Journal of The Korea Society of Computer and Information
Vol. 23 No. 10, pp. 73-80, October 2018

www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.10.073

A Study on the Application of Block Chain Ethereum Technology to Activate Digital Contents Trading as Sharing economy - data encryption and modify merkle tree-

Youn-a Min*, Yeong-Tae Baek**

Abstract

The shared economy began with the concept of sharing the physical and intellectual assets of individuals with others. Nowadays, the concept of shared economy is becoming one of the industries as an enterprise type. Especially, with the development of the Internet and smart devices, various forms of shared economy have been developed in accordance with the need of sharing of individual income. Digital content is also a shareable commodity and it is seeking to utilize it as an item of shared economy. Accordingly, when digital contents are used as a shared economy, there are various possible threats -security threats that may arise in the course of transactions, potential for theft, alteration and hacking of contents.

In this paper, we propose transaction method and content protection method using block chain-ethereum technology to reduce security threats and transparent transactions that can occur in digital contents transactions. Through the proposed method, the trust of the consumer and the supplier can be measured and the encryption can be performed considering the characteristics of the data to be traded. Through this paper, it is possible to increase the transparency of smart transaction of digital contents and to reduce the risk of content distortion, hacking, etc.

▸Keyword: Block chain, Ethereum, Smart Contract, shared economy

I. Introduction

전 세계적으로 공유경제에 대한 관심이 높아지고 있다.

공유경제는 개인이 보유한 다양한 형태의 자산을 타인에게 공유하고 재화로써 이익을 취할 수 있다는 측면에서 새로운 산업화 방법이라고 할 수 있다[1].

디지털 콘텐츠도 다양한 형태의 공유경제로써 새로운 가치를 추구하고 있는 상황이다. 개인이 보유한 자산을 활용하여 새로운 경제적 이익을 창출한다는 의미에서 공유경제를 통한 경제발달을 기대할 수 있지만 공유경제의 활성화와 더불어 발생하는 다양한 문제점도 제기되고 있다.

비전문적인 개인과 개인 간의 거래에 대한 개인 정보보안의 위험성과 거래 시 발생할 수 있는 다양한 위변조의 문제 등은 여전히 연구하여야 할 문제이다.

디지털 콘텐츠의 산업생태계는 오프라인을 통한 유통, 모바일과 케이블을 통한 유통 등으로 나뉘어져 있고 제작자, 배급업자, 소비자 등의 가치 사슬 면에서도 공정하지 못한 관계를 가지고 있다. 기존의 디지털 콘텐츠는 워터마크 표시 등의 방법을 통하여 저작권을 보호하고 상업화하여 거래되었다[2]. 하지만 디지털 콘텐츠를 불법으로 재가공하여 유통하고 저작권을 침해

• First Author: Youn-a Min, Corresponding Author: Youn-a Min
* Youn-a Min (yah0612@gachon.ac.kr), Dept. of Software, Gachon University
** Yeong-Tae Baek (hannae@kimpo.ac.kr), Dept. of Multimedia, Kimpo University
• Received: 2018. 08. 27, Revised: 2018. 10. 10, Accepted: 2018. 10. 17.
• This paper is a revised and expanded version of a paper entitled 'Development Tool based on A Study on the Application of Block Chain Ethereum Technology to Activate Digital Content Trading as Sharing economy' presented at the 2018 summer Conference of The Korea Society of Computer and Information
• This study was conducted as a result of a study of SW centered university project of Ministry of Science and ICT and Institute for Information & communications Technology Promotion (IITP) (2015-0-00932)

하는 다양한 행위는 아직도 시도되고 있다.

또한 유통과정에서도 중간 업자에 의해 디지털 콘텐츠에 대한 거래 시 상당한 수수료가 지급되고 있으며 중간거래 과정을 통하여 해킹의 위협도 도사리고 있다.

이에, 유통채널상의 다양화 모색과 디지털 콘텐츠 창작자에 대한 권익보호를 위하여 블록체인을 통한 디지털 콘텐츠 거래에 대한 관심이 높아지고 있다.

본 논문에서는 디지털 콘텐츠를 공유경제의 방법으로 거래할 수 있는 방법으로 블록체인의 Ethereum 기술 기반 Smart Contract를 통한 계약방법과 거래 시 발생 가능한 보안상의 위협을 감소시키는 방법으로 블록체인 기술 중 Merkle Trees 해싱 시 처리되는 일부 데이터에 대한 해싱함수를 적용하여 처리방법의 수정을 제안하였다.

II. Preliminaries

1. Digital Contents Market

다양한 유형의 콘텐츠 개발과 스마트 디바이스의 발전에 힘입어 디지털 콘텐츠 시장이 증가하고 있다.

