

ICON & KLAYTN

6기_이희제



Contents

ICON | 1ST

- 1-1. 개념
 - 1-2. 네트워크
 - 1-3. LFT 알고리즘
 - 1-4. 서비스
-

KLAYTN | 2ND

- 2-1. 개념
- 2-2. 네트워크
- 2-3. 블록의 전파



ICON

개념



1. 한국의 이더리움

2017년 10월 런칭, 단기간에 암호화폐 상위권 도달.
한국에서 메이저 코인 반열에 오른 첫 사례

2. 아이콘 코인(ICX)

총 4억개의 발행량, 블록체인 ID를 발급받아 안전전하게 전자서명 가능

3. 인터체인 알고리즘을 활용한 대표적인 암호화폐

루프체인, 여러 블록체인을 연결 가능

Vision



1. Hyper Connect the World

탈 중앙화, 분산화된 연결

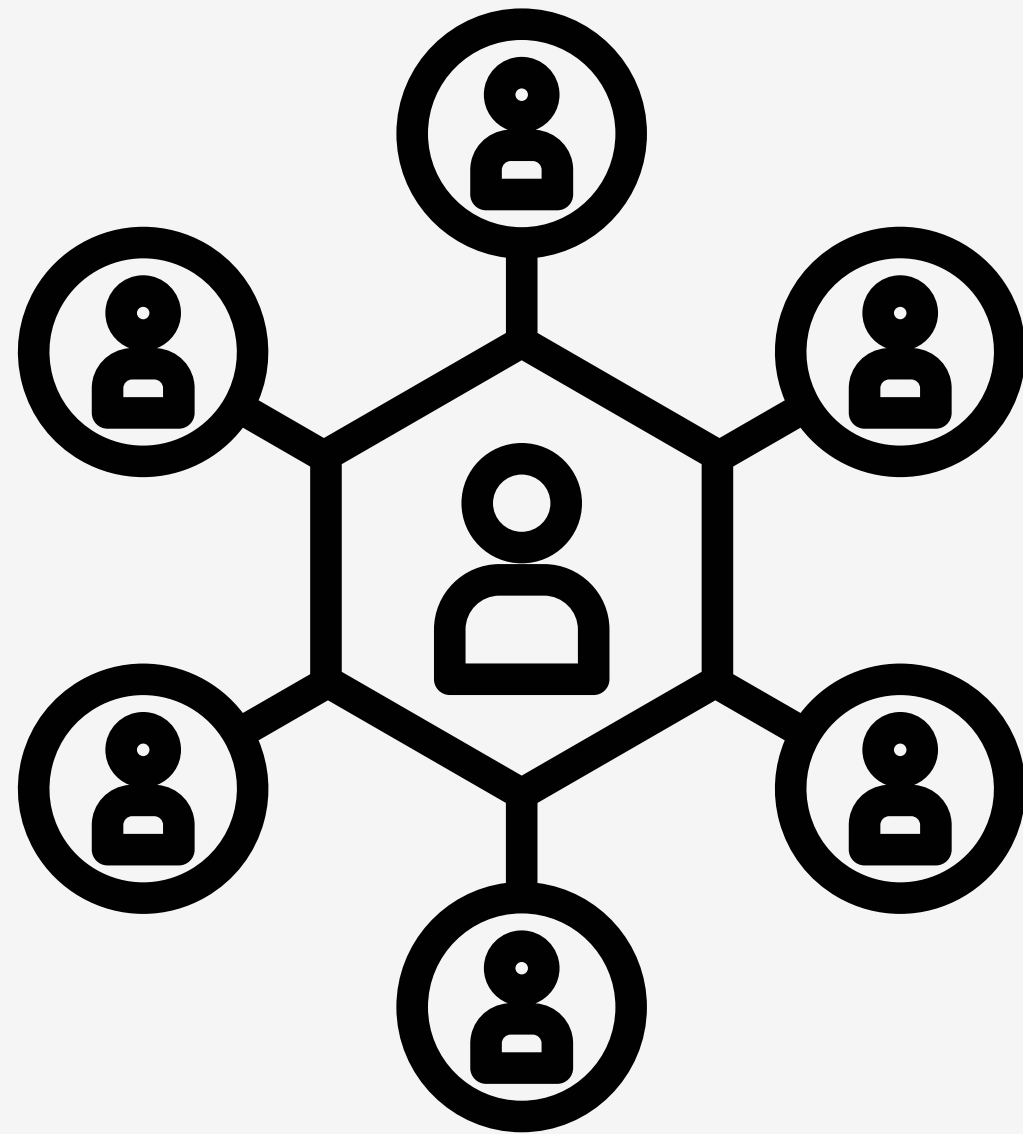
2. 커뮤니티와 커뮤니티의 연결

Node들의 연결을 넘어선 커뮤니티 간의 연결

3. 가상세계를 넘어서 현실세계와의 연결

무형의 가치화

Network



Components of the ICON Network

- ① Community
- ② C-Node(Community Node)
- ③ C-Rep(Community Representative)
- ④ ICON Republic
- ⑤ Citizen Node

Network

① Community



동일한 거버넌스를 가지는 Node들로 구성된 네트워크.

금융, 정부, 학교, Healthcare, BTC, ETH 등이 각각 Community가 될 수 있음.

② C-Node (Community Node)



Community의 구성단위로 Community 내의 합의 또는 거버넌스를 결정하는데 영향을 미침.

