프로토콘 황서

2편 : 팩트 해시 (FACT HASH)

팩트, 팩트 해시 그리고 크로스체인

최윤일, 배민효

May 16, 2022

목차

1. 개요

본 문서는 프로토콘 네트워크의 심장인 미텀(Mitum) 블록체인의 데이터 처리 핵심 요소인 팩트(Fact) 및 팩트 해시(Fact Hash)를 논한다. 블록체인 산업에서 처음 제시되는 팩트 및 팩트 해시 개념을 소개하고 정의하며, 이들의 특징 및 효용성에 대해 기술한다.

이 밖에 팩트 해시의 활용 예제에 대해 설명하고, 특히 팩트 해시를 이기종 블록체인[1]과의 연동에 있어 활용하는 방법을 기술하고자 한다.

크로스체인(Crosschain) 즉 이기종 블록체인을 연동할 경우 두 블록체인을 오프체인으로 연결하는 브릿지[2](Bridge) 서비스를 믿어야 하는 신뢰(Trust) 문제가 발생한다. 만약 브릿지에 헛점이나 공격 포인트가 존재한다면 이는 바로 해킹과 같은 사고로 이어질 수 있다. 팩트 해시는 이러한 부분에서 매우 효과적인 해법을 제시한다. 본 황서는 이 부분에 초점을 맞춘다.

1장에 이어 2장에서는 팩트 및 팩트 해시의 도입 배경과 필요성을 제시하고, 3장에서는 팩트 및 팩트 해시의 정의와 그 효용을 설명한다. 4장에서는 일반적인 크로스체인(Crosschain)의 구조와 동작원리, 이에 따른 보안 이슈를 설명하고, 이 이슈에 효과적으로 대응할 수 있는 팩트 해시 기반의 해법을 기술한다. 5장에서는 본 논고의 결론을 제시한다.

2. 배경 및 필요성

2.1 배경

블록체인은 디지털 자산의 전송에 대한 트랜잭션(Transaction, 거래내역) 기록이다.[3] 특정 트랜잭션의 기록을 찾기 위해서는 이를 유일하게 나타낼 수 있는 ID가 필요한데, 이를 트랜잭션 해시(Transaction Hash) 또는 트랜잭션 ID (Transaction ID) 라고 부른다.

대부분 블록체인의 트랜잭션은 일반적으로 아래 [그림1, 이더리움 트랜잭션 구조]의 트랜잭션 구조와 대동소이한 구조를 갖는다.

---

[1] 이기종 블록체인에는 비트코인, 이더리움, 솔라나 등의 퍼블릭 블록체인 뿐 아니라 하이퍼레저 패브릭과 같은 프라이빗 블록체인이 있을 수 있다.
[2] 블록체인 브릿지는 사용자가 서로 다른 블록체인 네트워크 간에 자산과 데이터를 전송할 수 있도록 하는 시스템을 가리킨다.
[3] 디지털 자산의 전송 이외에도, 스마트 컨트랙트를 지원하는 블록체인의 경우 스마트 컨트랙트를 구성하는 인스트럭션(instruction) 하나 하나의 수행 내용도 트랜잭션으로 기록된다.

Field	Description
Nonce	Account Nonce
From	Sender address
To	Recipient address
Value	Amount of cryptocurrency sending to the recipient
Payload	Transaction data
Gas Limit	The gas limit for the transaction
Gas Price	The price of the gas determined by the transaction initiator
V, R, S	The signature output values

[그림1] 이더리움 트랜잭션 구조

각 트랜잭션의 구분자가 되는 트랜잭션 해시(또는 트랜잭션 ID)는 위 그림에 기술된 트랜잭션 콘텐츠에 대한 해시 값으로 계산된다. 이더리움의 경우에는 아래와 같은 계산식으로 구성된다.

