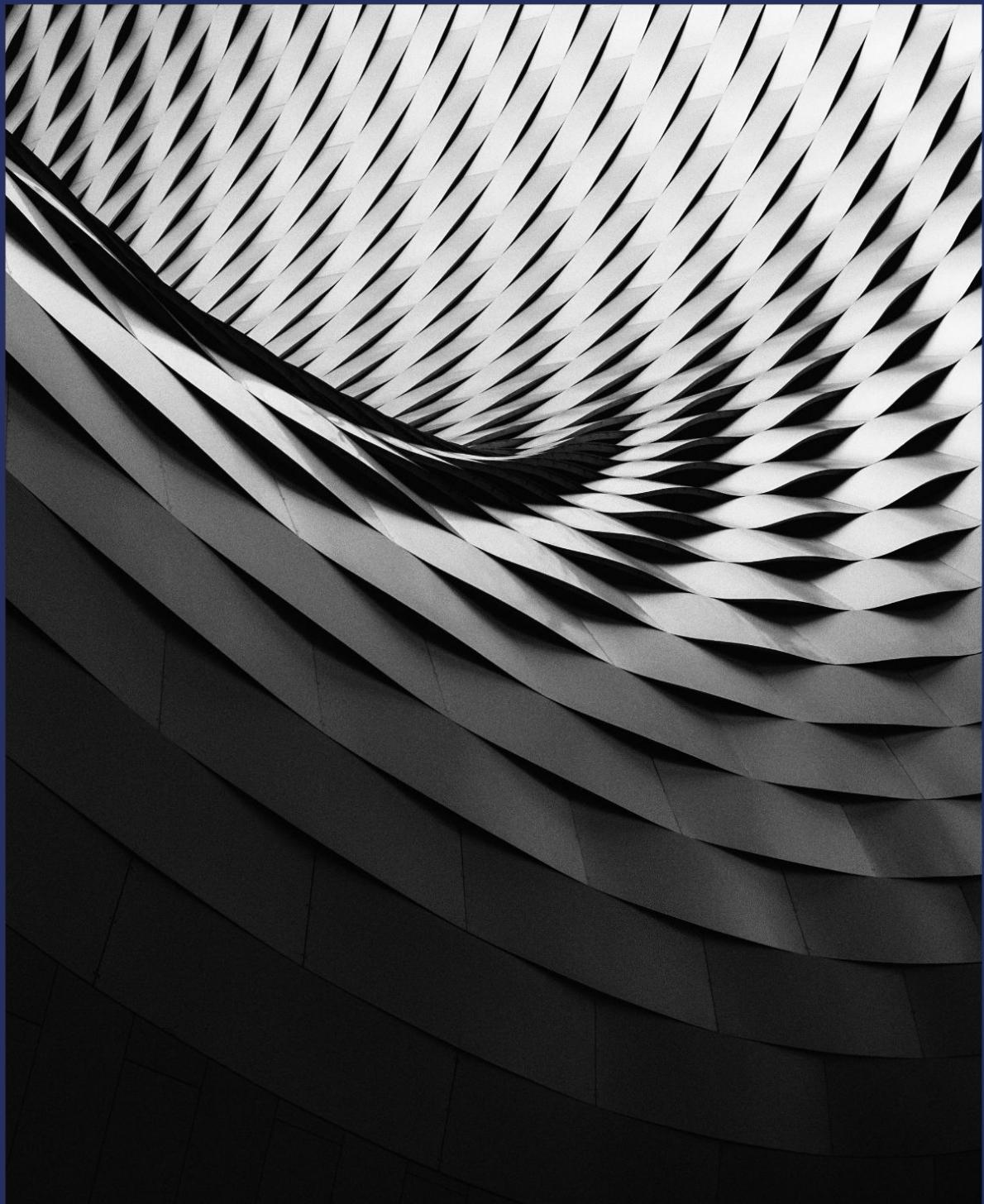


November 25, 2024



Blockchain Infra

Security Token Offering Whitepaper



블록체인스크립 흘페이지

□ www.shinhandigitalasset.com

Contact Information

✉ shs.block@shinhan.com



I. Intro

새로운 금융 인프라의 구축, 토큰증권

토큰증권(Security Token) 발행·유통 규율체계 정비방안

정부, 토큰증권 발행·유통 제도

구축, 2023년 금융위

가이드라인 발표

우리 정부는 국정과제인 “디지털 금융 혁신”정책의 일환으로 토큰증권 발행·유통 제도를 구축해 가고 있다. 2023년 2월 6일 금융위원회는 “토큰증권(Security Token) 발행·유통 규율체계 정비방안(이하 ‘토큰증권 가이드라인’)”을 발표하여 토큰증권 규율 체계와 증권성 판단을 위한 기준을 제시했고 자본시장법과 전자증권법의 개정 계획을 밝혔다.

특히 토큰증권 가이드라인에서는 증권의 권리추정력을 인정하는 분산원장이 갖추어야 할 요건과 그에 필수적으로 포함되어야 하는 데이터를 정의했고 규제의 측면에서는 이해상충 방지를 위해 발행과 유통(시장운영) 시스템을 분리하여 설계할 것에 제한을 두었다.

법제화 난항에 따른 혁신금융 블록체인 인프라 서비스 구축

법안 폐기로 토큰증권 업계

혼란, 당사는 토큰증권 관련

혁신금융사업자 대상으로

BaaS 서비스 제공하며 전략적

대응

금융위원회는 토큰증권 가이드라인을 발표했지만 제 21 대 국회의 임기 종료로 인해 토큰증권(STO) 비즈니스 제도화 관련 법안이 폐기되면서 플랫폼 구축을 위해 대규모 발주를 넣은 증권사들은 혼란에 빠졌다.

이러한 상황에서 당사는 도입되지 않은 제도를 대비한 고비용 인프라 구축을 추진하는 대신 토큰증권 사업자를 중심으로 ‘기초자산 상품 구조 설계’, ‘증권신고서 작성 자문’, ‘혁신금융서비스 지정 전략 컨설팅’, ‘분산원장 인프라 서비스 제공’ 등 토큰증권 벤류체인 전반에 걸친 종합 서비스를 제공하여 급변하는 시장상황에 신속하고 유연하게 대응하는 비즈니스 모델을 구축하기 위해 노력했다. 특히 토큰증권 법제화가 이뤄지지 않은 현재, 제도적 불확실성 아래서 비즈니스를 영위하고자 하는 혁신금융 사업자들은 레거시와 연동된 대규모 분산원장 시스템보다 제도화 이후에도 적은 비용으로 피봇 가능하고 법적 리스크에 유연하게 대응할 수 있는 BaaS(Blockchain as a Service)형 분산원장 서비스를 사용하는 것이 그들의 가장 합리적인 선택일 것으로 판단된다.

Pulse Network, 한국형 토큰증권을 위해 적절히 설계된 금융 인프라

본 백서에서는 블록체인 네트워크가 올라가는 클라우드 시스템 아키텍처를 설계하는 과정에서 정리한 필수 요건들을 분석하고 금융위원회 ‘토큰증권 가이드라인’에서 제시된 분산원장 요건 및 발행·유통 분리구조가 펄스 인프라 시스템에 구체적으로 어떻게 접목되어 구현되는지 살펴볼 것이다.

특히 클라우드 네트워크 위에서 제공되는 BaaS 시스템 아키텍처를 설계함에 있어 무엇이 ‘적절히, 그리고 우수한’ 인프라를 완성시키는지 고민했다. 이에 따라 필수적으로 ‘사용자 수에 따른 규모 확장성’, ‘Latency’, ‘DR(Disaster Recovery)’, ‘Monitoring’, ‘보안’, ‘Interface’ 등이 충족되어야 함을 결론 내렸다.

또한 블록체인 네트워크를 설계하며 금융위원회가 요구하는 요건에 맞는 '합의 알고리즘', '스마트 컨트렉트', '네트워크 업그레이드', 'Key Management', 'Node' 아키텍처를 설계하기 위해 노력했다.

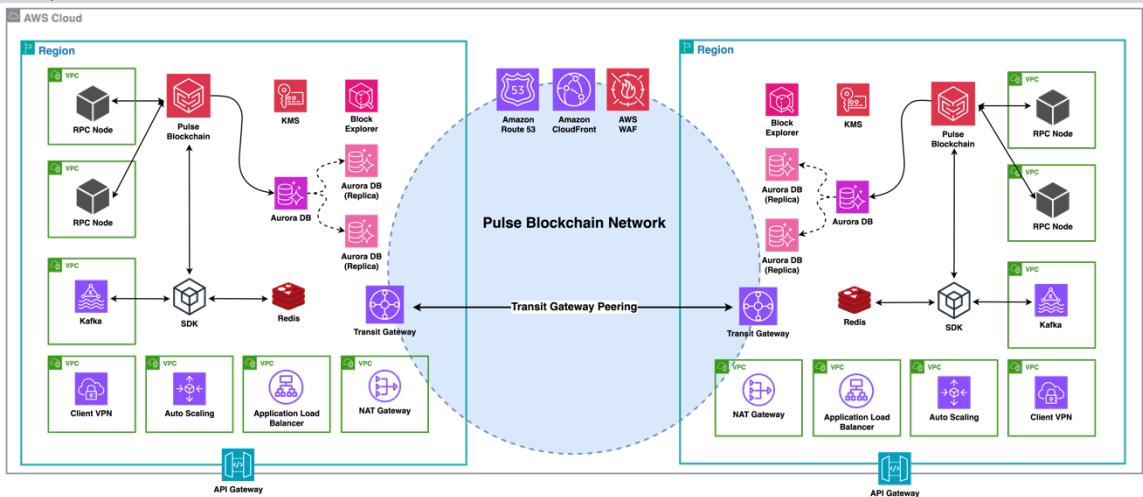
펄스 네트워크는 기술적 고민과 함께 실제 Usecase를 만들기 위해 규제 영역까지 함께 고려된 플랫폼이다. 앞으로 펄스 네트워크는 비즈니스 영역을 지속적으로 확장해가며 한국형 토큰증권 비즈니스에 최적화된 금융 인프라로 자리매김해나갈 것이다.