Network

③ C-Rep(Community Representative)



1. 커뮤니티를 대표(Representation)하는 단위이며, 동시에 I CON Republic의 거버넌스를 구성하는 단위
2. 거래에 대한 검증과 거버넌스에 대한 투표권을 보유
3. 각각의 커뮤니티의 의사결정에 의해 선정, 변경 가능, 보상을 받음

Network

④ ICON Republic



1. 커뮤니티들이 연결되고 모이는 지점
2. C-Rep(대표)와 Citizen Node들로 구성
3. 거버넌스는 C-Rep(대표)의 투표로 결정됨
4. 다른 커뮤니티의 거버넌스에 영향을 미치지 않음

⑤ Citizen Node



1. ICON Republic의 Node 중 하나
2. 누구나 loopchian 기반의 DApp 생성을 통해 참여할 수 있음
3. Citizen Node는 ICON Republic의 거버넌스에 대한 직접 투표 권한은 없고, 거래 생성 권한만을 가짐

Network

How to Connect?

1. 단일 커뮤니티 내 노드 간 연결

-> 각각의 커뮤니티들은 특성에 맞는 블록체인을 선택할 수 있고, 각기 다른 합의 알고리즘을 사용할 수 있음

2. ICON Republic 내 노드 간 연결

-> Loopchain 기반 연결. 각각의 커뮤니티와는 별개의 거버넌스를 가지고 있고, 독자적 합의 알고리즘(LFT)로 작동

3. 커뮤니티와 ICON Republic의 연결

-> 커뮤니티와 ICON Republic은 DEX(Decentralized Exchange)를 통하여 실시간 연결, 교환비율 제공.

4. 커뮤니티와 커뮤니티의 연결

-> ICON Republic을 통해서 연결 가능, DEX를 통해 실시간으로 각각의 커뮤니티와 연결

Network

How to Operate?

1. 커뮤니티

-> 각 Community는 해당 Community에서 사용하는 블록체인의 특성에 따라 자체 거버넌스를 바탕으로 독립적으로 운영됨.

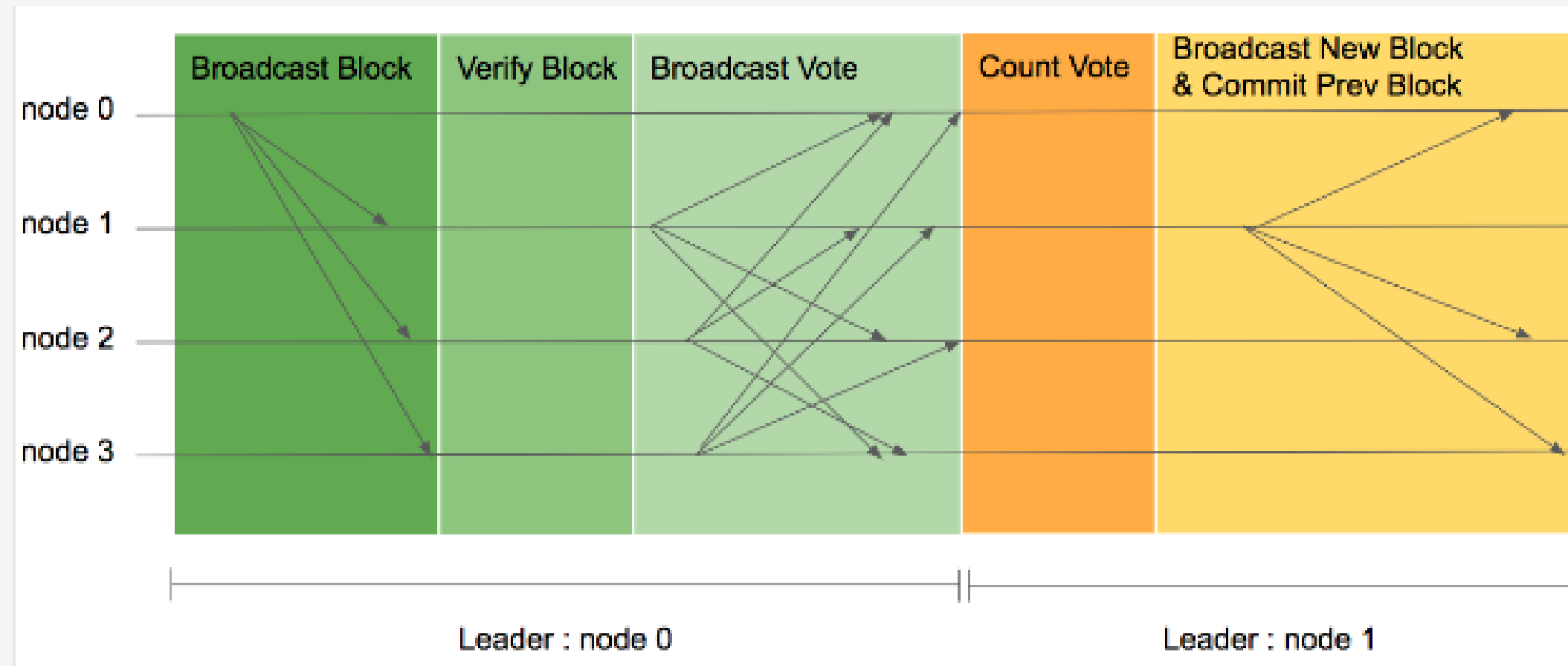
-> 합의 알고리즘, 합의 참여 Node, Community 내 가상화폐 운영 등 모든 사항에 대하여 ICON Republic과는 독립적으로 합의하고 의사결정 할 수 있음,

