Blockchain of Blockchains

WORLD'S FIRST NON-INVASIVE &
FULLY INTEROPERABLE BLOCKCHAIN PLATFORM

개요

블록체인 기술은 상호연결과 성능의 반비례와 함께 이전에 없었던 탈중앙화와 투명성을 제공한다. 가까운 장래에, 블록체인이 제공하는 솔루션, 특히 스마트 계약 등이 상호 신뢰 없이 단순한 합의와 협력을 달성하며, 이가 모든 일상에 적용되는 데 도움이 될 것으로 생각된다.

그러나, 이 목표를 달성하기 위한 현재의 접근법은 특정 블록체인의 기능 중 일부를 대체, 삭제하거나, 해당 블록체인 표준에 따라야하는 변화를 강요하고 있다. KardiaChain은 "동화 없는 통합" 의 접근법으로 유저와 개발자 쌍방을 위한 간단하고 사용하기 쉬운 솔루션 구축에 중점을 둔다.

KardiaChain은 "듀얼 마스터 노드" (혹은 듀얼 노드) 라고 불리는 비침습성 솔루션을 개발했으며, 이것은 미래의 블록체인 뿐만 아니라 기존 블록체인 간의 상호작용을 가능하게 한다.

KardiaChain의 최종 목표는 개발자들이 서로 다른 블록체인 에서 작동될 수 있는 스마트 계약을 쉽게 만들 수 있고, 트래픽과 비용의 최적화와 함께 다양한 블록체인들의 스마트 계약 간의 통신이 신뢰 없이 안전한 환경에서 이루어지는 통합된 생태계를 만드는 것이다.

I. KardiaChain의 철학

KardiaChain은 가까운 미래에 블록체인 솔루션 중에서 특히 스마트 계약이 제공하는 서로에 대한 무신뢰 기반 합의가 사람들의 삶 전반에 쉽게 적용될 경지에 곧 도달할 것이라고 믿는다.
현재 많은 블록체인들이 이전의 다른 블록체인들을 대체할 목적으로, 모든 상황에 적용되는 유일한 블록체인이 되려는 접근법을 택하고있다. 이와중에, 우리는 실제로는 상황이 매우 다른 방향으로 발전할 수 있을거라 생각한다. 인터넷이 수많은 네트워크들의 대규모 네트워크인 것처럼, 우리의 블록체인에 대한 비전은 많은 퍼블릭 블록체인과 프라이빗 블록체인 간의 연결이다. 각 블록체인은 특정한 목적을 위해 특정한 구조를 가지고 있으며, 이들 블록체인의 고유성은 충분히 포용되어야 한다.

따라서, 여타 블록체인의 강점을 찾아낼 수 있는 가능성과 특정 대형 프로토콜들의 폐쇄적인 문제를 해결할 수 있는, 모든 블록체인들의 집단적 강점을 활용하고 최적화할 수 있는 스마트 생태계가 있어야 한다. 우리는 이를, 각 블록체인이 신체부위나 장기로 표현될 수 있는 하나의 유기적 조직으로 생각하며, 여기서 KardiaChain은 심장 (Heart) 과 같이 신체상 모든 부위에 필요한 트래픽과 거래들을 각 부위의 특정한 요구에 알맞게 공급하는 것이다.

기존의 블록체인간 상호 작용에 대한 문제 해결을 위하여 여러 대안들은 기존 시스템의 근본적인 변화, 아니면 새로운 블록체인에 대규모의 프로토콜/프레임워크 적용을 요구하며 변화하고 있다. 이에 비해 KardiaChain 고유의 접근법은 현실적이며, 참여하는 블록체인들은 변화될 필요 없이 쉽고 빠르게 블록체인간 연결을 구축할 수 있다. KardiaChain은 유저와 디앱 개발자 모두의 관점에서 간소화와 단순성에 초점을 맞춘 " 동화 없는 통합 " 접근법을 따른다.

KardiaChain 팀은 서로다른 블록체인들이 연결될 수 있는 스마트 생태계를 소개하며, 이것이 블록체인의 대중화에 기여할 것이라 믿고 있다.

II. 배경

A. 단일 체인

블록체인 기술은 이전에 없었던 분산과 투명성을 제공하나 성능과 상호 연결성은 상반된다. 대부분의 단일 체인들은 확장성, 또는 처리속도의 상승을 우선시 하며, 초당 거래 처리 속도(TPS)를 주요한 측정치로 한다. 이에 사용되는 잘 알려진 방법 중 하나는 샤딩이다[1]. 이는 블록체인을 작은 조각으로 나누어(sub-chains) 동시에 거래를 처리하는 것인데, 해당 방법으로 블록체인은 1초에 수천, 수백만 건의 처리 속도를 달성할 수 있다.

그러나, 현존하는 프로젝트들의 이론적인 추정을 근거로 들어도 대중화에 필요한 속도와 성능에 도달할 수 있는 단일 블록체인 프로젝트는 없다. 예를 들어, 페이스북의 주요 상호작용은 매 분마다 51만 건의 댓글, 293,000건의 업데이트, 136,000장의 사진이 업로드되며 이는 초당 16,000건의 거래 처리 속도를 요구한다 [2]. 인스타그램은 하루에 40억 번의 '좋아요' 가 일어나며, 1초에 4만 6천의 TPS가 필요하다 [3]. 유튜브의 경우 일당 10억 시간의 동영상이 재생되며, 매 유저가 6초 마다 서비스를 1건식 요청한다는 가정하에 초당 700만 건에 가까운 처리가 이루어진다 [4].

TPS에 대한 집착의 주요한 까닭은 단일 체인들은 상호 운용성이 부재하는 경우가 흔하기 때문이며, 이는 단일 체인 간 상호 통신이 불가능 하기 때문에 다중 블록체인 운용이 불가능하다는 의미이다. 상호 운용성의 부재는 다양한 사업들에서 실시간으로 일어나는 문제에 적합한 블록체인 기반의 솔루션이 찾을 기회를 상당부분 줄여버린다. 예를 들어 스마트 계약을 지원하는 많은 블록체인이 있고, 각 플랫폼은 서로 다른 연산처리능력을 가지고 있다. 극단적인 경우로서, 비트코인 기반 블록체인들은 스마트 계약 자체를 지원하지 않는다 [5]. 이는 사실상 단일 체인으론 완전한 솔루션을 개발할 수 없다는 것을 의미한다. 모든 어플리케이션에 적합한 단일 솔루션의 부재는 여러 다른 블록체인에서 스마트 계약을 개발하고자 하는 이들에게 어려움을 초래한다.

B. 상호연결된 블록체인

1. 확장큐브

단일 체인을 컴퓨터나 로컬 네트워크로 생각하면, 매우 빠른 슈퍼컴퓨터 하나를 개발하는 것보다, 다수의 컴퓨터들을 서로 연결하여 작업량을 분산시키는 것이 더 나은 확장성을 기대할 수 있다. 다음은 널리 쓰이는 시각화 방식인 확장큐브를 통해 더 나은 블록체인 확장성에 대한 접근들을 표현한다 [7].

- X축 = 수평 복제 = 거래 라우팅: 트래픽 감소와 정체를 회피하기 위해 데이터가 복수의 노드에 저장된다.
- Y축 = 기능 확장 = 서로 다른 블록체인들이 다른 작업을 맡는 것: 솔루션들은 각각 분리된 데이터베이스를 쓰는 다른 서비스들로 분리된다. 이는 한 작업에서 높은 정체가 일어날 시 다른 작업의 퍼포먼스에 영향을 미치지 않게 한다.
- Z축 = 데이터 분할 = 각 블록체인 부분 간 작업량 공유 (샤딩 등): 작업량 공유를 위해 다수의 노드에서 동일한 코드를 실행한다.

많은 단일 체인 솔루션들은 Z축 확장방식인 샤딩 적용에 초점을 맞추고 있다. 예시로서 이더리움 네트워크의 경우 샤딩을 다음 버전의 주요점으로 설정한다[11].

우리는 존재하고 있는 블록체인과 앞으로 개발될 블록체인의 샤딩을 지렛대 삼아 X축과 Y축 확장방식에 집중하는, 3개 축 모두 아우르는 확장성 달성을 목표로 한다. 상호 운용성을 염두하여 비슷한 작업들은 다른 블록체인 플랫폼들 상에서 공유될 수 있으며 이는 X 축 확장을 달성한다. Y축 확장은, 블록체인 상 작업이 더 작은 작업들로 나눠져 각기 다른 블록체인들 상에서 실행되는 것이다. 이것이 KardiaChain이 의도하는 상호운용과 연결이 가져올 수 있는 강점이다.

2. 관련 연구

다른 블록체인 간 상호운용성을 적용하기 위한 많은 시도들이 있었지만, 대다수는 참여하고자 하는 블록체인에 특정한 변화들이나 포크(소프트 및 하드) 를 요하기도 한다. 운영되고 있는 블록체인 네트워크에 변화를 주는 것은 두 가지의 중대한 부작용을 초래할 수 있다:

1) 새로운 변화를 위한 하드포크;
2) 블록체인의 핵심 설정에 변경을 시도할 시 일어날 수 있는 보안상 위험.