한국에서 토큰증권 사업자를 위한 금융 블록체인 인프라 서비스를 설계한다는 것은 매우 어려운 과제다. 문제 범위가 아주 크고 선례가 존재하지 않으며 표준적이고 정확한 답이 없기 때문이다. 그럼에도 불구하고 해당 백서가 가보지 않은 길을 개척해나가는 이들에게 길잡이 같은 역할을 할 수 있기를 기대한다.

II. Infra

Infra Architecture

Project Pulse Infra Architecture



출처: 신한투자증권 블록체인스크럼

사용자 수에 따른 규모 확장성

Intro

펄스 인프라, 수평적 확장성
확보 위해 스케일 아웃 방식
채택, 로드 밸런서와 오토
스케일링 활용

충분히 많은 사용자를 지원하는 시스템을 설계하는 것은 도전적인 과제이며, 지속적인 계량과 끝없는 개선이 요구되는 여정이다. 이번 장에서는 펄스 인프라 서비스가 어떻게 사용자 규모에 따른 확장성을 가져가고 있는지 설명할 것이다.

클라우드 인프라가 확장성을 가져가기 위한 방법은 크게 두 가지가 존재한다. 하나는 '스케일 업(scale up)'이라고도 하는 수직적 규모 확장(vertical scaling) 프로세스이고 나머지 하나는 '스케일 아웃(scale out)'이라고도 하는 수평적 규모 확장(horizontal scaling) 프로세스이다. 스케일 업은 기존 서버의 자원(CPU, Memory, Storage, RAM 등) 자체를 향상시키거나 증가시켜 확장성을 가져가는 방법이고 스케일 아웃은 더 많은 서버를 추가하여 성능을 개선하는 행위를 말하는데, 서버로 유입되는 트래픽의 양이 적고 그 변화량의 폭이 충분히 예측 가능하거나 제한적일 때는 스케일 업이 더 좋은 선택이다. 하지만 펄스 인프라에서는 스케일 아웃 방식을 통해 규모 확장성을 확보하기 위해 노력했다. 스케일 업은 '하드웨어의 물리적 한계', '클라우드 인프라 비용 이슈', '단일 장애점 노출과 다중화(Single Point of Failure and Redundancy)', '자동복구(Failover)' 문제를 해결할 수 없는 치명적인 단점이 존재하기 때문이다. 토큰증권 시장은 그 규모가 아직은 영세하지만 앞으로의 성장 가능성을 고려하고 NYSE, KOSPI 등 현대적인 증권 거래소에서는 하루에

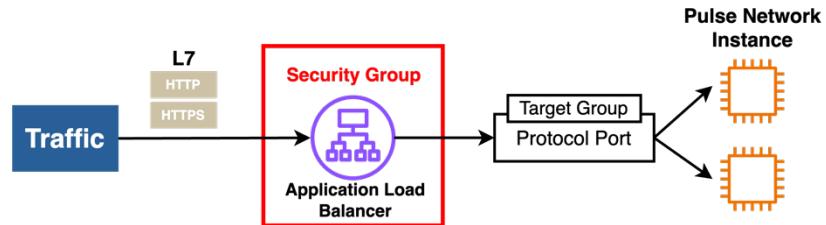
수십 억, 수천 만 건의 거래를 체결시키고 있는 것을 감안했을 때 스케일 아웃 방식으로 규모 확장성을 확보하는 것이 바람직하다. 본 장에서는 펄스 인프라가 어떻게 로드 밸런서(Load Balancer), 오토 스케일링(Auto Scaling), 데이터 베이스 규모 확장을 통해 수평적 규모 확장성을 확보하고 있는지 설명할 것이다.

로드밸런서 (Load Balancer)

펄스 인프라는 ALB를 적용해 트래픽 분산, 성능 및 가용성 유지

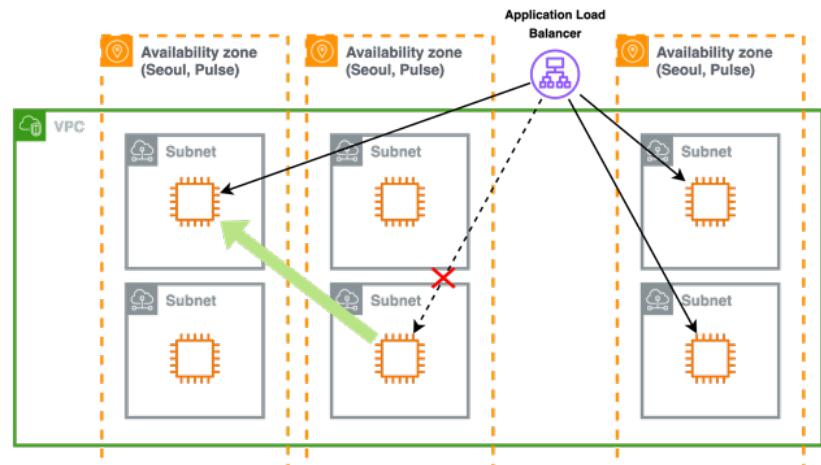
로드 밸런서는 클라이언트로부터 요청을 받아 여러 서버(부하 분산 집합)에 트래픽을 분산시켜 사용자가 증가할 때 인프라의 성능과 가용성을 유지하도록 돋는 중요한 도구다. 펄스 인프라는 Multi Available Zone, 다중화된 데이터 베이스와 통신 계층에 따라 트래픽을 분산처리할 수 있도록 ALB(Application Load Balancer)를 적용하고 있다.

ALB (Application Load Balancer)



출처: 신한투자증권 블록체인스크럼

가용영역 전체를 관할하는 ALB



출처: 신한투자증권 블록체인스크럼

트래픽 증가 시 데이터베이스 확장, 서버 수평 확장, 로드밸런서 자동 분산

▶ 고가용성 확보

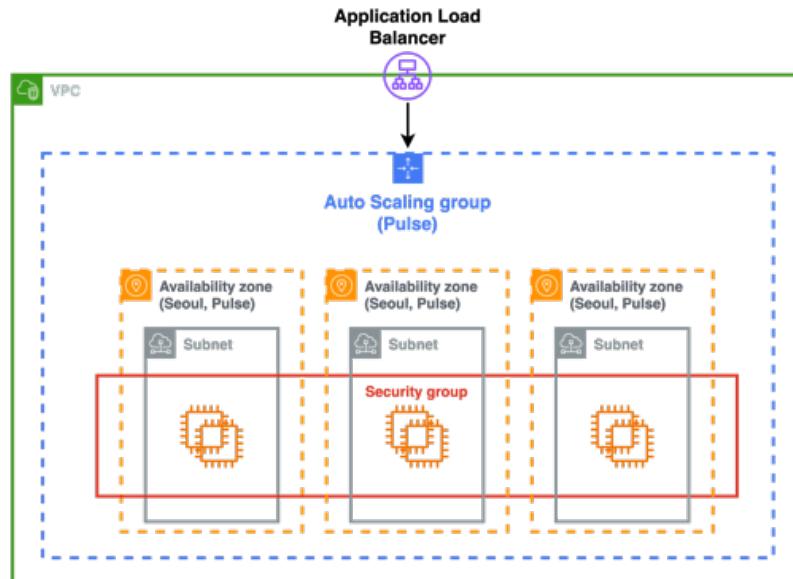
서울에 존재하는 클라우드 센터(AWS)에 자연재해가 일어나거나, 펄스의 Master 또는 Slave DB 가 다운되는 경우 로드 밸런서에 따라 트래픽은 자동으로 Running 상태인 서버로 전송된다.

▶ 확장성 확보

펄스 인프라로 유입되는 트래픽이 가파르게 증가하면 데이터 베이스 규모를 확장하거나 백엔드 서버를 수평적으로 확장할 것이고 이에 맞춰 로드밸런서는 자동적으로 트래픽을 분산한다.

오토 스케일링 (Auto Scaling)

Auto Scaling



출처: 신한투자증권 블록체인스크럼

오토 스케일링 기술 적용해 네트워크 부하 대응 및 비용 절감

Auto Scaling은 클라우드의 확장성을 만들어내는 기술로써 CPU, 메모리, 디스크, 네트워크 트래픽과 같은 시스템 자원들의 메트릭(Metric) 값을 모니터링하다가 서버 사이즈를 자동으로 조절하는 기술이다. 펄스 인프라 역시 예상치 못한 네트워크 부하 변동성에 효과적으로 대응하고 비용 절감 효과를 누리기 위해 Auto Scaling 기술을 적용 중이다.

데이터 베이스 규모 확장과 가용성 확보 (Replication)

저장할 데이터가 많아지면 데이터베이스에 대한 부하도 증가한다. 데이터 베이스의 규모를 확장하는 데에도 인프라의 사용자 수에 따른 규모 확장처럼 두 가지 접근법이 있다. 하나는 수직적 규모 확장법이고 다른 하나는 수평적 규모 확장법이다.



수직적 확장법은 서버 자원 증설 방식이나, 물리적 한계로 수평적 확장이 주로 사용됨

Aurora DB로 수평적 확장 및 고가용성 확보, Master/Slave DB 구조로 쿼리 분산 처리

👉 수직적 확장

스케일업이라고 부르는 수직적 확장법은 기존 서버에 더 많은, 또는 고성능의 자원을 증설하는 방법이다. 가령 AWS의 MariaDB, MySQL 및 PostgreSQL과 같은 RDS는 데이터베이스 엔진에 따라 저장할 수 있는 스토리지 크기와 최대 처리량이 달라진다. 특정 서비스는 단 하나의 master DB를 통해 데이터를 저장하고 트랜잭션을 처리하기도 하지만 대부분의 서비스는 하드웨어의 물리적 한계 및 단일 장애점 노출과 같은 문제로 인해 수평적 확장 방법을 사용한다.

