	···	···	···	···	Sign N

서명알고리즘을 통한 가속

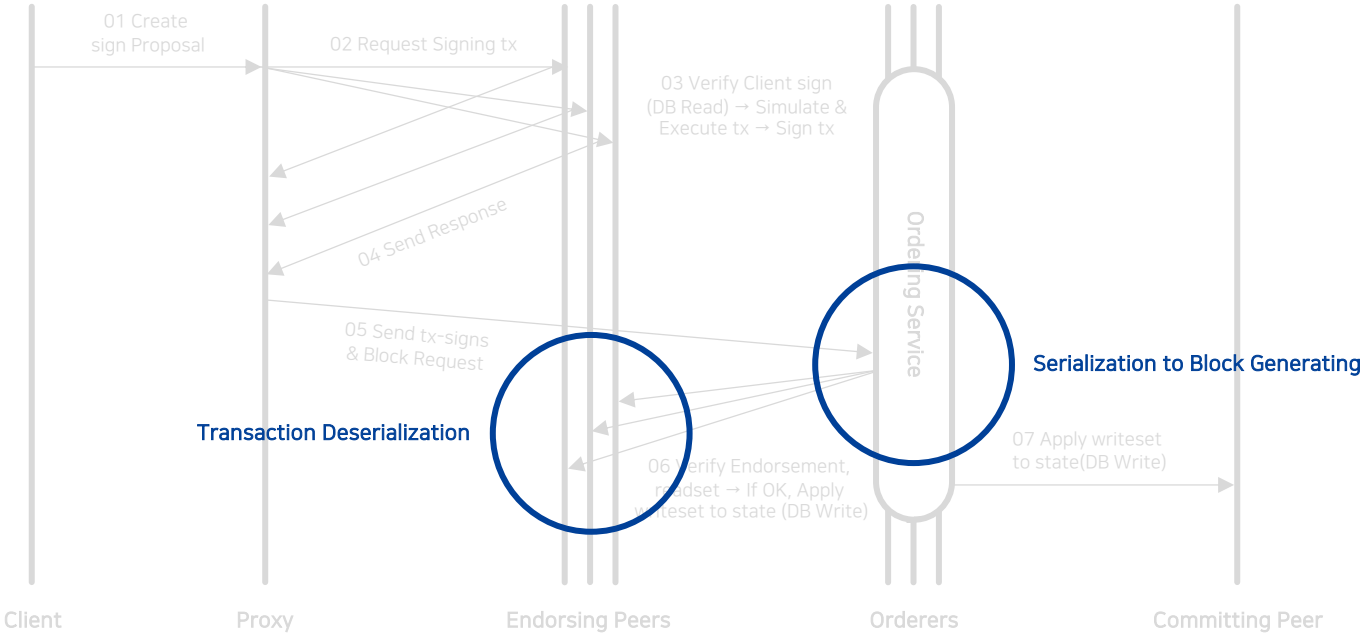
Tx 1	Peer 1	Peer 2	Peer 3	Peer 4	Peer 5	···	Peer N-2	Peer N-1	Peer N
Tx 2	X Signatures								
Tx 3	X Signatures								
⋮	X Signatures								
Tx M	X Signatures								

[그림13] 서명 전용 알고리즘의 개선 효율

(2) Data Processing 이슈와 그 해결방안 2가지

a. Data Processing 과정에서 성능 저하의 원인

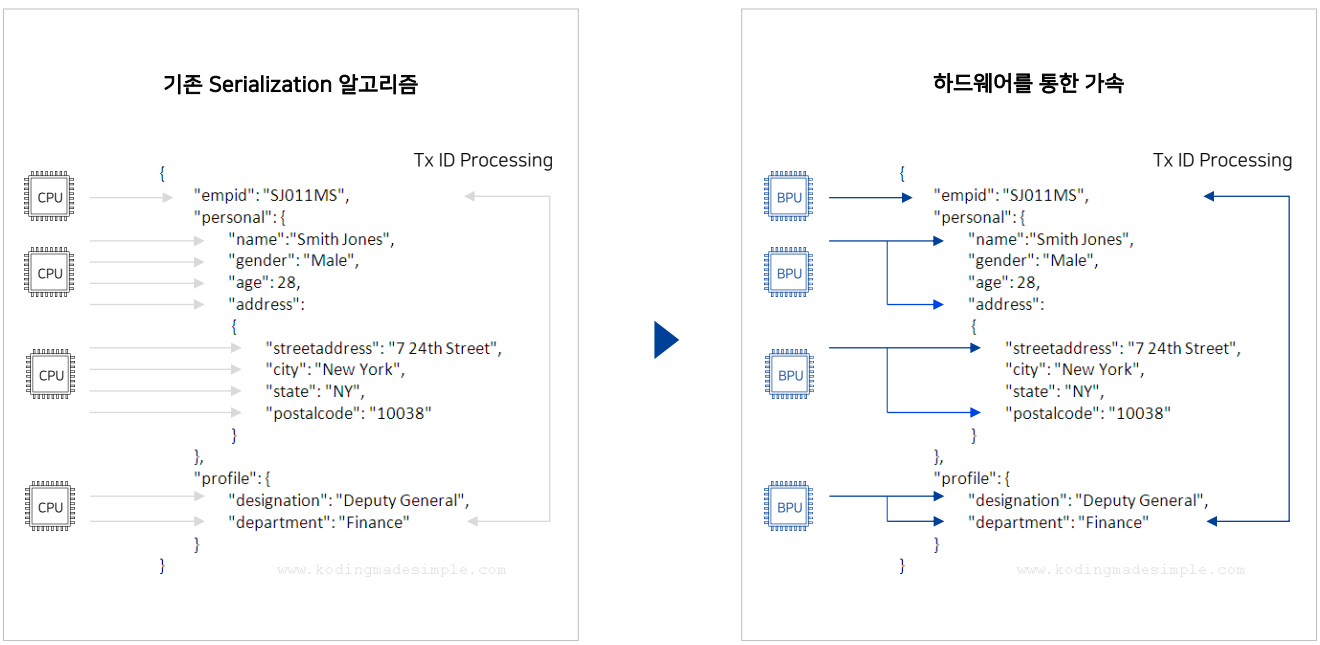
- 트랜잭션 Flow 과정에서 데이터를 수신하고 블록을 생성하는 절차에서 수신한 데이터의 규격을 직렬화하고 기록하는데 많은 CPU 자원이 소모되어 다수의 트랜잭션을 넣는 블록 처리가 어려운 현상 발생



[그림14] Read / Write Process in DB Flow에서 성능 저하 원인

b. Solution3 : 직렬화(Serialization), 직렬화 복원(Deserialization)을 H/W 추가

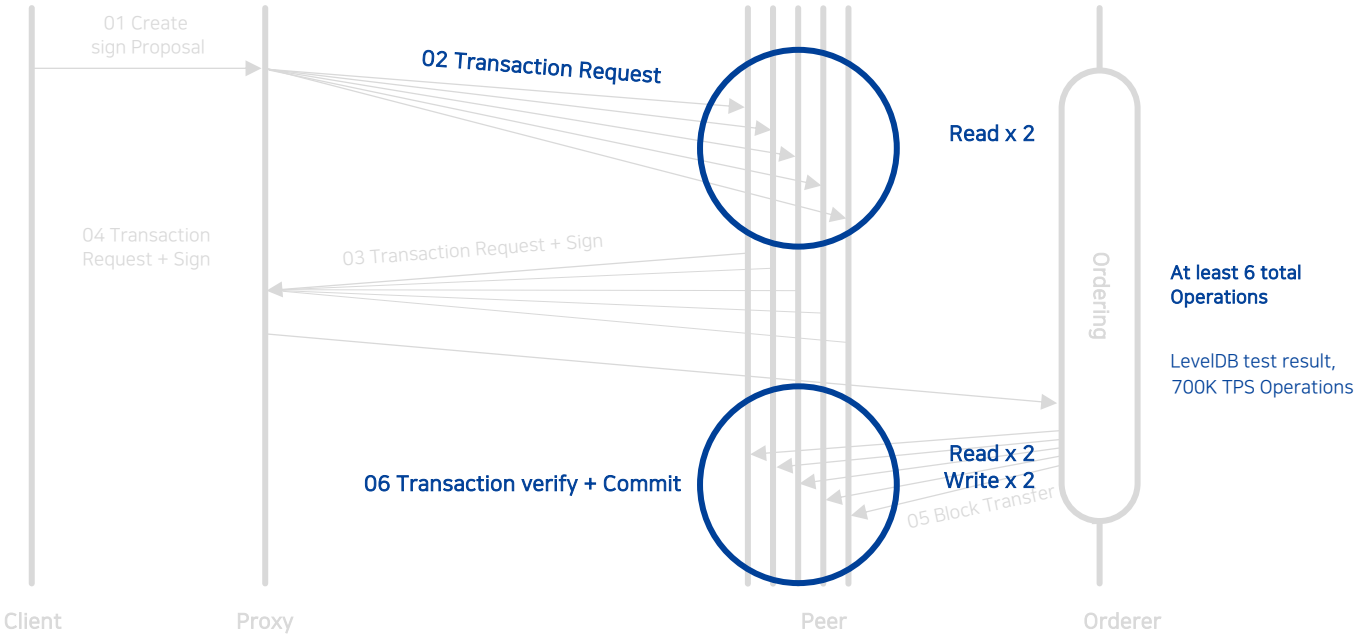
- 직렬화(Serialization), 직렬화 복원(Deserialization) 명령을 수행할 별도의 H/W를 추가 증설하여 성능향상