Ethereum Transaction Hash
= Keccak-256(RLP(nonce,gasPrice,gasLimit,to,value,data,v,r,s))

[그림2] 이더리움의 트랜잭션 해시 계산식

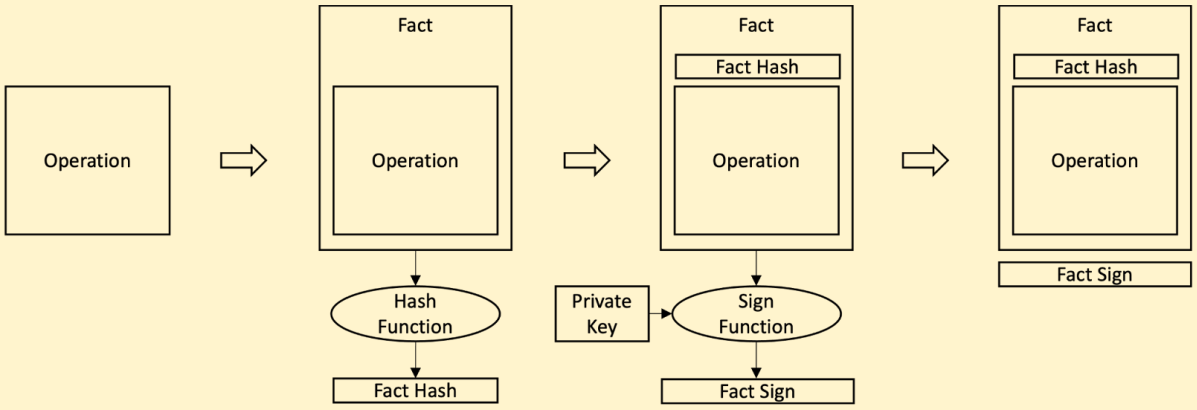
이더리움 트랜잭션 해시는 트랜잭션의 각 필드값(Nonce, Gas Price 등)과 전자서명에 사용되는 파라미터(v, r, s 등)를 RLP 인코딩 및 Keccak-256 해시 계산을 거쳐 만들게 된다.

계산을 통해 트랜잭션 해시(Transaction Hash) 값을 알아내기 위해서는 트랜잭션의 각 필드값을 알고 있어야 한다. 하지만 전자서명의 경우 프라이빗 키가 필요해 트랜잭션을 생성한 계정(account) 소유자가 아니면 계산할 수 없다. 사실상 계정의 소유자 외에는 계산이 불가능한 셈이다. 따라서 이더리움의 경우 암호화폐의 전송기록을 비롯한 거래내역을 검색 및 확인하기 위해 트랜잭션 해시(Transaction Hash) 자체를 별도로 기록해뒀다가 필요한 경우 이를 키로 활용해야 한다. 즉, 트랜잭션 처리 결과에 대해 자동화 및 시스템화된 검증 또는 확인이 불가능하며, 이것이 이기종 블록체인의 브릿지를 구성할 때 보안적 허점으로 작용하게 된다.

2.2 필요성

프로토콘 네트워크의 미텀 블록체인은 트랜잭션의 주요 내용만으로도 해시를 계산할 수 있도록 설계됐다. 특정 트랜잭션을 계산해 검색하고 검증할 수 있는 것이다.

[그림3]은 미텀 블록체인에서의 트랜잭션 생성 프로세스를 나타낸다. 그림 상의 각 용어에 대해서는 3장에서 정의하겠으나, 팩트는 트랜잭션, 팩트 해시는 트랜잭션 해시, 팩트 사인은 트랜잭션의 서명 값으로 이해하면 큰 무리가 없겠다.



[그림3] 미텀 블록체인 트랜잭션 생성 프로세스

암호화폐의 전송 등 트랜잭션이 발생하면 미텀 블록체인에서는 이를 하나의 오퍼레이션으로 인식하고 '팩트'로 추상화 한다. 해시함수로 팩트를 연산해 팩트 해시를 생성하고 이를 다시 팩트의 한 요소로 포함시킨다.

여기 까지의 과정에는 어떠한 형태의 키도 포함되지 않아 콘텐츠만 알고 있다면 누구나 계산을 통해 팩트와 팩트 해시를 계산할 수 있다.

예를 들어 암호화폐를 전송하는 트랜잭션의 경우, 전송하는 주소 (sender address)와 받는 주소 (receiver address), 수량 (amount) 을 알면 트랜잭션 해시에 해당하는 팩트 해시를 계산할 수 있다. 팩트 해시 자체를 모르더라도 추후 계산을 통해 트랜잭션 검색 및 상태 확인이 가능하도록 설계했다.