2. ICON Republic

-> ICON Republic의 거버넌스는 C-Rep들의 합의과정을 통해 결정되고, 거버넌스의 범위는 ICON Republic으로 한정

LFT Algorithm

LFT(Loop Fault Tolerance) 알고리즘

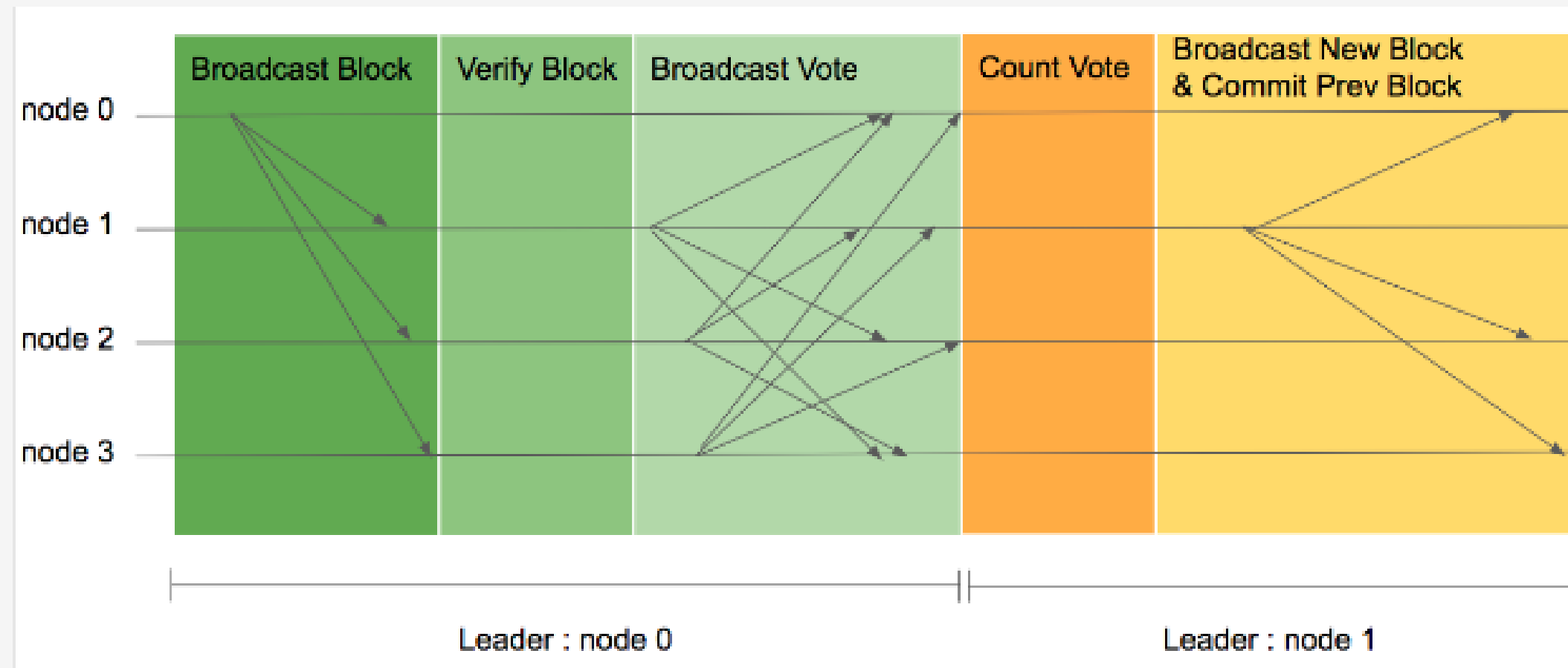


1. LFT는 전통적인 BFT 방식의 합의 알고리즘

2. 블록체인 네트워크 특성에 최적화 되도록 개선한 합의 알고리즘

LFT Algorithm

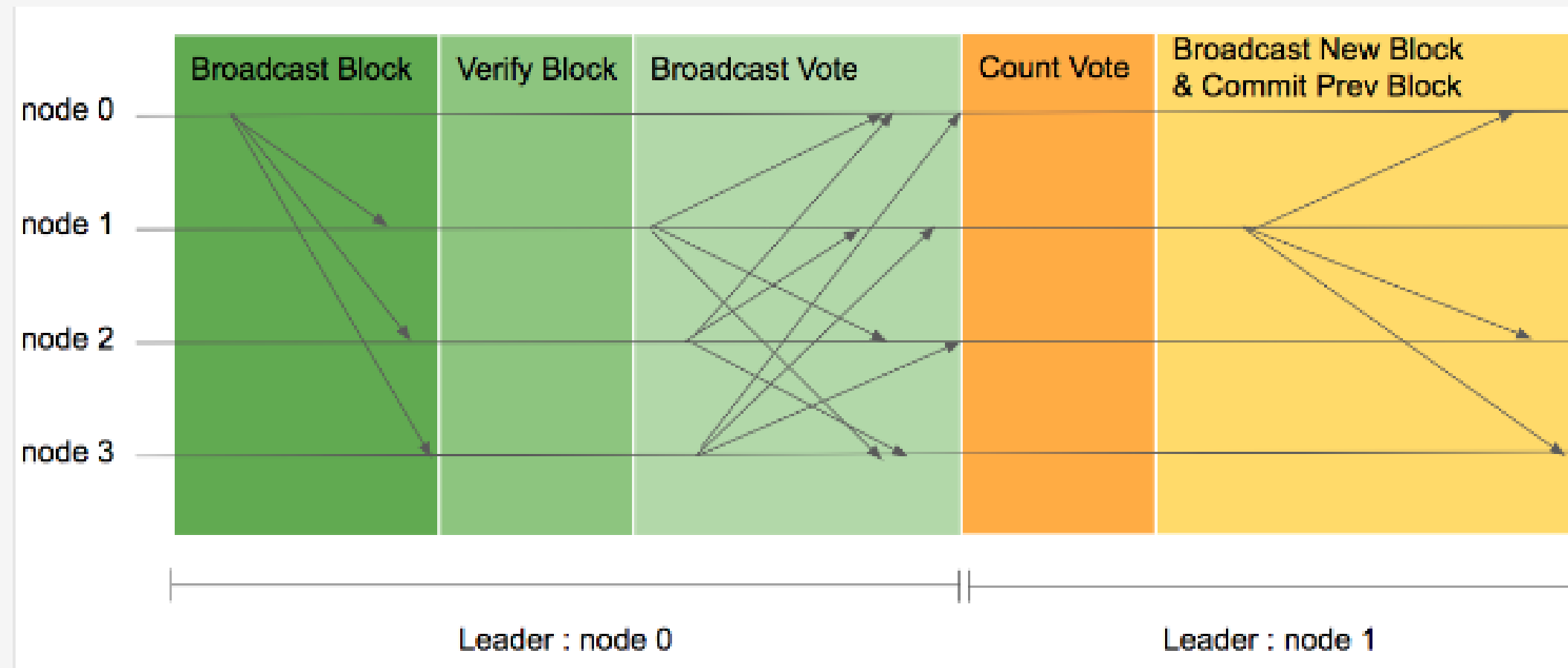
LFT 동작방식 (1)



