

대체불가 디지털자산의 실물담보 방법 및 전자금화폐의 발행

김성진, 강수연^o, 강인준
주식회사 한국전자금화폐

ksj84@kaist.ac.kr, syk709@snu.ac.kr, wnsdl0423@smartgoldcoin.com

Method of decentralized real-guaranteed non fungible token and issuing digital gold currency

Kim Sung-Jin, Kang Soo-Yeon^o, Kang In-Joon
SMART GOLDCOIN Co., Ltd

요 약

본 연구는 대체불가 디지털자산(NFT, Non Fungible Token)에 필수불가결하게 결합되는 물리적 실물 대상과 발행된 디지털 소유 NFT간의 동일성을 담보할 수 있는 방법 및 위 방법을 실물금에 반영한 대체불가 고유 전자금화폐를 발행하는 것에 관한 연구이다. 대체가능 토큰 ERC20의 표준과 완전 대비되는 대체불가 토큰 ERC721의 추가 표준이 수립되며, 소유 디지털자산을 동종끼리는 교환불가 시킴으로서 고유성이라는 새 교환법칙을 확보했고, 이러한 법칙은 그 자체로 대체불가 디지털자산에 희소성을 부여하게 된 바, 이는 시대적으로 매우 중요한 연구적 가치를 가진다.

1. 서 론

디지털자산의 대표주자인 비트코인은 사람들이 정부의 개입없이 개인간 탈중앙적 자산거래를 원한다는 강력한 수요적 욕구를 가시적으로 증명하였고, 탈중앙의 기본적 구현체제되는 블록체인 기술사상을 통해 분산장부의 특성상 그 거래와 소유자를 위·변조 할 수 없다는 강력한 신뢰적 이익을 발견하는데 획기적 기여하였다.

이러한 수요 및 이익에 기초해 새로운 유형의 디지털 자산인 이더리움이 탄생하였고, 급기야 이더리움은 1:1 교환 가능한 ERC2.0규격을 넘어서 동종간 교환을 금지시키는 ERC721규격을 수립하는데 성공하며, 종전의 대체가능 토큰(fungible Token)과는 그 개념이 완전 반대되는 대체불가 토큰(NFT)의 개념을 파생시켰다.

ERC721규격의 고유ID는 이더리움의 퍼블릭 개방형 블록체인상의 JSON파일로 관리되는 256비트 식별자인 URI와 결합함으로써, URI식별자에 기록된 작성자, 소유자, 작성일 등의 정보를 기준으로 대체불가 구조를 만들 수 있게 된다.

위 규격은 2017년 DApp기반 게임 크립토키티(CRYPTOKITTIES)로부터 발전된 이 세상 단 하나뿐인 나만의 고유한 애완고양이를 다른 (애완)고양이와 똑같은 것처럼 바꿀 수 없다는 디지털 희소성 기능으로 적극 사용되며, 그 규격의 필요성에 대해 비로소 긍정적인 평가가 시작되었다.

이후, 위 고유한 대체불가 토큰 NFT는 애완고양이 외에도 영상, 그림, 음악 등의 디지털 지식재산권과 폭발

적 결합되며, CD, USB, 종이와 같은 저장매체물로만 존재하였던 그 유형적 내재가치가 무형적 토큰에서도 계속 유지됨으로서, 디지털자산은 쓸모없는 것이라는 종전의 전통적 비판을 잠식시키기에 이른다.

하지만, 실물이 필수불가결 존재할 수 밖에 없는 대상인 부동산, 화폐, 자동차, 경주마, 운동화, 그림 등과 같은 유형의 대체불가 토큰의 경우(더 구체적으로는, 시날 인증ID와 구매자의 소유권을 결합한 실물기반 토큰화된 나이키 특허의 2019년 운동화 토큰과 같은 경우), 실물에 의해 그 내재가치를 동시에 유지시킬 수 밖에 없는 데, 네트워크 장부상의 위·변조는 예방할 수 있다지만 실물은 위·변조를 예방할 방법이 없고, 또한, 그 실물이 대체불가 토큰과 동일한 것인지에 대한 신뢰까지 담보할 수는 없는 치명적인 문제점이 있다.