정보통신산업진흥원이 발표한 2016년 국내 디지털 콘텐츠 실태조사에 의하면 Fig. 1과 같이 세계 디지털 콘텐츠 시장은 2015년 1조 3,080억 달러에서 2020년에는 연평균 11% 성장이 되는 2조 2,010억 달러가 될 것으로 예측하고 있다[3]. 또한 국내 디지털 콘텐츠 산업 역시 2016년 434,206억 원에서 2019년 565,510억 원으로 연평균 9.2%의 성장을 기대하고 있다[4].

Fig. 1. Digital contents Market size

미래창조과학부에서 조사한 2016 디지털 콘텐츠 실태조사에 의하면 2015년 디지털 콘텐츠의 6대 새로운 시장의 규모는 모두 1조 97억 원으로 5대 신기술 분야에 대한 국내 유통시장은 2018년 9조 원 가량으로 예측하고 있다[3].

Table 1. Prediction of Domestic Distribution in 5 New Technologies
Unit: 100 million won

DIVISION	2016	2017	2018(e)	2019(e)	2020(e)	Annual average growth rate
VR	4,734	13,019	20,120	29,588	36,689	66.8
AR	8,903	10,146	11,512	13,061	14,818	13.5
CG	3,390	3,812	4,287	4,821	5,421	12.4
hologram	5,435	6,138	6,876	7,489	8,155	10.2
Five senses interaction	4,510	5,367	5,936	.	.	17.5
Smart media distribution	74,252	81,653	90,258	.	.	12.5

새로운 유형의 디지털 콘텐츠를 유통하기 위해서는 보다 합리적인 계약과정과 콘텐츠에 대한 철저한 보호가 필요하다. 가상현실, 홀로그램, 오감 인터렉션 등 디지털 콘텐츠 시장에서 다양한 형태의 신기술이 개발됨에 따라 새로운 기술의 다각적인 측면으로의 산업화가 필요해지고 개개인이 보유한 다양한 형태의 콘텐츠에 대한 새로운 가치창출 방법으로 공유경제가 제안되고 있다. 디지털 콘텐츠의 공유경제화에 의해 개인 및 기관이 소장하고 있는 재화에 대하여 또 다른 채널의 유통경로로써의 경제 활성화를 기대할 수 있다.

2. Shared Economy

공유경제는 특정 서비스를 보유한 개인 및 기업 공급자와 해당 서비스를 사용하고자 하는 수요자 간의 거래를 ICT플랫폼을 활용하여 사용하는 경제로 정의할 수 있다[1].

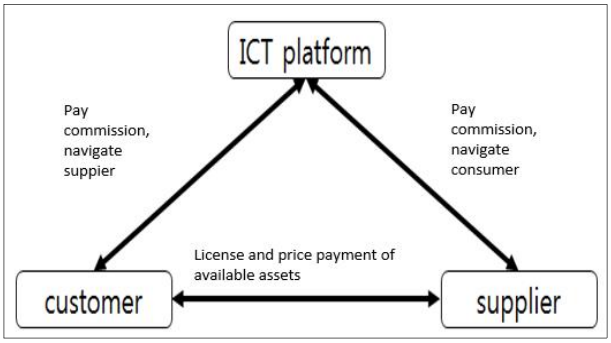

Fig. 2. Definition of shared economy

세계의 공유경제는 급격히 증가하고 있다. 에어비엔비(airbnb), 우버(uber) 등의 비즈니스 모델이 아니더라도 각 국에는 하이테크 설비의 다양한 공유경제 서비스와 정책을 내놓고 있다. Fig. 2와 같이 공유경제는 수요자와 공급자간의 ICT 플랫폼을 통한 거래탐색을 통하여 거래 성사를 통하여 공급자는 자신이 보유한 자산의 사용권을 제공하고 수요자는 적절한 시장가격을 지불하며 플랫폼은 각각 중개수수료를 취하는 형태이다[5]. 이 과정에서 거래되는 자산은 유·무형의 자산이 될 수

있으며 거래성사는 온라인을 통하지만 실제 서비스 제공 및 이용은 대부분 오프라인에서 이루어진다.

현재 사용되고 있는 공유경제의 주요 분야는 숙박, 차량, 금융, 재능 등으로 이루어지며 Fig.3과 같이 공유경제의 규모는 2013년 51억 달러의 시장크기를 고려하였을 때 매년 50% 이상의 성장을 하고 있으며 2025년 22배 상승한 3,350억 달러의 시장 크기를 예상하고 있다[1]. Fig.3은 세계 공유경제 시장의 크기이다.