[그림15] Read / Write Process in DB Flow에서 성능 저하 원인

c. 기존 Key-value store의 한계

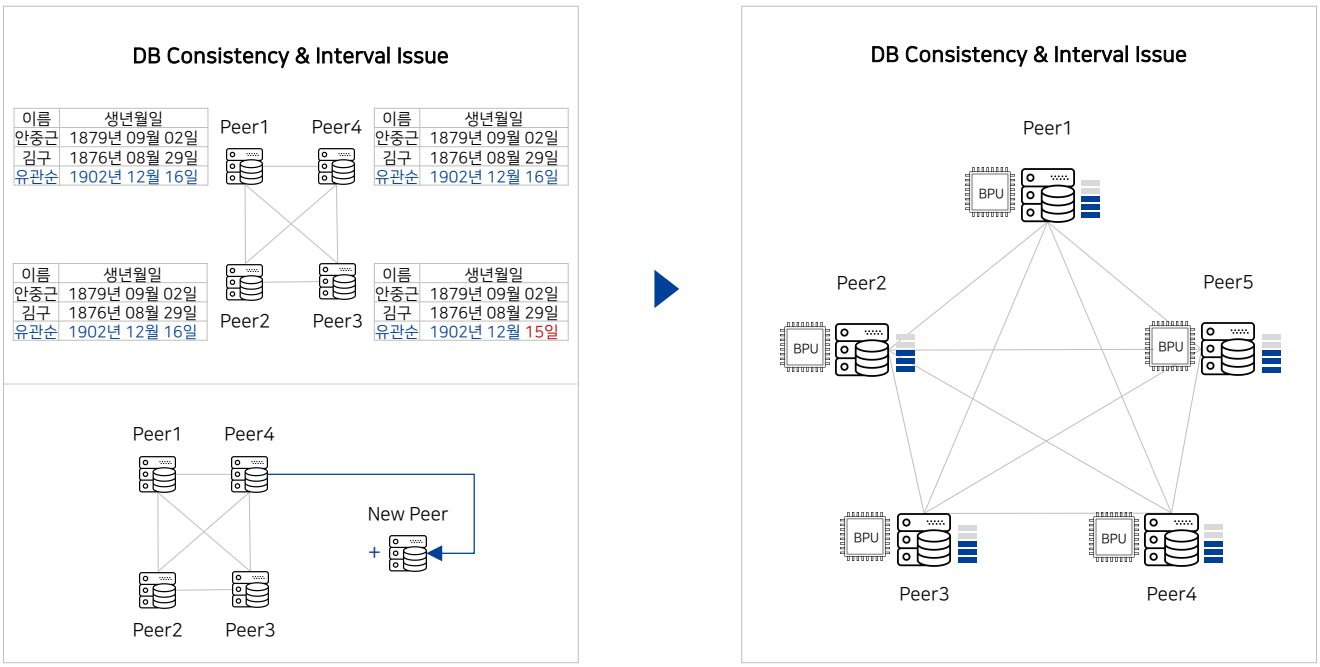
- Tx Read / Write 과정에서 발생하는 기존 데이터 베이스 성능의 한계로 인해 발생하는 전체 성능저하 문제
- Peer간 데이터의 일관성을 유지하지 못하는 경우가 발생하는 문제
- 추가된 Peer의 데이터 복제 문제



[그림16] 트랜잭션 Read / Write DB 성능 문제

d. Solution4 : Key-Value Storage

- 하드웨어 기반 Key-value storage의 구조 개선을 통해 획기적인 성능개선 가능
- 일관성을 유지할 수 있도록 전체 데이터에 대한 일관성의 주기적인 확인하는 하드웨어 추가
- DB의 복제를 빠르게 할 수 있는 네트워 및 데이터 처리 하드웨어 추가