- 합의가 시작되면 검증 노드들은 리더 노드에 처리하기 원하는 트랜잭션을 전송
- 리더 노드는 수집한 트랜잭션을 이용하여 블록을 생성하고 자신의 서명과 함께 다른 모든 검증 노드에 전송. (Broadcast Block)

LFT Algorithm

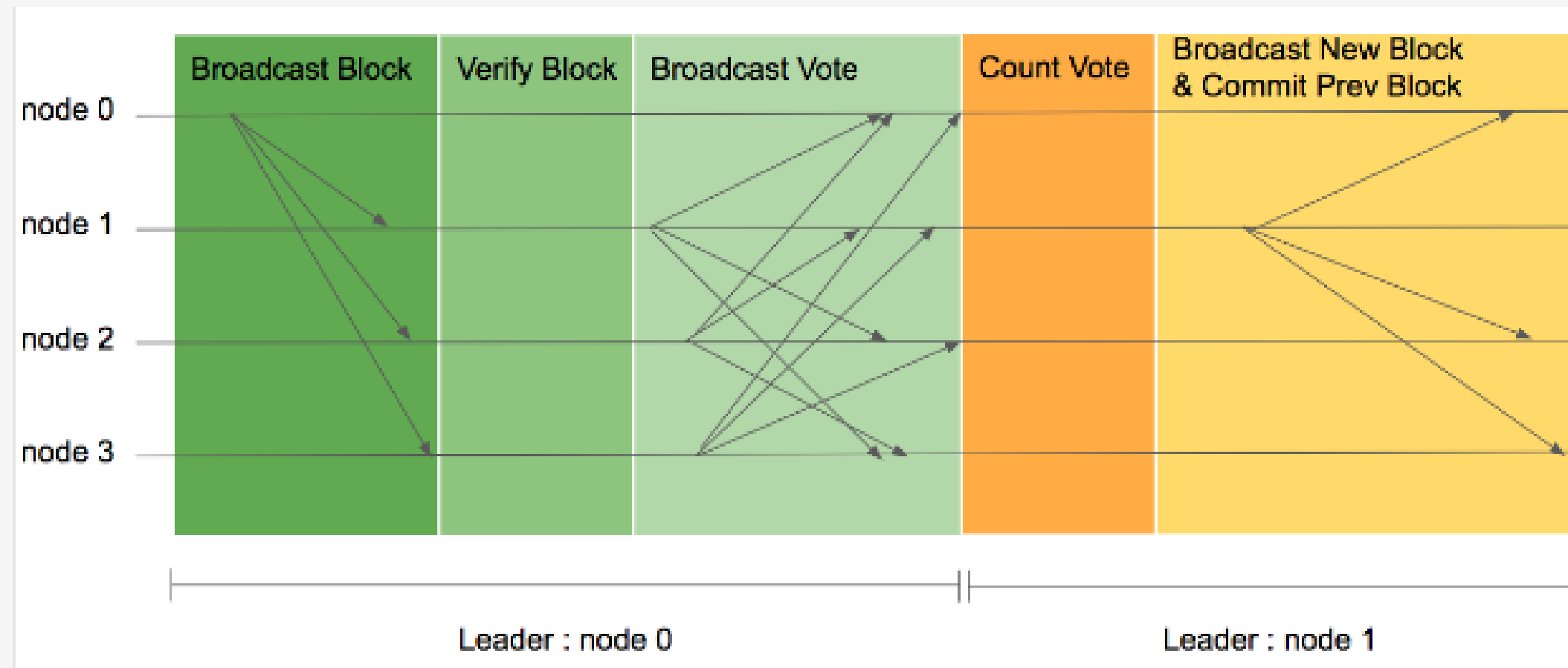
LFT 동작방식 (2)



각 검증 노드들은 블록을 받으면 1) 현 리더가 블록을 생성했는지 확인, 2) 블록의 높이와 이전 블록 해시가 올바른지 확인, 3) 블록의 메시지가 올바른지 확인. (Verify Block)