2. 본 론

앞서와 같이, 실물과 대체불가 토큰간의 동일성 확보가 안되는 치명적 문제가 존재하다보니, NFT공급자들은 실물을 폐기시키는 비상식적인 방법까지 동원하고 있는데, 그 대표적인 사례가 얼굴 없는 화가인 뱅크시의 '멍청이(Morons)' NFT작품에 대한 실물 폐기 사례이다.

NFT공급자 블록체인기업 인젝티브프로토콜은 위 뱅크시 작품을 NFT로 전환한 뒤 이를 경매에 내놓으며, 트위터 'Burnt Banksy'계정의 생중계에서 실물을 폐기시키면 NFT의 전환그림이 대체불가의 진품이 된다는 극단적 설명과 함께 실물 그림을 실제 불태우는 화형식을 거행하였다.



그림1. 뱅크시 화가의 '멍청이' NFT 실물작품을
불태워 폐기시키는 영상장면

(주소 : https://www.youtube.com/watch?v=C4wm-p_VFh0)

위와 같은 방법은 실물이 가지는 고유의 가치를 회복 불가능케 훼손시킬 뿐 아니라, 동시 병존하면 더 큰 가치로 고도화시킬 수 있는 기회마저 상실하는 것으로서, 이는 그저 작품명 '멍청이'와 다를 바 없는 방법이라 할 것이다. 가사, 이러한 방법이 대항불가한 부득이한 방법이라고 가정하더라도, 실물이 폐기되어 부존재한다는 사실을 도리어 입증시켜 주어야 하는 바, 결국은 존재하지 아니하든, NFT의 실물은 실물이 존재하는 그 순간부터 이미 동일성의 신뢰성을 담보해주어야 한다는 거래의 본질적 책임엔 변함이 없고, 오히려 부존재를 입증하는 것이 자연법칙상 훨씬 어렵다. 심지어 부동산, 주화형태의 화폐는 태울 수조차 없다.

본 연구는 이러한 문제를 해결하고자 실물과 대체불가 토큰간의 위·변조 방지 및 동일성의 확보를 목표로 한다.

2.1. 대체불가 디지털자산의 결합실물 표면에 고유식별 마이크로 패턴을 형성하여 위·변조의 예방 및 디지털인식

대체불가 디지털자산의 실물대상 표면에 초정밀 마이크로 패턴을 형성하여, 위·변조를 예방 및 시장의 혼동과 가치하락을 막을 수 있고, 그 형성된 무늬를 디지털인식의 수단으로 이용해 대체불가 토큰과 1:1 직결시킬 수 있다.

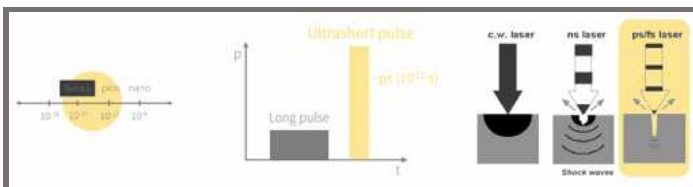


그림2. 레이저 어블레이션(Laser Ablation) 기술을 통한
고유식별패턴의 미세형상

표면에 피크파워가 상당한 울트라쇼트 레이저를 조사함으로써 재료의 결합을 와해시키는 공정방식의 고유식별패턴을 미세 형상시킬 수 있는데, 이는 마이크로급 정밀 선폭으로 위·변조를 방지시키는 물리적 기술이다. 가

공선폭은 $10\mu\text{m}$ 상당의 정밀성이 요구되고, 이러한 정밀성은 패턴의 비가시성을 구현할 수 있어서 실물의 패턴을 세밀하면서도 정교히 감출 수 있다.

고유식별패턴의 다양한 모양적 구성을 통해 실물에 대한 고유 식별성을 획득하고, 각 패턴에는 그에 대응하는 등록문자열, 대체불가 토큰 주소가 데이터베이스에 저장되어 이를 디지털분석 방법으로 인식 후 기초정보로 활용하게 된다.