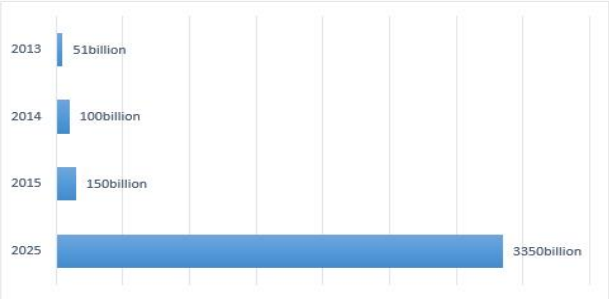

Fig. 3. Size of the World Shared Economic Market

국내의 스마트폰 보급률 증가와 SNS 이용 활성화에 힘입어 국내의 공유경제 규모는 세계 공유경제 시장보다 더 높은 증가율로 성장할 것이 예측된다.

3. Block Chain

블록체인은 거래되는 정보가 특정한 알고리즘에 의하여 암호화되어 연결되어 있는 모든 구성원에게 공유되는 디지털 원장을 의미한다. 거래되는 모든 내역에 대한 합의는 다양한 방법으로 이루어지며 구성원과 모든 내용을 공유하는 퍼블릭 방식과 구성원의 합의와 공유에 의하여 공개 여부가 결정되는 프라이빗 방식, 특정인에게만 거래내역이 공개되고 거래를 할 수 있는 컨소시움 방식 등 다양한 방법으로 거래에 관련된 내용을 투명하게 보호하고 공유하며 제 3자의 개입 없이 안전하게 거래가 가능하다[6].

Fig. 4는 블록체인의 Transaction을 나타낸 것이다.

각 Transaction간의 처리 시 해시함수를 사용하여 처리된다.

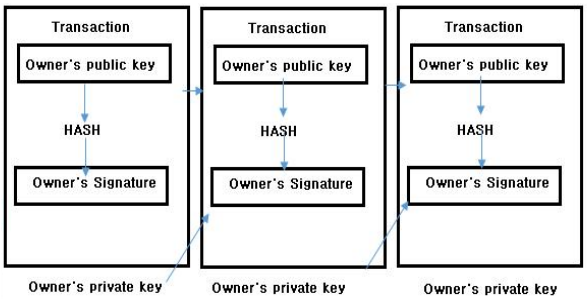

Fig. 4. Block chain transaction [7]

Table 2는 블록체인을 활용한 글로벌 스타트업의 활용사례이다. 상품거래서비스와 IoT 및 투자, 대출 및 보안 분야에서 블록체인을 활용한 다양한 사례가 있으며 영국의 소프트웨어 회사인 프로비넌스(Provenance)는 소비자에게 음식의 유통경로에 대한 투명한 계약 Tracking을 제공하여 소비자와 음식점과의 기존과 다른 신뢰관계를 제공하였다[8].

현재 블록체인을 활용한 디지털 콘텐츠 활용 관련 연구는 'Allrights' 콘텐츠 저작권 유통업체에서 활용하는 스트리밍 방법이 대표적이며 '인텔'에서도 디지털 콘텐츠 수수료나 저작권 보호를 위한 노력을 하고 있다. 또한 온라인을 통한 게임 및 광고시장에서도 블록체인을 통한 거래 시도가 다각적으로 연구되고 있다.

Table 2. Use of a block chain in startup[9,10,11]

DIVISION	CONTENT
Commodity Trading Service	Kraken: Collaborating with Fidor Bank of Germany to develop digital call service platform Lykke: Block Chain Based Leaky Coin Trading Platform
IoT.	Ascribe: Share and sell disital content assets through copyright registration
invest, loan	Funderbeam : Provide start-up connectivity platform with investors
security	Chainalysis : Block Chain based AML and KYC service
circulation route	Provenance :circulation route tracking

흔히 "2세대 블록체인"이라 일컫는 Ethereum은 기존 단순 거래 뿐 아니라 Smart Contract를 통하여 예약관련 코드를 삽입하여 기존의 중계자를 통한 개입을 배제하고 중계자에게 돌아가는 수수료에 대한 부담이 제공자와 수요자간에 존재하지 않는다[5]. 블록체인을 통하여 거래에 참여한 구성원들에게 거래정보를 투명하게 노출하고 거래내역을 누락 없이 기록하고 보관하게 함으로써 신뢰성과 더불어 거래에 있어 발생할 수 있는 다양한 보안상의 문제를 해결 할 수 있기 때문에 블록체인을 통한 많은 거래가 시도되고 있다. 특히 금융권과 공유경제와 같이 거래상의 보안과 신뢰가 중요한 경우 더욱 활발하게 적용되고 있다.

본 논문에서 제안하는 Ethereum 기술은 SHA256이라는 해싱함수를 이용하여 거래내역을 해싱하고, 해싱 한 내용을 다시 해싱하여 Merkle Trees를 구성하므로 거래내역에 대한 누락과 해킹이 사실상 불가능하다[12].

또한 Solidity를 활용한 Smart Contract를 활용하여 스마트 거래를 가능하게 하여 거래 시 발생 가능한 부적절한 위변조와 해킹을 방지할 수 있다.