👉 수평적 확장

데이터 베이스의 수평적 확장은 DB 여러 대의 서버를 추가하여 부하를 분산시키는 방법이다. 즉 데이터 베이스를 여러 인스턴스로 분산하여 처리 능력을 향상시킨다. 펄스 인프라는 API Gateway를 통해 발행 및 유통 플랫폼으로부터 들어오는 Database Query를 효율적으로 처리하기 위해 AWS의 Aurora DB를 사용하며 Replication이 구현되어있다.

Database Replication을 통해서 아래와 같은 효용을 추가할 수 있다.

[Database Query 성능 향상]

펄스 클라우드 인프라 서버 위에 존재하는 RDS(Relational Database Service)는 Master / Slave로 나눠져있고 데이터 원본은 Master 인스턴스에, 사본은 Slave 인스턴스에 저장된다. 이때 Master DB는 Insert, Delete, Update와 같은 쓰기 연산(write operation)을 담당하고 Slave DB는 Select와 같은 읽기 연산(read operation)을 담당하여 Query 트랜잭션을 분산하여 처리한다(일반적으로 읽기 연산이 Query 요청의 대부분을 담당하고 Slave DB는 이에 맞춰 서버를 수평적으로 확장).

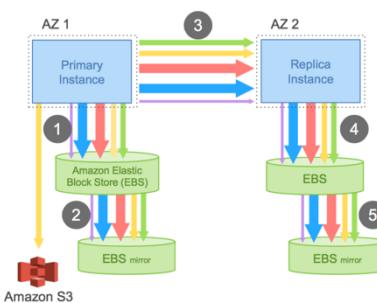
[고가용성 확보]

데이터 베이스를 여러 곳에 복제해 둠으로써, 하나의 데이터 베이스 서버에 장애가 발생하더라도 다른 서버에 있는 데이터를 가져와 가용성을 확보할 수 있다. 자세한 사항은 아래 DR(Disaster Recovery) 챕터에서 후술한다.

👉 MySQL, Aurora

MySQL with Replica

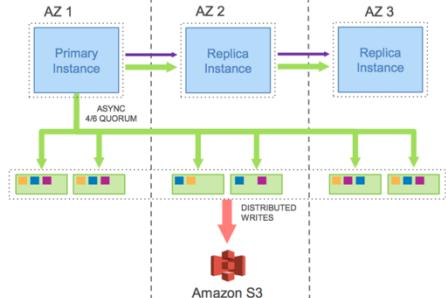
MySQL WITH REPLICA



출처: Amazon Web Services

AWS Aurora

AMAZON AURORA



출처: Amazon Web Services

MySQL, Aurora Read Scaling



출처: Amazon Web Services

Aurora DB는 MySQL 보다
빠른 확장성과 고가용성을
제공, 펄스 인프라에 적용됨

MySQL과 Aurora DB의 가장 큰 차이점은 Storage 및 Replication의 근본적인 프로세스 차이다. MySQL의 경우 Primary Instance의 EBS로 데이터를 쌓고 쌓은 데이터를 다시 EBS로 미러링한 다음 Replication을 통해 Replica Instance로 데이터를 보낸다. 보내진 데이터는 다시 Replica의 EBS에 쌓인다. 반면 Aurora의 경우에는 4/6 쿼럼을 사용하여 각 다른 가용영역에 데이터를 저장하며 Replica Instance로 보내는 데이터는 FRM(DB의 테이블 구조를 정의하는 파일)과 Redo Log(DB 로그파일)다. 때문에 무거운 데이터를 계속해서 옮기지 않으며 빠르게 Sync를 맞출 수 있다 (Network Bandwidth 최소화). 결국 Aurora DB는 Instance 영역과 Storage 영역을 분리하여 설계되었기 때문에 MySQL 보다 빠른 확장성과 고가용성을 확보할 수 있다.

펄스 인프라에서 사용되는 RDS는 빠른 읽기 확장성과 고가용성을 확보하기 위해 Aurora DB를 통해 데이터 베이스를 구성하고 있다.

Latency

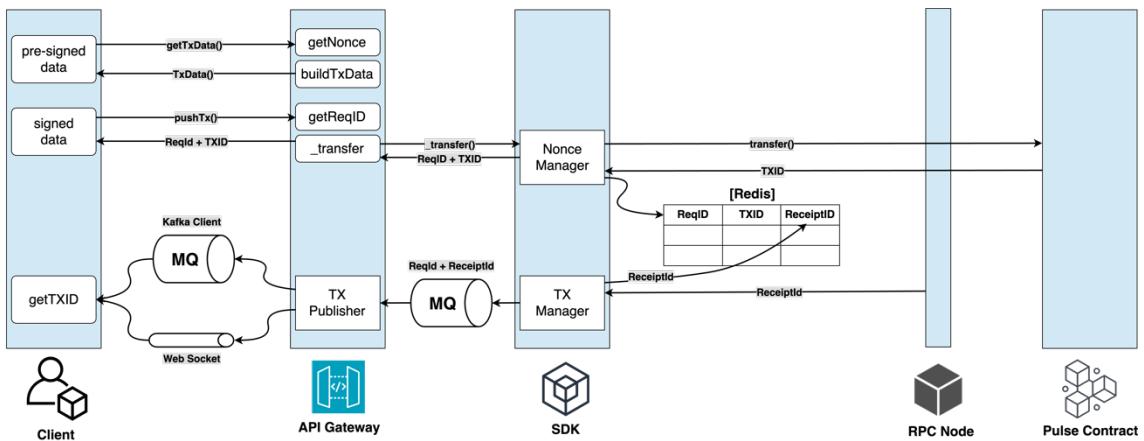
캐시 (Cache)

Redis

Redis 캐시로 블록체인
트랜잭션 응답 속도 개선,
Latency 감소

캐시(Cache)는 값비싼 연산 결과 또는 자주 참조되는 데이터를 메모리 안에 두고, 뒤이은 요청이 보다 빨리 처리될 수 있도록 하는 저장소다(DB(Database)보다 빠르게 응답). 펄스 네트워크에서는 블록체인의 Write Transaction 처리 시 Redis(Remote Dictionary Server)를 사용하여 보다 빠른 트랜잭션 응답을 Return 함으로써 Latency 를 개선한다.

Write Transaction의 비동기 처리방안



출처: 신한투자증권 블록체인스크럼, 블록체인글로벌

Write Transaction 처리 시
Redis 와 Kafka 로 순서 보장

블록체인 트랜잭션의 종류는 블록체인에 데이터를 기록하거나 상태를 변경하는 Write Transaction 과 단순히 블록체인 원장에 존재하는 데이터를 조회하는 Read Transaction(Query Transaction) 등으로 나뉜다. 특히 Swap()과 같은 Write Transaction 은 펄스 네트워크의 유통 시스템으로부터 서명된 체결 데이터를 받아와 블록체인에 영구히 기록하는 작업을 수행하기 때문에 그 적시성과 순서보장이 매우 중요하다.

펄스 네트워크에서는 Client 의 Write Transaction 요청 시 순서에 따라 API Gateway 뒤에 존재하는 SDK Layer, Kafka, Redis, RPC Node 가 서로 유기적으로 통신 함으로써 Clinet 에게 응답 데이터를 전송한다. 특히 이 과정에서 백그라운드에서 항상 실행되는 daemon process 에 맞춰 일정 주기마다 Redis 데이터 테이블을 참조하여 Client 의 요청이 블록체인 원장에 포함되어 Confirmed 되었음을 확인함으로써 Latency 를 최소화시킨다.

TXID 가 Confirmed 되었음을 확인하면 TX Manager 는 Kafka Message Queue 에 체결완료 데이터를 집어넣고 TX Publisher 는 MQ 또는 Web Socket 통신방법을 통해 Client 에 데이터를 전파시킨다 (Client 는 체결완료

데이터를 수신받을 때 MQ 또는 Web Socket 통신방법 중 어느것을 사용해도 무방하다).

DR (Disaster Recovery)

Intro

다중 데이터베이스와 장애
조치로 99.99%
고가용성 확보

거래 인프라 시스템에는 가장 엄격한 수준의 신뢰 및 안정성이 요구된다. 단 몇 초 정도의 장애로도 고객으로부터 신뢰를 잃을 수 있기 때문이다. 이러한 점을 고려하여 펄스 인프라는 다중 데이터 베이스, 다중 가용영역 등을 통해 단일 장애 지점(SPOF)을 제거하였고 최소 99.99%(하루 8.64 초 미만의 서버 장애 시간)의 고가용성을 확보하기 위해 설계되었다.

뿐만 아니라 펄스 인프라는 단일 장애 지점에 대해 장애 감지 및 백업 인스턴스로의 장애 조치 결정 로직이 잘 마련되어 있다. 데이터 베이스나 체결엔진처럼 상태를 저장하는 컴포넌트는 유사시 주 인스턴스에서 부인스턴스로 권한과 데이터를 옮겨 시스템이 연속적으로 운영될 수 있도록 운영되어야 하기 때문이다.