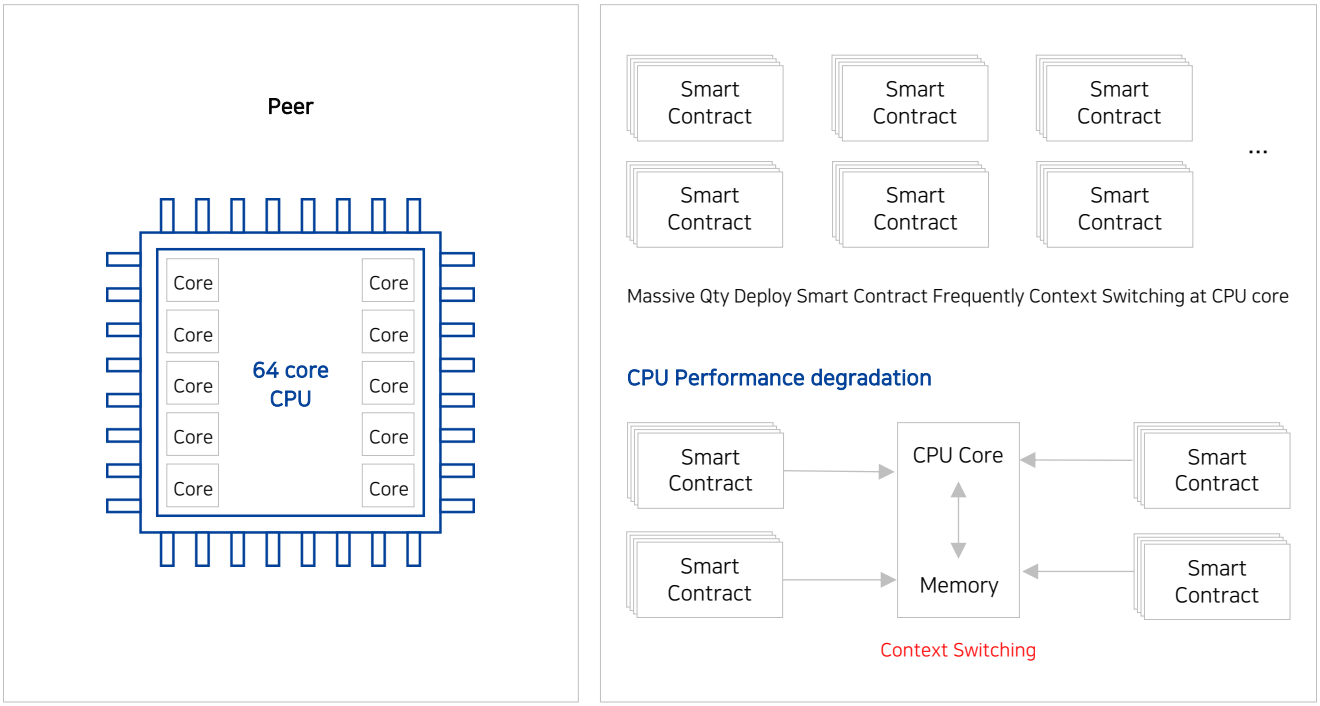


[그림17] Key-Value Storage for DB Consistency & Interval Problem

(3) Operation Process of Smart Contract 이슈와 그 해결방안

a. Smart Contract Operation Issue

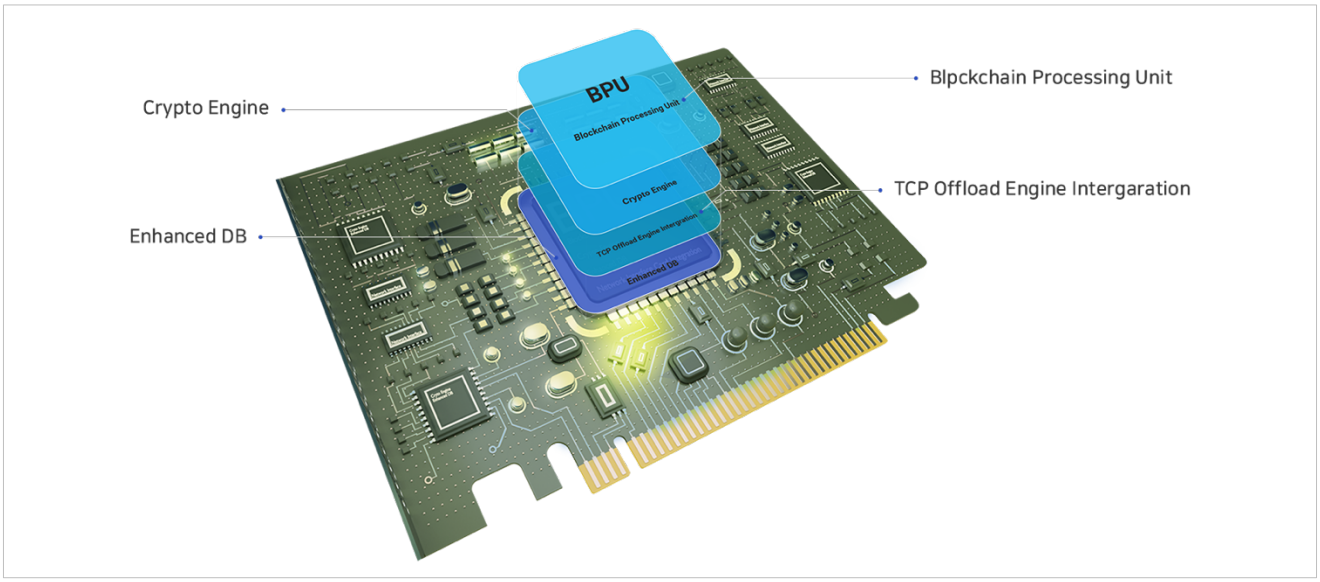
- 대규모의 Smart Contract 배포 시, CPU Core에서 잦은 Context Switching으로 시스템 성능 저하되는 문제



[그림18] Smart Contract Operation Issue

b. Solution5 : Increase Smart Contract Parallelism (Peer에 Smart Contract 프로세서 보드 설치)

- 서버 하나에 전용 프로세서를 병렬적으로 확장 함으로써 코어의 수를 높여 동시에 여러 스마트 컨트랙트를 실행할 수 있으므로 확장성을 높일 수 있고, Smart Contract가 단독 OS에서 실행되는 구조로 보안성을 높임

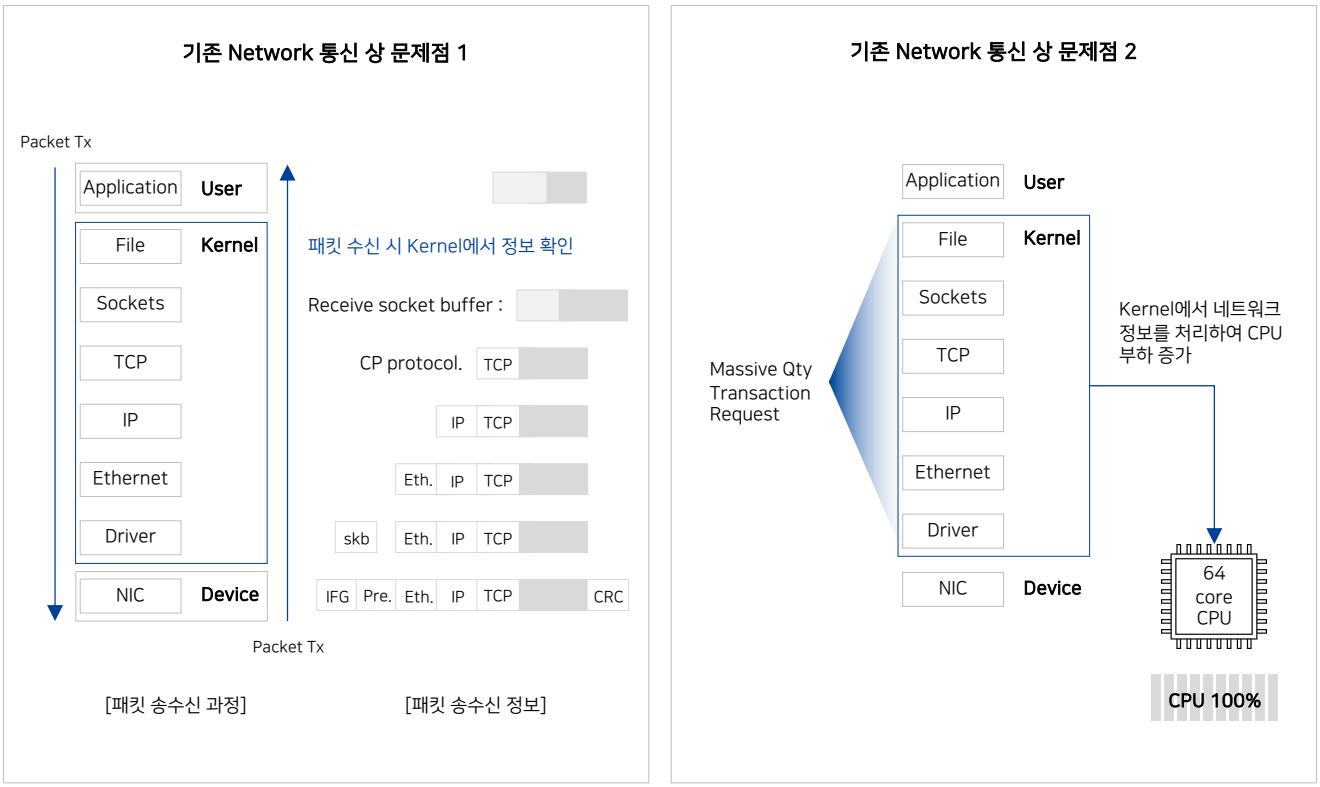


[그림19] Smart Contract Processor board 개념도

(4) Network Overhead 이슈와 해결방안

a. Network Overhead Issue

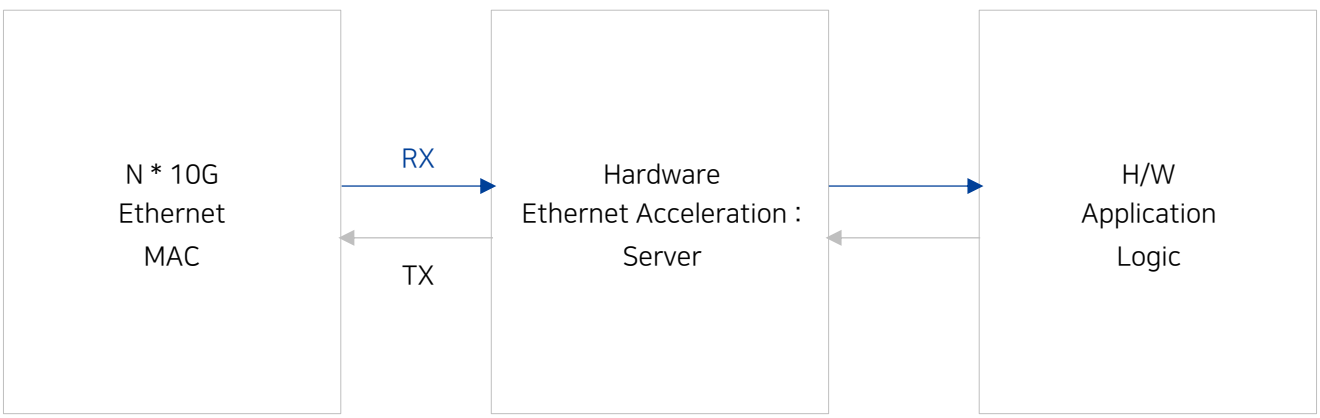
- Network 모듈의 통신 방식에 있어서 패킷을 수신하고 Kernel에서 Packet 정보를 해석하는 과정에서 CPU의 많은 부하가 걸리게 되며 순간적으로 초당 수십만 건 이상의 Request를 수신할 경우 높은 병목지연현상을 야기



[그림20] Network Overhead Flow Diagram

b. solution6: Network H/W Module 추가

- Network 모듈 또한 마찬가지로 별도의 H/W Chipset을 개발하여 Packet 정보처리를 단독 병렬 수행
- TOE(TCP Offload Engine) 등 기존의 하드웨어를 이용한 Kernel 사용 부하 감소 방법 연구
- 대량의 트랜잭션 요청 처리를 위한 높은 대역폭 확보

