차세대 블록체인을 위한 VRF 기반의 해시그래프 기법

김민섭*, 강진영**, 조인휘✉
한양대학교 컴퓨터 소프트웨어학과
e-mail : minseop, achieve365, iwjoe {@hanyang.ac.kr}

A VRF-based Hashgraph Scheme for Next Generation Blockchains

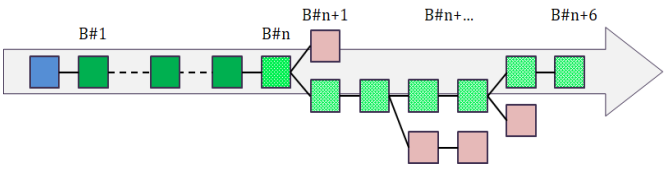
Min-Seop Kim*, Jin-Yeong Kang**, In-Whee Joe✉
Dept. of Computer and Software, Hanyang University

요 약

최근 여러 블록체인 플랫폼에서 잇따라 51% 공격에 대한 소식이 들려 옴에 따라 새로운 블록체인의 필요성이 부각되고 있다. 그중 Hashgraph 는 기존의 블록체인과 다르게 블록단위가 아닌 이벤트 즉, 블록에 기록되는 트랜잭션 그 자체로 체인이 구성되는 메커니즘을 가지고 있기 때문에 차세대 블록체인으로 대두되고 있다. 그러나 트랜잭션 단위로 Hash 또는 Hash 검증을 수행하기 때문에 연산 량이 기하급수적으로 늘어나며, 검증 또는 합의에 소요되는 시간이 상당하다. 본 논문에서는 이를 해소하기 위해 Verifiable Random Function 을 이용하여, Hash 에 대한 검증 절차와 연산 량을 감소하여 최종적으로 합의에 소요되는 시간을 단축하는 방법에 대해 제시한다.

1. 서론

일반적인 블록체인 네트워크는 제 3 자를 거치지 않고 사용자들이 직접 채굴을 통해 블록을 생성할 수 있다. 시간의 흐름에 따라 생성된 블록은 이전에 생성된 블록과 해시를 이용하여 연결되며 fork 될 수 있다. Fork 는 특수한 경우에 발생하며, 가장 긴 체인이 메인이 되고 이를 검증된 체인으로 삼는다. 대표적으로 기존의 블록체인(Bitcoin)에서 블록에 대한 검증은 이후에 블록 여러 개가 체인에 연결되면 해당 블록은 검증된 것이다. 이것은 개인이 거래를 할 때 생성되는 블록의 개수만큼 신뢰성 검증에 소요되는 시간이 길어 진다는 것을 의미하며, Bitcoin 에서의 블록체인 기준으로 한 블록이 생성하는 시간이 10 분이 소요되므로 검증에 이르기까지 6 블록이라면, 생성되기까지 1 시간 정도 시간이 걸린다. 따라서, 기존의 블록체인은 계좌이체와 같은 현실 세계에서 실시간으로 사용하기에 어렵다.



(그림 1) 비트코인의 블록 검증 과정

비트코인에 블록체인보다 블록 검증 시간이 빠르다고 알려진 이더리움에서 2019 년 초 51% 공격이 발생했다. 이는 Longest chain 정책에 따라 긴 블록을 우선시하는 취약점을 이용한 방법이다. Public 블록체인(비트코인)에서, 노드가 악의적으로 블록을 변경하거나 공격할 때, 51% 이상의 컴퓨팅 파워를 가지고 있으면 해당 블록체인을 붕괴시킬 수 있다.

하지만, 51%미만의 전력을 가진 노드조차도 특정한 목적을 가진 마이닝으로 전체 블록체인 파워의 51%을 넘어설 수 있다는 것을 보여주었다[2][3]. 또한, 컴퓨터 자원의 25% 미만을 가진 공격자들이 여전히 특정한 마이닝으로도 블록체인의 일부분을 공격하는 방법이 있다[4][5].

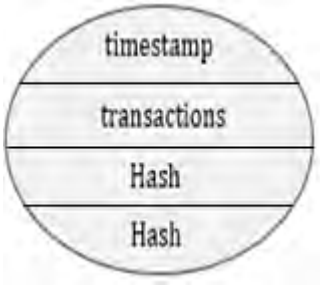
본 논문은 블록 단위가 아닌 이벤트단위를 사용하여 거래내역 즉, Transaction 자체를 검증할 수 있고 51% 공격 가능성을 줄일 수 있는 Hashgraph 에 대해 다루며, 2 장에서는 Hashgraph 에서 이벤트 검증 연산량을 줄이기 위해 사용한 Verifiable Random Function (VRF)에 대해, 3 장 에서는 Hashgraph 에서 검증 시 나타나는 비효율적인 검증 방법을 개선하는 방안에 대해, 4 장은 제안하는 알고리즘의 성능 및 평가, 5 장은 결론에 대해 서술한다.