여기서 몇가지 일반적인 크로스체인 접근방식을 다루고자 한다.

a) 사이드체인

사이드체인은 하나의 메인 블록체인과 병렬로 동작하는 블록체인으로, 상호운용성을 통해 두 블록체인 간 토큰의 이동/동기화를 탈중앙적인 방식으로 기능성을 높이는 방법으로 이용된다 [12]. 즉, 이용자는 자신의 암호화폐를 사이드체인으로 옮기고 다시 메인 체인으로 돌아올 수 있다. 사이드체인의 문제점은 자산이 사이드체인으로 전송될 때 (그리고 메인 체인으로 돌아갈 때) contestant 기간동안 전송 직전까지 동결되어야 하는 것이다. 사이드체인에 대한 발상은 2014년부터 있어왔지만, 아직까진 적용 및 즉시 개발이 가능할 만큼 기술이 성숙하지 않다.

b) 메시지 레이어

메시지 레이어는 외부 블록체인에서 생성된 데이터를 모으는 중간 레이어로서 디자인 되었다 [13]. 여기서 모든 것을 메시지로 간주할 때, 필터링과 순차 정렬을 위한 추가적인

레이어의 필요성이 생겨난다. 간단히 말해서, 네트워크는 메시지를 원장에 포함시키기 전 일종의 필터링 과정을 필요로 한다. 해당 프로세스는 실제로 네트워크 성능에 영향을 끼칠 추가적인 처리량을 필요로 할 것이다. KardiaChain은 블록체인의 불역성을 통해 외부에서 이루어지는 거래에서 직접 필수적인 데이터를 추출할 수 있을 것이며, 추가적인 레이어를 생략할 수 있다.

c) 허브 / 커넥터 / 어댑터

허브 (커넥터/어댑터)는 참여하는 블록체인들 간 통신 채널로서 디자인 되었다. 이러한 채널을 통해 블록체인들 간 자산 거래 및 교환의 상호작용이 이뤄질 수 있다. 허브 접근방식의 가장 유명한 사례로선 Polkadot이 있다 [14]. 허브의 치명적인 문제는 채널에 참여하는 블록체인들은 크로스 체인 통신을 위해 허브와 호환성을 가져야 하며 이는 해당 블록체인은 변경이 필요하다는 것이다(포크). 다시 말해서, 허브를 활용하는 접근방식은 다른 블록체인들에 적응하는 것이 아니라, 참여하는 블록체인들이 적응을 해야 하는 것이다. 이것은 상호운용성과 실용성의 의미에 상반된다.

3. KardiaChain의 접근법 - “동화 없는 통합” 접근법

간단히 말해서 KardiaChain 의 접근방식은 다른 블록체인에 적응을 하는 것이다. KardiaChain의 궁극적인 목표는 시장성이 있는 접근법을 제공하는 것이며 이는 여러 요건들을 충족시킬 수 있다. 특히:

- 솔루션부터 개발까지 진척이 동시에 이루어 질 수 있어, 생태계에 참여하고자 하는 블록체인과 적합하다.
- 참여 블록체인의 강점과, 특히 보안성과 합의도출 메커니즘을 보존할 수 있어 절충이 불필요하다.
- 디앱 개발자들에겐 투명성과 단순함을 유지하여 KardiaChain은 개발자들의 로직을 적용시킬 수 있는 여지를 남기며, 블록체인 간 통신을 책임질 것이다.

III. KardiaChain의 솔루션 (특허 신청중)

상호운용의 난제를 해결하면서 전체적인 블록체인 환경의 확장을 이루기 위해, KardiaChain은 상호운용을 실현시키면서 가능해지는, 여러 플랫폼들에 걸친 솔루션 개발을 할 수 있으면서 개발자 관점에서의 적용성은 최대의 단순함을 유지하는, 통일된 인프라 제공을 목적으로 한다. KardiaChain의 여러 특징 중 하나는, 유저는 KardiaChain을 통해 한 블록체인 상 이벤트로 다른 한 쪽의 블록체인에 결과가 반영되는 상호작용이 가능하다는 것이다.

KardiaChain은 블록체인 생태계에 존재하는 서로 다른 네트워크들과 어플리케이션들을 연결하는 블록체인 네트워크이다. 우리의 목적은 모든 참여 네트워크들의 단결된 강점이 실현될 수 있는 통일된 생태계를 만들고, 이후 다가올 블록체인의 대중화를 위한 초석을 놓는 데에 있다.

듀얼 마스터 노드 (혹은 듀얼 노드)는 KardiaChain의 주요 솔루션이며 이는 크게 Translator, Router 그리고 Aggregator 이 세 요소로 구성된다. 해당 솔루션은 실용적이고 안전하며, 탈중앙적인 방식으로 블록체인 간 연결과 비용 절감, 속도 상승이 가능한 온건한 방식이다.

A. 기술적 장점

KardiaCahin의 솔루션은 다음과 같은 기술적 장점을 제공한다.

- 비용과 속도 최적화를 위한 처리 라우팅에 대한 알고리즘적 접근법
- 개발성 개선을 위한 통일된 스마트 계약 언어.

- 통합성을 고려하여 변경사항이 필요 없는, 백워드 호환성을 갖춘 비침습식 솔루션.
- 실용성과 적용성.
- 안전하고 탈중앙적인 블록체인간 데이터 처리능력.

B. 중요 요소

- 듀얼 마스터 노드들은 동시에 다른 두 블록체인의 원장들에 대한 접근성이 있다 (KardiaChain과 또 다른 블록체인). 듀얼 노드들은 외부 블록체인에서 거래 데이터를 수신할 수 있으며 두 블록체인에 영향을 끼치지 않고 안전하게 KardiaChain 원장 상에 업데이트들을 처리할 수 있다.
듀얼 마스터 노드는 누구나 실행할 수 있기에 탈중앙화 되어 있으며 노드 간 합의를 통하여 두 블록체인에서 나오는 데이터를 검증할 수 있다. KardiaChain에서 오가는 블록체인 간 거래 데이터는 슈노르 서명 알고리즘과 같은 [8] 다중서명으로 보호받으며 [9] 불변이기에 듀얼 마스터 노드들은 보안성을 가진다.

- Translator는 카디아 통합 스마트 계약 언어 (Kardia unified Smart contract Language, KSML) 를 활용하여 서로 다른 스마트 계약 플랫폼 간 언어장벽을 없애며 KardiaChain과 외부 블록체인 간 스마트 계약 지시사항에 대한 이해를 가능하게 한다.

- Router는 현재 성능, 비용, 대기시간과 수용량 등 여러 요소를 토대로 번역된 리퀘스트 수행에 있어 가장 적합한 블록체인을 결정하며, 이를 해당 블록체인으로 명령, 유도한다.

- Aggregator 는 다른 블록체인 상 업데이트들을 배치화 하여 (Batching) KardiaChain에 가해질 네트워크적 부담을 덜어주며, 잠재적으로 KardiaChain 상 한 블록의 업데이트를 한 거래로 줄일 수 있다. 상기된 개념들의 조합은 수 많은 기회들을 창출하고 블록체인 대중화에 대한 초석이 된다.

듀얼 노드의 운용 흐름은 다음과 같은 과정으로 나눠질 수 있다:

- Step 0: 한 사용자가 $i = 1,2,3$ 인 SMC_A 스마트 계약을 목표로 하는 $TX(r(i))$ 을 실행한다.
- Step 1, 2: Router 와 Translator는 이를 감지하고 처리한다.
- Step 3: 듀얼노드는 확인을 위해 외부 블록체인을 향한 $j = 1,2,3$ 인 $Func\_call(j)$ 를 생성한다.
- Step 4: 결과는 외부 블록체인의 $l = 1,2,3$인 $TX(u(l))$ 이다.
- Step 5: 듀얼 노드는 해당 $TX(u(l))$ 를 외부 블록체인의 양식으로 돌려놓는다.
- Step 6, 7: Aggregator와 Translator는 하나의 거래, $TX(k) = [value : (1,2,3)]$ 를 생성한다.
- Step 8: 변동사항 (1,2,3) 이 SMC_A에 실행되고 원장에 기록된다.

이와 같이, 이 새로운 절차는 KardiaChain이 참여하는 체인들의 처리능력들을 합치게 하며 TPS 단위 개념을 재정의한다.

$$KardiaTPS = \sum_{i=0}^{n} K_i + \left[min(R, E, Kt) \times (1 - \tfrac{1}{t}) \right]$$

K_i는 듀얼 노드 그룹들, KardiaChain의 고유 TPS이며, R 은 듀얼 노드들의 라우팅 능력의 총합, E 는 참여하는 블록체인들의 총 TPS, 그리고 t 는 배칭 비율이다. 유의할 것은 KardiaChain에 더 많은 블록체인들이 지원될수록 t 가 변하며, 이는 각 블록체인의 Block_Size 와 Block_Time 에도 의존한다. 일반적으로, t 의 범위는 1부터 시작하여 아래의 최댓값을 가질 수 있다:

$$t_{max} = \frac{\sum_{i=1}^{n} (tps)_i}{\sum_{i=1}^{n} \frac{1}{Block\_Time_i}}$$

n 은 참여하는 블록체인의 수 이다.[1]

[1]t = 1은 한 건의 거래만 라우팅 되었을 시 나오는 특별한 경우로, KardiaChain의 업데이트는 1 건이며 이에 따른 배칭 비율은 1이다.

