블록체인 가상 채널 연구 현황 조사

이준하○ 문수묵
서울대학교 전기정보공학부
{joonha.lee, smoon}@snu.ac.kr

A Survey on the Blockchain Virtual Channels

Joonha Lee○ Soo-Mook Moon
School of Electrical and Computer Engineering, Seoul National University

요 약

블록체인(Blockchain)은 느리고 비싸므로 실사용과는 거리가 멀다. 이를 개선하기 위해 지불 채널(payment channel)이 제안되었다. 지불 채널은 지불 채널 네트워크(payment channel network)로 확장되었고 현재 시장에서 활발하게 사용되고 있다. 그러나 지불 채널 네트워크에는 거래 결과를 확정 짓기 위해서 여전히 블록체인과의 통신이 필수적이라는 한계점이 존재한다. 이를 극복하기 위해서 최근에 가상 채널(virtual channel)이 제안되었다. 가상 채널은 지불 채널 네트워크 위에 개설되는 채널로, 블록체인과의 직접적인 통신 없이 즉각적이고 저렴하게 거래를 확정 지을 수 있는 방법이다. 본 논문은 가상 채널 연구의 현황을 조사하여 블록체인의 확장성 문제 연구의 한 갈래가 향하는 방향의 이슈와 한계를 고찰한다.

1. 서 론

블록체인(blockchain)은 네트워크 참여자들이 공통된 거래 내역을 각각 저장하게 하기 위하여 채굴이라는 보상 시스템을 사용한다. 채굴을 통해 만들어진 암호화폐는 기존 화폐와 달리 중앙화[1]된 운영 주체가 없는 탈중앙 화폐다. 암호화폐는 탈중앙성이라는 장점을 가져 큰 관심을 불러일으켰음에도 불구하고 두 가지 기술적 이유로 인해 실제 지불에 사용되기에는 어려움이 있다.

첫째, 느리다. 블록체인은 네트워크 참여자 모두가 같은 거래 내역을 보유하는 것을 목표로 하는데, 네트워크 연결 상태에 따라 참여자 간 불균형이 생길 수 있다. 따라서 블록체인은 매번 합의에 이를 수 있는 시간을 네트워크 시간보다 길게 설정한다. 대표적인 블록체인인 비트코인(Bitcoin)은 10분, 이더리움(Ethereum)은 15초로 설정하고 있다[1][2]. 즉 거래가 블록체인에 기록되기 위해선 각각 10분과 15초를 기다려야 하는 것이다.

둘째, 비싸다. 블록체인에서 거래는 블록(block)이라는 단위로 확정되는데, 블록에는 크기 제한이 있다. 즉 모든 거래가 한 번에 확정될 수 없으므로 거래들은 다른 거래들보다 높은 수수료를 제안하여 블록에 포함될 우선순위를 높여야 한다. 그 결과 수수료는 점점 높아져 비트코인은 거래당 평균 1 USD 이상, 이더리움은 14 USD 이상의 높은 수수료를 지불해야 한다.

이 같은 한계를 보완, 암호화폐를 실사용할 수 있게 하기 위하여 지불 채널(payment channel)이 제안되었다[3]. 거래 참여자들은 블록체인에 본인들이 사용할 금액을 미리 기록하여 지불 채널을 개설한다. 그 후 블록체인과의 통신 없이 지불 채널을 통해 즉각적이고 저렴하게 거래를 하고, 최종적인 거래 결과만을 블록체인에 기록하여 거래를 종료한다.

지불 채널은 지불 채널 네트워크(payment channel network)로 확장되었다[4]. 이 네트워크에서는 지불 채널을 개설하지 않은 상대와도 공통된 중개자를 채널을 통해 공유하기만 하면 즉각적이고 저렴하게 지불이 가능하다. 지불 채널 네트워크는 활발히 사용되고 있다. 대표적인 비트코인의 지불 채널 네트워크인 라이트닝 네트워크(Lightning Network)에는 1억 USD 이상, 이더리움의 지불 채널 네트워크 아비트럼(Arbitrum)에는 30억 USD 이상의 금액을 갖는 채널이 개설되어 활용되고 있다[5][6].

그러나 지불 채널 네트워크에도 한계가 있다. 매 거래를 중개자가 승인해야 하므로 지연 시간(latency)이 생기고 거래 내역이 유출된다. 또한 중개자를 거칠 때마다 중개자에게 수수료를 지불해야 하는 문제도 있다.