그러나 디지털 환경에서 생산되고 거래되는 디지털 콘텐츠의 경우 공유경제 거래 시 기존의 제품보다 보다 높은 보안이 필요할 것이다. 이에 3장과 같이 콘텐츠 자체에 대한 보안을 추가로 실시하였다.

III. Block Chain Ethereum Technology base Digicon system

본 논문에서는 디지털 콘텐츠를 공유경제로써 활성화하기 위하여

필요한 항목으로 '거래와 계약의 투명성', '거래되는 콘텐츠의 보안강화'에 초점을 두었다. 이를 위하여 블록체인 기술 중 계약관련 코드를 사용하여 계약의 투명성을 보장하고 유통 시 위·변조 및 해킹을 방지하기 위한 디지털 콘텐츠 자체 암호화 방법을 연구하였다.

이를 통한 거래의 우수성을 증명하기 위하여 블록 거래에 대한 시험을 통하여 거래에 대한 다양한 위협 요인에 대한 우수성을 증명하였다. table 3과 같은 Design 방법으로 시스템을 설계하였다.

Table 3. Design method

1.Transparency in Transactions and Contracts: Smart contract of block chain Ethereum 2. Securing the content of transactions: Password handling for random portions of content

본 논문에서 제안하는 디지털 콘텐츠 공유 시스템(이하 「디지스(Digi_S)」)는 EVM (Ethereum Virtual Machine)을 플랫폼으로하여 Ethereum을 활용한 Smart Contract 가능한 환경을 제공하며 세부적 환경은 다음과 같다.

Table 4. environment

Server : ubuntu 16.04LTS Platform : EVM browser : geth (Web3.js) Solidity implement : browser solidity Blockchain : ethereum

디지스 시스템에서 사용할 구매요청 처리 프로세스는 Fig. 5와 같다.

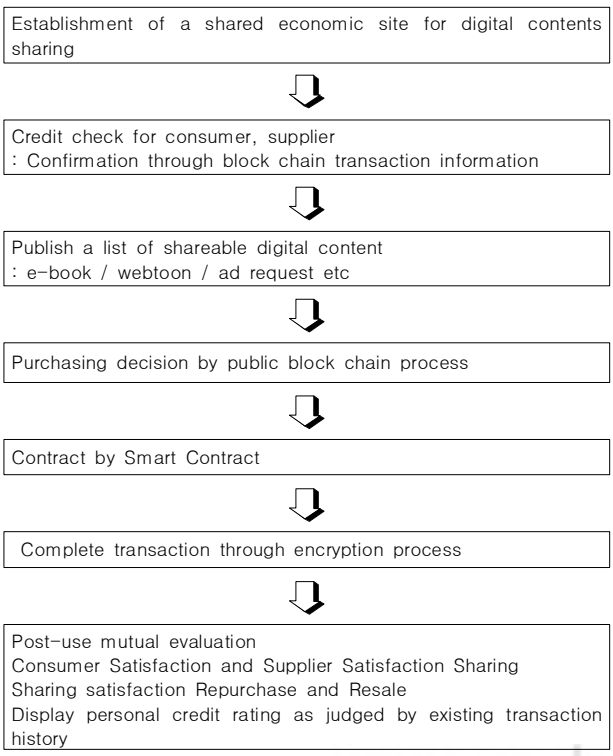

Fig. 5. Processing process

위의 거래 프로세스 중 Smart Contract와 암호화 프로세스 관련 evaluation 내용은 4장에서 설명한다.

IV. Design and implement

1. Smart Contract Design

공유경제는 대부분 온라인에서 거래가 이루어지고 오프라인을 통하여 활용된다. 온라인상의 거래에서 발생 가능한 다양한 형태의 보안 위협은 언제나 존재한다. 공유경제로써 디지털 콘텐츠가 성공적으로 자리매김하기 위하여 중요한 부분 중 하나가 투명한 계약이다.

본 논문에서는 solidity 기반 Smart Contract를 통하여 수요자와 공급자가 투명하게 거래할 수 있도록 한다. Fig.5와 같이 계약서에 대한 코드 입력이 이루어지면 컴파일을 통하여 바이트 코드로 포맷으로 변경된다. 바이트 코드를 p2p를 통하여 인증된 거래 대상자에게 공유하기 위하여 Web3.js를 통하여 JSON RPC를 호출하게 된다. Fig. 6은 Smart Contract 처리 과정이다.