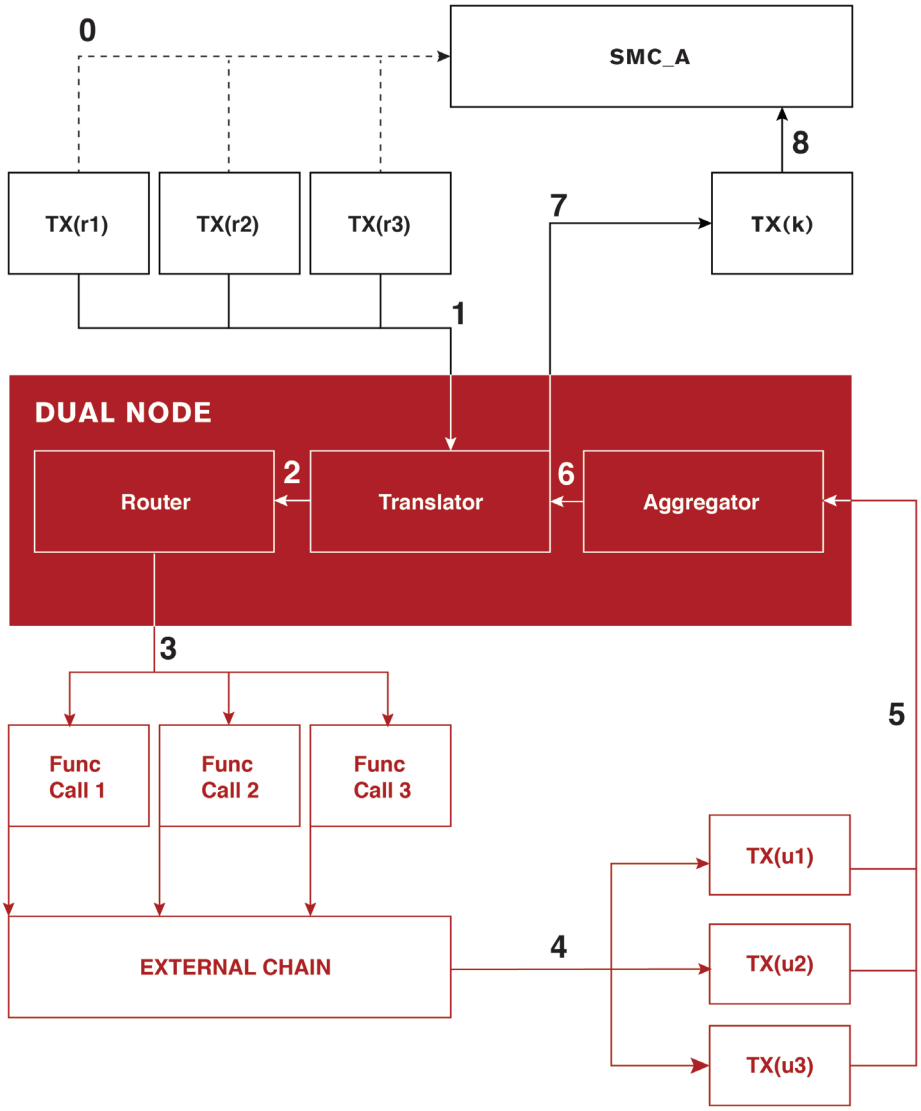

Fig 1. 간소화된 듀얼 노드 운용

IV. KardiaChain의 기술

A. 노드 구성

노드는 세 부분으로 나누어지는데, 더 나은 설명을 위해 노드의 구조를 생물학적 장기 구조의 예를 들어 Heart, Artery, Vein 세 부분으로 나누었다. 듀얼 노드는 블록체인 간 연결을 위해 세 가지 구성요소를 모두 능동적으로 사용한다. 거래들은 Heart에 저장되고 내보내지며, Artery을 따라 다른 블록체인들에 도달하고 Vein을 통해 KardiaChain으로 다시 돌아온다.

만약 어떤 이유로 간에, 한 노드가 생태계 상호연결에 기여하지 않기로 결정했다면, 해당 노드는 Heart의 기능만 유지한 채 내부 거래들을 처리하는 기본 노드가 될 것이다.

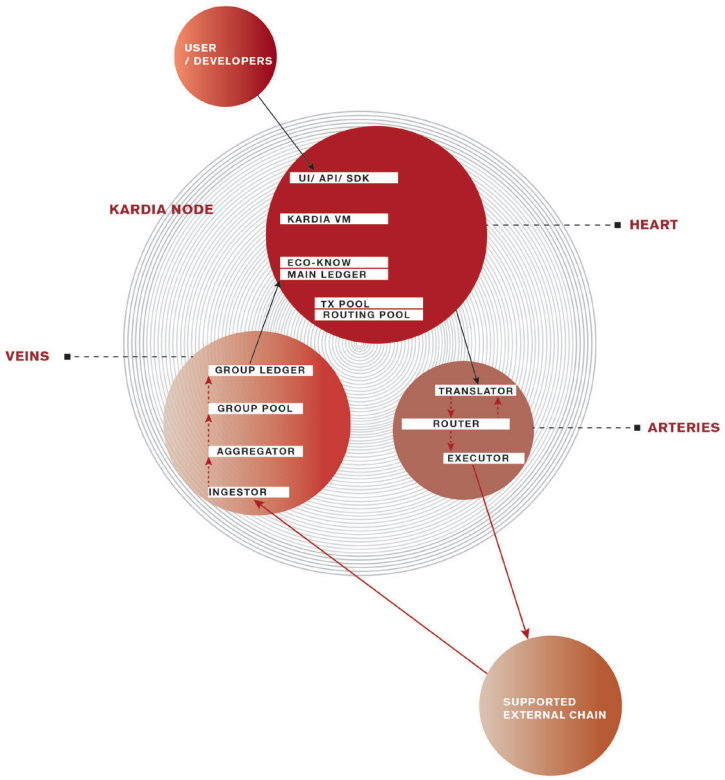

Fig. 2. 노드 구성

1. Heart

a) KardiaChain 개발 툴킷

서로 다른 블록체인 간 스마트 계약 프레임워크를 익히는 데 있는 어려움의 해결이 KardiaChain 의 목표임으로, KardiaChain 상에선 간편한 스마트 계약 개발을 위한 직관적인 구조를 가진 UI, API 그리고 SDK 가 마련될 것이다. 이를 Conduction 시스템이라 하며 Heart가 지속적으로 운영될 수 있게 한다.

- 사용자 친화적인 UI는 KardiaChain 상 간략한 스마트 계약 개발을 위해 제공되는 템플릿이다. 이 템플릿은 스마트 계약 언어에 대한 지식이 적거나 전무한 개발자들에게, 몇 가지의 대중적으로 쓰일 스마트 계약을 만들고 커스터마이즈 하는 데에 도움이 될 것이다.
- 효율적인 API는 KardiaChain 상에서 좀 더 복잡한 스마트 계약을 직접 구축하기 위한 것이다. 해당 기능은 다수의 블록체인 상 실행 되는 커스텀 로직을 전개하고 싶어하는 중급 개발자들에게 사용되는 것을 목표로 한다.
- 강력한 SDK는 디앱 개발자들이 KardiaChain상 존재하는 모든 스마트 계약 기능들을 자유롭게 탐구할 수 있게 하기 위함이다. SDK는 개발자들에게 KardiaChain 상 모든 블록체인 간의 스마트 계약 흐름에 대한 완전한 제어권을 제공한다: 어떻게 하위 계약들이 외부 블록체인들에서 만들어지는지, 업데이트들이 어떻게 모이는지, 이 모든 것이 개발자들이 결정할 수 있게 될 것이다.

b) 카디아 가상 머신 (Kardia Virtual Machine, KVM)

카디아 가상 머신은 블록체인들 간 상호작용기능을 추가한 이더리움 가상 머신의 개선된 버전이다 [10]. KVM 상 실행되는 스마트 계약은 합의도달 매커니즘에 변동을 주지 않으면서, 각 원장들의 최종 상태에 도달을 위한 외부 블록체인들의 이벤트 처리를 할 수 있다. KVM은 내부와 외부 블록체인 간 거래를 위한 두 종류의 수수료 체계를 가진다.