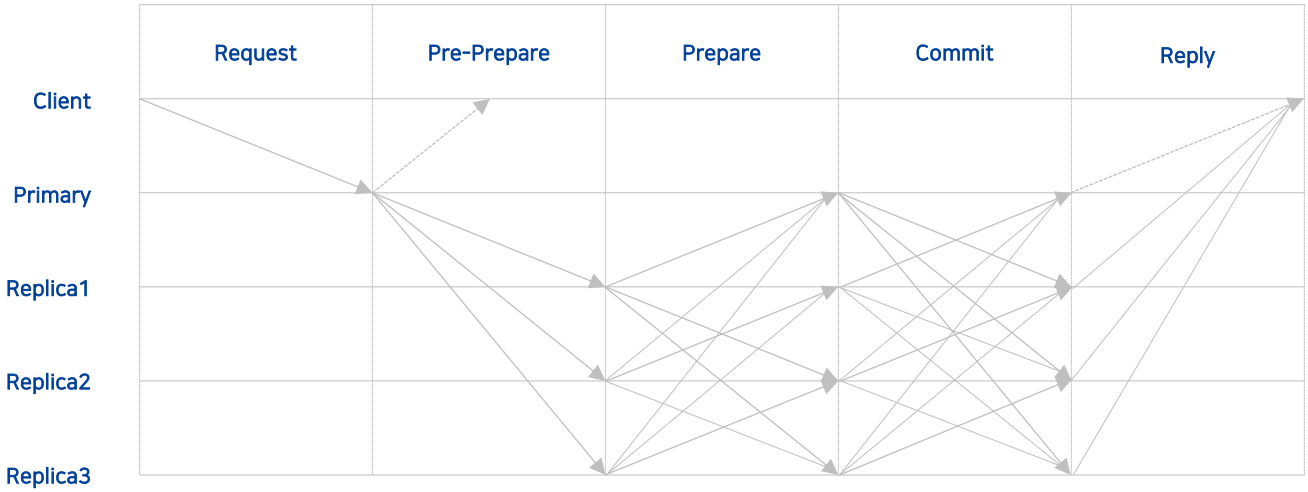


[그림21] Network Module Concept Diagram

(5) Ordering Consensus 이슈와 해결방안

a. 기존 BFT 계열 알고리즘의 문제점

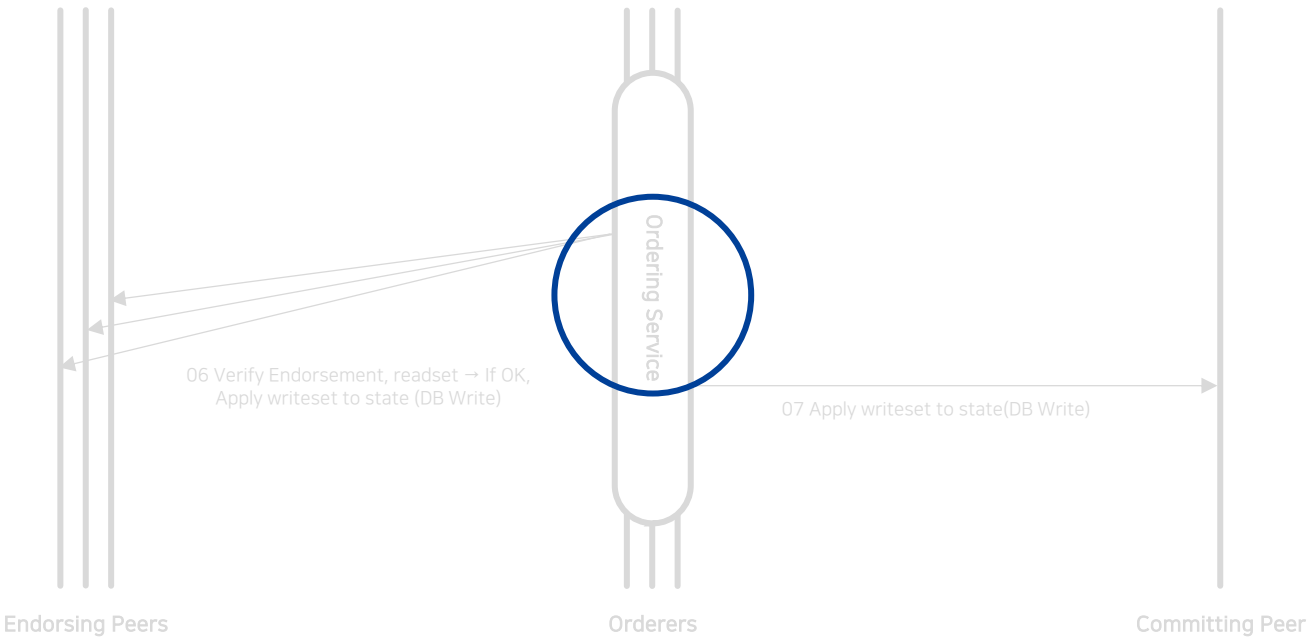
- BFT(Byzantine Fault Tolerance) 계열 알고리즘(ex> PBFT)은 합의 특성에 의해 수 십만 개의 트랜잭션을 처리하기 위해 높은 성능 필요



[그림22] PBFT Consensus Algorithm Example

b. Solution7 : Accelerating by H/W

- Orderer에 BFT를 위한 하드웨어 기반 고속의 Scalable한 알고리즘 및 전용 H/W 제작



[그림23] Network Overhead Flow Diagram

5) MEDIUM 기술의 핵심과 발전방향

비트코인으로부터 최초로 시작된 블록체인 기술은 P2P 네트워크상에서 거래데이터의 원장을 저장하고 생성하고 관리한다는 새로운 개념을 제시하였고 이전까지 없었던 신뢰 구축 방법을 소프트웨어적으로 구현하였다. 우리 MEDIUM은 비트코인으로부터 창조된 블록체인 기술을 전세계 다양한 ICT 산업에 적용하고 보급시키기 위하여 BPU를 그 핵심 기술로 생각하며 지속적인 혁신과 개선을 통해 진화시켜 나가고자 한다.

(1) BPU 성능 고도화에 따른 MEDIUM Appliance® 상용화

MEDIUM 블록체인 플랫폼의 기술 연구 성과는 그 핵심인 BPU의 성능으로 발현될 것이고 MEDIUM 플랫폼 아키텍처 기술과 통합적으로 결합된 MEDIUM Appliance®로 비로소 상용화 될 것이다. 앞으로 전세계 적으로 블록체인 비즈니스 구현이 범용화됨에 따라 정부기관, 기업, 단체 등에서 개별적으로 고성능 플랫폼을 구축하고자 한다면 MEDIUM의 Appliance® 제품을 우선적으로 검토하게 될 것이고 시장 발전방향에 부합하도록 제품이 본격적으로 상용화될 것이다.

(2) 1M TPS 구현

앞서 MEDIUM 블록체인의 최종 목표에서 언급한 바와 같이 MEDIUM은 최종적으로 1M TPS를 구현하기 위하여 소프트웨어의 성능개선 뿐만 아니라 맞춤형 H/W를 별도로 제작하여 목표를 달성하고자 연구개발을 지속하고 있다. 그에 있어 가장 핵심적인 기술이 BPU이며 현재 Crypto Engine, Enhanced DB Engine, SC Engine, NIC Engine의 네 가지 모듈 파트에서 전문 분야를 확장 시켜 나갈 것이며 BPU 전용 Cache Memory, Core 등의 연구개발을 통해 최종적인 1M TPS를 현실화 시킬 것이다.

(3) 적용 분야의 확대

블록체인 기술은 앞으로 스마트시티, 인공지능, 공유경제 등 4차산업 유망 기술분야에 다양하게 활용될 수 있게 그 제공 방법과 형태가 진화될 것이다. MEDIUM의 플랫폼 기술 또한 그에 적용될 수 있도록 고도화가 진행될 것이지만 무엇보다 BPU의 활용처가 다양한 방면으로 확장될 수 있을 것으로 예측하며 성능 뿐만 아니라 기능적 측면의 발전 방향을 고려하고 있다.

가까운 미래에 IoT 기술이 상용화 됨에 따라 기기들 간의 통신 방식과 데이터 교환에 있어 신뢰 검증과 합의 검증을 위하여 필수적으로 블록체인 기술이 활용될 것이며 다양한 IoT Device에 부착되어 활용될 수 있는 micro BPU 또한 개발되고 상용화될 수 있을 것이다.

또한, 미래 현대인의 생활방식에서 새로운 통신수단이 등장하고 보급되면서 미래형 스마트폰에 직접적으로 블록체인 기술과 서비스가 활용될 수 있도록 Mobile BPU, Application BPU등이 개발 되어 블록체인 전용 스마트폰이 상용화 될 수 있을 것으로 본다. 블록체인 스마트폰이 상용화 된다면 암호화폐가 좀 더 많은 응용서비스에 적용되면서 사용 형태가 확대할 수 있을 것이며, 개인의 식별과 인증 방식 또한 한 차원 진화되면서 스마트폰의 활용도가 극대화 될 수 있을 것으로 예측된다.