2. 관련 연구

2.1 Hashgraph

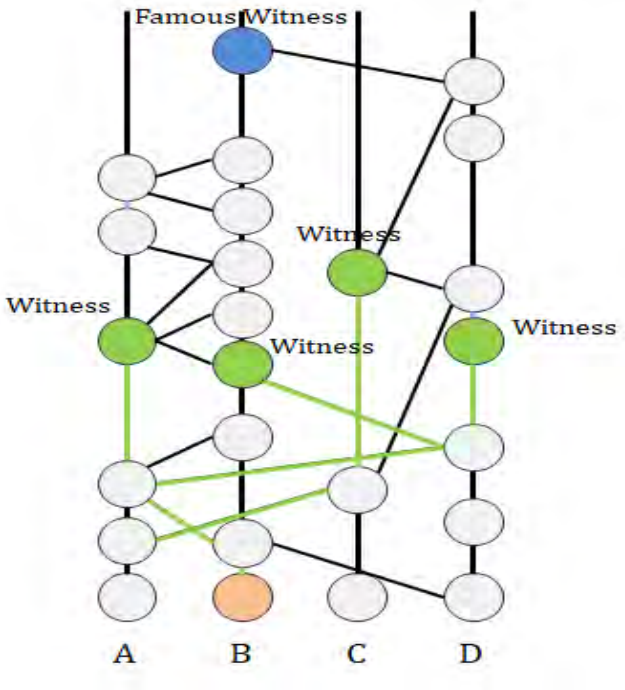
Hashgraph 는 기존의 비트코인에서 사용하는 블록체인 또는 이더리움에서 사용하는 블록체인과는 다르게 분산형 합의를 사용한다. Hashgraph 는 다음과 같은 개념에 기초하여 합의에 이른다.

Hashgraph 에서 Transaction 은 유저 사이에서 일어난 거래를 의미하며, Gossip 은 의사 난수를 통해 Transaction 을 다른 사람에게 전파하는 것을 뜻한다 [6]. 이벤트는 Transaction, 유저 간 Gossip 기록, 발생 시간을 가진 구조로 이루어져있다. 또한 이벤트는 하나의 유일한 Transaction 을 가지며, transaction 의 내용과 자신의 Hash 값, 그리고 Gossip 에 대한 Hash 값으로 구성되어 있다.



(그림 2) 이벤트 구조

이벤트는 기존의 블록체인에서 블록에 해당되는 개념이다. 발생 시간(Timestamp)은 원자 시계를 사용해 다른 원자 시계 시간 간의 동기화되어 측정되며, 쉽게 조작할 수 없고, 자체적인 Timestamp 를 통해 이벤트 간의 발생 순서를 결정한다.



(그림 3) Hashgraph의 Witness와 Famous Witness

Witnesses 는 다른 사람들 중에서 검증하려는 이벤트를 알고 있는 이벤트이다. 알고 있다는 것은 See 를 통해서 증명할 수 있다. Famous Witnesses 는 많은 유저들(유저의 2/3)에게 Gossip 되어 검증하려는 이벤트를 Strongly See 할 수 있고, 검증할 수 있는 이벤트이다 [7]. See 는 현재 이벤트가 다른 사람으로부터 왔다는 것을 이벤트 내의 타인의 해시 값을 순회하면서 알 수 있으며, Strongly See 또한, 이와 비슷한 방법이다.

즉, 사람들 사이에서 일어난 이벤트를 Gossip 을 통해 모두에게 알리고 이를 See 와, Strongly See 로 해당 이벤트를 검증하는 것이 합의과정이라 볼 수 있다.

Hashgraph 는 기존의 블록체인과는 다르게 사용자가 마이닝을 하지 않아도 되고, 가상투표방식을 이용하여 이벤트를 검증한다. 이 때 이벤트에는 단일 개의 Transaction(거래내역)이 기록되며, 이벤트들의 집합(라운드)을 생성하는데 소요되는 시간이 블록의 발생 주기 동안 대기하는 Longest chain 을 사용하는 비트코인이나 이더리움보다 짧지만, 합의에 핵심 개념인 See 와 Strongly See 를 통해 검증하는 과정에서 과거 이벤트를 순회해야하는 작업으로 인해 합의에 오버헤드가 따른다.

