JKIICE

Short Paper

한국정보통신학회논문지 Vol. 24, No. 11: 1558~1561, Nov. 2020

분산 저장 블록체인 시스템을 위한 효율적인 결함 내성 향상 기법

Fault Tolerance Enhancement for Distributed Storage Blockchain Systems

Junghyun Kim*

*Assistant Professor, Department of Bigdata Engineering, Soonchunhyang University, Asan, 31538 Korea

ABSTRACT

In this paper, we propose a blockchain scheme to enhance fault tolerance in distributed storage blockchain systems. Traditional blockchain systems suffer from ever-increasing storage cost. To overcome this problem, distributed storage blockchain techniques have been proposed. Distributed storage blockchain schemes effectively reduce the storage cost, but there are still limitations in reducing recovery cost and fault tolerance. The proposed approach recovers multiple errors within a group by utilizing locally repairable codes with availability. This improves the fault tolerance of the blockchain systems. Simulation results show that the proposed scheme enhances the fault tolerance while minimizing storage cost and recovery cost compared to other state-of-art schemes.

Keywords : Blockchain, Distributed storage, Locally repairable codes, Secret sharing, Fault tolerance

Ⅰ. 서 론

블록체인은 네트워크 상에서 모든 참여자가 공동으로 거래정보를 검증 및 보관할 수 있는 분산 장부 기술이다[1]. 중앙 서버나 중앙 기관 및 관리자의 제어 없이 누구나 신뢰할 수 있는 거래를 할 수 있다는 장점으로 인하여, 스마트 계약, 결제 및 송금, 인증 등 각종 금융 시스템뿐만 아니라 물류 거래 내역 관리와 운송 정보를 포함한 유통 서비스, 의료 데이터 관리 등 블록체인의 활용 분야는 점차 확대되고 있다[2].

전통적인 블록체인 시스템에서 모든 노드들은 거래 참여 여부에 상관없이 해시 체인의 형태로 구성된 거래 장부 전체에 대한 데이터 블록과 해쉬값을 모두 저장해야 한다. 또한 시간이 흐름에 따라 저장 비용은 지속적으로 증가하게 된다.

이러한 문제를 해결하기 위해 비밀 공유 기법[3]과 비밀키 기반의 암호와 및 정보 분산 기법[4]을 사용한 분산 저장 블록체인[5]이 제안되었다. 분산 저장 블록체인은 각 노드가 데이터 블록 전체를 저장하지 않고 각 그룹 내 노드들이 데이터 블록을 나누어 저장한다. 따라서 각 노드의 데이터 블록에 대한 저장 비용을 그룹 크기만큼 감소시킬 수 있다. 이러한 저장 비용 감소에도 불구하고 분산 저장 블록체인은 외부 공격이나 자연적인 이유로 저장장치에 오류가 발생했을 때 복구에 필요한 데이터 블록 통신 비용이 크게 발생한다는 단점이 있다.

최근 전통적인 블록체인의 저장 비용 문제와 분산 저장 블록체인의 복구 비용 문제를 극복하기 위하여 부분접속 복구 부호[6]를 활용한 계층적 비밀 공유 블록체인[7]이 제안되었다. 계층적 비밀 공유 블록체인은 분산 저장 블록체인과 유사하게 시스템 내의 노드들을 그룹화 한다. 임의의 노드에 오류가 발생하면 그룹 내 다른 노드들로부터 복구가 가능하도록 부분접속 복구 부호를 활용하여 데이터 블록을 부호화한다. 부호화된 데이터 블록은 그룹 내 노드들에게 분산 저장된다. 또한 전역 비밀키와 그룹 비밀키를 별도로 생성하지 않고 전역 키로부터 비밀키를 생성하여 사용한다. 이를 통해 저장 비용과 복구 비용을 동시에 감소시키는 효과를 얻을 수 있다. 그러나 계층적 비밀 공유 블록체인은 그룹 내 단일 오류만 복구 할 수 있는 한계를 갖는다.

본 논문에서는 가용도를 갖는 부분접속 복구 부호[8]를 활용하여 그룹 내 다중 오류를 극복함으로써 결함 내성을 향상시킴과 동시에 저장 비용과 복구 비용을 최소

Received 6 September 2020, **Revised** 14 September 2020, **Accepted** 26 September 2020

*** Corresponding Author** Junghyun Kim(E-mail:kimjh@sch.ac.kr, Tel:+82-41-530-1252)
Assistant Professor, Department of Bigdata Engineering, Soonchunhyang University, Asan, 31538 Korea

Open Access http://doi.org/10.6109/jkiice.2020.24.11.1558 print ISSN: 2234-4772 online ISSN: 2288-4165

화하는 효율적인 블록체인 기법을 제안한다.