외부 블록체인간 거래는 노드들의 블록체인간 운영 참여가 장려될 수 있도록 커스터마이즈 된 수수료 체계가 도입될 것이며 이는 시스템이 전체적으로 원활하게 작동될 수 있게 할 것이다.더하여, KVM 은 외부 블록체인에서 들어오는 업데이트들에 대한 프로세싱과 종합에 대한 크로스체인 로직을 처리하는 데 도움이 되는 특수한 작업 세트 또한 지원한다.

c) 생태계지식 (EcoKnow)

EcoKnow는 KardiaChain과 활발하게 대응하고 있는 블록체인들의 통계치들을 기록, 유지한다. 이는 스마트 라우팅 알고리즘을 위한 방대한 지식을 제공하며 KardiaChain 을 우월한 솔루션으로 만드는 요소 중 하나이다. 거래 업데이트 이외에, 여타 통계치들의 업데이트들 또한 실시간으로 수집되고 분석된다. EcoKnow는 해당 정보들을 추출, 기록하여 하나의 종합적이고 사용 가능한 생태계 데이터로 구성한다. EcoKnow는 전체적인 네트워크의 기반지식으로 간주된다. 새로 참여하는 노드들에게도 접근이 열려 있으며, 노드들에게 네트워크 전체에 대한 정보가 즉시 제공될 수 있다.

d) 메인 원장

메인 원장은 모든 노드들 (일반, 듀얼 모두) 에 저장되며 메인 블록들로 구성되어 있다 (' 블록 구성" 참고). 메인 원장은 듀얼 노드들이 생성한, 브렌치 원장들에 대한 레퍼런스를 저장한 메인 블록들로 구성된 트리 구조의 원장이다. 메인 원장엔 KVM의 글로벌 상태또한 저장되며, KardiaChain내부에서 발생하는 거래 뿐만 아니라, 외부 블록체인들에서 이루어지는 거래들로도 상태변경이 일어난다. 메인 원장의 목적은, 어떠한 블록체인에서 거래가 실행되었는지와 무관한, 일관성있는 데이터 히스토리 관점을 제공하는 것이다.

e) 마스터 지갑

마스터 지갑은 다수의 블록체인 간 거래에 필요한 사용자의 여러 개인/공공키 세트 등

개인정보들을 안전히 보관할 수 있는 방법이며, 높은 보안성과 함께 다수의 블록체인 사용시에 번거로움을 없앨 수 있다.

2. Artery (KardiaChain -> 외부 블록체인)

Artery는 거래가 KardiaChain에서 다른 블록체인들로 원활히 흐를 수 있도록 하며, 동시에 블록체인 간 작업이 매끄럽게 수행되도록 한다. 이는 Translator과 Router사이에 쌍방 흐름과 Executor를 통한 스마트 계약 제출이 이루어지는 다단계의 프로세스이다.

a) Translator

Translator은 알고리즘을 사용하여 기존 KardiaChain 스마트 계약에 관여된 블록체인들의 스마트 계약들을 포함한 KardiaChain 바이트코드, KardiaChain 상 스마트 계약 상태 머신의 상태변화에 필요한 로직들을 번역하며, 다른 블록체인 상 failure 들을 처리한다.

b) 카디아 스마트 계약 마크업 언어 (Kardia Smart contract Markup Language, KSML)

KSML은 개발자들이 상당량의 교육이나 이전 경험 없이도 KardiaChain 플랫폼에서 스마트 계약 개발을 할 수 있는 궁극적인 도구가 되도록 설계되었다. 사람이 읽을 수 있는 포맷 (JSON 및 YAML 등)의 코드 명령어 세트를 대량으로 제공함으로써, 개발자들은 특정 블록체인을 위한 코드에 대한 지식 필요 없이 손쉽게 일반적인 로직을 작성할 수 있다 (예를 들어, 이더리움은 Solidity을 요구하거나 Neo는 C#, Java 또는 Python을 요구하는 등).

KSML은 개발자들이 자신들이 작성한 KSML 스마트 계약이 올바른지, KardiaChain 플랫폼에 파싱될 수 있는 지 빠르게 확인할 수 있는 신택스 체커와 같이 제공된다. 개발자들이 각자의 솔루션들을 KardiaChain상에 적용시킬 수 있게, KSML과 여타 도구들은SDK로 패키지화 되어 통일된 툴킷으로 제공 된다.

향후에, KardiaChain 은 KSML 스마트 계약뿐만 아니라, 다른 개발자들이 사용하는 블록체인 전용 코드들 (이더리움의 Solidity등) 또한 쓰일 수 있게 하여, KSML로 작성될 수 있는 로직을 넘어서 개발자들에게 무한한 개발성을 발휘할 수 있게 할 것이다.

c) 블록체인 간 기계학습 네트워크 라우터 (Inter-chain Machine-Learning Network Router, CMNR)

CMNR 은 SON 기반 선택 알고리즘을 사용하여 [16] 블록체인 간 거래 시 참여하기에 가장 적합한 블록체인들을 찾아낸다. 선택은 거래비용, 컨펌 시간, 트래픽 등 많은 요인을 근거로 한다. CMNR은 고급 분석 프레임워크인 동적 스코어링 알고리즘을 사용하며, 특정 블록체인인 X의 특정 시간 t 에 일어나는 특정한 리퀘스트 R에 대한 점수를 매기며 이는 다음과 같이 이루어진다.

ScoreXt = f(h, f, v, d)

h:블록 높이

f::최근 기록된 거래 비용

v: X 의 블록형성 시간

d: 각 스마트 계약 간 난이도 차이를 알아내기 위한, 특정한 공식으로 계산된 일반적인 난이도

위에서 기술한 바와 같이 실시간 데이터는 EcoKnow로부터 지속적으로 가져오며, CMNR은 스마트 계약 라우팅을 효율적으로 이루어낸다. 따라서 가장 경쟁성 있는 비용으로 최고의 성능을 달성할 수 있다. 자기정리성과 자기최적화 덕분에 핵심 SON 알고리즘에 대한 모든 수정과 개선은 사람의 행동 없이 자동적으로 이뤄질 수 있다. 로직 상에서 CMNR은 두 개의 인터페이스를 가질 것이다: 내부 인터페이스엔 SNode 가 KardiaChain으로 거래를 라우팅 시키는 기능을 제공하는 JSON-RPC API, 외부 인터페이스는 스마트 계약 call을 위한 최적의 라우팅을 위해 개발자들이 사용할 수 있는 RESTful API이다.

d) Executor

Executor은 CNMR의 명령에 따라 번역된 스마트 계약의 바이트코드를 목적지 블록체인의 JSON-RPC를 통한 전달을 수행하며 이는 가장 로직 부담이 적은 작업이다.

3. Vein (외부 블록체인 -> KardiaChain)

Vein은 생태계로부터 업데이트들을 효과적으로 수집, 처리하여 원장으로 안전하게 전송하는 일을 담당한다. Vein은 다음과 같은 주요 특성들이 있다:

a) Ingestor

Ingestor은 듀얼 노드에 엮여있는 블록체인에서 새로운 블록들을 취한다. 여기에 연관된 업데이트들은 Aggregator에게 실시간으로 추출, 전송된다.

b) Aggregator

Aggregator은 Ingestor에게 실시간 업데이트를 수신하며:

(1)라우팅 된 거래들을 외부 txID에 올바른 레퍼런스와 매칭 시키며,

(2) 호환 가능한 거래들을 새로운 KardiaChain 거래들로 배칭하고 이를 거래 풀로 보낸다.

c) 그룹 풀 및 그룹 원장

그룹 풀은 듀얼 노드들에 의해 레퍼런스된 라우팅 거래들이 모이는 곳이며 다음 블록으로 처리되는 곳이다. 그룹 원장은 이 라우팅된 거래들의 포괄적인 기록이다. 그룹 원장들이 메인 원장에 어떻게 연결되는 지는 '블록 구조' 파트를 참고한다.

B. 시스템 구조

시스템에 참여하는 모든 새로운 노드들은 기본 노드들로 설정된다. 노드들은 일정의 지분을 예치하고 듀얼 노드가 될 수 있으며 자신이 지원할 블록체인을 선택할 수 있다. 지분 예치 과정은 기본적인 지분증명 합의 프로토콜을 따른다 [17]. 듀얼 노드들은 같은 블록체인을 지원하는 듀얼 노드들간 연결에 따른 그룹으로 운영된다.

주목할 점은 각 듀얼 노드는 한번에 하나의 블록체인에만 걸쳐 있다는 것이다. 이는 하나의 노드가 다수의 외부 블록체인들의 거래들을 동시에 처리하는 것은 비효율적이고 비실용적인 이유에서다. 멀티 노드에 대한 실용성에 대해선 향후 연구가 필요하다.

아래 그림에서 같은 그룹에 있는 듀얼 노드들이 흩어져있는 것을 볼 수 있다. 노드들은 자신들이 지원할 네트워크에 대해 임의적으로 선택할 수 있기 때문이다.
네트워크는 모든 노드들 간 최적의 연결성을 보장하기 위해 주기적으로 최적화 알고리즘을 실행한다 (인센티브 메커니즘 기반 탄력적 샤딩의 일부).