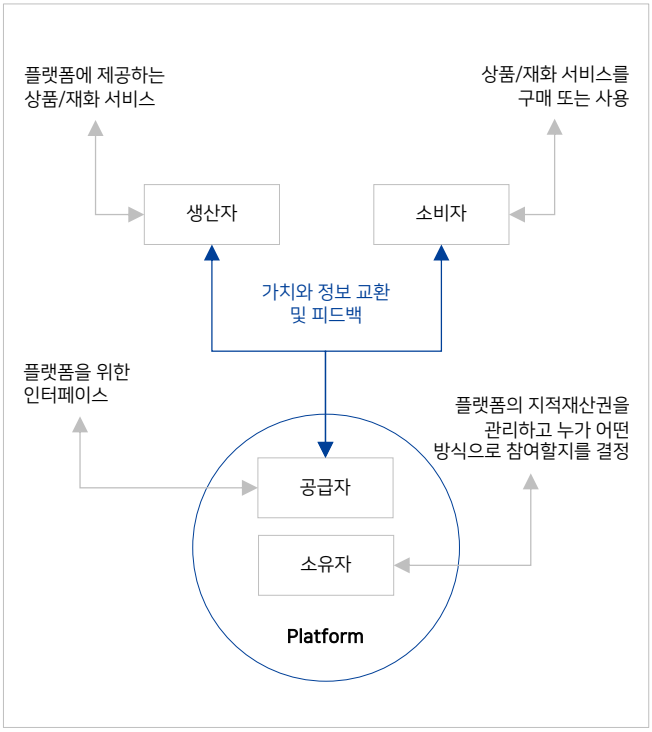
03 MEDIUM 블록체인 에코시스템

본 장에서는 위에서 서술한 MEDIUM 블록체인 플랫폼 기술을 기반으로 생태계를 어떤 방식으로 구현할지에 대한 설명을 하기 위해 플랫폼의 주요 구성요소와 가치사슬을 설명한다. 또한 MEDIUM 블록체인에서 발행될 암호화폐 기반의 경제시스템과 화폐의 흐름에 대해서 설명하고자 한다.

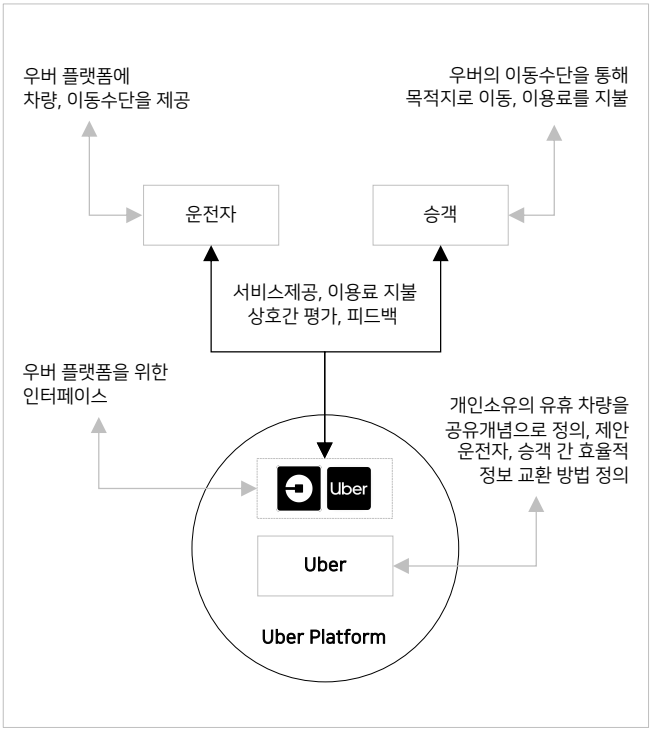
1) 블록체인 플랫폼과 비즈니스 생태계에 대하여

블록체인 플랫폼 생태계 구성에 대하여 설명하기에 앞서 디지털 비즈니스가 일반화된 현대적 시점과 관점에서 플랫폼의 의미에 대해서 상기해보며 플랫폼을 지향하고자 하는 기술이 어떤 가치를 우선시 해야하는지에 대한 고찰이 필요하다고 생각된다.

ICT 기술이 보편화됨에 따라 글로벌 비즈니스 스케일이 일반화된 현재의 시점에서 기본적으로 플랫폼이란 생산자와 소비자 간에 가치 있는 재화를 교환가능하게 함으로써 비즈니스 통합을 추구할 수 있게 해주는 연결자라고 할 수 있다. 이러한 플랫폼 비즈니스에서 플랫폼 사업자/소유자는 플랫폼 본질과 핵심에 대한 지적재산권과 플랫폼의 관리방식을 제어하고 구성요소들간의 이해관계를 조율한다. 공급자는 플랫폼과 사용자/이용자를 연결시키는 인터페이스/채널 역할을 한다. 생산자는 플랫폼안에서 사용자/이용자에게 제공될 수 있는 상품, 서비스 등의 용역을 제공하는 주체를 이야기한다. 이를 글로벌 공유 플랫폼 Uber로 예를 들어보면 아래 그림과 같이 예시를 들 수 있다.



[그림24] Pipelines, Platforms, and the New Rules of Strategy 응용[5)]

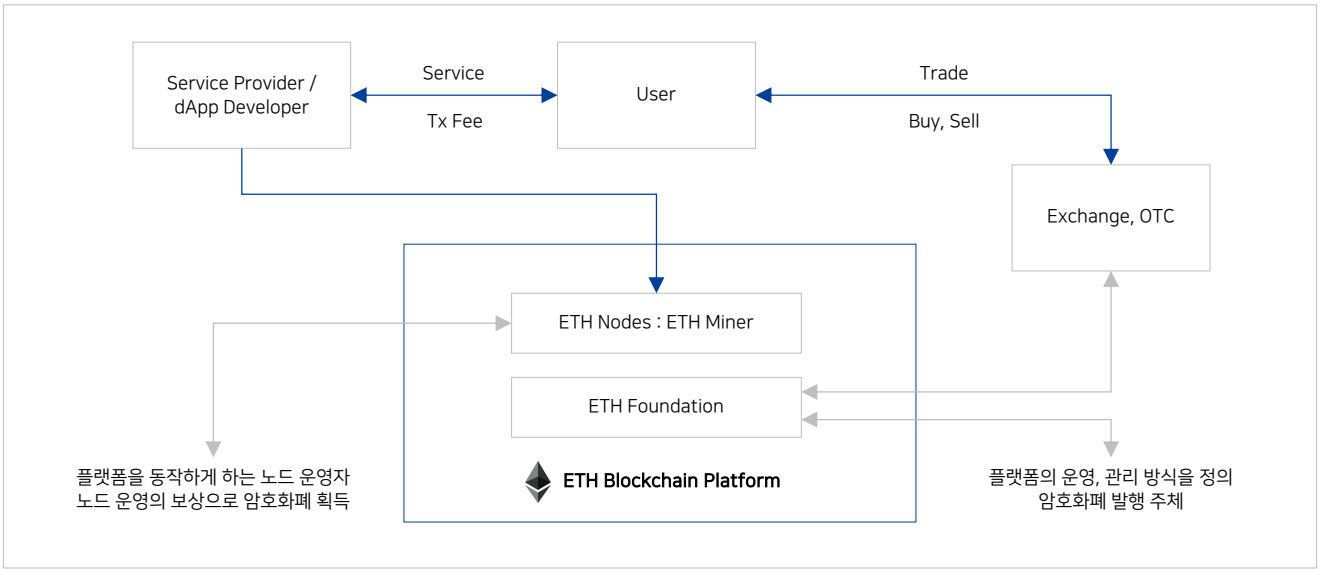


[그림25] 우버 플랫폼에서 플랫폼, 공급자, 제공자, 이용자 관계 개념도

5) Pipelines, Platforms, and the New Rules of Strategy at hbr.org :
https://hbr.org/2016/04/pipelines-platforms-and-the-new-rules-of-strategy#comment-section