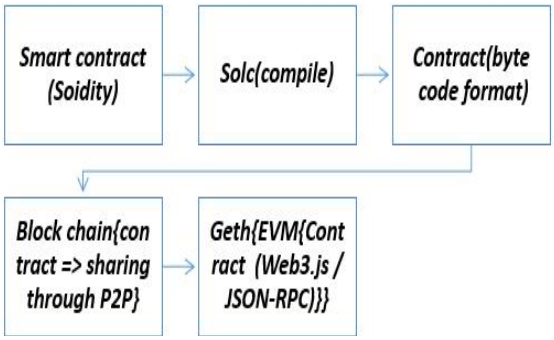

Fig. 6. Smart Contract processing

공유경제에서 중요한 요인 중 하나가 거래자들 간의 신임을 고려하여 본 논문에서 제안한 Smart Contract는 단순한 거래 계약이 아닌 거래당사자들에 대한 신용도를 추가하였다. 거래를 위한 Smart Contract의 Struct의 일부는 Fig.7과 같다.

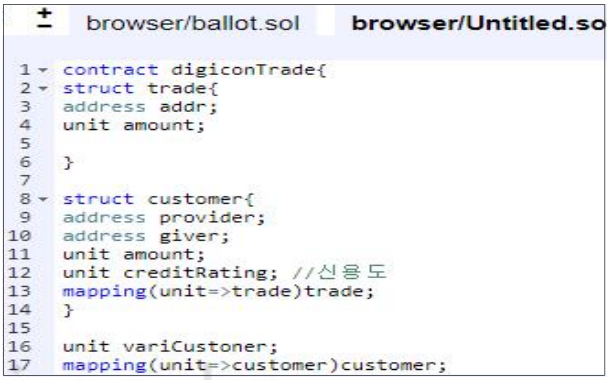

Fig. 7. Smart Contract structure

수요자와 공급자의 신용에 대한 평가를 위하여 unit 형태의 creditRating을 추가함으로 쌍방의 신뢰지수 측정이 가능하고 creditRating은 기존 다른 거래에서 측정된 수치에 기인하므로 계약 시 유용하게 활용가능하다.

Smart Contract가 시스템에 적용되기 위하여 geth를 이용하여 블록을 생성시키고 browser solidity를 통하여 Smart Contract를 수요자와 공급자가 공유할 수 있도록 한다. Solidity는 계약을 위한 프로그래밍 언어로써 EVM에서 구현되도록 프로그래밍 가능하며 블록체인이 사용되는 플랫폼에서 Smart Contract가 가능하도록 개발된다. Fig.8을 통하여 browser solidity를 Smart Contract를 만들고 제안한 구조를 가진 Smart Contract의 내용을 공유하고 계약사항에 대하여 투명하게 거래하도록 한다.

Fig. 8. browser solidity

Remix를 사용하는 경우 더욱 편리하게 거래당사자간의 확인이 가능하다. Fig.9와 Fig.10은 본 논문에서 제안한 시스템에 대한 거래관련 Transaction을 가상 네트워크를 통하여 공개하고 거래 시 활용 가능한 API를 적절하게 사용하고 거래가 완료되었음을 보여주는 화면이다.

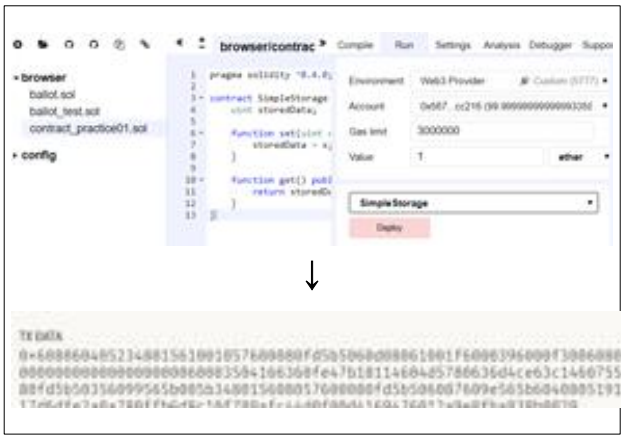

Fig. 9. Transactions through virtual networks

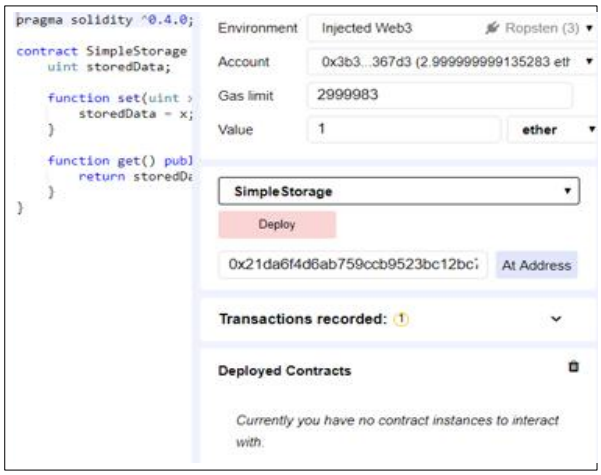

Fig. 10. Contract complete screen by application

만일 Fault Tolerance를 위하여 거래에 대한 확실한 증거를 제시하기 위하여 Transaction Receipt를 확인하고 Address를 확인할 수 있다. Fig 11을 통하여 Transaction이 처리되어 Block로 묶여 Transaction Receipt의 정보에 Address가 추가되었음을 알 수 있다.