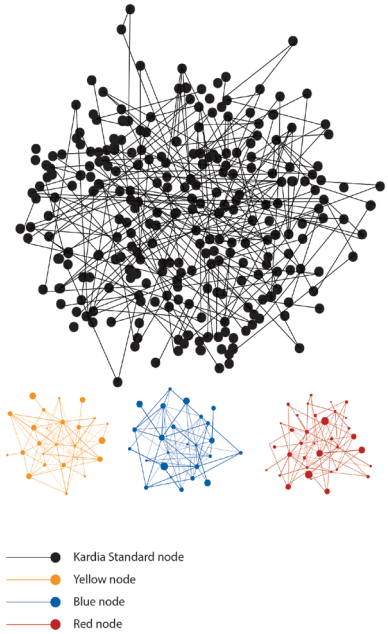

Fig. 3. 초기 단계 – 모든 노드들은 일반 노드들이다.

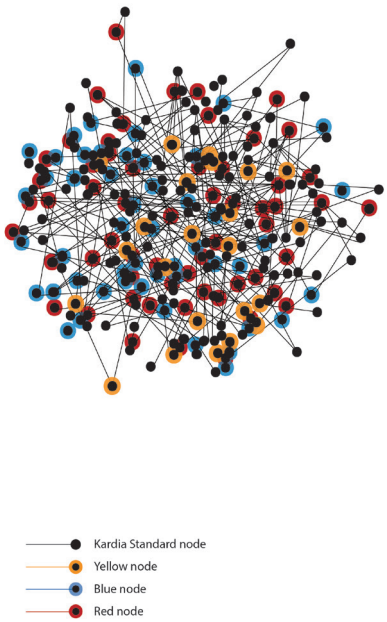

Fig. 4. 전환 단계 – 노드들은 지원하는 네트워크에 대한 전환을 할 수 있다.

C. 인센티브 메커니즘 기반 탄력적 샤딩 (ESWIM)

듀얼 노드들의 인센티브는 일반적으로 복잡한 기능 실행에 따른 블록 생성 보상과 거래 수수료 총합 (TX fee)에 대해 더 큰 몫을 차지하는 것이다. ESWIM의 목적은 각 그룹에 적절한 노드 수가 유지되어 최적의 네트워크 성능을 보장하는 것과, 메인 네트워크와 그룹에 속한 검증인들의 지분 위력 조정을 통한 네트워크 보안성을 확보하는 것이다.

ESWIM은 노드들의 듀얼/일반 상태의 전환과, 수요 그룹의 블록 생성 보상 분배, 거래비용, 특정 체인들에 대한 노드 요구사항 등의 여러 수단의 조정을 장려한다.

예를 들어, 최소 지분 예치량 증가는 몇몇 노드들을 과도하게 몰린 그룹에서 떠나게 할 것이며, 최소 요구량을 줄인다면 더 많은 노드들이 참여를 필요로 하는 그룹에 끌어들일 수 있다.
아래 그림들과 같이, 시기 t1과 t2 사이의 파란 체인과 붉은 체인의 거래 수수료 변경은 KardiaChain 상 듀얼 그룹의 변경을 야기한다. 붉은 체인에서의 운영이 더욱 비싸졌기에 붉은 체인에 대한 라우팅 수요는 줄어들며 파란 체인은 그와 반대가 된다. ESWIM은 향후 일어나는 라우팅 된 거래 수 변화예측에 따라서 그룹 A와 B에 속한 듀얼 노드 수에 대한 조정을 결정한다. 거래 수수료는 ESWIM이 작동하는 가준의 하나일 뿐 임을 유의한다.

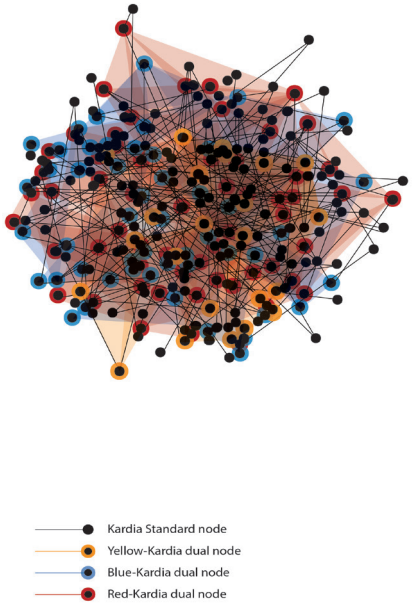

Fig. 5.듀얼 그룹들의 초기 분포

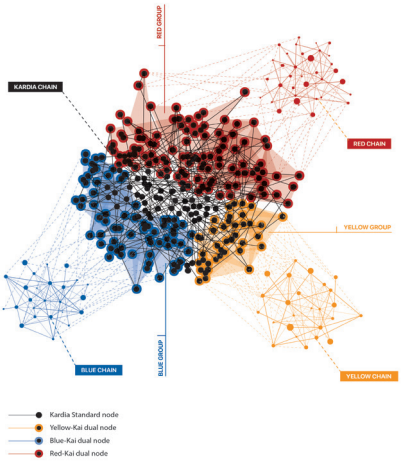

Fig. 6. 최적화된 듀얼 그룹 분포

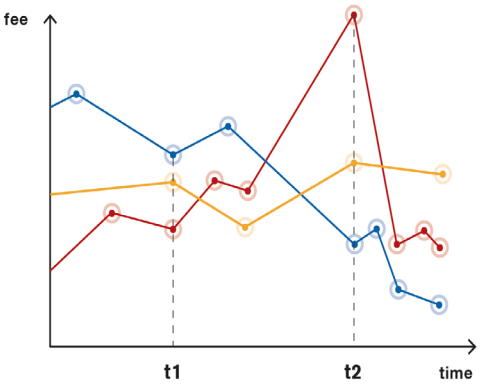

Fig. 7. 시간에 따른 파란 체인과 붉은 체인의 거래 수수료 변화

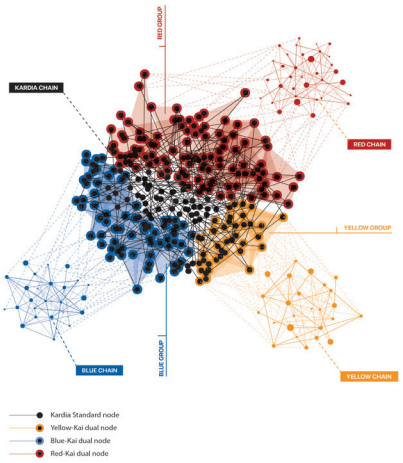

Fig. 8. 시간 t1의 그룹 분포

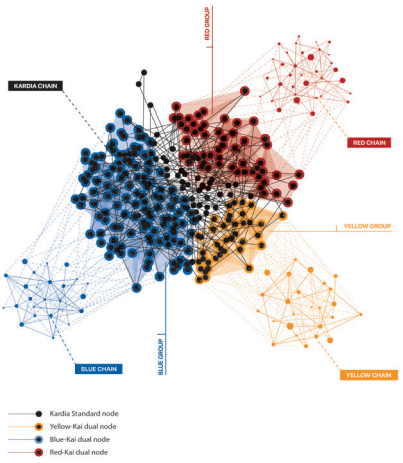

Fig. 9. 시간t2 의 그룹 분포

D. 합의 프로토콜

KardiaChain은 주요 합의 (MCon)와 그룹 합의 (GCon)를 위한 두 가지의 비잔틴 장애 허용 (BFT) [6] 위임 지분 증명 합의를 실행한다 (dPoS). MCon 참여자들은 메인 검증인들이라 불리며 (MVals), 이들은 KardiaChain 원장을 유지한다. GCon 참여자들은 그룹 검증인들이며 (GVals), 블록체인 간 거래들의 검증과 이를 해당 그룹 원장에 추가하는 역할을 한다.

1) 과정: GCon은 다음의 다섯 단계의 과정을 따른다:

GCon 은 다음의 다섯 단계의 과정을 따른다:

- 선거: GVals 은 그들 중 그룹 제안자를 뽑는다.
- 제안: 그룹 제안자는 블록을 생성하고 이를 그룹 내 다른 노드들에게 알린다. 그룹 제안자가 주어진 시간 내에 블록 생성에 실패할 경우에도, 네트워크는 다음 단계로 넘어간다. 추가로, 그룹 제안자는 거래 포워딩을 처리한다 (1).
- 검증: GVals들은 제안된 블록을 수신하고, 블록의 유효성에 대한 투표를 실시하며 <Approval/Reject/Nil>, 해당 투표를 가십 프로토콜을 통해 다른 이들에게도 전송한다.
- 승인: 그룹 제안자가 2/3의 표를 받을 시, 그룹 제안자는 해당 블록은 메인 제안자에게 알린다 (2). 모든 듀얼 노드들은 메인 블록 승인 전까지 대기한다.
- 완결: 해당 블록이 네트워크에 승인되면, 블록 높이는 1만큼 올라가며 이는 블록의 완결을 나타낸다.