이후 트랜잭션을 발생시키는 계정 소유자의 전자서명이 적용돼 트랜잭션 ID가 만들어진다. 전자서명이 적용된 트랜잭션 ID는 트랜잭션 및 트랜잭션 해시를 생성한 이후 추가로 만들기 때문에 트랜잭션 해시 그 자체는 계정 소유자의 전자서명 즉 프라이빗 키가 없어도 계산이 가능하다. 요약하자면, 기존의 트랜잭션 ID는 공개되어 있지 않고 공개 되어서도 안되는 프라이빗 키 사인 값을 포함하고 있어 검색이 어렵고 트랜잭션을 특정하기 어렵다는 문제가 있다. 하지만 미텀 블록체인에서는 공개된 정보만으로 팩트 해시가 구성되기 때문에 트랜잭션 키 값으로 사용할 수 있다. 보안상 안전하고 트랜잭션 확인이 훨씬 용이한 장점이 있는 것이다.

이러한 해시계산 방식을 활용하면 암호화폐 지갑과 오프체인, 브릿지 등에서 프로토콘 네트워크의 모든 블록을 동기화하는 수고 없이도 검증이 필요한 트랜잭션을 임의의 시점에 검색해 상태를 확인할 수 있다.

블록체인 간 연동에 신뢰성을 확보할 수 있어 오프체인의 데이터 신뢰성을 획기적으로 제고할 뿐만 아니라 이기종 블록체인 및 암호화폐를 활용한 디파이(De-Fi) 서비스를 가능토록 한다.

3. 정의

3장에서는 팩트(Fact) 및 팩트 해시(Fact Hash)의 개념을 정의하고 그 효용을 설명한다.

3.1 팩트의 정의

미텀 블록체인에서는 블록체인 상의 모든 오퍼레이션[4]을 팩트(Fact)로 정의한다. 즉, 미텀 블록체인은 블록체인 상의 모든 오퍼레이션을 팩트(Fact)라는 개념으로 추상화 하고, 오퍼레이션의 모든 내용(contents)과 해시값을 팩트 내에 포함한다.


```
{
  "_hint": "mitum-currency-create-accounts-operation-fact-v0.0.1",
  "hash": "3Zdg5ZVdNFRbwX5WU7Nada3Wnx5VEgkHrDLVLkE8FMs1",
  "token": "cmFpc2VkIGJ5",
  "sender": "8PdeEpvqfyL3uZFHRZG5PS3JngYUzFFUGPvCg29C2dBn-a000:0.0.1",
  "items": [
    {
      "_hint": "mitum-currency-create-accounts-single-amount-v0.0.1",
      "keys": {
        "_hint": "mitum-currency-keys-v0.0.1",
        "keys": [
          {
            "_hint": "mitum-currency-key-v0.0.1",
            "weight": 100,
            "key": "2Aopgs1nSzNCWLvQx5fkBJCi2uxjYBfN8TqneqFd9DzGcmpu"
          }
        ],
        "threshold": 100
      },
      "amounts": [
        {
          "_hint": "mitum-currency-amount-v0.0.1",
          "amount": "333",
          "currency": "MCC"
        }
      ]
    }
  ]
}
```


[그림4] (예) 계정생성 오퍼레이션 팩트의 구조

[그림4]는 계정 생성 오퍼레이션를 나타내는 팩트의 한 예제다. 팩트는 팩트의 내용을 설명하는 “_hint”, 팩트 해시로 정의되는 팩트의 해시값 “hash”, 팩트의 유일성 보장을 위한 “token”, 팩트를 생성하는 계정의 주소 “sender”, 그리고 오퍼레이션의 컨텐츠를 나타내는 “item”으로 구성된다.

[4] 오퍼레이션에는 계정생성과 토큰전송, 키 업데이트, 암호화폐 등록, 암호화폐 정책 업데이트 등이 포함된다.

구성요소	개요
hint	팩트의 내용을 설명
hash	팩트 해시로 정의되는 팩트의 해시값
token	팩트의 유일성 보장을 위한 값
sender	팩트를 생성하는 계정의 주소
item	오퍼레이션의 컨텐츠

[그림5] (예) 계정생성 오퍼레이션 팩트의 구성요소

위 그림이 나타내듯 팩트의 구성에 전자서명 관련 정보가 들어있지 않아 누구든 오퍼레이션의 콘텐츠와 토큰 값만 알면 팩트를 재구성하고 팩트 해시를 계산할 수 있다.