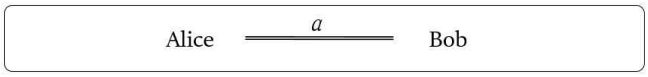
이에 Dziembowski et al.은 '가상 채널(virtual channel)'을 제안하였다[7]. 가상 채널은 지불 채널 네트워크에서 중개자의 개입을 최소화한다. 가상 채널을 통해 참여자들은 지불 채널을 개설하지 않은 상대와도 더욱 즉각적이고 저렴하게, 그리고 거래 내역 유출의 염려 없이 거래를 수행할 수 있다.

본 논문은 초기부터 가장 최근까지의 가상 채널 연구를 조사하여 그 흐름과 방향을 보인다.

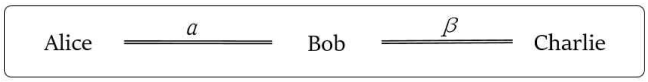
2. 배경지식

2-1. 지불 채널

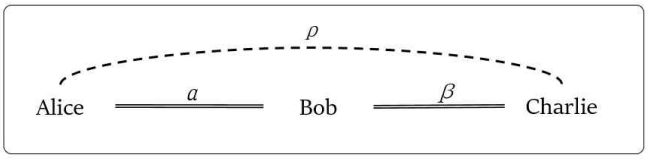
* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2021-0-01835)



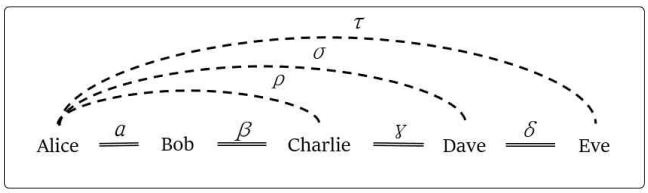
[그림 1] 지불 채널



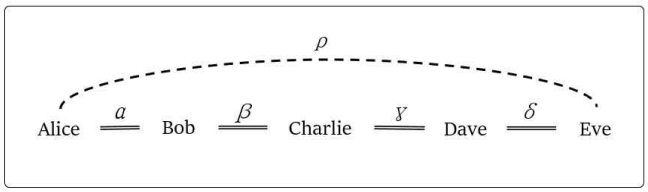
[그림 2] 지불 채널 네트워크



[그림 3] 가상 채널



[그림 4] 반복적 가상 채널



[그림 5] 다중-홉 가상 채널

지불 채널[3]에서 참여자들은 블록체인과의 통신 없이 거래한다. [그림 1]과 같이 앨리스(Alice)와 밥(Bob)이 지불 채널을 통해 거래하는 상황을 가정해 보겠다. **(채널 개설)** 앨리스와 밥은 어떤 특정한 조건이 만족되어야만 사용할 수 있는 금액을 블록체인에 거래의 형태로 기록하여 채널을 개설한다. **(채널 업데이트)** 앨리스와 밥은 블록체인과의 통신 없이 서로 간 네트워크 통신만으로 미리 기록해둔 금액을 어떻게 배분할지 합의한다. 합의를 할 때마다 거래에 서명을 하고, 이전 합의는 만료시킨다. **(채널 종료)** 최종적으로 합의된 금액 정보를 다시 블록체인에 거래의 형태로 등록하면, 기존에 기록해둔 금액을 최종 금액에 맞게 앨리스와 밥에게 분배한다.

2-2. 지불 채널 네트워크

[그림 2]와 같이 밥은 앨리스, 찰리(Charlie)와 각각 채널을 개설하였다. 그러나 앨리스와 찰리는 채널을 개설하지 않았기에 앨리스와 찰리가 거래하려면 블록체인과의 통신이 필요했다. 그런데 밥이 중개를 해준다면 블록체인을 거치지 않고 거래를 할 수 있다[4]. 앨리스가 채널 α를 통해 밥에게 송금하면, 밥이 그와 동일한 금액을 채널 β를 통해 찰리에게 송금한다. 결과적으로 밥이 가진 총 금액에는 변화가 없으며 앨리스는 찰리에게 송금을 할 수 있다. 밥은 중개의 대가로 앨리스와 찰리로부터 수수료를 받는다.

3. 가상 채널

[그림 2]와 같은 지불 채널 네트워크에서 앨리스와 찰리가 거래를 하려면 밥에게 매번 송금을 요청해야 하며, 그때마다 수수료를 지불해야 한다. 거래 내역이 밥에게 드러날 뿐 아니라 거래량이 많을수록 많은 비용을 지불해야 하는 단점이 있다. 따라서 가상 채널이 제안되었다[7][8].

