허가된 블록체인에서의 공정성을 보장하는 임계값 쿼럼 합의 기반의 데이터 공유 시스템에 관한 연구 †

라경진*, 이임영**
*순천향대학교 소프트웨어융합학과
**순천향대학교 컴퓨터소프트웨어공학과
rababi@sch.ac.kr, imylee@sch.ac.kr

A study on data sharing system based on threshold quorum consensus for fairness in permissioned blockchain

Gyeongjin Ra*, Imyeong Lee**
*Dept. of Software Convergence, Soonchunhyang University
**Dept. of Computer Software Engineering, Soonchunhyang University

요 약

허가형 블록체인 기반 데이터 공유 시스템은 분산 환경에서 신뢰 수준을 구축하고 일관된 메시지를 기록 및 공유함으로써 서비스의 상호 운용성을 가능하게 한다. 그러나 허가형 블록체인은 종종 탈중앙화, 보안 및 상호 운용성과 충돌한다. 이는 중앙 집중식 시스템으로 돌아가거나 데이터의 독점 및 남용 및 오용으로 이어질 수 있다. 따라서 CAP (Consistency, Availability, Partition tolerance)에 이론 검증에 따라 메시지 공유, 비잔틴 내결함성 및 메시지 일관성을 고려하고 적용해야 한다. 기존의 PBFT(Practical Byzantine Fault Tolerance) 합의 알고리즘는 노드의 증가시, 장애내성을 갖기위해 계산되어야 할 합의 처리시간이 증가하며, DPOS(Delegated Proof of Stake) 알고리즘은 보상, 리더 선출의 공정성 문제 등에 따라 허가형 블록체인에서의 적합한 방식이 연구되고 있다. 본 논문에서는 서비스의 상호 운용성과 과제에 대해 논의하고 허가된 블록체인의 합의 개선을 통한 데이터 공유 시스템을 제안한다.