3.2 팩트 해시의 정의

팩트 해시는 앞서 정의한 팩트의 해시 값을 일컫는다. 이 때, 팩트 해시의 유일성 보장을 위해 팩트의 구성요소(element)로 토큰(token)이라는 값을 활용한다. 토큰은 팩트를 유일하게 만들어 주는 요소로 사용되며 임의의 난수(random number)로 구현할 수 있다.

미텀 블록체인에서는 오퍼레이션이 수행돼 팩트가 생성되는 순간의 시간 기록을 토큰으로 활용한다. 이는 유일성을 가져야 한다는 토큰의 요구사항을 만족시킨다.

3.3 팩트 해시의 효용

팩트 해시는 단순히 하나의 데이터 값에 대한 해시 값만을 의미하는 것은 아니다. 미텀에서 팩트 해시는 아래와 같은 몇 가지 중요한 성질을 갖는다.

첫째, 팩트 해시는 블록체인 상에서 유일한 값을 갖는다. 즉, 오퍼레이션 별로 유일한 팩트 해시 값을 갖게 돼 오퍼레이션을 구분하는 키(key)로 활용할 수 있다.

팩트 해시의 유일성을 이용해 블록체인 내 오퍼레이션이 처리완료 됐는지, 또는 그 결과 트랜잭션이 블록 내에 저장 되었는지를 검색해 확인할 수 있는 것이다.

둘째, 동일한 트랜잭션에 대해 중복 처리되는 것을 방지할 수 있다. 각 오퍼레이션이 수행될 때마다 팩트 해시가 계산되고 팩트 내에 한 구성요소로 기록된다. 이렇게 생성된 팩트는 블록체인에 저장된다.

예컨대 특정 사유로 이미 처리된 오퍼레이션에 대해 중복적인 처리 요청이 발생하는 경우를 가정해보자.[5] 미텀 블록체인에서는 각 팩트를 처리할 때마다 동일한 팩트 해시의 블록체인 유무 여부를 조회하는데,

[5] 네트워크 상의 acknowledge 패킷의 손실로 요청이 처리되지 않은 것으로 판단하여 재요청 하는 경우가 발생할 수 있다. 이 경우 요청을 받은 쪽에서는 이미 처리 했는데, 요청하는 쪽에서는 처리 안된 것으로 판단하고 재요청할 수 있다.

동일한 값의 팩트 해시가 발견되는 경우 이미 처리된 것으로 파악하고 그 요청은 기각돼 중복 처리되는 것을 막는다.

셋째, 오프체인에서도 팩트 해시를 계산할 수 있어 이를 통해 특정 오퍼레이션에 대한 검증이 가능하다. 다시 말하면, 블록체인에 속한 노드가 아니더라도 특정 오퍼레이션에 대한 정보 (송신자, 수신자, 커런시ID, 수량) 와 이에 적용된 토큰 정보만 있으면 팩트 해시를 쉽게 계산해 낼 수 있다.