2) 블록체인 플랫폼 생태계의 속성과 특징

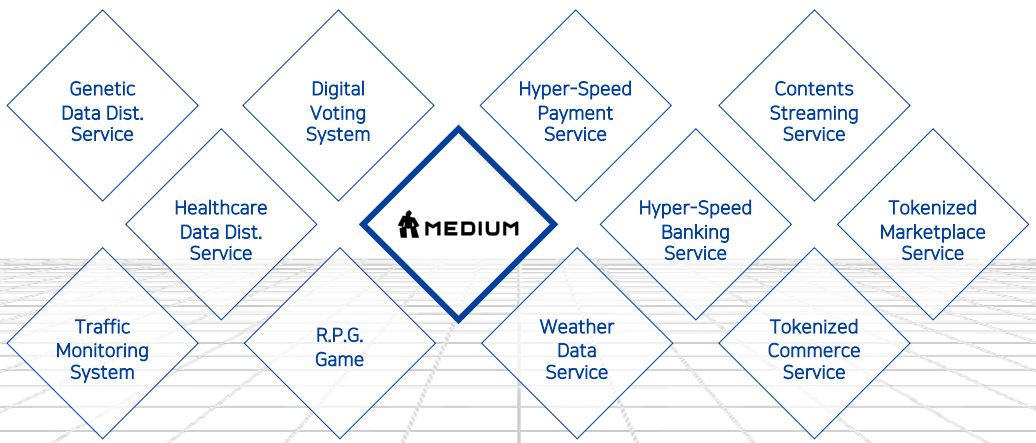
그렇다면, 위에서 우버의 예로 살펴본 플랫폼 비즈니스의 생태계와 달리 블록체인 플랫폼의 생태계 구조와 특징은 어떤 차이가 있는지 살펴볼 필요가 있을 것이다. 이해를 돕기 위하여 이더리움을 예로 들었다.



[그림26] 이더리움 플랫폼 생태계 가치사슬 개념도

블록체인 플랫폼 생태계가 지금까지의 플랫폼 비즈니스 생태계와 다른 가장 큰 차이점은 무엇보다 암호화폐를 기반으로 각 주체별 이해관계가 성립된다는 부분이다. 플랫폼의 동작원리와 운영방침, 관리규칙등을 Foundation에서 정의하고 그에 상응하는 암호화폐를 발행하면 플랫폼을 동작하게 하는 노드 운영자들이 컴퓨팅 자원을 제공하여 플랫폼을 안정적으로 작동하게 돕는다. 그리고 그에 따른 해당 노드의 운영에 대한 보상으로 암호화폐를 획득할 수 있다. 서비스 제공자/개발자는 플랫폼의 자원을 활용하여 서비스를 개발/운영하여 사용자에게 서비스를 제공하고 사용자는 서비스를 이용하는 과정에서 발생할 수 있는 이용 수수료(트랜잭션 수수료)등을 지불하기 위하여 암호화폐를 트레이드, 구매 방식으로 획득할 수 있으며 직접 노드 운영에 참여하여 해당 암호화폐를 획득할 수도 있다.

3) MEDIUM 블록체인 플랫폼의 생태계 비전



[그림27] MEDIUM 블록체인 플랫폼 비전 개념도

비트코인 등장 이후 많은 연구들에서 시도되어져 왔던 다양한 분산화 서비스들은 플랫폼의 환경과 성능의 한계에 부딪쳐 개발 검증 단계에서 진보되지 못했다. 실시간 처리와 대용량 처리가 전제되어야 하는 지불결제 시스템, 수 백만 건 이상의 빅 데이터를 초단위로 연산해야하는 날씨, 교통 서비스, 수 십만명 이상의 동시 접속 요청을 처리해야하는 온라인 게임, 디지털 투표 시스템 등 고성능의 탈중앙화 시스템이 요구되는 영역은 현재 ICT 서비스가 보편화된 모든 영역에 해당될 것이다.

MEDIUM 블록체인 플랫폼은 현존하는 모든 ICT 서비스가 탈중앙화된 네트워크 자원을 활용하여 서비스를 구현하고자 할 때 초고속의 성능과 최저 비용의 환경을 보장한다. 초고속 블록체인 플랫폼 환경은 암호 화폐로 새롭게 창조될 새로운 경제 시스템 기반에서 다양한 분산화 서비스 분야의 혁신을 가져올 것이라 확신한다.

4) MEDIUM 블록체인 플랫폼의 제공방법

MEDIUM 블록체인 플랫폼은 다양한 형태의 인프라 환경에 대응할 수 있게 여러 형태로 제공하고자 한다.

(1) MEDIUM 퍼블릭(Permissioned) 블록체인 플랫폼 모델

퍼블릭 블록체인 플랫폼 모델은 일반적으로 여타 많은 프로젝트에서 제공하는 방식과 동일한 방식으로 플랫폼의 자원을 활용할 수 있다. MEDIUM 퍼블릭 블록체인 플랫폼은 앞서 “2.1 MEDIUM 블록체인의 정책과 방향성 - 2.1.2” 에서 정의한 바와 같이 MEDIUM의 노드는 전세계의 각 대륙별 운영 기관의 컨소시움으로 구축될 예정이므로 엄밀하게 범주를 분리하자면 허가형(Permissioned) 블록체인이 정확한 표현이지만, 이용자의 이용 행태에 따라 분류하기 위하여 퍼블릭 블록체인 모델로 명명하기로 한다. MEDIUM 퍼블릭 네트워크의 자원을 활용하고자 하는 서비스 제공자 또는 개발자는 제시된 연동규격과 SDK에 맞추어 자신의 서비스를 개발할 수 있다.

(2) 클라우드-형(Cloud Type) 블록체인 플랫폼 모델

클라우드-형 블록체인 플랫폼 모델은 MEDIUM 블록체인 인프라와 동일한 수준의 인프라를 클라우드 소싱 형태로 이용할 수 있는 모델로서 플랫폼이 MEDIUM H/W 기반의 클라우드 인프라 상에서 동작하기 때문에 수요 기관에서 블록체인의 Deploy 및 기타 자원관리를 웹 기반의 콘솔과 대시보드를 통해 개별적으로 정의하고 업데이트할 수 있으며 독립적인 사설 블록체인 플랫폼, 공용 블록체인 플랫폼, 컨소시움 블록체인 플랫폼 등을 자유롭게 만들 수 있다. 마찬가지로 아키텍처의 정의를 자유롭게 할 수 있으므로 구축할 플랫폼 기반의 암호화폐를 발행 시 거버넌스 정책과 통제 정책 등을 MEDIUM 플랫폼의 종속적이지 않게 설계할 수 있는 장점이 있다.

(3) 프라이빗(Private) 블록체인 플랫폼 모델

프라이빗 블록체인 플랫폼 모델은 어떠한 외부환경의 시스템과도 자원을 공유하지 않고 독자적인 탈중앙화된 네트워크 시스템을 구축하고자 하는 기관에서 도입하고자 할 때 도입하는 모델로서 MEDIUM H/W 장비를 해당 기관의 사설망 내부에 위치하여 별도의 플랫폼을 운용하는 방식이다. 기관의 요구사항에 따라 MEDIUM에서 플랫폼 기술 및 dApp 연동과 관련된 직접적이며 밀도 높은 기술 지원을 받을 수 있다.

(4) 하이브리드(Hybrid) 블록체인 플랫폼 모델

하이브리드 블록체인 플랫폼 모델은 도입하고자 하는 기관에서 기 보유중인 프라이빗 블록체인 또는 탈중앙화 서비스가 있을 경우 MEDIUM 퍼블릭 블록체인 모델과 연동해서 사용할 수 있는 모델이다. 해당 기관에서 외부 네트워크와 분리 운영중인 사설 블록체인 플랫폼이 있음에도 불구하고 MEDIUM 퍼블릭 블록체인 모델의 자원을 활용하고자 할 때 수요 기관에서는 MEDIUM 퍼블릭 네트워크와 연동을 위한 프록시(Proxy) 시스템을 도입하여 연동할 수 있다.

프록시 시스템은 기본적으로 MEDIUM에서 표준규격으로 제작하여 관련 라이브러리와 함께 제공되며 블록체인 업계 동향과 분포 수준에 따라 지속적으로 업데이트될 예정이지만, 도입하고자 하는 기관의 내부 정책과 기보유 플랫폼과의 정합성과 일관성을 유지하기 위하여 완전 최적화(Fully-Customizing)될 수 있도록 기술지원 한다.