2.2 Verifiable Random Function

Verifiable Random Function[MVR99][8]는 암호화된 공개키 해시를 사용하여, 함수의 값에 대한 정확성을 검증 가능한 proof 를 제공하는 의사 난수 함수이다 [9]. 예를 들면, 어떤 거래나 행위에 대한 입력 x 를 주었을 때, 타원 곡선 상에 임의의 점 하나를 결정하여 비밀키 SK 를 생성하고, $y = F_{SK}(x)$ 을 계산 할 수 있다. 이는 π_x 로 검증 할 수 있으며, 이러한 검증은 VRF 의 공개 키에 대한 것으로 실제 누구나 $y = F_{SK}(x)$가 정확하다는 것을 계산할 수 있다[9].

크게 키를 생성하는 GENERATE, VRF 값과 Proof 를 계산하는 PROVE, 계산한 것을 검증하는 VERIFY 부분으로 나눌 수 있다.

GENERATE 는 타원 곡선 $y^2 = x^3 + ax + b$에서, a 와 b 를 정하고, Subgroup 의 크기를 나타내는 n 과 Cofactor h, 모듈로 P 를 계산하고, 타원곡선상의 임의 점 g 를 선택한다. 그러고 n 보다 작은 값을 가진 수를 암호화하여 SK를 계산한다.

PROVE 는 $F_{SK}(x) = e(g,g)^{1/(x+SK)}$ 와 Proof $\pi_{SK}(x) = g^{1/(x+SK)}$을 계산한다.

VERIFY 는 누구나 알 수 있는 PK 를 사용하여 $e(g^x \cdot PK, \pi) = e(g,g)$ 와 $y = e(g,\pi)$ 을 검증하는 과정이다.

3. 제안하는 알고리즘

본 논문은 기존 블록체인 메커니즘에 비해 51%의 공격으로부터 자유롭고, 컴퓨팅 파워에 관계없이 이벤트를 동등하게 생성할 수 있어 차세대 블록체인으로 떠오르는 Hashgraph에 대해 다룬다. 이를 개선한 방법에 대해 논의하기에 앞서 핵심 개념에 대해 서술한다.

먼저, See 한다는 것은 Gossip 된 이벤트가 검증하려는 이벤트에 의해 파생이 되었는지 확인 하는 것을 의미하며, Hash 값을 통해 알 수 있다. 검증할 이벤트를 See 할 수 있는 이벤트를 Witness 라 부른다.

참여하고 있는 모든 멤버들의 체인에서 검증할 이벤트에 대한 각자의 Witness 가 결정되면, 원자시간순으로 가장 먼저 Witness 를 생성한 이벤트 시간대를 기준으로 Round 를 정의한다. 즉, 검증하려는 이벤트는 Round1 에 Witness 들은 Round2 시작부분에 위치하게 된다.

이후 Round2 의 Witness 를 See 할 수 있는 이벤트가 각 모든 멤버들의 체인에 정해지면 Round2 를 정의한 것과 같은 방식으로 Round3 를 정의한다. 즉, Witness 의 Witness 들이 Round3 에 위치해 있다.

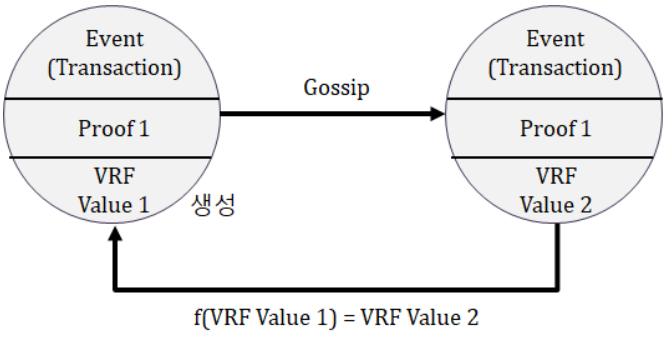
Strongly See 는 현재 이벤트가 얼마나 많은 유저들의 Gossip(전체 멤버의 2/3)을 거쳐 생성된 이벤트인지 판단하는 것이다. 전체 유저의 2/3 를 거쳐 Gossip 된 이벤트라면 검증할 이벤트를 Strongly See 한다고 할 수 있다.

Famous Witness 는 검증하려는 이벤트가 모든 유저 중 2/3 보다 많은 유저들이 See 하는 이벤트가 있고 검증하려는 이벤트를 Strongly See 하는 한 이벤트가 있으면 Strongly See 한 이벤트를 Famous Witness 라 부른다. Famous Witness 가 되는 것과 동시에 이벤트는 검증되며, 검증이 완료되는 시점까지 합의 과정으로 본다.