Fig. 11. Transaction Receipt

2. Encrypting digital content

블록체인으로 거래 시 발생되는 블록에는 거래내역을 관리하는 Merkle Trees가 포함되어 있다. Merkle Trees는 해시 알고리즘을 사용하여 복호화가 불가능한 해시값으로 변경이 되며 거래 시 발생 가능한 다양한 Transaction을 삭제 없이 관리할 수 있다. 현재 블록체인 Ethereum에서는 거래내역에 대한

관리를 위하여 SHA-256 해싱알고리즘을 통하여 거래의 투명성을 보장하고 있다. 하지만 엄밀하게 이야기하자면 거래되는 내용 자체를 암호화 하는 것은 아니다. 만일 디지털 콘텐츠가 거래된다면 디지털 콘텐츠 자체에 대한 보안이 이루어지는 것은 아닌 것이다. Merkle Trees를 통하여 거래내역에 대한 투명성과 정당성을 보장할 수 있으나 거래되는 내용 자체에 대한 보다 안전한 보호가 필요하다. 매우 빈번히 발생하는 Transaction에 일일이 복잡한 암호를 활용하여 암호화 하는 경우 거래 시간, 암호화시간, 복호화 시간 등으로 인하여 거래의 효율성에 문제가 있을 것이다.

본 논문에서는 거래되는 다양한 콘텐츠에 대하여 Smart Contract의 메타데이터를 통하여 기록하도록 하고 기록된 메타데이터를 토대로 암호화 가부를 결정하여 처리하도록 한다. Fig.12는 본 논문에서 제안한 Merkle Trees의 암호화 프로세스 이다.

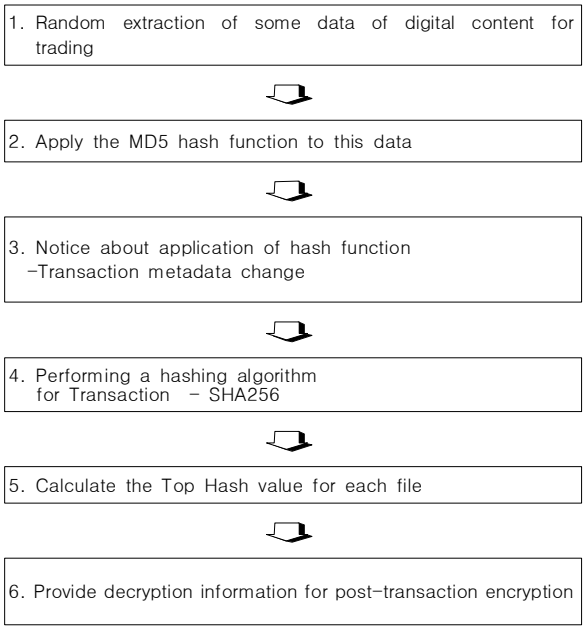

Fig. 12. Processing Process

제안한 프로세스에서는 디지털 콘텐츠의 랜덤한 일부 데이터를 추출하여 MD5 해시함수를 적용한다. 랜덤한 데이터에 대한 위치를 결정하기 위한 시드(Seed)값이 필요한데 본 연구에서는 간단하게 현재의 날짜를 적용하였다. 이를 통하여 각 거래내역에 대한 메타데이터가 변경되고, 이를 통하여 해시값도 변경되게 된다.

디지스 시스템에 적용되는 MD5 알고리즘은 128비트 암호화 해시함수이며 간단한 알고리즘이지만 디지털 콘텐츠의 랜덤한 부분에 대한 암호화를 통하여 위변조 여부를 판단하고 안전한 디지털 콘텐츠 유통을 위한 신뢰성을 향상시킬 수 있다.

Fig. 13은 디지스 시스템에서 발생하는 임의의 데이터를 추출하여 MD5처리하는 과정이다.

```
<input> : unit variCustoner;
mapping(unit=>customer)customer;
<output> : : AD636260E1843576883BB244C1BAFB08
```

Fig. 13. MD-5 process

제안한 바와 같이 공유되는 디지털 콘텐츠 자체에 대하여0 랜덤 영역을 암호화 처리하여 공유경제에 적용 시 거래되는 콘텐츠 자체에 대한 안정성을 높일 수 있다.

V. Evaluation

본 논문에서는 공유경제로써 디지털 콘텐츠를 활용하기 위하여 투명한 계약과 거래되는 콘텐츠의 보안을 목적으로 디지스 시스템을 설계하고 개발하였다. 성능평가를 위한 지표 중 속도는 본 논문에서는 의미가 없다.