3-1. 가상 채널

[그림 1]에서 블록체인이라는 중개자를 통해 앨리스와 밥이 지불 채널을 개설한 것처럼, 앨리스와 찰리는 밥이라는 중개자를 통하여 가상 채널을 개설할 수 있다. 이는 [그림 3]과 같다. **(가상 채널 개설)** 앨리스와 찰리는 특정 조건이 만족되어야만 사용할 수 있는 금액을 거래의 형태로 채널 α와 채널 β에 기록함으로써 가상 채널 ρ를 개설한다. **(가상 채널 업데이트)** 앨리스와 찰리는 밥과의 통신 없이 네트워크 통신만으로 금액을 어떻게 배분할지 합의한다. 합의를 할 때마다 서명을 하고 이전 합의는 만료시킨다. **(가상 채널 종료)** 최종 합의에 이르면 그 금액 정보를 채널 α와 채널 β에 기록하고, 밥은 최종 금액만큼의 송금을 중개한다. 예를 들어 최종적으로 앨리스가 찰리에게 10 코인을 송금하는 경우, 밥은 앨리스에게 채널 α에서 10 코인을 받고, 채널 β에서 찰리에게 10 코인을 준다.

지불 채널 네트워크와 달리 앨리스와 찰리는 몇 번의 거래를 하든, 밥과는 가상 채널 개설과 종료 시, 단 두 번의 통신만을 하면 된다. 따라서 수수료는 두 번만 지불하며, 세부 거래 내역을 숨길 수 있다.

3-2. 반복적 가상 채널

가상 채널을 기반 채널로 하여 그 위에 다시 가상 채널을 개설할 수 있다[8]. 이를 반복적 가상 채널(recursive virtual channel)이라 한다. 가상 채널 위에 가상 채널을 개설하는 방법은 지불 채널 위에 가상 채널을 개설하는 것과 같은 방법을 사용한다. **(반복적 가상 채널 개설)** [그림 4]에서 앨리스와 데이브(Dave)는 특정 조건이 만족되어야만 사용할 수 있는 금액을 거래의 형태로 ρ와 ɣ에 기록함으로써 가상 채널 σ를 개설한다. **(가상 채널 업데이트)** 앨리스와 데이브는 찰리와의 통신 없이 금액 배분에 합의한다. 합의를 갱신할 때마다 이전 합의는 만료시킨다. **(가상 채널 종료)** 최종 합의에 이르면 그 금액 정보를 ρ와 ɣ에 기록한다. 찰리는 최종 금액만큼의 송금을 중개한다. 이 경우에도 가상 채널과 마찬가지로 중개자와의 통신은 단 두 번 수행한다. 같은 방법으로 앨리스와 이브(Eve)도 σ와 δ에서 데이브의 중개로 가상 채널 τ을 개설하여 이용할 수 있다.

그러나 반복적 가상 채널에는 두 가지 단점이 있다. 이 두 단점은 거래가 여러 채널, 여러 중개자를 거쳐야 하기에 발생한다. 첫째, 기반이 되는 기반 채널이 종료되면 그 위의 가상 채널은 더불어 종료되어야 한다. 가상 채널의 길이가 길어질수록, 즉 기반 채널 개수가 많아질수록 가상 채널은 강제 종료를 당할 위험에 더 노출된

다. 둘째, 기반 채널 개수가 많아질수록, 가상 채널을 개설 및 종료하는 데 오랜 시간이 걸린다. 가상 채널에선 중개자를 신뢰할 수 없기 때문에 중개자로 하여금 보증금을 거래의 형태로 기록하게 한다. 가상 채널이 종료된 후 중개자가 보증금을 돌려받을 수 있도록 하기 위해 가상 채널은 제한된 수명을 가진다. 그런데 기반 채널의 수명은 그 바로 위 가상 채널의 수명보다 길어야 한다. 가상 채널에서 분쟁이 발생한 경우, 이를 중재하기 위한 충분한 시간이 기반 채널에게 주어져야 하기 때문이다. 그 시간의 차이를 Δ라 하면 채널 간 수명의 관계식은 [식 1]과 같다.

$$lifetime(upper\ channel) - lifetime(lower\ channel) \geq \Delta$$

[식 1]

최상위 가상 채널에서 기반 채널로 내려갈수록 수명은 더 길어져야 한다. [그림 4]와 같은 네트워크 배치의 경우, τ를 개설하기 위해 밥은 적어도 3 * Δ 이상의 시간 동안 보증금을 돌려받지 못한다. 반복적 가상 채널의 이와 같은 한계점들을 보완하기 위해 다중-홉 가상 채널(multi-hop virtual channel)이 제안되었다[9].

3-4. 다중-홉 가상 채널

다중-홉 가상 채널은 [그림 5]와 같이 여러 채널을 거쳐야만 도달할 수 있는 상대와 직통으로 개설되는 가상 채널이다.