LFT Algorithm

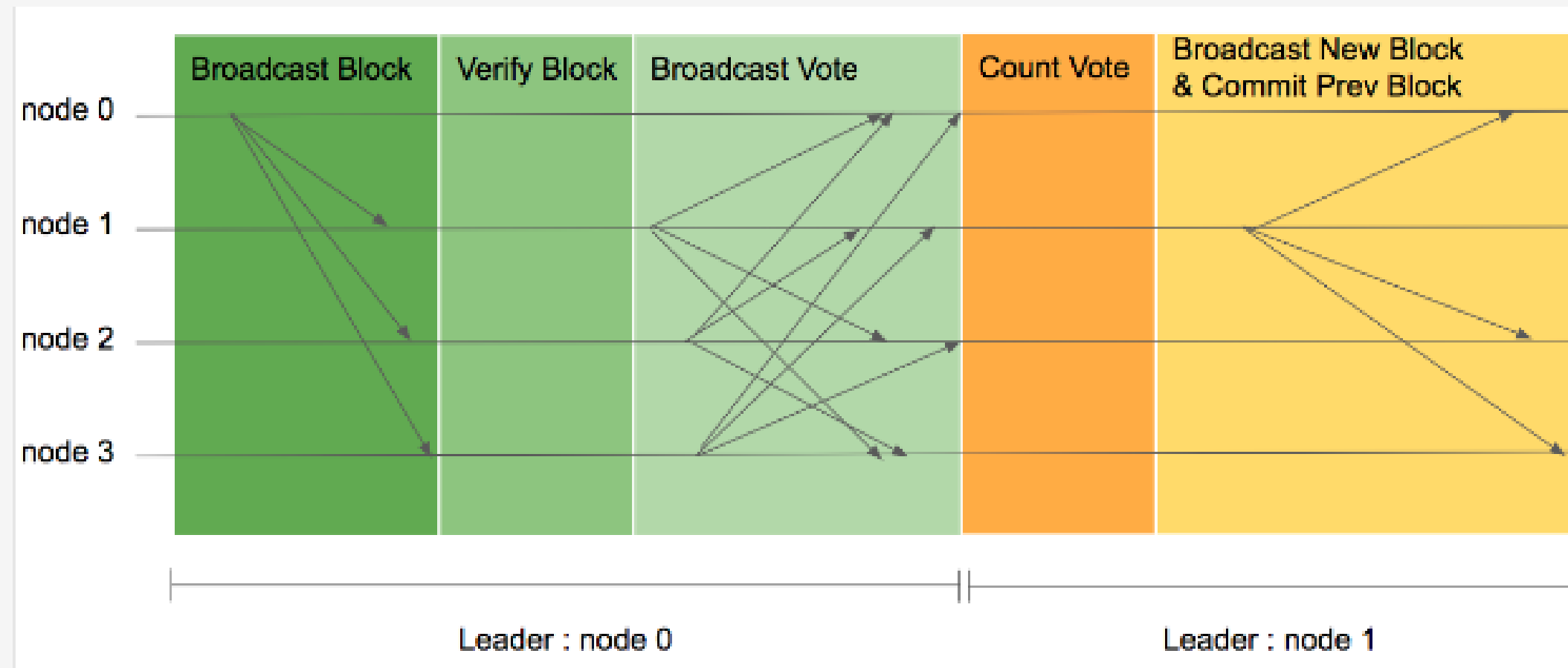
LFT 동작방식 (3)



검증 노드는 검증 결과에 따라 투표 메시지를 모든 노드들에게 보냄. (Broadcast Vote)

LFT Algorithm

LFT 동작방식 (3)



각 노드가 정족수 이상의 투표를 받게 되면 해당 높이의 블록을 자신의 블록체인에 추가할 수 있음. (Count Vote)

?

Loopchain?

loopchain은 스마트컨트랙트를 지원하는 고성능 엔터프라이즈 블록체인을 목표로 개발되었으며 업무에 따라 다양한 커스터마이징을 지원하고 특히 다른 독립적인 블록체인과의 연계를 통해 블록체인 네트워크를 확장할 수 있도록 함.

DEX?

DEX는 일반적인 가상화폐 거래소처럼 Third party를 통해 거래하는 Centralized exchange가 아닌 블록체인 상에서 자동으로 거래를 처리해주는 시장이다.



<https://icon.foundation>

Service

SERVICES

블록체인 DID 신원인증 서비스

풍 (Zzeung)

좋은 다양한 인증 수단을 한 곳에 담아두고 사용할 수 있는 블록체인 신원인증 서비스입니다. 지문이나 QR코드 촬영만으로 간편하게 인증할 수 있습니다.

- [실명인증] 금융업무에서 실명인증이 필요할 때 지문 한 번으로 인증하세요.
- [QR인증] QR 찍으면 바로 방문 인증할 수 있어요.
- [증서서 관리] 증서서를 한 곳에서 관리할 수 있어요.
- [높은 보안성] 안심하고 믿을 수 있어요.
- [금융위원회의 혁신금융서비스 선정]

[홈 사이트 바로가기](#) →
[Google Play 앱 다운로드](#) →
[iOS 앱 다운로드](#) →

안전하고 간편한 인증을 쏘 하나로
인증이 필요할 때, 쏘



블록체인 기반 방문 자격 인증 서비스

비젯미 (VisitMe)



“비짓미[VisitMe]”는 분산 ID(DID, Decentralized ID) 기술을 활용해 방문자의 신원을 보다 투명하고, 항상에서 비회원 체크인이 가능하도록 하는 **“디지털인기 기반 방문객 관리 솔루션”**입니다. 현재까지, 방문자 확인 및 적대 등 방문 절차를 대체할 수 있는 처리와 업무 효율성을 높인 물론, 방문자 절차를 디지털화 하고 블록체인의 기술로 보호해 정보 유출을 줄이고 보안을 강화했습니다. 기업 및 가계에서 방문 정보로 사전 등록한 여행객에게 방문을 알릴하면 방문자는 비짓미 모바일 애플리케이션을 통해 방문객에 비치된 QR코드 스캔을 후 즉시 출입이 가능합니다.