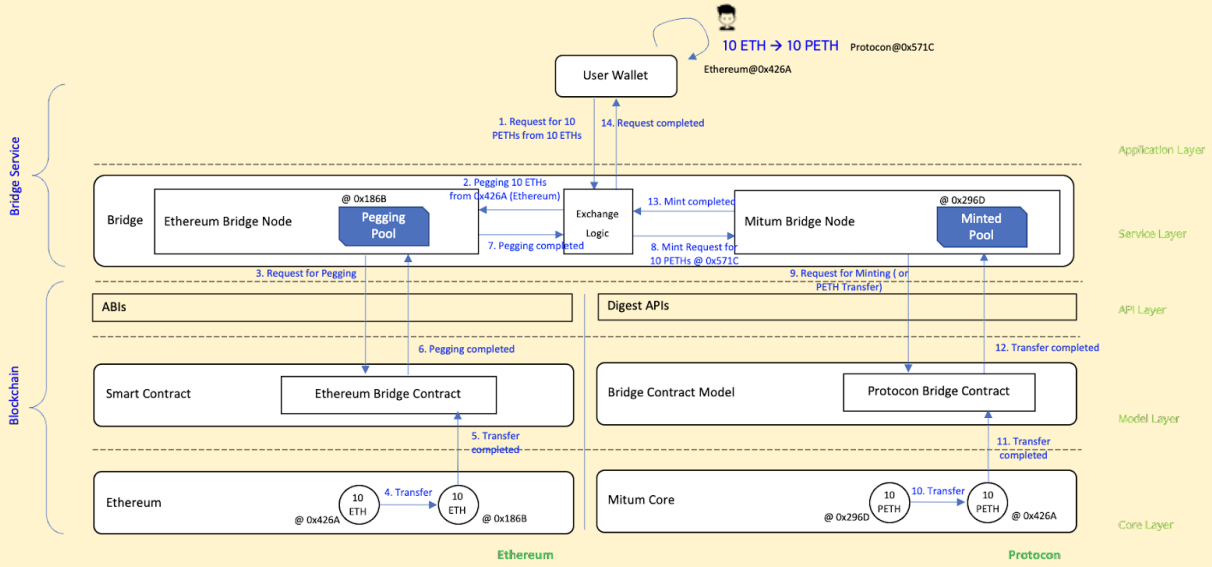
이 특징은 이기종 블록체인 간 크로스체인 브릿지를 구현할 때 유용하다. 가령, 이더리움과 프로토콘 네트워크를 연결하는 크로스체인 브릿지를 구현하는 경우, 프로토콘 네트워크의 모든 블록을 브릿지에 저장하지 않고도 브릿지 동작과 연관된 오퍼레이션의 바이너리 트리 (binary tree)를 구성하고, 검증이 요구되는 오퍼레이션에 대한 팩트 해시를 계산하는 것만으로도 오퍼레이션을 검증할 수 있다.

4. 팩트 해시와 크로스체인 브릿지

4장에서는 일반적인 크로스체인 브릿지의 구조 및 동작방식을 설명하고, 프로토콘 네트워크를 이기종 블록체인과 연동하기 위한 크로스체인 브릿지 구현에 있어서 팩트 해시를 어떻게 활용할 수 있는지 설명한다.

4.1 크로스체인 브릿지

이기종 블록체인 연동에 활용되는 크로스체인 브릿지는 한 블록체인에서 토큰을 페깅(Pegging)함에 따라 연동되는 다른 블록체인에서 페깅 토큰에 상응하는 가치의 토큰을 민팅(Minting)하는 방식이다.[6]



[그림6] 프로토콘 크로스체인 브릿지의 기본 동작 (e.g. 이더리움-프로토콘 브릿지)

[6] 이 때, 페깅된 토큰에 상응하는 가치를 갖는 토큰을 Wrapped Token 이라고 부른다. 이러한 개념의 토큰으로 Wrapped BTC, Wrapped ETH 등의 토큰이 있다.

위 그림은 프로토콘 크로스체인 브릿지 동작의 한 예제다. 이 그림은 사용자가 자신이 보유한 10ETH를 이더리움 블록체인의 브릿지 서비스에 페깅하고 프로토콘 네트워크에 동일한 가치의 Wrapped ETH 인 PETH를 획득하는 프로세스를 담고 있다.

사용자는 브릿지 서비스에 자신의 10ETH를 송금하면서 프로토콘 네트워크 상에 10PETH 생성을 요청한다. 이 때, 자신의 10ETH는 이더리움 브릿지 서비스 노드로 전송된다.[7]

전송된 10ETH는 이더리움 상의 스마트 컨트랙트인 'Ethereum Bridge Contract'에 의해 페깅되며, 페깅 정보는 브릿지 서비스의 'Exchange Logic'을 통해 프로토콘 브릿지 노드에 전송된다.

이어 프로토콘 브릿지 노드는 이더리움 상에 페깅된 수량 만큼의 10PTH를 'Protocon Bridge Contract'를 통해 민팅해 요청한 사용자 지갑 주소로 송금하게 된다.

4.2 크로스체인 브릿지 이슈

이기종 블록체인의 연동은 두 블록체인을 오프체인으로 연결하는 브릿지 서비스를 믿어야 하는 '신뢰의 문제'가 발생한다.