따라서 제안하는 연구내용에 대한 성능평가를 위하여 블록의 생성, 확정시간을 알아보았다. 일반적인 p2p환경이 아닌 private network의 가상 네트워크를 통하여 거래하였으며, 거래요청자와 제공자를 감안하여, 2개의 노드를 설정하고 geth플랫폼을 통하여 평가항목에 대하여 실험하였다.

이때 사용되는 event function 다음과 같다.

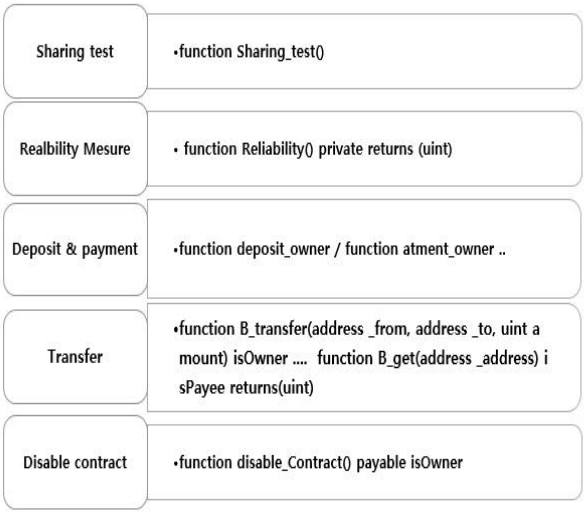

Fig. 14. Event function

위에서 언급한 바와 같이 성능평가를 위한 factor는 블록체인의 속도(TPS)를 통한 블록체인의 생성시간과 확정시간이다. ethersscan.io를 통하여 조사한 최근 Ethereum의 Transaction은 Fig. 15과 같다.

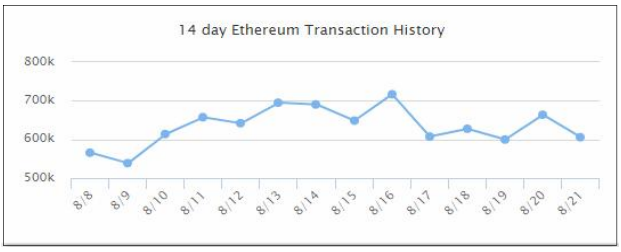

Fig. 15. Ethereum Transaction History [6]

본 논문의 실험을 위하여 준비한 각기 다른 2개 계정과 Smart Contract를 초당 50개의 속도로 요청하였으며 contract creation부터 transaction 처리를 통한 결과를 통하여 블록체인 생성시간과 확정시간을 알아보았다.

각 처리과정에서 대하여 Contract creation과 deploy를 통하여 발생한 Message Transaction을 분석하고 간단한 Call을 통하여 transaction pre clock를 파악하여 실험결과를 추출하였다.

실험의 결과는 Fig. 16와 같은 프로세스로 처리되었다.

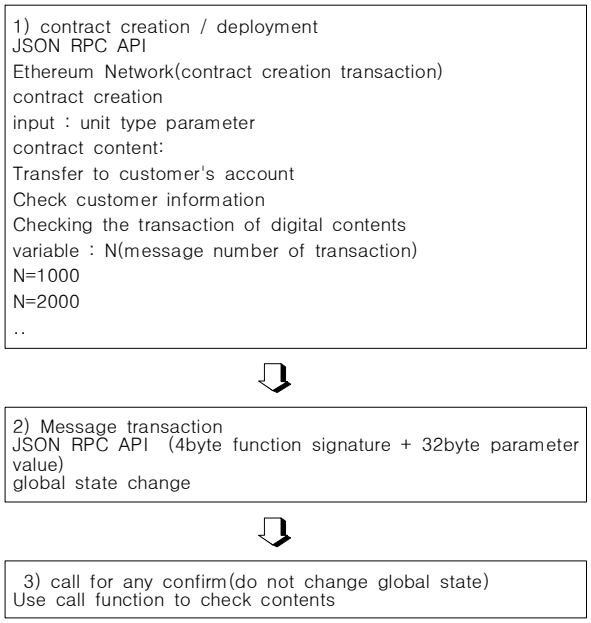

Fig. 16. evaluation process

위의 실험을 통하여 Table. 5와 같은 결과(transaction per block)를 얻었다.