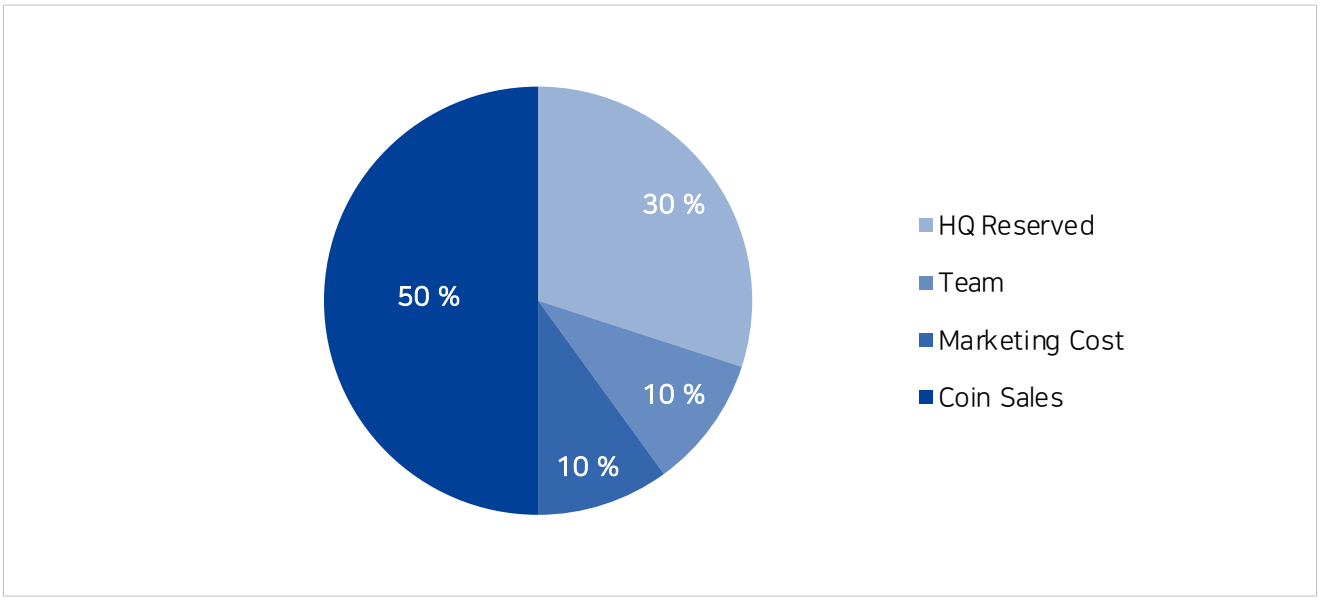
또한, 앞서 여러차례 언급한 바와 같이 MEDIUM 블록체인 플랫폼은 하이퍼레저 플랫폼과 호환성을 보장하기 때문에 하이퍼레저 패브릭 기반의 프라이빗 플랫폼 또는 dApps을 운용중인 기관이 별도의 초고속 네트워크를 사용하고자 하는 수요가 있을 경우 앞서 언급한 프록시 서비스와 연동을 거쳐 MEDIUM 퍼블릭 블록체인 플랫폼의 자원을 자유롭게 활용할 수 있다.

5) MEDIUM 암호화폐 (Cryptocurrency) – MDM Coin의 정의

MEDIUM 코인은 MEDIUM 프로젝트 공개와 함께 한정수량으로 발행되며 이는 MEDIUM 블록체인 플랫폼 내부에서 발생하는 모든 비용을 지불할 수 있고 플랫폼 리소스 사용 수수료로 사용할 수 있다.

(1) MDM Coin Information

a. Total Generating Coin : 1,000,000,000 MDM
b. MDM Coin Distribution : Coin Sales 50% | HQ Reserved 30% | Marketing Cost 10% | Team 10%

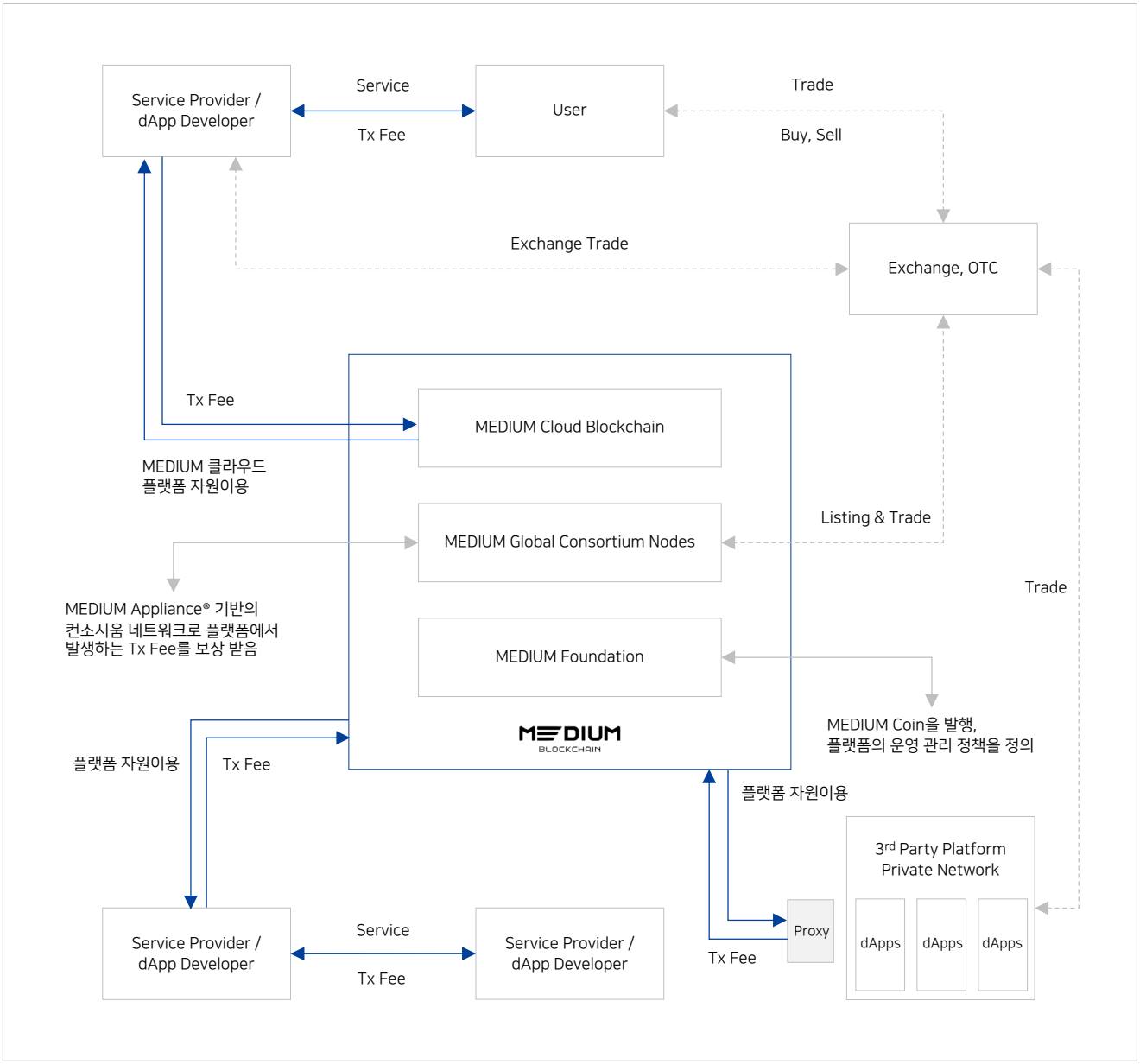


[그림28] MEDIUM Token 배분 정보

6) MEDIUM Coin / Token Economics

(1) MEDIUM Coin / Token Economics 개요

MDM Token Economics는 위 3.(4) 절에서 서술한 총 4가지 형태의 제공 방법 중 (3)번째 프라이빗 형태를 제외한 모든 형태의 플랫폼에 적용되며, MEDIUM 컨소시움 네트워크가 연동과 함께 시작될 예정이다. 프라이빗을 제외한 모든 유형의 서비스 형태는 MEDIUM 컨소시움 네트워크의 자원을 사용하기 위하여 MDM Token으로 지불하게 되며 지불된 Token은 컨소시움 구성원들에게 지급된다.



[그림29] MEDIUM 블록체인 Coin / Token Economics 개념도

(2) MEDIUM 플랫폼 네트워크 사용료

MEDIUM 플랫폼에서 구동되는 모든 유형의 서비스는 플랫폼 사용을 위하여 사용량에 비례하여 사용료를 지불하여야 하며 플랫폼 내에서 이루어지는 모든 결제와 지불은 MDM Token으로 할 수 있다. MEDIUM 플랫폼에서 네트워크 자원의 사용료는 항상 TPS 단위로 정산하며 정산 시점의 MDM Token의 글로벌 평균 거래시세정보에 맞춘 공시정보를 따르게 되며, MDM Token의 가격의 변동성에 대비하기 위하여 글로벌 Fiat Market의 기축통화인 달러(USD)를 기준으로 네트워크 사용료 기본안을 적용할 예정이다.