각 블록체인은 각기 다른 독립적인 합의 메커니즘을 갖기 때문에 필연적으로 이 둘을 연동하려면 블록체인 간 오프체인을 통해야 한다. 이 때 오프체인에서 의도적으로 또는 의도치 않게 데이터가 변조될 가능성이 존재하기 때문에 브릿지 서비스의 신뢰를 확보하기 위해서는 각 블록체인 트랜잭션에 대한 투명성과 검증 가능성이 담보되어야 한다.

여기서 투명성을 확보하는 방법으로는 트랜잭션의 처리과정을 모든 사용자가 임의의 시점에 쉽게 찾아볼 수 있도록 하는 '도구 제시'가 있다. 예컨대 아래 그림 7에서 보여지는 바와 같이 블록체인 익스플로러를 통해 브릿지를 통해 페깅/언페깅 되는 토큰들을 쉽게 확인할 수 있도록 하는 것이다.

[7] 일반적으로는 브릿지 스마트 컨트랙트의 어카운트 주소로 송금이 되며, 이를 페깅 된다고 표현한다. 여기서는, 스마트 컨트랙트 어카운트를 Pegging Pool로 일반화 하여 표현한다.

FACT HASH	CONFIRMED AT	BLOCK HEIGHT
32ds7KXj7dRYumaVBPJ9tG24U3MUt4g5q7trBABkADoX	2022-03-22, 15:20:07.328	224932
5enBkWRYE4TqVhZtMmx7TMELJcD3xYRNLtmS4Ud92933	2022-03-22, 15:20:07.328	224932
ExF9xUvNScSQ9iZ8Ju8CeMKZvDx2Vo8YjBYJ7LuPzJMG	2022-03-22, 15:20:07.328	224932
Arc322wWGG5octZL9G5r9YCwEX41soeCZs61HH7AgRwL	2022-03-22, 15:20:07.328	224932
5U7vRD58a3TYuPscoaviQwYjXbRPBLfYw1CQPXrarCSq	2022-03-22, 15:19:07.772	224904
5yXb8wgn9UdyzLcK1ECrvtacwajjHxyzv8d6W1RGwWTq	2022-03-22, 15:19:07.772	224904
S3wiZHL9V26QYoFtR7n9RJoqVGUhgkGUNwD8eySAufk	2022-03-22, 15:19:07.772	224904
1xQTfPnmn2wm6SxK4Mcy4VLErN2vpLboTvbjw7XUQC5	2022-03-22, 15:19:07.772	224904
2fQAwisr7JCPGsNU5MghTJzT5eQcTgt2zFReV13WQDFk	2022-03-22, 15:18:08.574	224876
BrRBedK5Yc3hMNMUWRoKBdZVLpbCnFUNr6eQkwAGg9aS	2022-03-22, 15:18:08.574	224876

[그림7] 프로토콘 테스트넷의 블록체인 익스플로러에 노출되는 팩트 해시 정보[8]

검증 가능성을 높이는 방법으로는 제3자의 외부 검증 노드를 다수 확보해 다자에 의한 브릿지 페깅/언페깅 트랜잭션을 감시 및 검증하는 것이 꼽힌다.

그러나 기존의 블록체인 데이터 처리 구조로는 이 두가지를 확보하는 것이 쉽지 않다. 최근 솔라나와 이더리움의 브릿지인 웜홀(Wormhole)[9] 네트워크에서 발생한 해킹[10]이나 액시 인피니티와 이더리움의 브릿지인 로닌(Ronin)[11] 네트워크에서 발생한 해킹[12]사건만 보더라도 크로스체인 트랜잭션에 대한 온전한 검증 방법을 찾지 못하고 있다는 것을 명확하게 확인할 수 있다. 이 두 사건으로 각각 약 3천 800억원, 약 7천 700억 상당의 자산이 탈취됐다.

특히 로닌 네트워크의 경우 브릿지 검증 노드들의 키를 획득해 51% 공격 방법으로 해킹을 감행한 것으로, 오프체인 검증 노드에 의한 브릿지의 무결성 확보에 심각한 문제가 존재한다는 사실이 밝혀졌다.