가용율에 따른 장애시간 (예상)

가용율	하루당 장애시간	주당 장애시간	개월당 장애시간	연간 장애시간
99 %	14.40 분	1.68 시간	7.31 시간	3.65 일
99.9 %	1.44 분	10.08 분	43.83 분	8.77 시간
99.99 %	8.64초	1.01 분	4.38 분	52.60 분
99.999 %	864.00 밀리초	6.05 초	26.30 초	5.26 분
99.9999 %	86.40 밀리초	604.80 밀리초	2.63 초	31.56 초

출처: 신한투자증권 블록체인스크럼

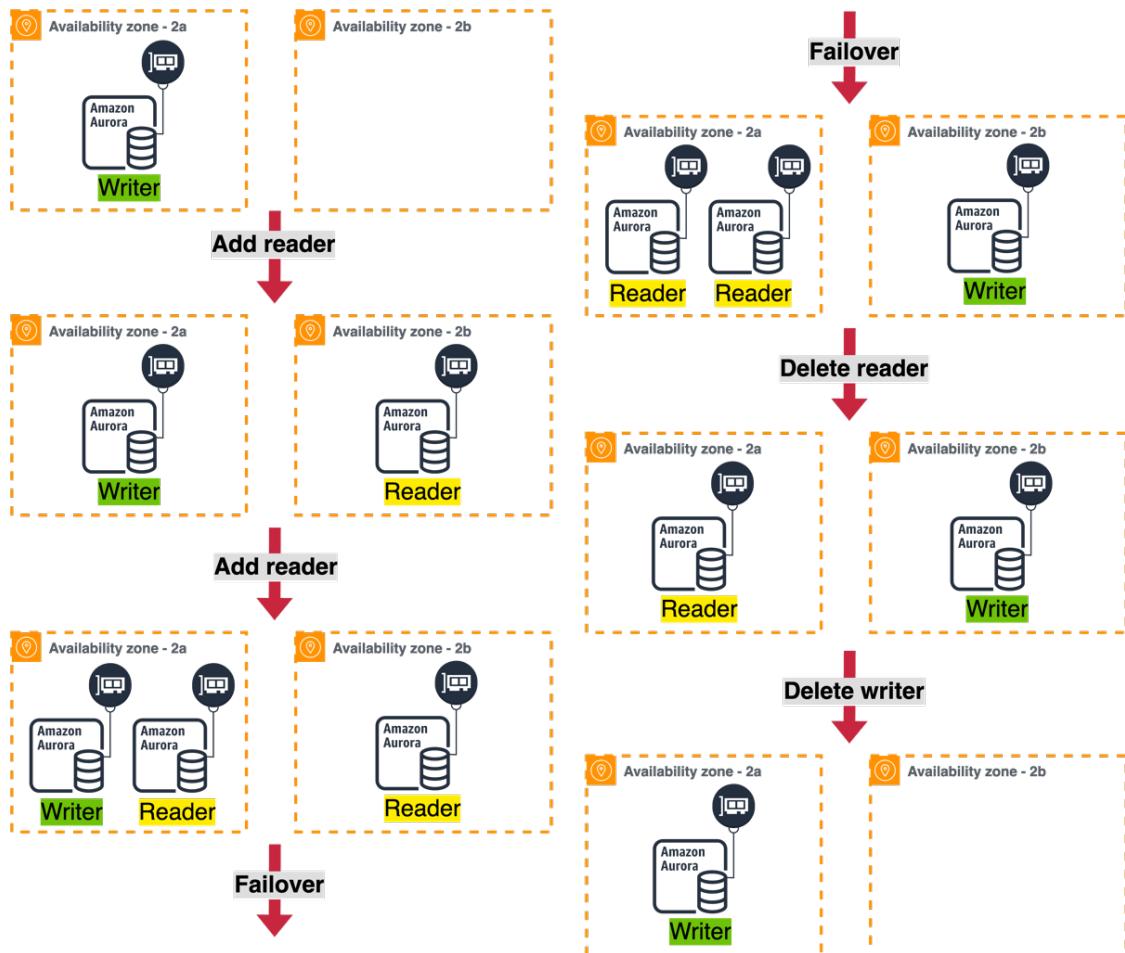
서울 AWS 클라우드 4 개
가용영역 사용해 높은 가용성
및 내결합성 보장

AZ (Available Zone)

데이터 베이스를 Master / Slave로 나눠 부분적으로 가용성을 어느 정도 확보할 수 있지만 천재지변의 이유로 펄스 클라우드 서버가 돌아가고 있는 데이터 센터가 무너지는 상황이 찾아오면 어떻게 될까? 분명한 것은 확률이 낮은 상황이지만 치명적인 상황이 발생할 수 있다는 것이다. 클라우드 인프라 관점에서 이러한 문제점은 Multi Available Zone(클라우드 인프라에서 물리적, 논리적으로 분리된 그룹을 의미하며 고가용성과 내결합성을 보장하기 위해 운영)을 통해 해결할 수 있다. 펄스 인프라는 매우 높은 가용성을 목표로 설계되었기 때문에 AWS 클라우드의 서울 Region 내에 총 4 개의 가용영역을 사용하여 설계되었다.

📍 장애처리 결정 로직

Aurora DB의 Instance 변화과정



출처: 신한투자증권 블록체인스크럼

위 그림은 Aurora DB 가 단일 AZ 상태에서 다중 AZ로 변하는 과정을 설명한다.

1. 단일 인스턴스 상태의 Aurora 에 읽기 노드를 추가한다.
2. 서브넷 그룹의 다른 멤버 서브넷에 읽기 노드가 생성된다. (기존 AZ-a 를 선택해 읽기를 추가할 수도 있다.)
3. 장애 조치를 하면 기본 인스턴스(Write)는 읽기 노드로 변경되고 AZ-2b 의 인스턴스가 기본 인스턴스(Write)로 변경된다.
4. AZ-a 의 읽기 노드를 삭제해도 클러스터에 변화가 없다.
5. AZ-b 의 기본 인스턴스를 삭제하면 읽기 노드가 기본 인스턴스로 변경된다.

로드밸런서 및 multi-AZ를 활용한 고가용성 시스템 구축

장애가 발생한 가용영역의 EC2 인스턴스의 상태 점검이 실패하기 시작하면 Application Load Balancer 는 자동적으로 트래픽을 다른 곳으로 보내기 시작한다.

Monitoring

로그 (log), 매트릭 (Metric)

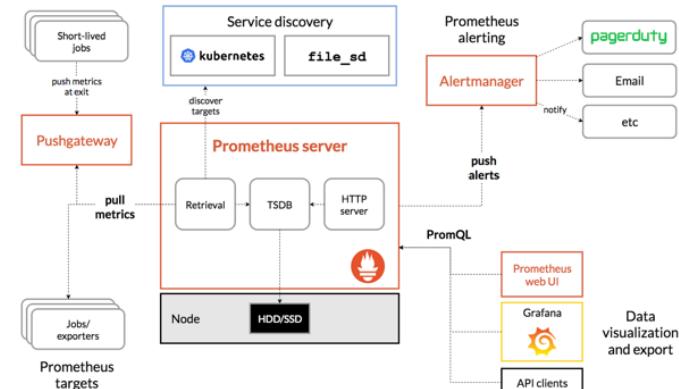
Kubernetes 기반으로

Prometheus 와 Grafana 통해
강력한 모니터링 시스템 제공

한두 개의 서버를 돌리는 수준의 소규모 서비스를 제공할 때는 반드시 Monitoring(모니터링) 시스템을 구축할 필요가 없다. 하지만 제공하고자 하는 서비스 이용자의 수가 늘어나고 사업의 규모가 커지면 모니터링 시스템은 장애대응과 서비스 안정성을 위해 필수적으로 필요한 기능이 된다. 펄스 인프라는 소규모 서버가 각각 Docker(도커) 컨테이너로 나눠져 있고 Kubernetes(쿠버네티스) 환경에서 통합되어 관리되기 때문에 Prometheus, Grafana 를 사용하여 고객사에게 효과적이고 강력한 모니터링 시스템을 제공하도록 설계되었다.

Prometheus, Grafana

Prometheus, Grafana



출처: Cloud Builders

Prometheus(프로메테우스)는 Metric 수집, 시각화, 알림, 서비스 디스커버리 기능을 모두 가지고 있는 오픈소스 기반의 모니터링 시스템이고 Grafana(그라파나)는 프로메네우스로 수집한 데이터를 관리자가 쉽게 파악할 수 있도록 시각화하는 도구다.

펄스 인프라에서는 주로 금융사가 추가됨에 따라 그 수가 계속해서 늘어나는 validator node 의 pod 와 2 개의 rpc node 가 구동되는 pod 로 부터 프로메테우스가 데이터를 수집하고 그라파나를 통해 시각화하여 인프라 참여사에게 제공된다.

Interface

API Gateway

API List (Partial disclosed)

구분	API	HTTP Method	End Point
Operator-Transaction	Transaction 전송	POST	/main/v1/transaction/send
Token Document	토큰 문서 등록	POST	/main/v1/tokens/{token}/documents
Token Document	토큰 문서 조회	GET	/main/v1/tokens/{token}/documents/{docName}
Token Document	토큰 문서 삭제	DELETE	/main/v1/tokens/{token}/documents/{docName}
KYC	지갑 주소 KYC 등록	POST	/main/v1/kyc/{token}/{holder}
KYC	지갑 주소 KYC 등록 해제	DELETE	/main/v1/kyc/{token}/{holder}
Token Holder	토큰 보유자 파티션 목록 조회	GET	/main/v1/holders/{holder}/tokens/{token}/partitions
Token Holder	토큰 보유자 토큰 잔액 조회	GET	/main/v1/holders/{holder}/tokens/{token}/balance
Token	토큰 환수	POST	/main/v1/tokens/{token}/redeem
Token	토큰 발행	POST	/main/v1/tokens/{token}/issue
Token	토큰 정보 조회	GET	/main/v1/tokens/{token}/info
Operator-Redeem	토큰 환수 트랜잭션 데이터 생성	POST	/main/v1/redeem/tx/data
...