Ⅱ. 본 론

2.1. 시스템 모델

블록체인 시스템의 각 노드는 해쉬 체인의 형태로 연결된 거래 장부들의 복사본을 저장한다. t번째 거래에 대해 $B^{(t)}$가 데이터 블록이고 $W^{(t)}=\left(H^{(t-1)},h_2\left(B^{(t)}\right)\right)$가 이전 해쉬와 현재 데이터 블록의 해쉬값이 결합된 값이라고 하자. 여기서 $H^{(t-1)}$은 두 개의 해쉬함수 h_1과 h_2를 통해 $h_1\left(H^{(t-2)},h_2\left(B^{(t-1)}\right)\right)$의 형태로 계산된다. $\mathbb{F}_q$는 원소의 개수가 q개인 유한체를 나타낸다고 할 때, $B^{(t)}\in\mathbb{F}_\eta$와 $W^{(t)}\in\mathbb{F}_q$라고 하면 전통적인 블록체인에서 거래당 한 노드의 저장 비용(storage cost)은 다음과 같이 나타낼 수 있다.

$$S=\log_2\eta+\log_2 q \tag{1}$$

전통적인 블록체인에서 모든 노드는 거래 장부 전체를 저장하고 있으므로 임의의 한 노드에 오류가 발생했을 때 오류가 발생하지 않은 한 노드로부터 데이터를 전달받아 복구가 가능하므로 거래당 단일 오류에 대한 복구 비용(recovery cost)은 다음과 같이 나타낼 수 있다.

$$R=\log_2\eta+\log_2 q \tag{2}$$

또한 시스템 상의 다수 노드에서 오류가 발생하더라도 적어도 하나의 노드에서 오류가 발생하지 않는다면 복구가 가능하므로 거래당 결함 내성(fault tolerance)은 다음과 같이 나타낼 수 있다.

$$T=n-1 \tag{3}$$

위의 정의들은 블록체인 시스템의 성능을 나타내는 중요한 지표이다.

2.2. 제안하는 블록체인

본 논문에서는 기존에 제안된 블록체인 시스템들의 한계를 극복하기 위하여 가용도를 갖는 부분접속 복구 부호(LRC)[8-10]를 활용한다. 이하 (n,k,d,r,t)-LRC는 길이가 n, 부호율 k/n, 최소거리 d, 부분접속수 r, 가용도 t인 부호를 나타낸다. (n,k,d,r,t)-LRC를 활용하여 다중 오류 복구 가능 블록체인 시스템을 동작시키는 과정이 알고리즘 1에 표현되어 있다.

우선 전체 노드를 크기가 $r+1$인 $n/(r+1)$개의 그룹으로 그룹화 한다. 이때 $n/(r+1)$가 정수인 경우만 고려한다. t번째 거래에 대해 $W^{(t)}$를 전역 비밀 $s^{(t)}$로 설정하고 (n,k,d,r,t)-LRC를 이용하여 그룹별 부분 비밀 $s_i^{(t)}$를 생성한다. 비밀 공유를 위하여 노드별 심볼 $f_j^{(t)}$를 생성하여 분산 저장한다. 각 그룹 내 노드들은 부분 비밀 $s_i^{(t)}$를 통해 데이터 블록 $B^{(t)}$을 암호화하여 $m_i^{(t)}$를 구한다. 부호율 $(r+1-t)/(r+1)$인 최대 거리 분리(MDS) 부호를 이용하여 $m_i^{(t)}$를 부호화한 $c_i^{(t)}$를 생성한 후 그룹 내 노드들에게 분산 저장한다.

Algorithm. 1 Multiple error recoverable distributed storage blockchain

Given Input: $A=\{A_1,\cdots,A_{n/(r+1)}\}$
1: Set $W^{(t)}$ as global secret $s^{(t)}$
2: Generate local secret $s_i^{(t)}$ for $i\in[1,n/(r+1)]$ and $f_j^{(t)}$ for $j\in[1,n]$ by using an (n,k,d,r,t)-LRC
3: Store $f_j^{(t)}$ for $j\in[1,n]$ into n peers
4: **for** $i=1$ to $n/(r+1)$ **do**
5: Encrypt $B^{(t)}$ with $s_i^{(t)}$ as $m_i^{(t)}=\Phi(B^{(t)};s_i^{(t)})$.
6: Encode $m_i^{(t)}$ into $c_i^{(t)}$ by using an $(r+1,r+1-t)$-MDS code
7: Distribute and store $c_i^{(t)}$ among peers in A_i.
8: **end for**