현재 Hashgraph 의 합의는 Gossip 을 통해 전달된 해시 값을 이용하며, See 와 Strongly See 의 특성상 현재의 이벤트부터 검증하려는 이벤트까지 모든 경로에 있는 해시의 무결성을 검사해야 하는 오버헤드가 존재한다.

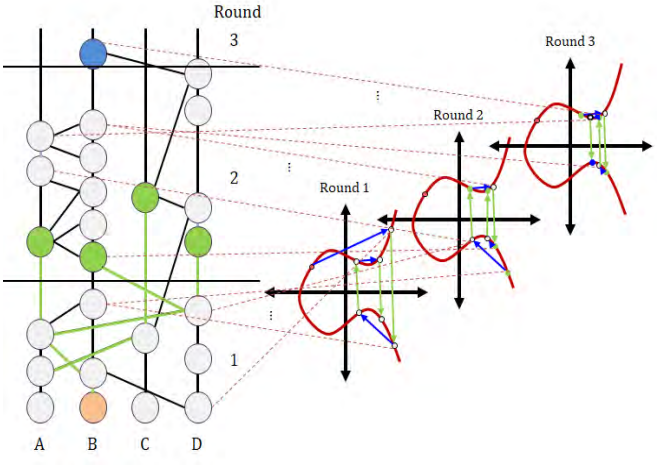
본 논문에서는 기존의 See 와 Strongly See 가 동작하는 메커니즘 대신 VRF 의 타원 곡선 상에서 비밀키로 만든 공개키를 사용하여 Proof 와 VRF Value 값만 알 수 있으면 해당 이벤트를 검증할 수 있다는 점을 이용해 한 번에 검증 가능한 방법에 대해 제시한다.

동일한 라운드내에서 이벤트 간의 Gossip 은 Proof 와 VRF Value 를 추가적으로 전달하여, 검증이 필요한 시점에 Message 와 Proof 를 이용하여 이벤트를 검증한다.



(그림 4) VRF를 이용한 이벤트 검증 프로세스

Witness 를 기준으로 라운드를 나눈다. 나눈 라운드를 VRF 의 타원 곡선 평면에 대응시킨다. 라운드 별로 타원 곡선은 서로 다른 평면에 존재하며, See 또는 Strongly See 시점에서 기존과 같이 검증할 이벤트와 검증하는 이벤트 사이의 모든 경로를 순회하는 것이 아니라 VRF value 와 Proof 를 통해 이벤트를 검증한다.

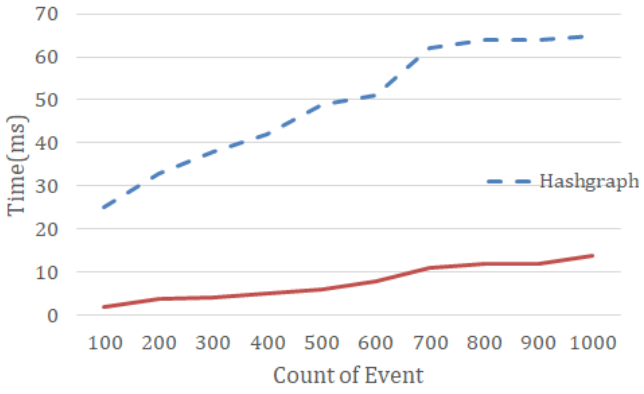


(그림 5) 제안하는 라운드 별 이벤트 생성 과정

타원 곡선 평면상에 대응에서 모든 이벤트를 한 평면상에 대응 시키므로, Cofactor h 또한 고려해야한다. $h = \frac{|E(\mathbb{Z}/p\mathbb{Z})|}{n} \leq 4$이 되도록 해야 한다[11][12].

4. 알고리즘 성능 및 평가

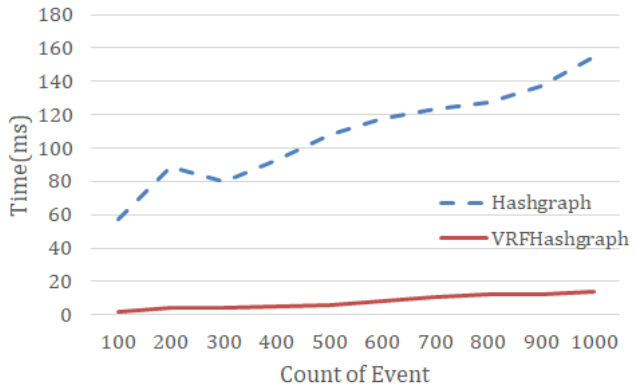
일반적으로 블록체인의 해시 알고리즘은 SHA-160 또는 SHA-256 을 사용하며, Hashgraph 역시 SHA-256 을 사용한다. 실험은 Genesis 즉, 최초의 이벤트가 발생한 시점부터 마지막 이벤트가 발생한 시점까지 소요된 시간을 측정하는 실험과, 검증이 필요한 시점에 See 를 수행하고 검증이 완료된 시점까지 소요된 시간을 측정하는 실험, 두 가지를 수행하였으며 ms 단위로 측정하였다.