4.3 팩트 해시를 통한 해법

프로토콘 네트워크로는 브릿지 동작과 연관된 오퍼레이션 팩트 해시를 통해 바이너리 트리 (binary tree)를

---

[8] https://info.demo.protocon.network/dashboard/protocon
이 웹사이트는 프로토콘 테스트넷의 블록체인 탐색기이다. 기능 개선 및 잦은 업데이트 등으로 일시적으로 접속이 안될 수도 있음을 미리 알려둔다.
[9] https://solana.com/wormhole
[10] 2022년 2월 발생한 해킹 사건으로 120,000 ETH가 유출되었다.
https://extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13
[11] https://bridge.roninchain.com/
[12] 2022년 3월 발생한 사건으로 173,600ETH와 25,500,000USDC 가 유출되었다.
https://www.gmw3.com/2022/04/the-ronin-bridge-hack-recapping-cryptos-largest-hack-ever/

구성하고 검증이 요구되는 오퍼레이션에 대한 팩트 해시를 계산하는 것만으로도 오퍼레이션의 정상성 여부를 검증할 수 있다.

예컨대 이더리움 블록체인에 페깅됐던 ETH를 언페깅하는 요청이 있을 경우, 조작된 요청인지, 아니면 프로토콘 네트워크에서 정상적인 오퍼리에션에 대한 요청인지를 확인해야 하는 경우를 상정하자.

이더리움 측에서 언페깅 요구를 받는 브릿지 노드는 이 요구의 정상성 (해당 토큰의 소유자에 의한 요청 여부)을 검증 후에 언페깅 절차를 진행해야 한다.

이 때 이더리움 브릿지 노드는 프로토콘 노드에 의존하지 않고도 자체적으로 팩트 해시를 계산할 수 있다. 그리고 이렇게 계산된 팩트 해시에 대해 팩트 해시 바이너리 트리[13]조회 및 검증을 통해서 언페깅 요청의 정상성을 확인할 수 있다.

또한 팩트 해시를 활용하면 프로토콘 생태계에서 어떤 필요성에 의해 오프체인을 구성하는 경우, 메인넷과 비슷한 수준의 신뢰성을 확보할 수 있다. 최근 블록체인 게임 영역에 활발하게 도입되면서 오프체인을 활용해 속도 확보, 비용 절감, UI/UX 상의 편의성을 제공하려는 시도들을 많이 하고 있는데, 이렇게 블록체인의 용도를 확장하는데 있어 팩트 해시는 신뢰성을 확보해주는 중요한 도구로 사용될 것이다.

5. 결론

본 황서에서는 프로토콘 네트워크의 심장인 미텀 블록체인의 핵심 요소 팩트(Fact)와 팩트 해시(Fact Hash)의 개념을 다루고 이들의 특징 및 효용성을 기술했다.

최근 크로스체인에서 해킹 및 대규모 토큰 유출이 빈번하게 발생하고 있다. 이 때 팩트 해시를 이용한 브릿지 오퍼레이션의 검증 기능은 데이터 처리과정의 신뢰성을 획기적으로 높이는 방법론으로 통한다.

팩트 해시의 유일성을 통해 오퍼레이션의 조회, 중복처리 방지가 가능하다는 것과 오프체인에서도 팩트 해시를 계산하고 오퍼레이션의 정상성 여부를 확인할 수 있음을 알아보았다.

특히 팩트 해시의 이러한 특징은 이기종 블록체인들을 연동할 때 뿐 아니라 사이드체인 및 오프체인의 신뢰성을 획기적으로 높여 줄 수 있다는 사실을 확인했다.

이것으로 프로토콘 네트워크에서는 아발란체와 같은 블록체인의 구조적 역할 구분 없이도, 보다 더 안전하고 효율적인 오프체인, 사이드체인, 멀티체인 구조가 자연스럽게 형성될 것으로 예상한다.

[13] 미텀 블록체인에서는 머클트리와 유사한 개념의 바이너리 트리를 적용하고 있다.

Project Info

Homepage : https://protocon.io/

Github : https://github.com/ProtoconNet

Protocon Yellow Paper
Part 1 : Contract Model
https://protocon.io/wp-content/uploads/Protocon-Yellowpaper-Part-1-Contract-Model-KOR.pdf

Contact : contact@protocon.io