위 알고리즘으로 구현된 블록체인 시스템에서 거래별 데이터 블록은 부호율 $(r+1-t)/(r+1)$인 부호로 부호화하기 때문에 거래당 한 노드의 저장 비용 S는 $(\log_2\eta)/(r+1-t)+\log_2 q$이다. 단일 노드 오류 발생 시 그룹 내 r개의 노드로부터 데이터를 전송 받아야 복구가 가능하므로 거래당 단일 오류에 대한 복구 비용 R은 $r(\log_2\eta)/(r+1-t)+rlog_2 q$이다. 또한 그룹별 최대 t개의 노드에서 동시에 오류가 발생해도 복구가 가능하므로 거래당 결함 내성 T은 $(t+1)n/(r+1)-1$이 된다.

Ⅲ. 성능분석

성능 비교를 위하여 전통적인 블록체인(TB)[1], 분산 저장 블록체인(DSB)[5], 계층적 비밀 공유 블록체인

(HSSB)[7], 제안하는 블록체인(PB)를 고려하였다. 표 1은 각 블록체인들의 거래당 한 노드의 저장 비용(S), 거래당 단일 오류에 대한 복구 비용(R), 거래당 결함 내성(T)을 요약하여 나타낸 것이다. 분산 저장 블록체인의 경우 특정 그룹 내 오류 발생 시 다른 그룹에 접속하여 복구해야하므로 이때 발생하는 접속 비용 ρ를 추가로 반영하였다.

Table. 1 Comparison of storage cost, recovery cost, and fault tolerance

	TB[1]	DSB[5]	HSSB[7]	PB
S	$\log_2\eta + \log_2 q$	$\frac{\log_2\eta}{r+1}+2\log_2 q$	$\frac{\log_2\eta}{r}+\log_2 q$	$\frac{\log_2\eta}{r+1-t}+\log_2 q$
R	$\log_2\eta+\log_2 q$	$\log_2\eta+2(r+1)\log_2 q+\rho$	$\log_2\eta+r\log_2 q$	$\frac{r\log_2\eta}{r+1-t}+r\log_2 q$
T	$n-1$	$\frac{n}{r+1}-1$	$\frac{2n}{r+1}-1$	$\frac{(t+1)n}{r+1}-1$

모의실험 환경은 $\eta=2^{400}$, $q=2^{40}$, $\rho=200$으로 설정하였고 제안하는 블록체인에서 $t=3$인 경우를 가정하였다. 그림 1은 그룹 크기$(r+1)$에 따른 저장 비용을 비교한 것이다. 제안하는 기법의 저장 비용은 그룹 크기가 작은 경우에 대해서 분산 저장 블록체인보다 다소 크게 나타났으나 그 이외의 모든 영역에서 계층적 비밀 공유 블록체인과 유사하게 작은 값을 가짐을 보였다. 전통적인 블록체인은 전 영역에서 상대적으로 매우 높은 저장 비용을 갖는 것을 확인하였다.

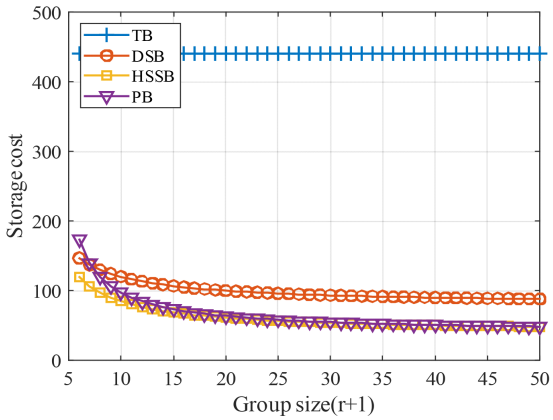

Fig. 1 Storage cost versus group size

그림 2는 그룹 크기$(r+1)$에 따른 복구 비용을 비교한 것이다. 제안하는 기법의 복구 비용은 그룹 크기가 작은 경우에 대해서 다소 크게 나타났으나 분산 저장 블록체인보다는 작은 값을 가짐을 보였다. 그 이외의 모든 영역에서는 계층적 비밀 공유 블록체인과 유사하게 작은 값을 갖는 것으로 확인되었다. 전통적인 블록체인을 제외한 나머지 세 가지 기법은 저장 비용을 감소시키기 위하여 그룹 내에서 데이터 블록을 분산 저장하므로 그룹 크기에 비례하여 복구 비용이 증가한다.