Table 5. Evaluation result

division	sec	transaction per block
N=1000	1~10	100
	11~	under 30
N=2000	1~10	100
	11~	under 20

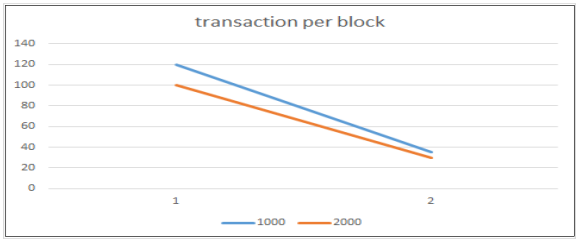

Fig. 17. Evaluation result-graph

Table. 5의 결과에서 많은 양의 message transaction이 요청되었을 때 플랫폼은 블록의 생성을 우선하여 수행하고 Smart Contract 수행을 더디게 수행한 것으로 나타났다.

VI. Conclusions

스마트 디바이스의 발전과 더불어 새로운 형태의 콘텐츠 발전에 따라 다양한 채널을 통하여 디지털 콘텐츠가 거래 및 관리 되고 있다. 기존 개인과 개인의 소소한 거래형태였던 공유경제 또한 새로운 산업유통경로로써 발돋움하고 있다. 이에 디지털 콘텐츠를 공유경제의 개념으로 거래하기 위한 연구가 활성화되고 있지만 공유경제로써 디지털 콘텐츠를 거래함에 따라 발생될 수 있는 거래 및 관리 정보보호의 위협도 증가하였다.

본 논문에서는 디지털 콘텐츠의 안전한 거래를 위하여 블록체인 Ethereum 기술을 활용하여 수정된 메타데이터를 활용한 Smart Contract를 적용하고 디지털 콘텐츠 자체에 대한 암호알고리즘 적용이 가능한 「디지스(Digi_S)」 시스템에 대하여 연구하였다. 제안한 시스템을 통하여 공급자와 수요자간 신용도를 체크하여 투명한 거래가 가능하다. 또한 콘텐츠 자체에 대한 부분적인 암호알고리즘 적용을 통하여 해킹을 통한 위.변조를 방지할 수 있다. 이를 통하여 디지털 콘텐츠의 효과적이고 투명한 거래와 저작권관리가 가능하고 향후 공유경제로써 디지털 콘텐츠의 새로운 유통 채널을 활성화 할 수 있을 것이다.

REFERENCES

[1] Min jung Kim and H.Y Lee, "Policy Direction for Stable Growth of Shared Economy", KDI Focus, 2017.
[2] Jung Sook Sung,"A Study on the Protection Plan of Digital Contents", journal of security engineering,pp,739-746, 2013.
[3] Survey, "Survey on the status of digital contents industry in 2016", IITP, 2016.
[4] Survey, "2016 Domestic Digital Contents Survey",National IT Industry Promotion Agency 2016.

[5] J. R. Douceur, “The sybil attack,” In the First International Workshop on Peer-to-Peer Systems, IPTPS ’01. London, UK: Springer-Verlag, pp. 251-260, 2002.
[6] URL : Ethereum Project https://www.ethereum.org.
[7] Survey, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Satoshi Nakamoto, 2008
[8] Survey, "Development Status of Block Chain Application Technology and Introductions by Industry",Financial Security Service, 2017.
[9] Survey, "Financial Supervisory Service: Status and major issues of distributed led technology", Bank of Korea, 2016.
[10] Survey, "Introduction of Block Chain for Activation of Shared Economy", Seoul Digital Foundation 2016.
[11] Survey, "Ledger fever : 95 bitcoin & blockchain startups in one market map",CB.Insights, 2017.
[12] S. Bag, S. Ruj, and K. Sakurai, “Bitcoin blockwithholding attack :Analysis and mitigation,” IEEE Transactions on Information Forensics and Security, PP(99), pp. 1-12, 2016.
[13] E. Heilman, A. Kendler, A. Zohar, and S.Goldberg, “Eclipse Attacks on Bitcoin's Peer-to-Peer Network,” In USENIX Security Symposium, pp. 129-144, 2015.
[14] I. Eyal, and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” In International conference on financial cryptography and data security, Springer, pp. 436-454, 2014.
[15] R. Zhang, and B. Preneel, “Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin,” In Cryptographers’ Track at the RSA Conference, Springer, pp. 277-292, 2017.
[16] Survey, "Sweden tests blockchain technology for land registry", Reuters, 2016.
[17] Vitalik Buterin. “Ehtereum White Paper A Nect Gerneration Smart Contract & Decentralized Application Platform”. 2014.

Authors

Youn-a Min received the doctor's degree in Computer Science from Dongguk University, Korea, in 2013 . Current, a Professor in the Department of Software at Gachon University. She is interested in Block chain, Embedded smart device Security, IoT platform Seuruty, and database Security

Yeong-Tae Baek received the B.S. degree in Computer Science from Inha University, Korea, in 1989 and M.S. and Ph.D degrees in Computer Science from Inha University, Korea, in 1993 and 2002, respectively. He is currently a Professor in the Department of Multimedia at Kimpo University. He is interested in multimedia contents, IoT platform, and mobile system.