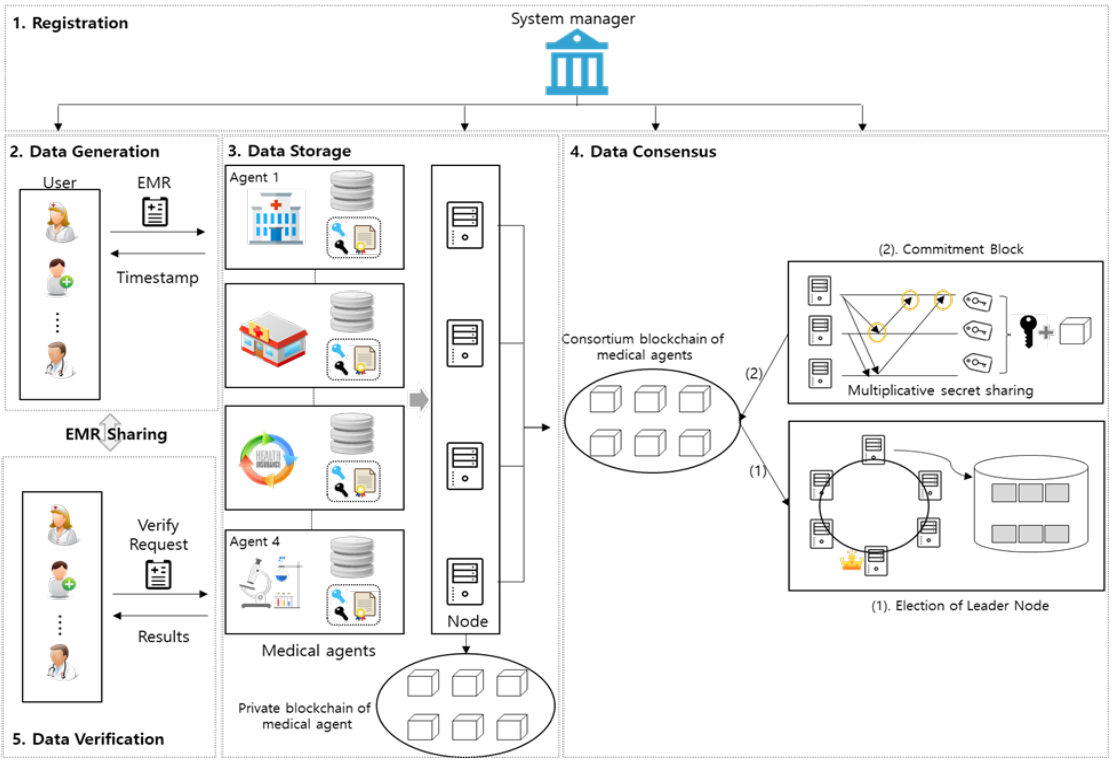
1. 서론

최근 블록체인 기반의 데이터 공유 시스템이 등장함에 따라, 사용자 프라이버시의 중요성이 증가하고 있다. 하지만 기존 데이터 암호화 방식과 단일 블록체인은 높은 복잡성과 비효율적인 데이터 처리로, 연결된 데이터를 기반으로 허가형블록체인과 개인정보 보호 접근 방식에 기반한 데이터 공유 시스템이 제공될 필요가 있다 [1]. 따라서 민감한 데이터를 외부 저장소에 저장하고 연결된 데이터의 토큰 값을 블록체인에 저장하여 데이터 리소스에 대한 액세스의 신뢰할 수 있는 프로비저닝을 제공하여야 한다. 블록체인의 고유한 검증 값은 데이터의 타임스탬프로서 인증 및 무결성을 제공하지만, 종종 기밀 통신은 제공하지 않아 민감한 정보 노출이 발생하거나 암호화 연산으로 오버헤드가 발생한다. 또한 최종 블록 퍼블리싱에 대해 소수 서버가 독점, 블록 생성 권한 선출의 공정성 저해, 합의계산 오버헤드 증가 등의 문제가 있다 [2]. 허가된 블록체인은 가용성을 위해 탈중앙화와 보안 사이에서 종종 절충되어 데이터의 독점, 남용 및 오용으로 이어질 수 있는 중앙 집중식 시스템으로의 회귀로 이어진다 따라서 본 논문에서는 계층 간의 계층적 인증과 최종 노드의 임계값 합의를 통해 블록 생성의 독점을 최소화한다. 최종 노드는 리더 노드로, 참여 에이전트 간 데이터 지분율에 의해 랜덤으로 선출된다. 선출된 리더를 시작으로 차순위 에이전트 들은 임계값 유효성 검사는 t 슬라이스를 저장을 위해 n 공유로 나누고 t 유효성 검사는 순차적 영지식 유효성 검사를 통해 입증된다. t 개 이상의 공유가 수신되면 데이터 트랜잭션이 블록 형태로 커밋된다. 보안 분석은 제안된 방법이 데이터 블록을 공정하고 안전하게 만들 수 있을 뿐만 아니라 기존 블록체인 기반의 데이터 공유 프로세스 보다 효율적으로 만들 수 있음을 보여준다.

2. 관련연구

데이터 활용을 위해 기관 간 공유가 시급하지만 현

† 이 논문은 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업(2021- 0-01516)과 2019년도 정부(교육부)의 한국연구재단 기초연구사업(No. NRF-2019R1A2C1085718)의 연구결과로 수행되었음



(그림 1) 제안방식 전체 시나리오

재 중앙 집중식 시스템으로 조달할 수 없으며 블록체인 기술을 기반으로 하는 많은 분산형 데이터 공유 서비스 시스템이 최근 몇 년 동안 더 많은 연구가 수행되었다 [3]. 블록체인 기술은 시스템 간의 데이터 공유에 대한 중요한 탐색을 제공하며 데이터의 기록, 분산 저장 및 변조하는 감시자 역할을 한다. 허가형 블록체인 데이터 공유 시스템에서 의료기록(Electronics Medical Record, EMR)과 같은 민감한 정보는 데이터 보안을 위한 개인 정보 보호 프로토콜 및 메시지 공유 방법과 실질적인 데이터 배포 방법이 고려되어야 한다. 기존 블록체인 합의방식은 계산 오버헤드, 토큰 기반의 합의 메커니즘, 리더선출 및 투표 기반의 합의 알고리즘이 존재하지만, 노드 수가 많아질수록 오버헤드가 증가하게 된다 [4]. 라서 공정성 및 랜덤성을 요구하는 허가형 블록체인에서의 효율적인 블록생성 방식이 필요하다. 따라서 블록생성 방식은 Shamir[24]가 제안한 메시지 공유 방식으로 원본 메시지를 n 개의 공유로 나누고 다음과 같이 할 수 있는 최소 t ($1 < t \leq n$) 공유 액세스 임계값을 통해 다중 서명 블록을 생성하도록 제안한다.