MCon 또한 다음의 차이점을 제외하고 비슷한 단계를 거친다:

- 선거: MVals 는 그들 중 메인 제안자를 뽑는다.
- 제안: 메인 제안자는전달받은 검증된 그룹 블록들에서 메인 블록을 생성한다.
- 승인: 제안된 블록이 충분한 표를 받으면 모든 노드가 해당 블록을 승인하기 시작한다.

(1)거래 포워딩: 그룹 제안자들은 자신들의 라우팅 TX 풀에 접근하여, 그들이 지원하는 블록체인에 매치되는 목적지 체인으로 대기중인 TX들을 처리한다. 포워딩의 거래증거를 받은 뒤, 제안자들은 해당 RTX들을 듀얼 풀로 옮기며, 이는 듀얼 노드들이 다음 블록 컨펌을 위해 업데이팅 되는 TX들을 저장하는 곳이다.

(2) 승인된 블록의 알림: 제안된 블록이 2/3의 표를 받은 후, 그룹 제안자들은 메인 제안자들이 해당 블록이 메인 제안에 들어갈 수 있게 블록을 메인 제안자와 다른 노드들에 알린다.

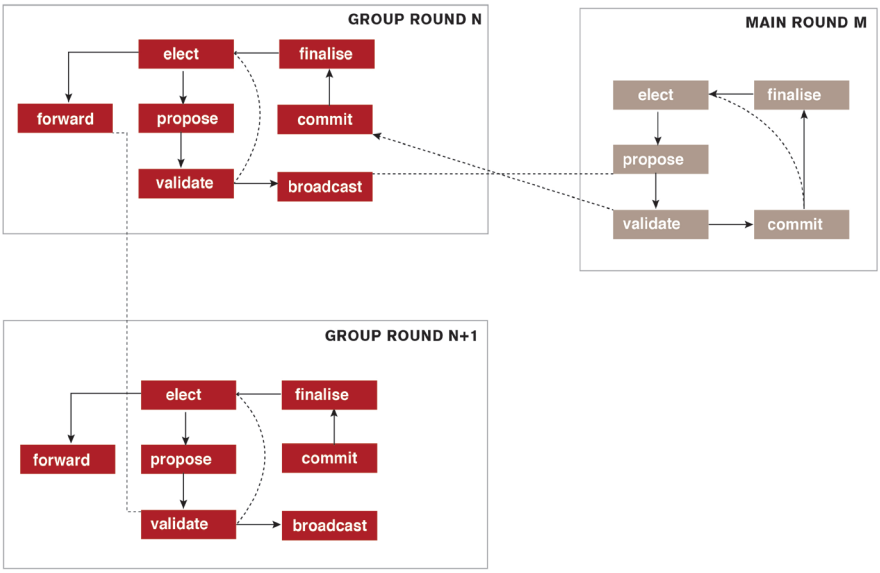

Fig. 10.합의 프로토콜

2) 블록 구조: KardiaChain은 두 종류의 블록, 메인 블록과 듀얼 블록이 있는 이중 블록 구조를 사용하며, 다음의 사항들은 두 종류의 블록이 공통적으로 가진다:

- Timestamp: 블록 생성 시간.
- Height: 블록체인의 길이. 제네시스 블록은 0부터 시작된다.
- Votes: 서명들과 더불어 해당 블록에 대한 모든 비잔틴 장애 허용 투표 들을 기록한다.
- PreviousHash: 부모 블록의 해쉬값.
- StateRoot: 트리 루트의 해쉬값, 이는 블록 거래들이 완결된 후의 글로벌 상태를 나타낸다.
- GasLimit: 해당 블록에 대한 현재 가스 한도.
- GasUsed: 해당 블록에서 소비된 가스 총량.
- Data: 해당 블록의 거래 데이터.

메인 블록은 KardiaChain 의 메인 블록체인의 거래들을 저장하며, 듀얼 블록은 듀얼 그룹에서 일어난 이벤트들을 저장한다.
듀얼 블록은, 이더리움 네트워크에 연결되어 있는 노드 그룹과 같은, 듀얼 노드 그룹의 상태를 저장하며, 메인 블록은 각 듀얼 노드 그룹들이 실행하고 있는 브랜치 듀얼 블록체인에 대한 레퍼런스들을 저장한다. 서로 다른 그룹들에서 나오는 듀얼 블록은 그에 맞는 식별자를 가진다. 예를 들어, 이더리움-카디아는 EK, 네오-카디아는 NK등 (표기법은 확정되지 않음).

그림 11은 하나의 듀얼 노드 그룹에 속한 메인 블록에 대한 듀얼 블록들의 연결을 보여준다. 메인 제안자는 모든 듀얼 블록들로부터 오는 번역된TX(u) 와, 모든 일반 노드들로부터 오는 TX(n) 을 통합하여 TX 데이터를 생성한다. 메인 제안자는 TX(n) 을 제출한 듀얼 블록들과 일반 노드들로 부터 모은 서명 데이터로 TX 리스트를 검증한다. 메인 제안자는 이러한 TX 를 상태 루트 업데이트에 적용한다. 이제 메인 블록은 필요한 데이터들과 메인 제안자의 서명과 함께 생성된 것이다.

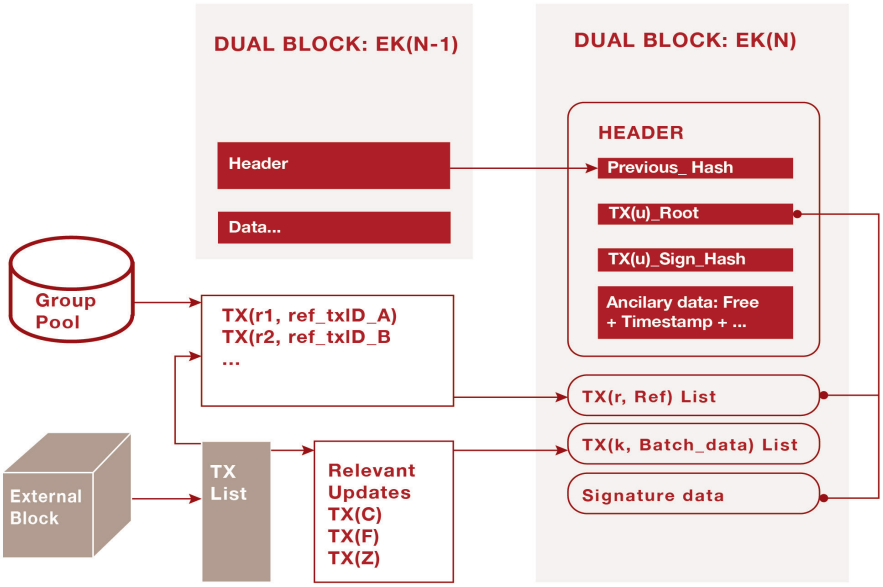

Fig. 11. 메인 블록과 듀얼 블록 간 연결

E. 지분 예치 모델

1) 지분 예치 모델: 검증인이 되기 위해선 노드 운영자는 현재 소지하는 카디아 토큰 (KAI) 잔액 모두를 lockBalance 거래를 통하여 동결해야 한다. 마스터 노드로서 검증인이 되기 위한 필요 지분 예치량은 s(M) 이며, 듀얼 마스터 노드로서는 s(M+D) 이다.

KardiaChain은 "코인 년수" 개념을 적용하여 효과적인 예치량을 검토하며, 이는 KAI 토큰이 lockBalance 에 쓰이기 위해선 해당 계정에 어느 정도의 블록 시간동안 존재했어야 한다는 의미이다 (mature-time).

KardiaChain은 네트워크 보안을 해치지 않는 탈중앙화 최적화를 위해 설정되어 있으며, 공격자에 대해 여러 단계의 방어선을 가진다.

mature_time 이 공격자가 새로운 지분 예치에 걸리는 시간을 지연하는 한편, mature_tiem 기간 중에 전체 예치량은 변할 수 있으며 결국 다수를 달성하기 위해 더 많은 예치량을 요구하는 결과를 낳는다.

예를 들어, 현재 지분 예치 총량이 1,000,000 KAI 라면, BFT 합의 보안 모델에 의해 공격자는 2,000,001 KAI 만큼의 예치량을 달성해야만 >66%을 이룰수 있다 [15]. 그러나 mature_time 이후, 다른 계정들이 검증인으로서 참여하며 예치량을 100,000 KAI 늘릴 시, 공격자는 이에 대해 200,000 KAI 를 추가로 예치하고 또 다른 mature_time 이 지나야 공격을 감행할 수 있다. 그러므로, 네트워크에 대한 공격은 불확실 해지며, 이는 악의적인 유저들의 공격에 대한 수익성을 감소시킨다. 듀얼 노드 그룹에 대한 공격 또한, 외부 업데이트들이 메인 원장에 반영되기 전에 메인 제안자들로부터 승인되야 하기에 메인 네트워크의 장악을 요한다. 또 다른 예시로 그림 12에 그려져 있듯이, 만약 공격자가 장악한 그룹이 10%의 지분 위력을 가진다면, 총 지분의 7% 만으로도 노란 체인으로 부터

악의적인 업데이트를 실행할 수 있다. 그러나, 해당 업데이트가 KardiaChain의 원장에 효력이 있으려면, 메인 검증인들을 통과해야 한다. 이것은 또 다른 60%의 네트워크 지분 위력을 확보해야만 성공적인 공격 기회를 마련할 수 있다는 의미이다. 공격 실패 시, 악의적인 거래들과 블록에 투표한 모든 지분 예치량은 동결되며 (토큰 소각), 이는 KardiaChain에 대한 어떠한 공격시도도 상당한 고비용을 요하게 한다.