출처: 신한투자증권 블록체인스크립트, 블록체인글로벌



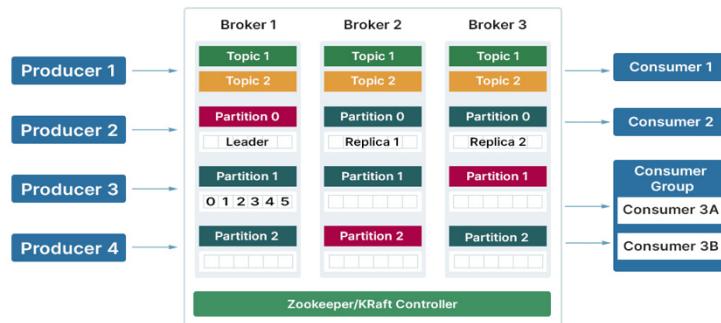
API Document

API Docs 화면

출처: 블록체인글로벌

Legacy 환경에서 DvP (Delivery versus Payment)를 효율적으로 달성하기 위한 Kafka 솔루션

Kafka Architecture



출처: KSOLVES

Kafka 솔루션

Kafka 메세지로 라우팅
처리에 증권사 Legacy 시스템
연계 문제 해결, DvP 달성

증권사의 Legacy(레거시) 시스템에서 발생하는 가장 큰 문제점은 종 하나는 EAI(Enterprise Application Integration)/FEP(Front End Processor) 등을 활용하여 대외계(B2B) 연계 시 빈번하게 에러가 발생하며 지속적인 수정개발이 필요하다는 것이다. 때문에 증권사 Legacy 원장에 외부 업체(증권사 포함)가 붙어 API Interface를 통해 프로토콜 통신을 만들어내는 작업은 매우 소모적이며 오랜 시간이 걸리는 일이다.

펄스 인프라 네트워크는 이러한 점을 개선하기 위해 Kafka를 통해 Message Routing 처리 솔루션을 제공한다. 이러한 솔루션을 바탕으로 펄스 네트워크 참여 금융사들은 직접 그들 간의 API Interface를 맞추지 않더라도 Legacy 환경에서 소통이 가능하며 이를 통해 효율적으로 DvP(Delivery versus Payment)를 달성할 수 있다.

III. Blockchain

금융위 분산원장 안에 맞는 블록체인 네트워크 설계

Intro

펄스 네트워크, 금융위원회의
토큰증권 분산원장 요건 충족

신한투자증권, SK 증권 노드
참여, ERC 표준 기반 스마트
컨트렉트 배포

금융위원회는 2023년 2월 자본시장법 규율 내에서 STO를 허용시키기 위한 초석으로 '토큰 증권 발행·유통 규율체계 정비방안'을 발표했고 관련 문서에는 분산원장이 갖추어야 할 요건이 명시되어 있다. 법제화가 진행되는 과정에서 향후 하위법령이 개정됨에 따라 분산원장이 갖추어야 할 요건이 변경 및 확대될 가능성이 있겠지만 펄스 네트워크는 현재 시점을 기준으로 금융위원회가 제시한 '분산원장 요건(안)'과 '분산원장에 포함되어야 하는 데이터'의 기준을 충족시키고 있다.

특히 금융위원회는 분산원장의 트랜잭션 처리에 있어 하나의 노드가 강력한 파워를 갖지 않을 것을 요구하였는데 현재 시점 기준(2024년 7월)으로 펄스 네트워크는 STO 플랫폼에 발행될 증권 관련 사무를 원활하게 처리할 수 있는 금융기관인 '신한투자증권, SK 증권'이 블록체인 노드로서 참여 중이다.

또한 펄스 네트워크는 Ethereum(이더리움) 표준에 맞는 ERC-20, ERC-721, ERC-1400 규격을 커스터マイ즈하여 Smart Contract(스마트 컨트랙트)를 배포하고 있는데 이때 '발행인, 계좌관리기관, 증권의 종류, 종목을 식별할 수 있는 정보, 보유 및 발행수량 또는 금액, 질권이 설정된 경우 그 수량 또는 금액, 신탁재산 여부' 등의 데이터를 포함시켜 분산원장에 기록하고 있다.

펄스 인프라가 이해상충 방지를 위한 발행과 유통(시장운영) 분리 원칙을 어떻게 구현하고 있으며 T+0(당일 내 결제)결제가 적용된 DvP 구현을 어떻게 만들어냈는지에 대해서는 3장에서 후술할 것이다.

분산원장 요건 (안)

- 권리자 정보 및 거래 정보가 시간 순서대로 기록되고, 사후적인 조작·변경이 방지될 것
- 분산원장에 기록된 권리자 정보 및 거래정보와 실제거래내역 사이의 동일성이 계좌관리기관의 책임으로 입증 가능할 것
- 권리자 정보 및 거래 정보가 복수의 분산된 장부에 동일하게 기록될 것
- 전자등록기관, 금융기관 또는 발행인과 특수관계인에 해당하지 않는 계좌관리기관이 다수 참여하여 분산원장을 확인할 수 있을 것
- 권리자 및 거래정보 기록을 위해 별도의 가상자산을 필요로 하지 않을 것
- 분산원장으로 기록하기 적합한 권리를 등록할 것
(상장증권, 상장 DR, 파생결합증권 제외)
- 개인정보보호법, 신용정보법 등 법령을 위반하지 않을 것
- 노드가 51% 이상 다른 금융기관 등*으로 구성되어야 하며, 발행하려고 하는 증권 관련 사무를 처리에 적합하여야 함

* 다른 금융기관, 전자등록기관, 특수관계인에 해당하지 않는 계좌관리기관

* 전자증권법상 전자등록기관 및 계좌관리기관으로 구성된 node

합의 알고리즘 (Concensus)

Intro

*비잔틴 장군의 문제는 1982년 래슬리 램포트, 마샬 피즈가 함께 쓴 논문에서 소개된 이후 컴퓨터 공학에서 고전적인 난제로 꼽히는 문제다. 어떻게 여려 노드(장군)들 중 일부 노드가 악의적이거나 오작동하는 상황에서도 일관된 결정을 내릴 수 있는지에 대한 질문을

**비잔틴 장애 허용(BFT, Byzantine Fault Tolerance)이란 장애가 있더라도 악의적인 노드가 전체의 3분의 1을 넘지 않는다면, 시스템이 정상 작동하도록 허용하는 합의 알고리즘이다.

합의 알고리즘은 블록체인 네트워크에서 합의를 달성하기 위한 메커니즘으로 정의할 수 있다. 이 과정에서 네트워크의 각 노드들은 Byzantine Generals Problem(비잔틴 장군의 문제)*를 해결해야 한다. Bitcoin(비트코인)의 작업증명(PoW, Proof of Work)을 가장 일반적인 예로 들 수 있다.

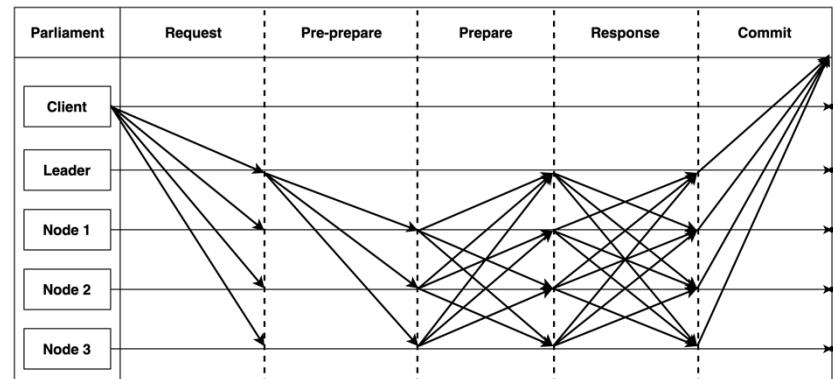
작업증명 방식의 합의 알고리즘은 블록체인 중 가장 처음 제시되었기 때문에 충분히 검증되었고 신뢰할 수 있는 알고리즘이지만 블록체인 네트워크 노드들이 Mining(채굴)이라 불리는 작업을 실행하기 위해 경쟁적으로 과도한 컴퓨팅 파워를 사용하고 즉각적인 합의를 이뤄낼 수 없다는 점에서 단점을 들어낸다.

펄스 블록체인 네트워크는 QBFT(Quorum Byzantine Fault Tolerance, 쿼럼 비잔틴 장애허용)** 알고리즘을 사용한다. 펄스와 같이 이미 검증된 금융기관이 노드로서 참여하는 프라이빗 네트워크에서는 즉각적인 합의(Finality)와 빠른 트랜잭션 처리가 보장되어야 하기 때문이다. 특히 QBFT는 PBFT(Practical Byzantine Fault Tolerance, 프렉티컬 비잔틴 장애 허용) 알고리즘의 변형으로써 PBFT 보다 뛰어난 보안성과 트랜잭션 처리 성능을 보여주기 때문에 국내 토큰증권 블록체인 네트워크의 합의 알고리즘으로써 사용되기 적합하다.

Byzantine Fault Tolerance (BFT)

👉 PBFT (Practical Byzantine Fault Tolerance)

The main process of PBFT



출처: 신한투자증권 블록체인스크립



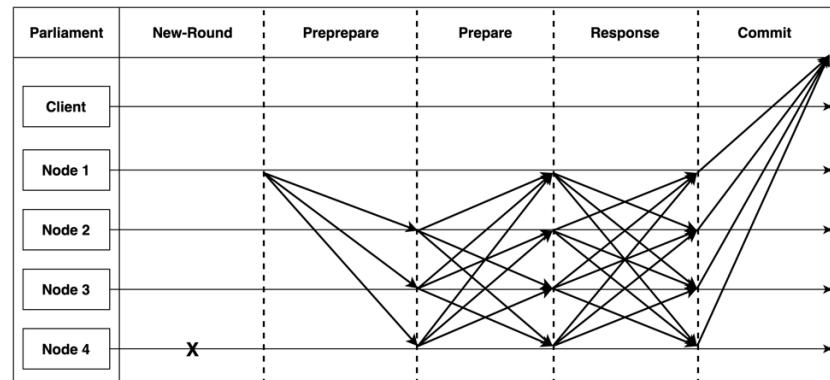
PBFT, 악의적인 노드에도 합의 가능, PoW·PoS 보다 빠른 Finality 확보

PBFT(Practical Byzantine Fault Tolerance)란 비동기 분산시스템 네트워크에서 악의적인 노드가 존재하더라도 해당 분산시스템에 참여한 모든 노드가 성공적으로 합의에 도달할 수 있도록 개발된 합의 알고리즘이다. 비잔틴 장애 허용 알고리즘은 네트워크에서 악의적인 노드가 f 개 있을 때, 총 노드 개수가 $3f+1$ 개 이상이면(악의적인 노드가 전체 노드의 30%미만) 해당 네트워크에서 이루어지는 합의는 신뢰할 수 있다는 것을 수학적으로 증명한다.