방법은 다음과 같다. **(다중-홉 가상 채널 개설)** 앨리스는 밥에게, 밥은 찰리에게, 찰리는 데이브에게, 데이브는 이브에게 거래할 금액과 동일한 금액의 보증금을 전송하는데, 이를 거래의 형태로 각각의 채널(α~δ)에 기록한다. **(다중-홉 가상 채널 업데이트)** 앨리스와 이브는 거래 금액을 어떻게 나눌지 합의하고, 매 합의마다 이전의 합의는 만료시킨다. **(다중-홉 가상 채널 종료)** 최종적으로 합의에 이르면 그 합의 결과를 하위 채널이 아닌 블록체인에 올린다. 그와 동시에 앨리스, 밥, 찰리, 데이브는 지불 채널에서 보증금을 모두 돌려받는다. 앨리스는 보증금을 돌려받으려면 이브와의 합의 결과를 블록체인에 기록해야만 하는데, 이는 앨리스와 이브의 블록체인 밖 거래가 블록체인에 기록되어야 할 불가피성을 제공하므로 거래는 안전하게 확정될 수 있다.

다중-홉 가상 채널은 반복적 가상 채널과 달리 기반 채널의 개수가 적기에 강제적으로 종료될 위험이 적고, 채널을 여닫는 데 걸리는 시간이 짧다는 장점이 있다. 그러나 최종 거래 결과를 채널에 기록하는 것이 아니라 블록체인에 기록해야 하는 오버헤드(overhead)가 있다.

4. 결 론

블록체인은 속도와 비용 면에서 실제 사용되기엔 무리가 있었다. 지불 채널은 거래를 블록체인과의 통신 없이 확정적으로 진행하며, 거래의 처음과 끝만을 블록체인에 안전하게 기록하는 방식을 제안하였다. 이는 여러 지불 채널이 서로 협력하여 운용될 수 있는 지불 채널 네트워크로 확장되었고 현재 시장에서 활발히 사용되고 있다. 그러나 지불 채널 네트워크에서 거래 중개자는 매 거래에 관여해야 하므로 이를 최소화하려는 노력이 계속되어 왔다.

최근 제안된 가상 채널 연구들은 이러한 한계점을 효과적으로 개선했다. 가상 채널에서 사용자들은 중개자와의 통신을 단 두 번으로 줄일 수 있었다. 가상 채널은 반복적 가상 채널로 발전되었고 멀리 떨어져 있는 상대와도 거래가 가능하게 되었다. 반복적으로 개설하지 않고도 단번에 멀리 있는 상대와 거래할 수 있는 다중-홉 가상 채널도 제안되었다.

가상 채널은 블록체인의 확장성을 크게 발전시킨 지불 채널 네트워크를 승인 절차, 비용, 보안 면에서 더 발전시켰음에 의의가 있다. 가상 채널을 통해 암호화폐는 실사용에 한 발짝 더 가까워질 수 있었다.

본 논문은 가상 채널 연구가 순차적으로 확장되며 최근에는 반복적 가상 채널, 다중-홉 가상 채널로 그 흐름이 갈라졌음을 보였고, 각 접근법의 이슈와 한계를 고찰하였다. 가상 채널 연구들은 발표된 지 얼마 되지 않은 새로운 연구들로 아직 그 가지(branch)가 길지 않다. 따라서 앞으로의 가상 채널 연구는 기존 방법론을 확장시키는 방법도, 혹은 새로운 갈래를 만드는 방법도 모두 가능할 것이다.

참 고 문 헌

[1] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system.” 2008.

[2] Vitalik Buterin. “Ethereum: a next generation smart contract and decentralized application platform.” 2013.

[3] Christian Decker. "A fast and scalable payment network with bitcoin duplex micropayment channels.” Symposium on Self-Stabilizing Systems. Springer, Cham, 2015.

[4] Joseph Poon. “The bitcoin lightning network: Scalable off-chain instant payments. Technical Report.” 2016.

[5] DeFi Pulse. 2022. [Online]. https://www.defipulse.com/projects/lightning-network

[6] L2BEAT. 2022. [Online]. https://l2beat.com/

[7] Stefan Dziembowski. "Perun: Virtual payment hubs over cryptocurrencies.” IEEE Symposium on Security and Privacy. 2019.

[8] Lukas Aumayr. "Bitcoin-compatible virtual channels." IEEE Symposium on Security and Privacy (SP). 2021.

[9] Maxim Jourenko. "Lightweight virtual payment channels." International Conference on Cryptology and Network Security. Springer, Cham, 2020.

[10] Lukas Aumayr. "Donner: UTXO-Based Virtual Channels Across Multiple Hops.” Cryptology ePrint Archive (2021).