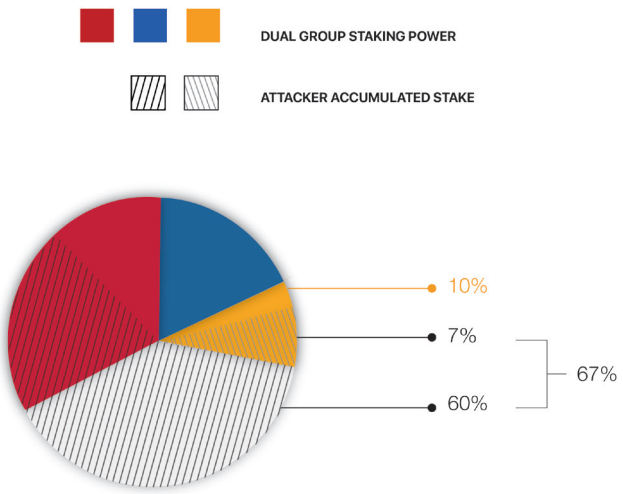

Fig. 12. 소규모 듀얼 그룹을 장악하기 위한 전체 네트워크 지분

2) 토큰의 사용: KardiaChain 의 암호학적으로 안전한 디지털 유틸리티 토큰 (KAI) 은 KardiaChain 생태계의 주 요소이며, 네트워크 상 주요 토큰으로 쓰이게 디자인 되었다. KAI 는 KardiaChain 참여자 사이의 교환 단위로, 비환불성을 가진 기능성 토큰으로 쓰이게 된다.

KAI의 도입 목적은 KardiaChain 상 생태계 안에서 참여자 간 편리하고 안전한 지불과 청산방식을 제공함에 있다. KAI는 그 어떠한 지분, 참여, 권리, 직책, 재단의 이익, 배포자와 그 재휴사들, 산하 업체 또는 그 어떤 기타 회사, 영리를 추구하거나 표하지 않으며, KAI 토큰은 토큰 소유자에게 그 어떠한 수수료, 배당금, 매출, 이익, 투자수익을 약속하지 않으며, 또한 싱가폴이나, 또는 연관된 그 어떤 관할의 지역에서 담보나 금융상품으로 구성되지 않는다. KAI의 소유는 KardiaChain과의 사용과 상호작용, 제 3 거래소로 옮겨지는 것 외에 그 어떠한 명시적, 암묵적 권리를 가지지 않는다.

추가적인 블록들과 블록체인 상 정보에 대한 검증은 연산 리소스를 필요로 하며, 그렇기에 리소스 제공자들은, 네트워크의 온전성을 위한 소비에 대한 보상을 필요로 하며 (KardiaChain 상 "채굴"), 이 때 KAI는 소비된 연산 비용을 수치화 하고 교환 단위 로써 쓰일 것이다. KardiaChain은 채굴자들이 채굴 참여 권리를 위해 일정량의 KAI를 예치 할 것을 요구할 것이다. KAI의 부재시엔 사용자들이 활동에 참여하기 위해 리소스를 쓸 이유도, KardiaChain 생태계 전체의 이익이 될 서비스 제공또한 하지 않을 것이기에, KAI는 KardiaChain 의 일부분이며 불가분하다. KardiaChain에 활발히 참여하지 않는 유저나 KAI 소유자들은 그 어떠한 KAI 인센티브를 받을 수 없다. 특히나, KAI는:

- 비환불성을 가지며 현금과 교환 할 수 없으며 (혹은 그에 상응하는 가치를 지닌 그 어떠한 가상 화폐), 혹은 재단, 배포자 또는 재휴사에 의해 지불의무를 가지지 않는다;

- 재단과 배포자 (혹은 이의 재휴사들, 산하기업) 그들의 매출이나 자산, 미래 배당금, 매출, 증권, 소유권 또는 지분, 담보, 투표권, 현금화, 상환, 자산배분, 상표 (모든 형태의 지적 재산권 포함), 또는 그 어떠한 금융 혹은 법적 권한이나 그에 준하는 권한들, 또는 지적 재산권에 대한 권한들이나 KardiaChain 에 그 어떠한 형태로의, 또는 관련된, 참여, 재단, 배포자 그리고/혹은 그들의 서비스 제공자들 에 대해 어떠한 권한을 묘사하거나 부여하지 않는다;

- 차액 거래에 대한 그 어떠한 권리 또는 영리 목적이거나 손해 회피의 목적 계약에 대한 그 어떠한 권리에 대해 표하지 않는다;

- 돈 (전자화폐 포함), 담보, 현물 또는 원자재, 채권, 공채 또는 그 어떠한 금융 도구나 투자도구로서 쓰이는 의도가 없다;

- 재단, 배포자 또는 이의 재휴사들, 산하기업에 대한 대출이 아니며, 재단 또는 배포자나 이의 재휴사가 지는 채무로서 의도되지 않으며, 그에 대한 수익또한 기대될 수 없다; 그리고

- 토큰 소유자에게 제단과 배포자 또는 이의 재휴사들, 산하기업에 대한 그 어떠한 소유권이나 이익을 제공하지 않는다.

토큰 판매 이후 기여금은 배포자 (혹은 이의 재휴사들, 산하기업) 들에 의해 보관될 것이며, 기여자들은 기여금, 혹은 자산에 대한 수익권에 대해 그 어떠한 경제적, 법적 권리를 가지지 않는다.

KAI의 표준 토큰 기반은 처음엔 ERC-20 일 것이며 이는 후에 KardiaChain 토큰과 스왑될 것이다. ERC-20 와 KardiaChain 토큰에 깔려있는 토큰 기준은 KAI 가 제 3 거래소를 통해 유통 시장에서 거래될 수 있게 한다. 그러한 제 3 거래소들은 제단과 배포자, KAI 의 판매와 KardiaChain과 완전히 독립적인 운영을 영위한다. 제단과 배포자 모두 그러한 유통시장을 만들지 않을 것이며 이 중 그 누구도 KAI를 위한 거래소로서 행동하지 않을 것이다.

V. KardiaChain의 장점

KardiaChain의 미션은 블록체인 개발자들이 하나의 블록체인에만 묶여있는 문제를 해결하기 위함이다. KardiaChain은 개발자들이 여러 블록체인들에 걸쳐 작동하는 디앱을 개발 할 수 있으면서, 동시에 해당 블록체인들 상에 스마트 계약 작성법을 알 필요 없이 이를 달성할 수 있게 한다. KardiaChain은 퍼블릭과 프라이빗 블록체인을 아우르는 포괄적인 네트워크를 만들어내는 것을 목표로 한다. 이 네트워크에서는, 한 블록체인이 네트워크에 속한 다른 블록체인과 내부의 커뮤니케이션의 변화 없이 상호작용 할 수 있다. 그러므로, KardiaChain의 확장성과 상호운용성은 증대된다.

- 확장성. KardiaChain 네트워크로 스마트 계약이 제출되면, 이는 네트워크 내 다른 (특정한) 블록체인으로 번역되어 보내질 수 있다. 최대의 성능이 발휘되기 위해 가장 적합한 네트워크 선별은 제출 당시에 이루어 지게 된다. 이는 특정 시간대나 특정 이벤트 하에 생기는 급작스런 트래픽 체증을 회피하는 블록체인을 위한 offloading 솔루션이다.

- 상호운용성. KardiaChain을 통해 네트워크상 모든 블록체인들간 데이터와 자산거래가 이루어 질 수 있다. 블록체인간 기능성은 디앱이 여러 다른 특정한 행동들이 다른 블록체인들에 반영되게 할 수 있다. 이는 특정 시간대 혹은 이벤트 하의 특정 블록체인의 체증을 offloading 할 수 있다.

- 개발성. 개발자들은 KardiaChain 스마트 계약 API를 통해 자신들과 친숙한 도구들과 언어들을 가지고 손쉽게 새로운 블록체인 기술을 사용할 수 있다. KSML은 사람들이 읽을 수 있게 디자인 되었으며, 대부분의 스마트 계약에서 이루지는 작업들을 수행 가능하게 하는, 즉각적으로 사용 가능한 언어이다. KSML로 스마트 계약 작성을 통해, 개발자들은 추가적인 노력 없이 손쉽게 KardiaChain 생태계에서 지원되는 어떠한 블록체인 내에서도 솔루션을 배포할 수 있다.