PoW나 PoS와는 달리 다수결로 의사결정한 뒤 블록을 만들기 때문에 블록체인의 분기가 발생하지 않는다. 또한 노드들이 경쟁적으로 컴퓨팅 파워를 사용하지 않기 때문에 빠른 Finality를 확보할 수 있다. 하지만 각 노드는 전체 네트워크와 의사소통을 해야 하기 때문에 참가자가 증가하면 그에 따라 통신량이 증가하고 처리량이 저하된다.

IBFT (Istanbul Byzantine Fault Tolerance)

The main process of IBFT



출처: 신한투자증권 블록체인스크립

IBFT, PBFT 기반으로 합의 노드를 동적으로 구성, 효율적 참가자 선발 가능

IBFT(Istanbul Byzantine Fault Tolerance)는 PBFT 합의 알고리즘의 변형이다. PBFT 와 마찬가지로 $2/3$ 이상의 합의 노드가 동의하면 블록을 생성할 수 있다($3f+1$) . PBFT 와 IBFT 의 가장 큰 차이점은 합의 노드를 동적으로 구성할 수 있다는 점이다. 라운드 로빈(round-robin) 방식 또는 Weighted Round Robin(WRR) 방식을 통해 매 블록 생성주기마다 Proposer 를 선출한다. 이를 통해 보다 효율적인 참가자 선발과 분산된 네트워크 활동을 도모할 수 있다.

QBFT(Quorum Byzantine Fault Tolerance)

QBFT, 금융기관 노드로 제한된 Prosper 사용, PBFT·IBFT 보다 금융규제에 적합

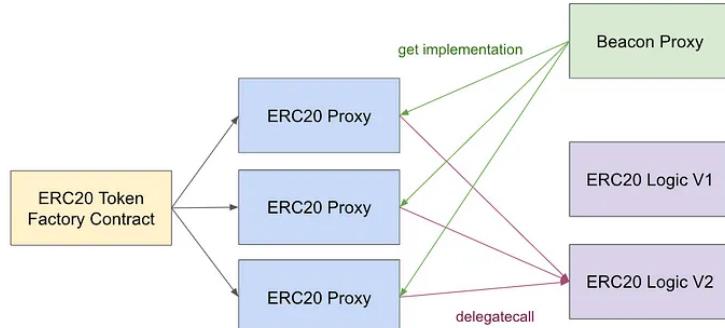
QBFT(Quorum Byzantine Fault Tolerance, 쿼럼 비잔틴 장애허용)는 프라이빗 블록체인 네트워크에서 사용되는 엔터프라이즈급 합의 알고리즘이다. IBFT 2.0 합의 알고리즘의 변형으로써 IBFT 와 비교했을 때 가장 큰 차이점은 권한을 가진 노드만 네트워크에 메세지를 전파하는 Proposer 가 될 수 있도록 설정할 수 있는 기능이 존재한다는 것이다. 금융위원회가 제시하는 규제 스펙에 맞는 토큰증권 분산원장에서는 '플랫폼에 발행될 증권 관련 사무를

'원활하게 처리할 수 있는 금융기관'이 노드로서 참여해야 하기 때문에 모든 노드가 검증 과정에 참여하는 PBFT, IBFT 보다 적합한 합의 알고리즘이라 판단할 수 있다.

스마트 컨트렉트 (Smart Contract)

Upgradable Smart Contract

Beacon Proxy

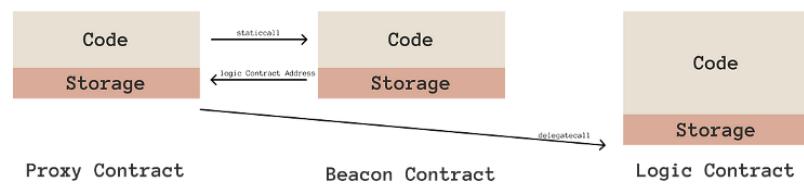


출처: 블록체인글로벌

펄스 블록체인 Proxy Pattern
적용한 업그레이더블 스마트
컨트렉트로 변화 대응

흔히 블록체인에 존재하는 스마트 컨트렉트 코드는 절대로 변경할 수 없다는 이야기를 많이 들어왔을 것이다. 이러한 특성은 네트워크 참여자에게 신뢰를 부여할 수 있는 블록체인의 가장 큰 장점이기도 하지만 코드를 변경할 수 없다는 점은 대부분의 개발자들에게 재앙으로 다가온다. 이러한 문제를 해결하기 위해 스마트 컨트렉트 개발자들은 Upgradable Smart Contract(업그레이더블 스마트 컨트렉트) 아이디어를 제시했다. 업그레이더블 컨트렉트는 말 그대로 기능에 대한 업그레이드가 가능한 컨트렉트를 의미한다. 업그레이더블 컨트렉트는 Proxy Contract(프록시 컨트렉트)와 Beacon Contract(비콘 컨트렉트)로 구현되는데 펄스 분산원장에서 배포되는 스마트 컨트렉트도 변화하는 규제방안과 인프라 참여자 니즈에 맞춰 동작할 수 있도록 Proxy Pattern 이 적용되어 업그레이드 가능하도록 작성되어있다.

Beacon Contract



프록시 컨트랙트와 로직 컨트랙트 사이의 비콘 컨트랙트

출처: 블록체인글로벌

Proxy Contract (프록시 컨트랙트)

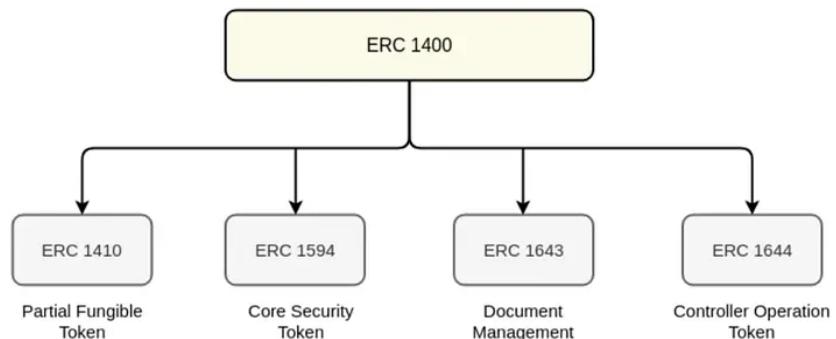
프록시 컨트랙트는 사용자의 요청을 비콘 컨트랙트가 가리키는 실제 로직 컨트랙트로 '전달'한다. 즉, 로직 컨트랙트에 실행을 위임(delegatecall)한다.

Beacon Contract (비콘 컨트랙트)

비콘 컨트랙트는 실제 로직이 포함된 컨트랙트의 주소를 가지고 있다. 즉, 프록시 컨트랙트가 어떤 로직 컨트랙트를 호출해야 하는지를 알려주기 위한 이정표 역할을 한다.

Security Token Standard Smart Contract

ERC-1400



출처: 블록체인글로벌

ERC-1400 표준 사용해 한국형
토큰증권 인프라 구축, 포괄적
기능 제공

ERC 는 "Ethereum Request for Comments"의 약자로, 이더리움 블록체인에서 새로운 스마트 컨트렉트 표준을 제안하고 정의하는 데 사용된다. 이러한 제안은 이더리움 커뮤니티에서 논의된 후 합의를 거쳐 이더리움 네트워크의 토큰, 스마트 컨트렉트 및 기타 기능을 개선하는 데 사용된다. 펄스 네트워크는 한국형 토큰증권 인프라를 설계하고 금융당국의 규제요건을 충족시키기 위해 ERC-1400 스마트 컨트렉트 표준을 사용하고 있다.

ERC-1400 스마트 컨트렉트는 실물자산을 기초하여 발행되는 증권형 토큰의 발행, 유통, 소유권, transfer 제한, 권리 등과 관련된 업무를 원활하게 처리할 수 있도록 지원함으로써 토큰증권에 대한 가장 포괄적인 표준을 제시한다. 특히 ERC-1400은 그림과 같이 ERC-1410, ERC-1594, ERC-1643, ERC-1655를 모두 통합하여 활용하는 Umbrella Architecture 형태로 구현되어 있는데 이는 각각 파티션 기능, 거래 유효성 검증 기능, 주요문서 저장 기능, 법적조치에 따른 강제 거래제한 기능 등을 지원한다.

👉 ERC-1410 (Partially Fungible Tokens)

- 부분적으로 대체 가능한 토큰(Partially Fungible Tokens, PFTs)에 대한 표준을 제공
- 토큰이 다양한 파티션 또는 하위 집합으로 분류될 수 있게 하여, 각기 다른 규제 준수 요구 사항이나 사용 조건을 가진 토큰의 관리를 가능하게 한다

👉 ERC-1594 (Core Security Token Standard)

- 토큰증권에 대한 핵심 표준을 정의
- 토큰증권의 전송 및 발행, 규제 준수 검사, 문서화 등의 기능을 포함한다

👉 ERC-1643 (Document Management Standard)

- 스마트 컨트랙트를 통한 문서 관리에 관한 표준을 제공
- 보안 토큰에 연관된 문서(예: 규제 준수 문서, 투자자 정보 등)를 저장, 갱신, 삭제할 수 있는 인터페이스를 정의
- 이를 통해 증권관련 문서가 투명하게 관리

👉 ERC-1644 (Controller Token Operation Standard)

- 토큰 컨트롤러가 토큰의 강제 전송이나 소각 등의 특별한 연산을 수행할 수 있는 권한을 정의
- 이 표준은 규제 준수 또는 기타 행정적 이유로 특정 토큰의 이동이 필요할 때 사용됨

Key Management

키 관리

트랜잭션 목적에 따라 3 가지

Key 생성 및 관리,

Operator-Issuer Key 분리

Pulse Infra는 트랜잭션의 목적과 권한에 따라 3 가지 Key가 생성되어 관리된다. Transfer, Swap 등의 트랜잭션을 Sign 할 수 있는 Operator Key와 Smart Contract를 배포할 수 있는 Issuer Key는 각각의 목적과 보안적 성격에 따라 각기 다른 곳에서 관리된다.