3. 제안방식

본 논문의 목적은 허가형 블록체인을 통해 메시지를 공유하고, 이를 위한 랜덤한 리더선출과 임계치 서명을 통해 블록합의를 수행하는 것이다. 따라서 우리는 허가형 블록체인과 링 코디네이터 기반 레이어 합의 분할 정복 전략을 선택한다. 리더선출의 평가 기준은 전체데이터에서 각 에이전트가 중복으로 차지하는 데이터의 비율이다. 제안방식은 다음의 5 가지 단계(시스템 초기설정, 사용자 등록, 데이터 생성, 데이터 저장, 데이터 합의, 데이터 검증)을 포함한다.

0. 시스템 초기설정

시스템 매니저 시스템 공개매개변수 public parameters $P = \{p, q, l_1, l_2, E, G, G_q, P, P_{pub}, H_1, H_2, H_3, H_4\}$ 및 메시지 공간 $M = \{0,1\}^{l_1}$를 게시한다.

1. 사용자 등록

참가자는 pp를 통해 개인키 $sk_i \in Z_q^*$를 선택한 후 공개키 $pk_i = sk_i \cdot P,\ 1 \leq i$ 를 생성하고, 그룹의단일 서명을 포함한 공개키 인증서를 등록한다.

2-3. 데이터생성 및 저장

Step 1. 사용자는 에이전트의 공개키로 암호화 한 데이터 암호문 집합 $CT = \{ct[1], \ldots, ct[i]\}$ 을 생성하고, 모든 $0 \leq j \leq n-1$ 에 대해 위치 $h_i(s_j)$의 비트를 1로 설정하여 Bloom 필터에 저장한다.($0 \leq i \leq k-1$ 및 $0 \leq j \leq n-1$).

Step 2. 에이전트는 해시트리를 통해 Private Blockchain을 생성하고, 각 에이전트의 BF 를 통한 병렬 BF 를 생성한다.

4. 데이터 합의

데이터의 최종 블록 생성 합의를 위해, 전체 데이터의 중복율을 통한 리더선출과 리더를 포함한 차순위 에이전트 3 후보 간의 비밀 다중 서명을 통한 블록확정 두단계를 포함한다.

(1) 리더 선출

Step 1. 에이전트는 투표를 시작하고 ID 와 비율을 포함하는 선거 메시지를 생성한다.

Step 2. 병렬 BF 와 자신의 BF 의 교집합의 비율을 계산한다.

$$\{E_{sk}(w_{j,1}), \ldots, E_{sk}(w_{j,n})\} \rightarrow pack\ RE_{sk}(w_j);$$

$S \rightarrow C : RE_{sk}(w_j)) \Rightarrow w_j;$
$\{c_1, \dots c_v\} \cap \{w_1, \dots, w_w\} \Rightarrow \{c_1, \dots c_v\} \cap \{s_1, \dots s_w\}$

Step 3. 메시지를 시계 방향으로 다음 노드로 보내고, 메시지가 처음의 에이전트에게 다시 전달되면 모든 유권자가 투표한 것으로 간주한다.

(2) 블록 확정

- Round 1 $(1 \le i \le t-1)$ (리더노드 = C_1)

노드 C_i 큰 소수 p와 q를 선택한다. Z_q에서 선택된 k_i을 통해 g_i을 계산한다. 차례로 모듈러스 q에서 g_i 및 β_i을 인코딩하는 α_i을 계산한다. 이 때, α_i, $\hat{\alpha_i}$, $\hat{\beta_i}$ 는 α_i과 β_i의 균등한 성질을 갖는다. $\alpha_i, \beta_i, \hat{\alpha_i}, \hat{\beta_i}$와 블록을 다음 노드 P_{i+1} 에 보낸다.

- Round 2 $(i = t)$

순위노드 C_i는 Z_q에서 선택된 k_i를 통해 g_i를 계산한다. R_i및 k_i를 사용하여 R_i를 비밀 계산 G로 계산하고 R_i과 함께 이전 노드 P_{i-1} 에 보낸다.

- Round 3 $(1 \le i \le t-1)$ (리더노드 = C_1)

노드 C_i 는 R_{i+1}와 k_i을 사용하여 비밀 계산 G 로 R_i을 계산합니다. 이후 영지식 증명을 통해 Π_i 을 계산하고 R_i과 함께 블록을 P_{i+1}에 전송한다.

- Round 4 $(i = t)$

마지막 순위노드 C_i(i=t)는 자신의 값을 통해 Π_1 을 검증하고 영지식 증명을 통해 Π_2 을 계산하여 $R_i. R_{i+1}, \Pi_i, \Pi_{i+1}$를 에이전트에게 보낸다.