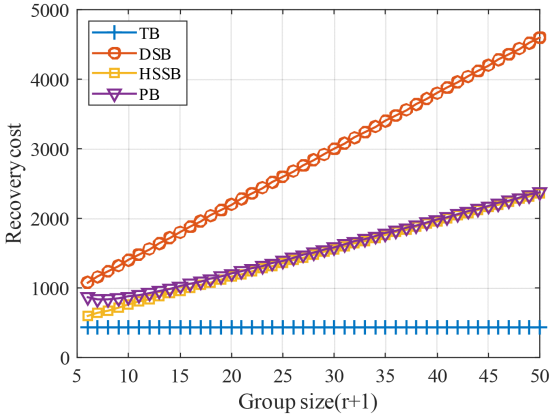

Fig. 2 Recovery cost versus group size

그림 3은 그룹 크기$(r+1)$에 따른 결함 내성을 비교한 것이다. 전체 노드의 수는 $n=800$으로 고정하고 정수개의 그룹으로 나눌 수 있는 경우만을 고려하였다. 제안하는 기법의 결함 내성은 전통적인 블록체인을 제외한 모든 기존 기법보다 매우 우수함을 확인하였다. 또한 제안하는 기법에서 t값을 증가시켜 시스템을 설계하면 결함 내성을 더욱 증가시킬 수 있다.

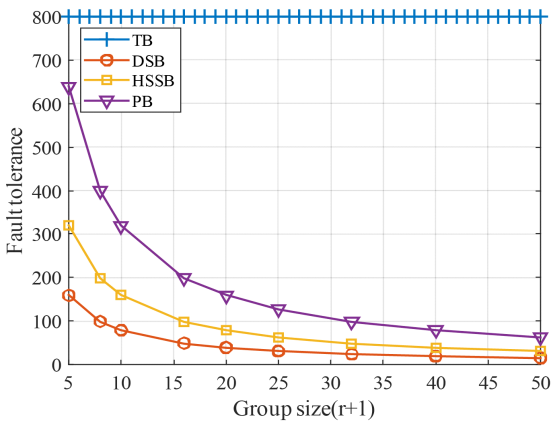

Fig. 3 Fault tolerance versus group size

Ⅳ. 결 론

전통적인 블록체인의 저장 비용 문제를 해결하고자 제안된 분산 저장 블록체인 기법들은 결함 내성이 매우 낮다는 한계를 갖는다. 따라서 본 논문에서는 그룹 내 다중 오류를 극복하여 결합 내성을 향상시킬 수 있는 효율적인 블록체인 기법을 제안하였다. 제안하는 기법은 결함 내성뿐만 아니라 저장 비용과 복구 비용 측면에서도 그룹의 크기가 매우 작은 영역을 제외한 대부분의 영역에서 매우 우수한 성능을 보였다.

본 논문의 결과를 토대로 향후 추가 연구로서 그룹 크기가 작은 경우에도 저장 비용과 복구 비용을 최소화하면서 결함 내성을 최대화하는 방안을 고려할 수 있다.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2019R1G1 A110000212).

REFERENCES

[1] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. [Internet]. Available: https://www.cryptovest.co.uk/

[2] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, “Blockchain applications for industry 4.0 and industrial IoT: A review,” *IEEE Access*, vol. 7, pp. 176935-176951, 2019.

[3] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[4] M. O. Rabin, “Efficient dispersal of information for security, load balancing, and fault tolerance,” *Journal of the ACM*, vol. 36, no. 2, pp. 335-348, Apr. 1989.

[5] R. K. Raman and L. R. Varshney, “Dynamic distributed storage for blockchains,” in *Proceeding of the IEEE International Symposium on Information Theory*, Veil, USA, pp. 2619-2623, Jun. 2018.

[6] I. Tamo and A. Barg, “A family of optimal locally recoverable codes,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4661-4676, Aug. 2014.

[7] Y. Kim, R. K. Raman, Y.-S. Kim, L. R. Varshney, and N. R. Shanbhag, “Efficient local secret sharing for distributed blockchain systems,” *IEEE Communications Letters*, vol. 23, no. 2, pp. 282-285, Feb. 2019.

[8] J.-H. Kim and H.-Y. Song, “Hypergraph-based binary locally repairable codes with availability,” *IEEE Communications Letters*, vol. 21, no. 11, pp. 2332-2335, Nov. 2017.