역할에 따른 키 관리 위치

역할	담당자	키 관리 위치	행위
Issuer (발행자)	혁금사업자 (펄스-BCG 대행)		토큰 발행
			토큰 소각
			토큰 전송 제한 설정
			컨트롤러 지정
			운영자 지정
Operator (운영자)	발행사 / 유통사		토큰 전송 및 Swap
			토큰 잔액 조회
			토큰 전송 가능 여부 확인
Controller (컨트롤러)	계좌관리기관		강제 전송
			토큰 동결
			토큰 압류

출처: 신한투자증권 블록체인스크럼, 블록체인글로벌

Block Explorer

Blockscout

Blockscout 기반 블록체인
익스플로러로 트랜잭션
명확하고 효율적 확인 지원

Explorer(익스프롤러)는 확인되지 않은 영역을 알아보고 탐색하는 무언가를 말한다. 블록체인 네트워크에서 익스플로러는 여러 참여자 즉, 노드들이 블록체인상에서 발생하는 활동을 감시하고 기록하며 서로의 데이터를 비교할 수 있도록 만든다. 펄스 네트워크에서는 Hyperledger Besu 네트워크를 지원하기 때문에 EVM(Ethereum Virtual Machine) 계열의 Blockscout를 커스터마이즈하여 노드 참여자 및 금융당국이 블록체인 트랜잭션을 명료하고 효율적으로 확인할 수 있도록 그 기능을 제공한다.

Blockscout 통해 확인할 수 있는 데이터

- 블록 높이, 처리상태 (Success, Pending, Denied), 생성 시간, 포함된 트랜잭션 및 컨트랙트 수, 블록채굴 보상, 블록보상 금액 수취인(증권사), 블록채굴 난이도, 블록사이즈
- 사용된 Gas량, Gas Limit, 소각량

- 트랜잭션 Hash, 처리상태 (Success, Pending, Denied), 생성 시간, From-to (주소 및 증권사), Value (보낸 양), 트랜잭션 수수료 (Fee), Gas Price
- Gas Limit, 트랜잭션에 사용된 Gas 량, 소각량, Nounce, Input Data, 트랜잭션 Type(EIP-1559)
- 스마트 컨트렉트 정보 (상품 이름, 심볼, 총 발행량, 발행사, 공적문서, 보유자 목록 등)

Blockscout 화면

Latest blocks

Network utilization: 0.00%

 1524881	1s ago
Txn 0	
Reward 0	
Validator 0x94...4002	

 1524880	5s ago
Txn 0	
Reward 0	
Validator 0x49...1568	

 1524879	10s ago
Txn 0	
Reward 0	
Validator 0xBB...F7F6	

[View all blocks](#)

Latest transactions

scanning new transactions...

 Contract call	Success	↳ 0xa905289ce95f79b264abfe2625...9c2e	5m ago	↓ 0x62...Ef57	ETH 0
 Contract creation	Success	↳ 0x92eac4f702fe3e33200a36f53...d92a	28m ago	↓ 0x62...Ef57	ETH 0
 Contract creation	Success	↳ 0x9c016fddc720ff6270b437a618c...da07	3d ago	↓ 0x62...Ef57	ETH 0
 Token transfer	Success	↳ 0x84abf52687c3ea482a9994eba3...baba	3d ago	↓ 0xFE..Bd73	ETH 0
 Contract creation	Success	↳ 0x2bae3ddb500cdb6b79f3b92aa8...80b6	3d ago	↓ 0x62...Ef57	ETH 0
 Token transfer	Success	↳ 0x16d1e93ebfb2e7a5341532864e0...1b9b	3d ago	↓ 0xFE..Bd73	ETH 0

[View all transactions](#)

출처: 블록체인글로벌

IV. 발행, 유통 및 총량관리

금융위 분산원장 안에 맞는 발행 유통 시스템 설계

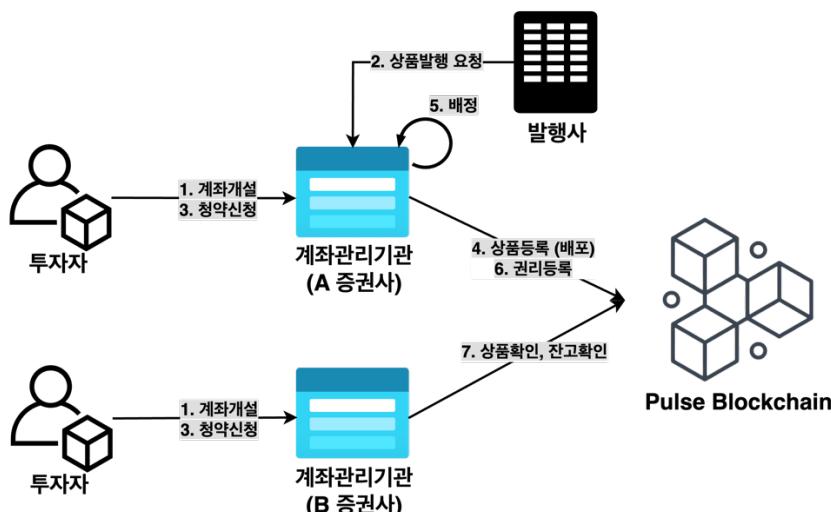
투자계약증권과 수익증권의 소규모 장외 유통플랫폼 제도화

- 이해상충을 방지하기 위한 발행과 유통(시장운영) 분리 원칙이 적용 즉, 발행인수·주선한 증권은 유통할 수 없고, 자기계약도 금지
- 장외거래종개업자는 자사 고객 간 거래를 다자간 상대매매(매수·매도호가 일치시 매매체결) 방식으로 중개

발행

발행 구조

발행 시스템 구조도



출처: 신한투자증권 블록체인스크럼

투자자·계좌관리기관·발행사

간 상호작용 통해 분산원장에

토큰증권 발행

위 그림은 Pulse 분산원장 인프라 내에서 투자자, 계좌관리기관, 발행사, 분산원장 등이 어떻게 상호작용하여 상품을 권리등록하는 과정을 설명한다.

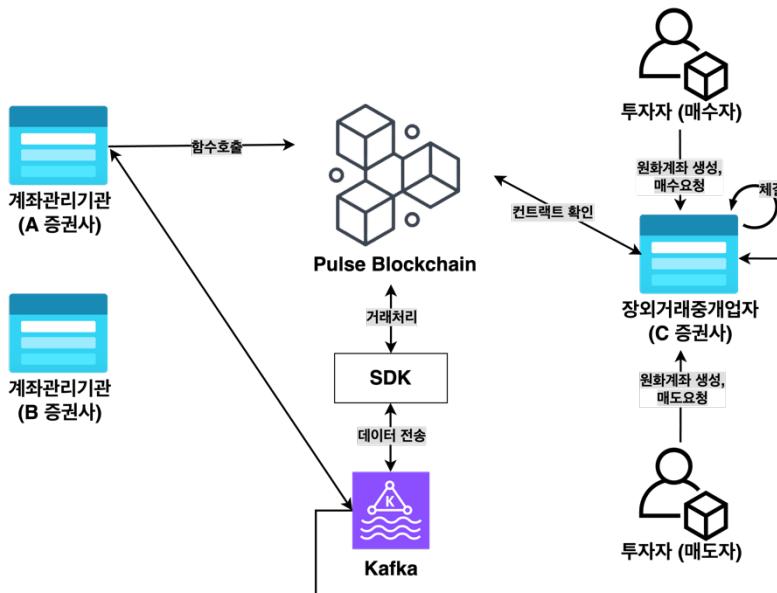
1. 투자자는 상품청약을 위해 계좌관리기관의 증권 계좌를 개설 또는 연동한다.
 - A. 계좌의 체계는 계좌관리기관마다 다르기 때문에 각 사의 정책을 따르고 Pulse에서 제공해주는 API를 통해 분산원장의 투자자 주소값을 생성하여 계좌관리기관의 계좌 번호와 주소값을 관리한다.
2. 참여가 합의된 계좌관리기관(증권사) 또는 발행인 계좌관리기관은 Pulse에 노드로 연결되어 있다. 발행사는 계좌관리기관에 상품등록을 요청한다.
3. 투자자는 각 발행사 정책에 따라 등록된 상품을 청약진행한다.

4. 발행사는 청약이 완료되면 계좌관리기관에게 상품등록 (배포)을 요청한다.
5. 투자자는 발행사 정책에 따른 배정물량을 확정받게 된다.
6. 상품 배정수량이 확정되면 Pulse 분산원장에 투자자들의 권리를 등록한다.
7. 발행사는 내부 로직에 따라 배정 업무를 수행하고 완료되면 계좌관리기관을 통해 Pulse 분산원장을 확인하여 상품을 확인할 수 있으며 각 투자자가 몇 개의 증권수량을 가지고 있는지 확인할 수 있다.

유통

유통 구조

유통 시스템 구조도



출처: 신한투자증권 블록체인스크립

위 그림은 Pulse 분산원장 인프라 내에서 투자자 (매수자, 매도자), 장외거래중개업자, 계좌관리기관, Message Queue, 분산원장 등이 어떻게 상호작용하여 거래체결 및 토큰증권의 권리이전 트랜잭션을 만들어내는지 설명한다.