비젯미 (VisitMe) 사이트 바로가기 →
비젯미 (VisitMe) 소개자료 다운로드 →

스마트한
체크인을
경험하세요.

VisitMe는 방문자 사전 등록,
체크인 및 관리를 간소화하는
스마트 방문자 관리 솔루션입니다.



**We keep your
time and honor**

총 754 개의 노력과 시간을
보관 중입니다.

블록체인 증명서 발급 서비스

브루프(broof)

#proof

아이콘루프의 블록체인 증명서 발급 서비스 '브루프'는 아이콘(ICON) 파블릭 블록체인의 네트워크에 기반해 위변조되지 않는 증명서 발급과 영구 보관을 지원합니다. 증명서 발급 기관은 데이터베이스 시스템을 별도 구축할 필요없이 종이문서 발급 및 보관 비용을 절감할 수 있으며, 발급 신청자는 언제 어디서나 블록체인의 증명서를 간단하게 발급받고 조회할 수 있습니다.

브루프 사이트 바로가기 →
브루프 소개자료 다운로드 →



Klaytn

개념



1. Klaytn 플랫폼은 카카오의 블록체인 기술 계열사 그라운드X가 자체 개발한 블록체인 플랫폼

2. Klaytn은 엔터프라이즈급 안정성을 목표로 고도로 최적화된, BFT(Byzantine Fault Tolerance) 알고리즘 기반 퍼블릭 블록체인

개념

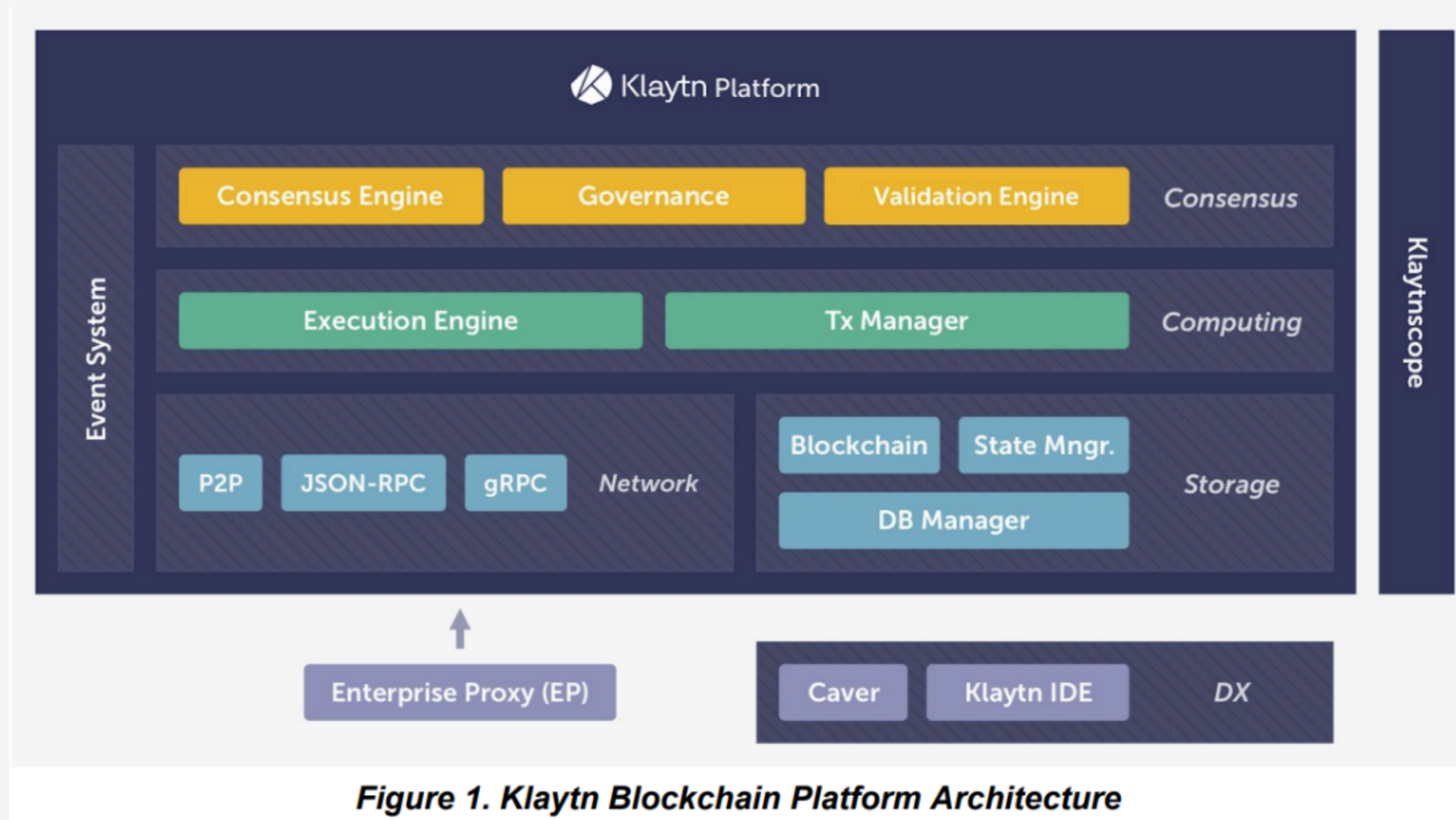


디자인 목표

- 즉각적인 완결성
- 실제 사용 사례에서 문제 없는 높은 *TPS
- Blockchain 애플리케이션 실행 비용 절감
- 사용자의 진입 장벽을 낮춤
- 산업계의 블록체인 기술 도입 촉진