(그림 6) 알고리즘에 따른 이벤트 생성 시간 비교

이벤트 생성 소요 시간에 대한 비교 실험은 100 개의 단위로 1000 개까지 증가하여 실험하였다. 기존의 Hashgraph 에서는 이벤트를 Gossip 할 때 마다, Hash 를 거듭 생성하여 이벤트를 발생시키기 때문에 이벤트가

100 개씩 증가할 때마다 5~10(ms) 정도의 크 폭의 변화 량을 보였다. 그러나 VRF-Hashgraph 는 VRF Value 즉, 검증에 필요한 암호화된 값을 재생성 하지 않고, 타원 곡선 위의 같은 평면상에 있는 점을 사용하여 전파하기 때문에 해시를 추출하는데 소요되는 시간을 현저히 단축시킬 수 있었으며, 이벤트가 100 개씩 증가할 때마다 1~2(ms) 정도의 변화 량을 보였다. 단, VRF-Hashgraph 경우 검증에 필요한 proof 를 필수적으로 한 번 생성해야 하는데, 이때 소요되는 시간은 평균적으로 400ms 가 소요된다.



(그림 7) 알고리즘에 따른 검증 시간 비교

검증 시간 비교 실험 또한 생성 시간 비교 실험과 동일한 조건으로 이벤트를 100 개 단위로 증가시키면서 이벤트에 대해 검증하였다. Hashgraph 는 검증하는데 소요되는 시간이 이벤트가 증가할 때마다 평균 10ms 정도 더 소요된다. 하지만, VRFHashgraph 는 depth 에 근거하여 Shift-Rotation 한 VRF value 와, 한 번 계산된 Proof 를 통해 이벤트를 검증하기 때문에, 검증에 소요되는 시간이 기존 Hashgraph 에 비해 현저히 감소했으며, 검증에 소요되는 시간은 평균적으로 6.5ms 로 나타났다.

5. 결론

본 논문에서는 차세대 블록체인으로 각광받고 있는 Hashgraph 의 효율적인 합의에 대해 다루고 있으며, VRF 통해 개선하는 방법을 제시하고 검증하였다.

그러나 제안하는 VRFHashgraph 에서 사용하는 Proof 는 검증에 사용되는 검증값으로써 노출되어도 큰 위험이 따르지는 않지만 Gossip 할 때, 한 Round 내에 모든 이벤트의 Proof 가 동일하기 때문에 검증 단계에서 어떠한 영향을 끼칠지 알 수 없다. 따라서 동일한 값의 Proof 가 전파될 때, 발생 가능한 여러가지 환경을 바탕으로 안정성 및 보안 강도 검증에 대한 연구가 필요하다.

참고문헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." Communications of the ACM 61.7 (2018): 95-102.

[3] Nayak, Kartik, et al. "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack." 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.

[4] Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar. "Optimal selfish mining strategies in bitcoin." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016.

[5] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." Work Pap.–2016 (2016).

[6] Schueffel, Patrick. "Alternative distributed ledger technologies blockchain vs. tangle vs. hashgraph-a high-level overview and comparison." (2017).

[7] Baird, Leemon. "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance." Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep. (2016).

[8] Micali, Silvio, Michael Rabin, and Salil Vadhan. "Verifiable random functions." 40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039). IEEE, 1999.

[9] Dodis, Yevgeniy, and Aleksandr Yampolskiy. "A verifiable random function with short proofs and keys." International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2005.

[10] Gueron, Shay, Simon Johnson, and Jesse Walker. "SHA-512/256." 2011 Eighth International Conference on Information Technology: New Generations. IEEE, 2011.

[11] Möller, Bodo. "Securing elliptic curve point multiplication against side-channel attacks." International Conference on Information Security. Springer, Berlin, Heidelberg, 2001.

[12] Brown, R. L. "SEC 1: elliptic curve cryptography. Standards for Efficient Cryptography Group (SECG)." (2016).