유통 시스템 주요점

▣ 매도 건에 대한 장외거래중개업자 소유 확인 방안

매도자가 소유하고 있는 증권 수량을 확인하기 위한 수단은 다양하게 존재한다. 기존 레거시 시스템에서는 외부 플랫폼이 투자가 소유하고 있는 증권 수량을 확인하기 위해 계좌관리기관과 Interface 를 맞춰 API 연계 작업을 진행했지만 토큰 증권 시대에는 단순히 분산원장을 조회하여 확인이



Shinhan

분산원장 조회로 증권 수량
확인, 펄스 분산원장에
커스터マイ즈된 투자자 지갑
체계 활용

Kafka 메세지 라우팅 기능
통해 계좌관리기관에 결제
정보 전달

가능하다. 특히 이러한 방법을 적용하기 위해서는 기존 레거시 증권 시스템을
포괄할 수 있고 분산원장 내에서도 사용될 수 있는 특별한 주소값 체계가
필요하다. 따라서 Pulse 네트워크에서는 개인 투자자들에게 아래와 같은 지갑
주소 체계를 적용하여 사용한다. (keccak256 알고리즘 사용 / 20byte 절삭)

구분	주소의 표시 (예시)
개인투자자	0xd14f723e859ec4f3edee57bf78ceb7c81de08dfb

▣ 체결 데이터 전달 방법

1 장에서 언급했듯이 금융사 대외연계 시스템은 강한 보안 규제와 태생적
인프라 설계의 비효율성이 존재하여 수정개발이 매우 빈번하게 일어난다.
Pulse 인프라 네트워크는 이러한 점을 개선하기 위해 Kafka Message
Routing 처리 솔루션을 제공한다.

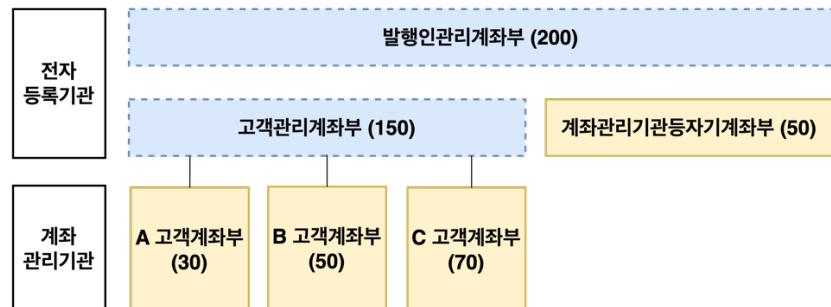
▣ 결제 처리

MQ를 통해 [체결 정보 + DT 서명 데이터]는 권리 변경 권한을 갖고 있는
계좌관리기관에게 전달되고 계좌관리기관은 데이터 확인 후 결제(Swap
function)함수를 호출한다.

총량관리

지갑주소 Customize를 통한 총량관리 방안

유가증권의 전자등록제도



*전자등록계좌 (파란색) : 발행 내역 관리, 총 수량금액 관리 (법적 효력
없음)

출처: 신한투자증권 블록체인스크럼

2019년 9월 16일부터 「주식·사채 등의 전자등록에 관한 법률」(이하
'전자증권법')이 시행되고 있다. 전자등록은 실물 증권 없이 계좌를 통해 증권의
발행 및 거래를 수행하는 방식으로, 증권의 무권화(無券化)를 의미한다.



2019년 시행된 전자증권법,
전자등록기관과
계좌관리기관으로 구성된
2 단계 구조 운영

고객계좌부 자기계좌부는
전자등록된 주식의 법적
권리를 증명하며, 법적 효력
있음

토큰증권 법제화 후 블록체인
기술이 기존
고객계좌부·자기계좌부
총량관리 방식 대체,
2-Tier에서 1-Tier로 개선

전자등록 제도의 운영을 위해 최상위 중앙 등록 기관인 「전자등록기관」이 있으며, 현재 한국예탁결제원이 이 역할을 수행하고 있다. 하위 등록 기관인 「계좌관리기관」은 투자자들과 직접적으로 접촉하는 증권회사와 같은 금융기관이 맡고 있다(법 제 19조). 즉, 전자등록기관, 계좌관리기관이 분리되는 2 단계 구조로 운영된다.

주식 발행 회사가 새로운 주식을 등록할 경우, 전자등록기관에 발행인관리계좌를 개설하게 된다. 전자등록기관은 발행인 별로 「발행인관리계좌부」를 작성하며, 이 계좌부에는 주식 발행 내역이 상세히 기록되지만 법적 효력은 부여되지 않는다.

투자자가 증권회사 등을 통해 고객 계좌를 개설하면, 계좌관리기관은 투자자 별로 「고객계좌부」를 작성하고, 전자등록기관에 고객 관리 계좌를 개설해야 한다. 이 고객 관리 계좌에는 전자등록된 주식의 총량과 총 금액만 기록된다. 전자등록기관은 계좌관리기관별로 「고객관리계좌부」를 작성하고 관리한다. 계좌관리기관이 직접 투자자로서 주식을 보유하는 경우에는 전자등록기관에 자신의 계좌를 개설할 수 있으며, 전자등록기관은 「계좌관리기관등 자기계좌부」를 작성하여 관리한다. 「고객계좌부」와 「계좌관리기관등 자기계좌부」에 전자등록된 자는 전자등록된 주식 등에 대해 적법한 권리를 갖는 것으로 추정되며, 이러한 장부는 법적 효력을 지닌다.

그러나 토큰증권 하에서는 분산원장 기술이 증권의 권리 발생·변경·소멸에 관한 정보를 기재하는 법상 공부(公簿·관공서가 법령 규정에 따라 만든 장부)의 기재 방식으로 인정된다. 따라서 토큰증권 법제화 이후에는 기존 상장주식과 같이 예탁결제원이 고객관리계좌부, 계좌관리기관등 자기계좌부를 직접 총량관리하는 것이 아니라 블록체인 기술이 이를 대체하게 될 것이며 예탁결제원은 블록체인 네트워크에 접속하여 계좌관리기관이 블록체인 분산원장에 각 투자자들의 증권수량을 적절히 기입·사용하고 있는지 확인할 것이다 (기존 2-Tier에서 1-Tier로 개선).

Pulse Network Wallet Address Structure

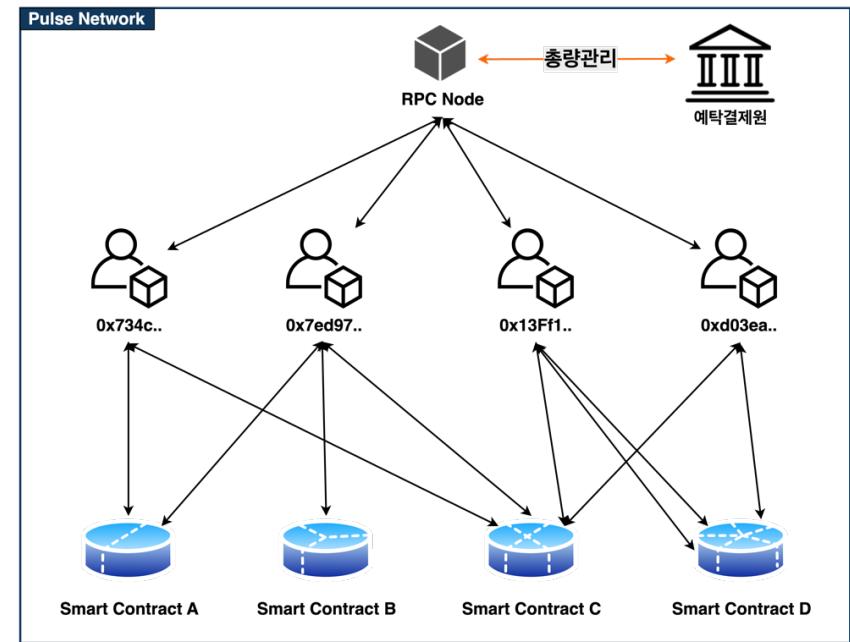
구분	주소의 표시 (예시)
개인투자자	0xd14f723e859ec4f3edee57bf78ceb7c81de08dfb
법인투자자	0x734c49630caC28EaaC33e9722268e64cA80AbcFd
발행사 (자기계좌부)	0xa13Ff1b6930c25d96baf2165A9f3B83d057D2D73

출처: 신한투자증권 블록체인스크럼, 블록체인글로벌

이를 위해 펄스 네트워크에서는 기존 42 자 문자열로 구성된 이더리움 지갑 주소 체계 일부를 커스터마이징하여 네트워크 참여자별로 위와 같은 지갑주소 체계를 사용하도록하였다. 펄스 네트워크는 해당 주소체계를 통해 특정 개인 또는 법인이 분산원장에 발행된 토큰증권을 얼마나 소유하고 있는지 파악하는

기능을 제공하여 전자등록기관이 손쉽게 총량관리 업무를 수행할 수 있도록 지원한다.

Pulse Network 총량관리



출처: 신한투자증권 블록체인스크립

■ Summary Notice

※ 본 콘텐츠는 **요약본**이며, 자세한 버전은 신한투자증권 블록체인스크립 메일을 통해 확인하실 수 있습니다. (shs.block@shinhan.com)

■ Regulatory Notice

※ 본 콘텐츠는 토큰증권 인프라에 대한 이해를 돋기 위해 제작된 것으로서 투자자의 투자 판단에 참고가 되는 정보제공을 목적으로 하고 있습니다.

※ 본 서비스에 해당하는 자료는 당사의 공식적인 조사 분석 자료가 아니며, 토큰증권 인프라에 대한 이해를 돋기 위해 작성되었습니다.

※ 투자에 따른 의사결정은 전적으로 투자자 자신의 판단과 책임하에 이루어져야 하며, 당사는 본 자료의 내용에 의거하여 행해진 일체의 투자행위 결과에 대하여 어떠한 책임도 지지 않으며 법적 분쟁에서 증거로 사용 될 수 없습니다.

※ 본 콘텐츠는 당사 고객에 한하여 배포되는 자료로 어떠한 형태로든 복제, 배포, 전송, 변형, 대여할 수 없습니다.