*TPS(Transaction Per Second): 초당 트랜잭션 수

개념



전반적인 구조

Network

1. 코어 셀 네트워크(CCN)

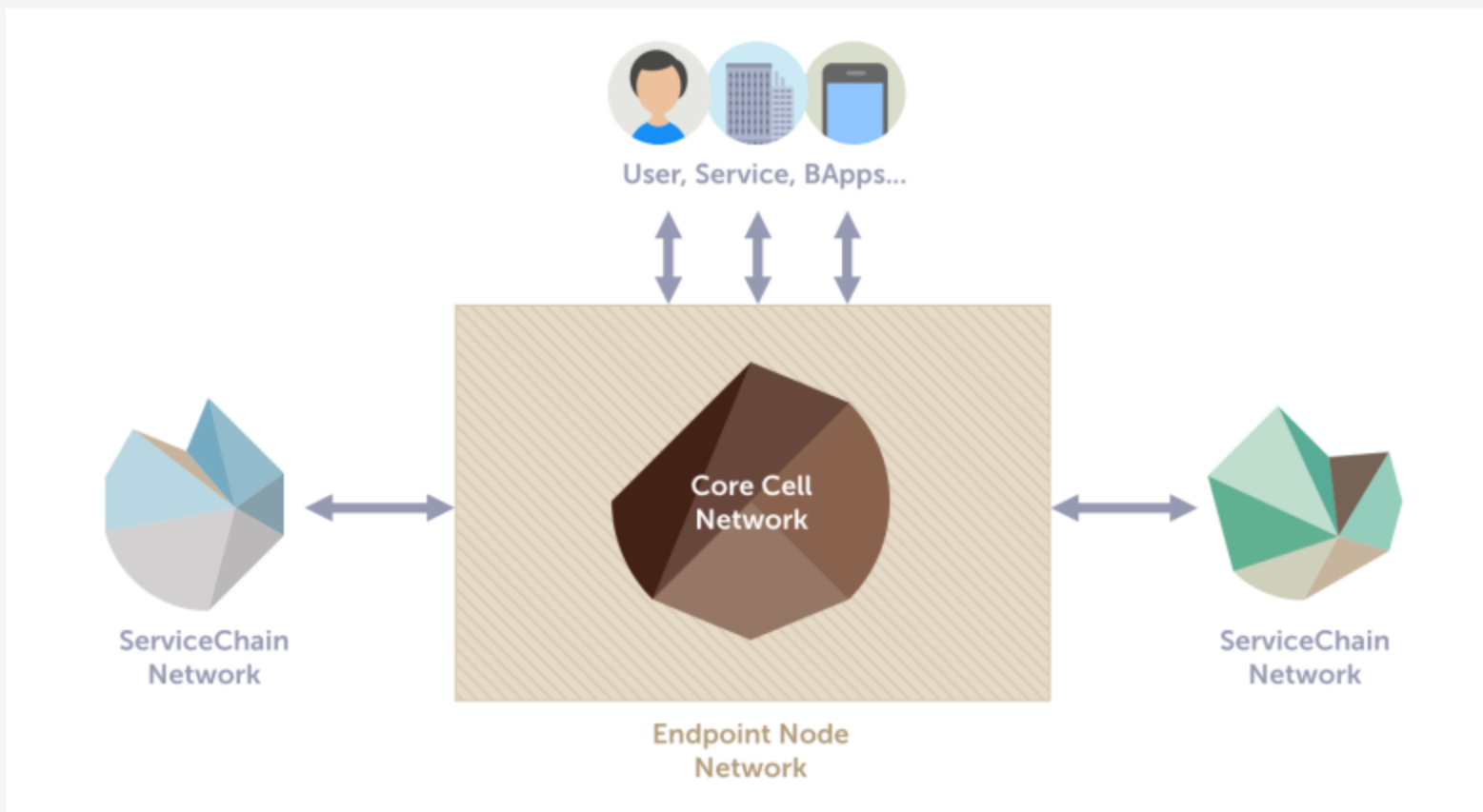
CCN은 엔드포인트 노드(EN)를 통해 제출된 트랜잭션을 확인하고 실행하는 코어 셀(CC, Core Cell)로 구성. CCN은 네트워크 전체에서 블록을 생성하고 전파.

2. 엔드포인트 노드 네트워크(ENN)

ENN은 주로 트랜잭션을 생성하고, RPC API 요청을 처리하며, 서비스체인의 데이터 요청을 처리하는 엔드포인트 노드(EN)로 구성.

3. 서비스체인 네트워크(SCN)

SCN은 블록체인 애플리케이션(BApp)에 의해 독립적으로 운영되는 보조 블록체인들로 구성된 Klaytn 서브네트워크. 서비스체인은 EN을 통해 메인 체인에 연결.