(3) MEDIUM 플랫폼 모델 별 정책

MEDIUM 플랫폼의 제공 방법 별 사용자에게 적용되는 정책은 다음과 같다. 본 정책은 본 성명서를 배포하는 시점의 가이드 라인이며, MEDIUM의 메인넷 공개 시 상세한 정책 및 Governance Rule에 대하여 별도 배포할 예정이다.

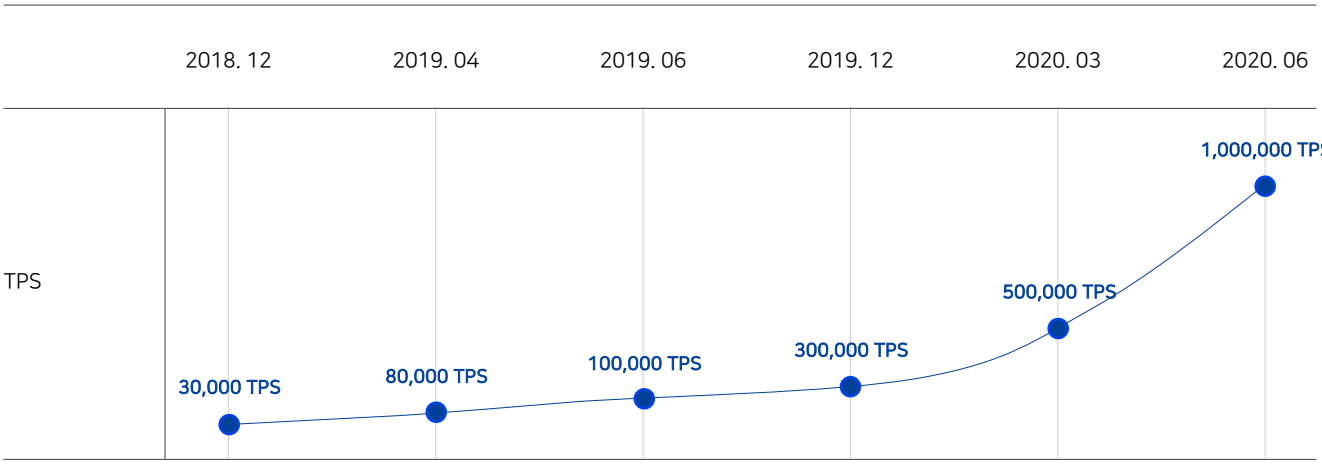
* MDM Token Hold

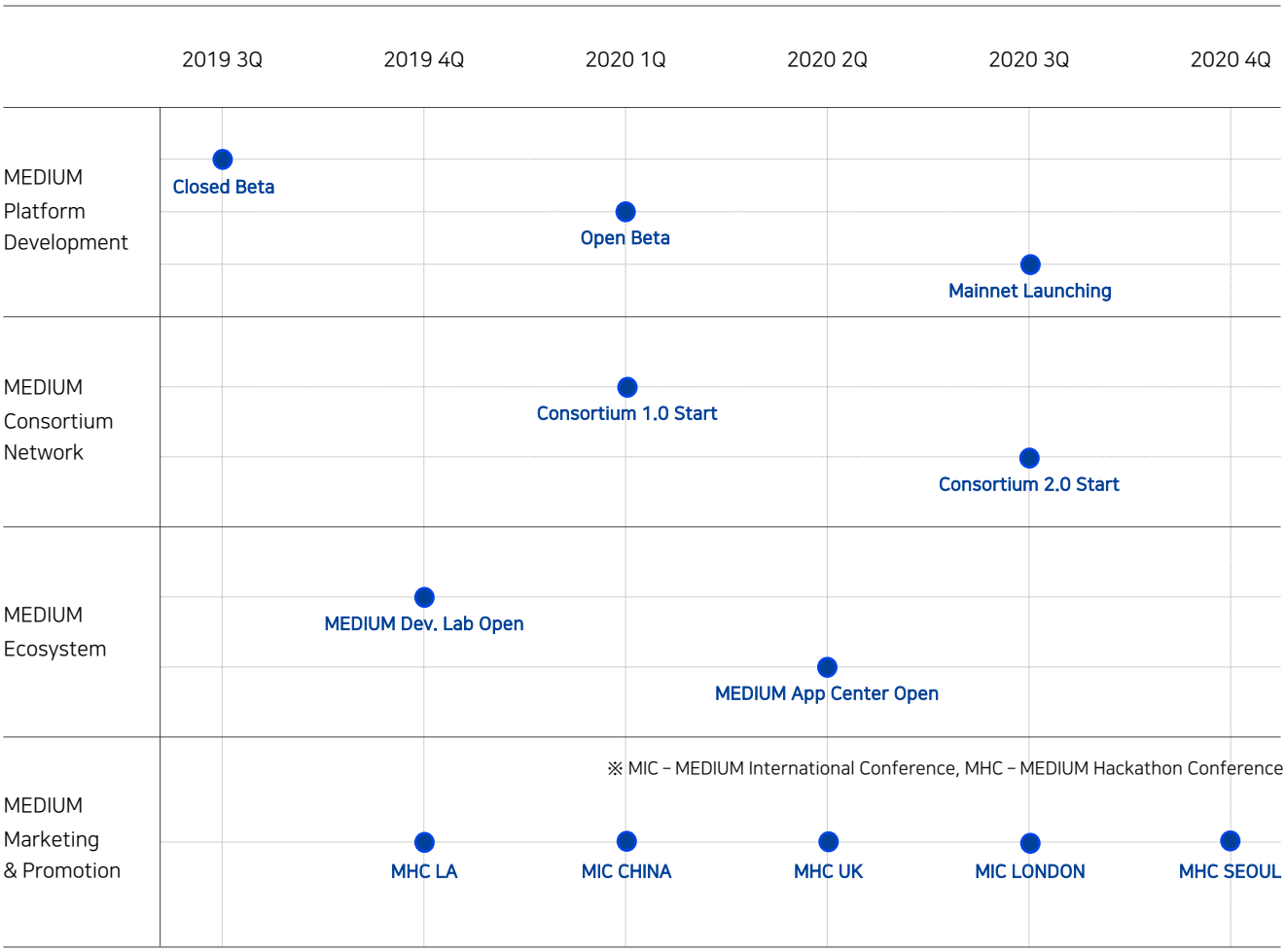
플랫폼 제공 형태별 해당되는 모델을 선택한 사용자 또는 이용자가 시스템 사용을 위하여 MDM Token을 일정 수량, 일정 기간 동안 보유해야 하는 정책

항목	Private	Cloud Type	Public (Permissioned)	Hybrid	컨소시움 참여 (Node)
MEDIUM H/W 도입	필수	해당 없음	해당 없음	선택 사항	필수
데이터 센터 Co-Location Service	선택 사항	해당 없음	해당 없음	해당 없음	필수
MDM Token Hold *	협의 사항	해당	해당	해당	필수
독립적 플랫폼 구현 (Governance Rule)	가능	가능	불가능	해당 없음	해당 없음
개별 컨소시움 구축	가능	가능	불가능	불가능	해당 없음

[표04] MEDIUM 플랫폼 모델 별 정책

04 Roadmap


2018. 12
2019. 04
2019. 06
2019. 12
2020. 03
2020. 06
TPS
30,000 TPS
80,000 TPS
100,000 TPS
300,000 TPS
500,000 TPS
1,000,000 TPS


2019 3Q
2019 4Q
2020 1Q
2020 2Q
2020 3Q
2020 4Q
MEDIUM Platform Development
Closed Beta
Open Beta
Mainnet Launching
MEDIUM Consortium Network
Consortium 1.0 Start
Consortium 2.0 Start
MEDIUM Ecosystem
MEDIUM Dev. Lab Open
MEDIUM App Center Open
※ MIC – MEDIUM International Conference, MHC – MEDIUM Hackathon Conference
MEDIUM Marketing & Promotion
MHC LA
MIC CHINA
MHC UK
MIC LONDON
MHC SEOUL

05 참고문헌

[1] Harish Sukhwani, Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network) Chrysoula Stathakopoulou IBM Research – Zürich, On Scalability and Performance of Permissioned Blockchain Systems

[2] Linux Foundation, “Hyperledger Architecture”, Linux Foundation, 2017

* 기타 참고문헌

1) Accenture 2018 - Connecting Ecosystems: Blockchain Integration

2) Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network) - Harish Sukhwani

3) EY GLOBAL BLOCKCHAIN BENCHMARKING STUDY - Dr Garrick Hileman & Michel Rauchs 2017

4) hbr.org - Pipelines, Platforms, and the New Rules of Strategy

5) IBM Research Blog - Behind the Architecture of Hyperledger Fabric