동의가 끝나면 각 플레이어는 다른 모든 플레이어의 증거를 가지고 있어야 한다. 그들은 이러한 증명을 확인하고 확인이 실패하면 중단한다. 암호문 M을 통해 D에 대한 분산 암호 해독 $s = D(\mu)\ mod\ q$을 호출한다.. 에이전트는 M에 대한 서명으로 (r, s)를 출력한다. 리더노드 L_1 블록을 최종 게시한다.

5. 데이터 검증

Step 1. 송신자는 데이터 암호문 $C_1, C_2 = sk_i'G, sk_i'PK + M$, 인증서 $(PK, ID, \sigma, \mathrm{ts}, \mathrm{Sig_{SM}})$, 검증 토큰 $(\mathrm{S_t}, \mathrm{SK_{gi}})$을 생성한다.

Step 2. 에이전트 네트워크는 해시 트리를 사용하여 인증서의 유효성을 확인하고 수신자의 메시지를 확인하기 위해 유효한 해시 경로 $\mathrm{Hash\ Path} = \sigma[\mathrm{n}+1, \mathrm{k}] = \mathrm{H}(\sigma[\mathrm{n}, \mathrm{k}] || \sigma[\mathrm{n}, \mathrm{k}+1]$ 를 반환한다.

4. 제안방식 분석

- Random Fairness: 허가형 블록체인의 참여 에이전트라면 누구나 후보에 참여 가능하고, 데이터의 교집합 중복율에 따라 리더가 선정되므로 고정이 아닌 랜덤하고 공정한 선출 방식으로 블록생성의 과독점을 방지한다.
- Privacy: 암호화를 수행하여 민감한 데이터 정보의 노출을 방지하고, 해시함수와 Bloom Filter를 이용하여 블록체인의 데이터 검증 요청 시에 정보의 식별 및 추론을 방지하여 프라이버시를 제공한다.
- Authentication: 서명을 통해 사용자를 인증하고, 블록체인의 고유한 데이터의 타임 스탬프 값을 통해 메시지의 출처와 위조와 변조를 보장하는 메시지 인증을 제공한다.
- Reliability: 에이전트간의 다중서명을 통한 블록합의와 원장 생성은 조작의 시도를 무력화하고, 단일지점장애 오류를 최소화하여 데이터 공유 시스템의 신뢰성을 보증한다.
- CAP: [5] 정리에 따라 최종 다중서명합의의 메시지는 브로드캐스트되고 검증을 수행하므로 나머지 에이전트의 (Consistency)가 유지된다. 노드수가 증가하여도 고정된3개의 에이전트 간 위원회를 구성하여 합의를 수행하므로 가용성(Availability) 속성이 유지된다. 마지막으로 데이터 중복 비율에따라 고정 리더가 아닌 랜덤 리더가 분할 선출되므로 분할내성(Partition tolerance)을 보장한다.

5. 결론

최근 블록체인 기반의 메시지 공유 시스템이 등장함에 따라, 사용자 프라이버시의 중요성이 증가하고 있다. 하지만 허가형 블록체인은 데이터 독점 및 남용 및 오용, 프라이버시 잠재적 문제가 발생한다. 본 논문에서는 데이터 공유 서비스의 상호 운용성과 과제에 대해 논의하고 허가된 블록체인의 합의 개선을 통한 데이터 공유 서비스 솔루션을 제안했다. 이를 통해 기존 보안요구사항 및 CAP 이론 검증에 따라 메시지 공유, 비잔틴 내결함성 및 메시지 일관성을 분석하였다.

참고문헌

[1] Li, M., Yu, S., Ren, K., & Lou, W., "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings", SecureComm, Vol. 10, pp. 89-106, 2010

[2] Bernstam, D.F. Sittig, Matching Identifiers in Electronic HealthRecords: Implications for Duplicate Records and Patient Safety, BMJ. Qual, Safety 22(3, pp. 219-224, 2013.

[3] S.KSimon, K. Sonai Muthu Anbananthen, S. Lee, A Ubiquitos Personal Health Record (uPHR) Framework, International Conference on Advanced Computer Science and Electronic Information (ICASCEI 2013), Atlantis Press, 2013.

[4] M. Schukat, & P. Cortijo, "Public key infrastructures and digital certificates for the Internetof things", In Signals and Systems Conference (ISSC), pp. 1-5, 2015

[5] A. Roehrs, C. Andre da Costa, R. Rodrigo da Rosa, OmniPHR:A Distributed Architecture Model to Integrate Personal Health Records, Journal of Biomedical Informatics 71, pp. 70-81, 2017.