Klaytn 생태계 및 논리적 서브 네트워크 (CCN, ENN, SCN)

Network

역할 기반 노드 유형



Klaytn 메인체인 네트워크 토폴로지

1. 코어 셀(CC)

코어 셀(CC)은 하나의 컨센서스 노드(CN)과 두 개의 프록시 노드(PN)로 이루어짐. 컨센서스 노드는 블록 생성 프로세서에 참여하고, 프록시 노드는 네트워크에 인터페이스를 제공. PN은 트랜잭션 요청을 컨센서스 노드로 전송하고 블록을 엔드포인트 노드로 전파

2. 엔드포인트 노드(EN)

EN은 Klaytn 네트워크의 엔드포인트 역할로, RPC API 요청을 처리하고 서비스 체인과 주고받는 데이터를 처리

3. 부트노드(Bootnode)

부트노드는 Klaytn에서 운영하는 특수 유형의 노드. 새로 참여하는 노드가 네트워크에 등록하고 연결할 다른 노드를 검색하는 것을 도움.

Network

계층화된 네트워크(Tiered Networks)



Klaytn 메인체인 네트워크 토폴로지

1. 컨센서스 노드 네트워크(Consensus Node Network, CNN)

-> CN은 CNN이라는 풀 메시 네트워크(full-mesh network)를 형성. CNN은 WAN(wide area network)에서 BFT를 적용하므로 각 CN은 충분한 성능 수준으로 BFT 합의 과정을 수행하기 위해 하드웨어 및 네트워크 리소스 요구사항을 엄격하게 충족해야 함.

2. 프록시 노드 네트워크(PNN)

-> PNN은 PN으로 구성. 일반적으로 PN은 인접한 코어 셀에서 PN과 하나의 연결만 유지.

3. 엔드포인트 노드 네트워크(ENN)

-> 가장 바깥쪽 서브 네트워크인 ENN은 서로 연결되거나 다수의 PN에 연결된 EN들로만 구성.

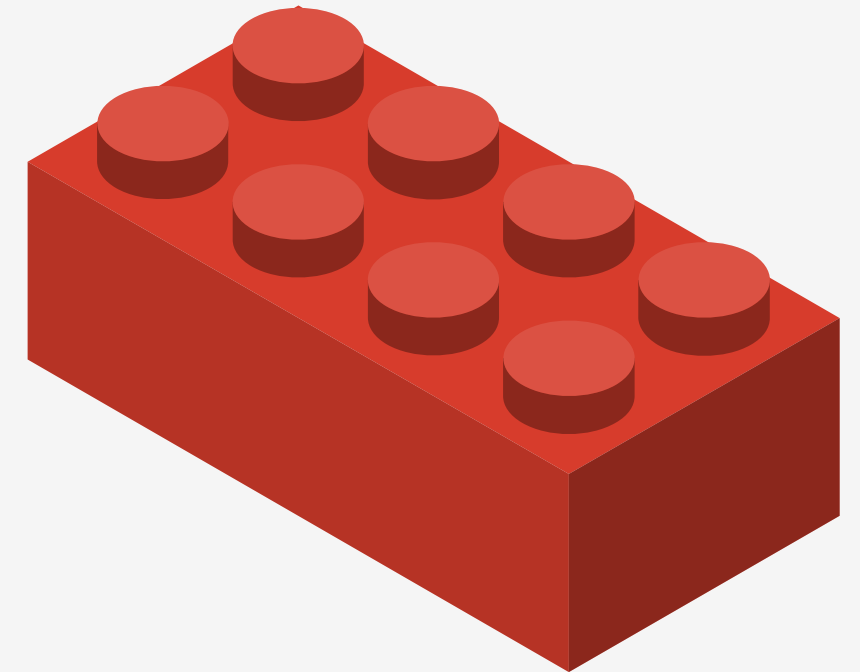
블록 생성 및 전파

1. 블록 생성주기

- '라운드'는 Klaytn의 블록 생성주기.
- 각 라운드마다 새로운 블록이 생성되고 바로 다음에 새로운 라운드가 시작.
- 블록 생성 간격은 네트워크 트래픽 및 노드 작동 조건에 영향을 받을 수 있지만 Klaytn은 매 라운드마다 대략 1초로 설정.

2. 제안자(Proposer) 및 위원회(Committee) 선택

- 매 라운드마다 Klaytn은 무작위로, 하지만 결정적으로(deterministically) 하나의 컨센서스 노드(CN)를 블록을 생성할 제안자로 선택.
- 하나의 CN 그룹을 그 라운드의 위원회로 선정.



블록 생성 및 전파

3. 블록 제안 및 검증

- ① 제안자는 그 라운드에 대한 선택 증명(즉, 제안자의 공개키로 확인 가능한 암호학적 증명)을 CN에게 브로드 캐스트.
- ② 해당 라운드의 위원회로 선택된 CN들은 제안자에게 그들의 선택 증명으로 응답.
- ③ 제안자는 트랜잭션 풀에서 트랜잭션들을 선택하고 순서대로 블록을 만듦.
- ④ 마지막으로, 제안자는 새롭게 만들어진 블록을 검증하고 과정을 마무리하기 위해 위원회와 합의 과정을 거침.

블록 생성 및 전파

4. 블록 전파(Block Propagation)

- 제안된 블록은 성공적으로 마무리되려면 위원회 멤버 3분의 2 이상의 서명을 받아야 함.
- 위원회가 합의에 도달하면, 새로운 블록은 모든 CN에 전파되고 컨센서스 라운드는 종료.
- 새 블록이 모든 CN에 전파되면, 블록 헤더와 블록 바디를 PNN을 통해 ENN에 전달하여 새로 생성된 블록의 정보를 모든 Klaytn 네트워크 참가자가 이용할 수 있게 만듦.

Thanks!