- 적용성. 어떤 단체나 개인도, 유저 친화적인 툴킷과 포괄적인 마크업 언어를 사용하는 KardiaChain 스마트 계약 API를 통해 블록체인을 경험할 수 있으며, 자신들의 첫 스마트 계약을 손쉽게 개발하고, 테스트하고 배포할 수 있다. 이 모든 단계는 준비된 환경 필요 없는 웹 기반 인터페이스에서 이루어 질 수 있다.

- 비용. 하나의 플랫폼만 사용하는 것은 향후 비용 예측이 힘들다는 것을 의미한다. KardiaChain에서는 CMNR이 유저가 어느 순간에서도 최고로 효율적인 블록체인을 찾아 선택할 수 있도록 도와준다. KardiaChain에 추가적인 비용이 붙는다 해도, 전체적인 비용은 항상 일반적인 블록체인의 평균 비용보다 낮을 것이다.

VI. 디앱 실용성의 새로운 지평선

KardiaChain 플랫폼의 디앱으로 있음으로서 가능해지는 세 가지 특성에 대한 비전을 제시한다.

A. 단순하고 높은 트래픽의 디앱

공공 투표는 이러한 디앱의 일반적인 예시이다. 여기서 우리는 네트워크에 특정 시간동안 국가 단위의 대량의 트래픽이 발생할 것으로 생각한다. 그러나, 이에 대한 솔루션은 상당히 간단하게 이루어 질 수 있다.

주최자는 KardiaChain이 제공하는 투표 스마트 계약 템플릿을 알맞게 커스터마이즈하고 KardiaChain 상에 Vote_SMC_ABC(K) 로 배포한다. 특정되지 않았다면, CMNR 은 Vote_SMC_ABC(K) 에 가장 적합한 블록체인들을 분석, 탐색한다. 그리고 번역된 SMC를 발견한 블록체인에 배포한다. 예를 들어, 이더리움에 Vote_SMC_ABC(Eth) 로 배포한다.

주최자는 이제 여러 블록체인에 배포된 Vote_SMC_ABC 의 다수의 주소들을 수신하고 이를 자신의 목적에 맞게 쓸 수 있다. 투표자들은 Vote_SMC_ABC 가 배포된 아무 블록체인을 통하여 투표에 참여할 수 있다. 하지만, 체증을 회피하기 위해서는 스마트 라우팅 알고리즘을 활용하는 KardiaChain을 통해 투표에 참여하는 것이 권장된다.

보수적으로 보았을 때, 투표 당시 KardiaChain은 두 개의 블록체인을 지원한다 가정한다 하고 (E 와 N). 각각은 2,000tps/10s 의 block_time과 1,000tps/5s 를 가지며, KardiaChain 의 본래 tps는 20초에 100tps 의 block_time 을 가진다 가정한다. 이는 전체적으로 3,100 의 tps를 가지며, 5천만 투표자들을 지원할 수 있는 수치이다. 모든 투표자들이 하루 8시간 내에 투표를 한다 가정하였을 때 사용량은 약 1,700tps 이다.

B. 다기능 디앱

크립토키티와 같은 디앱이 간단한 용례가 될 수 있으며 [18], 모든 중요치 않은 액션들이 블록체인 상 거래를 필요로 하는 것은 (브리딩, 이름 짓기 등) 금전적으로도, 시간적으로도 부담되는 것이다. 만약 중요치 않은 액션들이 더 적은 트래픽과 수수료를 가지고 있는 블록체인으로 옮겨질 수 있다면, 중요한 액션 (고양이 사기/팔기 등) 은 신뢰성을 갖춘 블록체인에 그대로 둘 수 있을 것이다. 이 접근법은 빈도의 차이에 대해서도 활용될 수 있다: 브리딩은 매우 자주 일어날 것이지만, 그에 비해 고양이들의 교환은 비교적 적게 일어난다. 이러한 두 작업들은 한 인프라 상에서만 일어날 필요가 없다. 소프트웨어 엔지니어링 관점으로 보았을 때, 서로 다른 기능들엔 다른 특성을 가진 다수의 데이터베이스를 쓰는 것이 효과적이다 (속도나 일관성 등).

C. 상호연결된 디앱

KardiaChain은 디앱들 간 데이터 교환과 상호작용이 안전하고 매끄럽게 이루어 질 수 있는 인프라를 제공한다. 다음 도표는 블록체인 상에 존재하는 뱅킹 디앱이 다른 블록체인의 디앱의 KYC 데이터를 활용하는 것을 보여준다 (KardiaChain 과 ChainX). 유저 A 가 KardiaChain 상 KYC_Dapp 에 KYC 데이터를 제출한다. 유저 A 가 ChainX 상 Banking_Dapp 을 사용 할 시, 유저 A 는 ChainX 상 Banking_Dapp 이 KardiaChain 상 KYC_Dapp 으로부터 KYC_A 데이터를 획득할 수 있게 허용할 수 있다. 이 모든 단계들은 안전하고 탈중앙화 된 방식 하에 이루어지며, 개발자들의 수고를 덜고 사용자 경험을 개선시킬 수 있다.

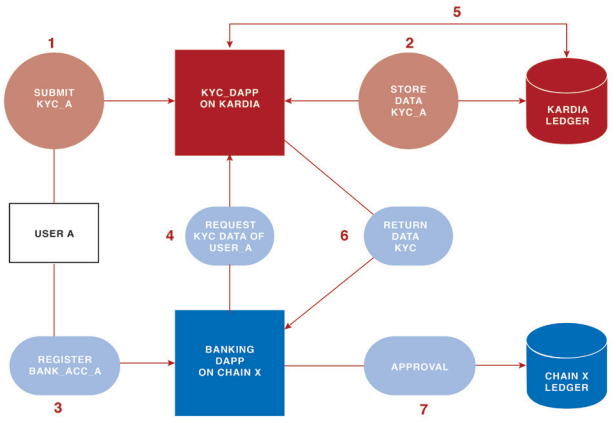

Fig. 13. ChainX 와 KardiaChain 상 두 디앱 간 상호작용

VII. 참고문헌(References)

[1] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, P. Saxena, “A secure sharding protocol for open blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016.
[2] D. Beaver, S. Kumar, H. C. Li, J. Sobel, P. Vajgel, ”Finding a needle in Haystack: Facebook’s photo storage,” in Proc. 9th USENIX Conf. Oper. Syst. Des. Implement. (OSDI), 2010.
[3] Facebook Inc, ”2018 Third Quarter Reports,” 2018 [Online]. Available: https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Third-Quarter-2018-Results
[4] https://www.omnicoreagency.com/youtube-statistics/
[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008 [Online]. Available: http://bitcoin.org/bitcoin.pdf.
[6] M. Castro, B. Liskov, “Practical Byzantine Fault Tolerance,” in Proceedings of the Third Symposium on Operating Systems Design and Implementation, ser. OSDI ’99. Berkeley, CA, USA: USENIX Association, 1999.
[7] M.L. Abbott, M.T. Fisher, ”The art of scalability: Scalable web architecture, processes, and organizations for the modern enterprise,” Addison-Wesley, 2009.
Ledger”, 2014 [Onine]. Available: https://ethereum.github.io/yellowpaper/paper.pdf
[11] M. Al-Bassam, A. Sonnino, V. Buterin, ”Fraud Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities,” ArXiv:1809.09044. Available: https://arxiv.org/abs/1809.09044
[12] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Tim´on, P. Wuille, ”Enabling Blockchain Innovations with Pegged Sidechains,” [Online]. Available: https://blockstream.com/sidechains.pdf

[13] G Verdian, P Tasca, C Paterson, G Mondelli, ”Overledger White Paper,” 2018. [Online]. Available https://www.quant.network/press/overledger-white-paper
[14] G. Wood, ”Polkadot: Vision for a heterogeneous multi-chain framework” 2017. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf
[15] N Chondros, K Kokordelis, M Roussopoulos, ”On the practicality of practical Byzantine fault tolerance,” in Proceedings of the 13th International Middleware Conference, Montreal, QC, Canada, Dec 2012.
[16] C. Brunner, D. Flore, ”Generation of Pathloss and Interference Maps as SON Enabler in Deployed UMTS Networks,” in Proceedings of IEEE 69th Vehicular Technology Conference, Barcelona, Spain, 2009.
[17] W. LiS´ebastien, A. BohliGhassan, G. Karame, ”Securing Proof-of-Stake Blockchain Protocols,” in Data Privacy Management, Cryptocurrencies and Blockchain Technology, DPM 2017, CBT 2017.s
[18] N. Bowles, ”CryptoKitties, Explained ... Mostly,” in The New York Times, Dec. 28, 2017. Available: https://www.nytimes.com/2017/12/28/style/cryptokitties-want-a-blockchain-snuggle.html

KARDIACHAIN

hello@kardiachain.io
www.kardiachain.io