고유식별패턴	등록 문자열	대체 불가 토큰 주소
	A79S896BEG936	Oxffff1234ab
	A79S896BEG936	Oxffff1234ac
	A79S896BEG936	Oxffff1234ad

그림3. 고유식별패턴과 등록문자열, 대체불가 토큰 주소의 각
대응 데이터베이스 표

형상패턴의 모양은 $\bigcirc$, $+$, $*$, Δ 등 다양하게 이용될 수 있으며, 필요에 따라서는 보안도를 향상시키기 위해 임의의 속임수 패턴을 덧붙여 식별패턴의 기준을 고의적 혼동시킬 수 있다.

이러한 패턴을 대체불가 디지털자산의 실물표면 위에 형상화 할 때, 순간적 물리학적 조건은 매우 중요하다.

짧은 파동 속 구간을 의미하는 주기(Pulse)와 속도(Speed) 조건이 충족되어야 유의미한 인식패턴을 획득할 수 있기 때문이다.

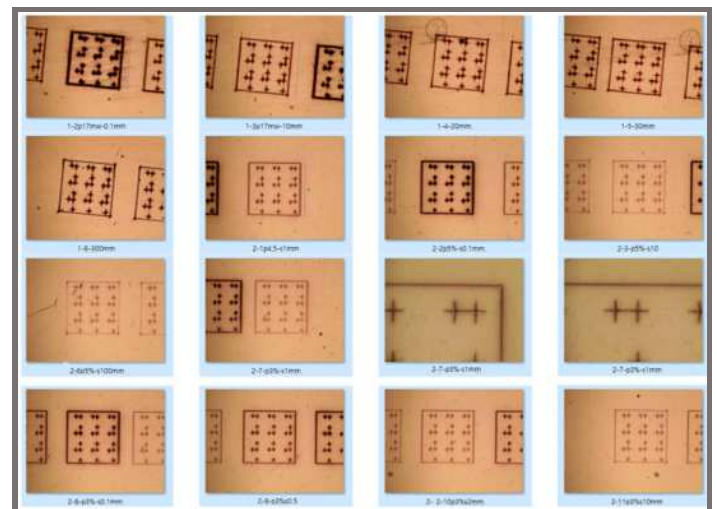


그림4. 다양한 P/S 조건을 통해 형상화된 십자패턴

전자단말기(예를 들면, 스마트폰 등)으로 고유식별패턴을 대체불가 디지털자산과 실물 사이의 동일성 확

인 목적으로 디지털인식 하는데 있어, 인공지능(AI) 영역인 계층적 패턴인식모델 HHMM(Hierarchical Hidden Markov Model)을 적용하며, 이미지 인식은 HTM(Hierarchical Temporal Memory) 모형을 이용한다. 이 두 모델은 고전적 전통기초모델이나 하위수준(Core Low Level)단계에서 다양한 인식변수를 섬세히 인식하는데 근본적 탁월성을 가진다.

패턴은 어떤 레벨이든 레벨과 관계없이 그 자체로 인정되어지는데, 획/글자/단어/그림 모두 기계에게는 패턴이 된다. 글/그림 모두 이미지로 계층적 패턴인식이 이루어지며, 결국 패턴인식이 하는 일은 ‘인식 대상패턴’이 실제로 유효한 입력에 의해 나타날 확률의 계산이다. 입력값이 반복되고 유사한 패턴이라고 판정할 지를 계산하는 것이므로, 각각의 입력되어 들어오는 관찰크기(지속시간, 공간 등)의 기존 저장한 크기 인자값과 비교하여 패턴이 인식될 최종 확률의 계산으로 처리된다고 봄이 정확하다.

이 확률의 고도성을 위해 크기 인자값에 QR Code에 해당되는 위치 확인 코드간격 1mm이상의 패턴을 대체불가 디지털자산의 실물표면에 형상화한다. QR(Quick Response)의 빠른 반응 원리를 차용하여, 인식의 속도를 신속화(=확률의 향상)하는 것이다. 이를 위해 역전파 알고리즘을 사용한다.

가령, 실물 내에 패턴이 형상되었다고 가정시, 격자의 각 칸을 입력노드 각각과 연결하여 검은 색은 값이 1, 하얀색은 0으로 해서 학습데이터를 데이터베이스화 함으로서 역전파 알고리즘을 가동할 수 있다.

데이터 ‘1’: 출력노드1의 활성값만 1, 나머지 0
 데이터 ‘2’: 출력노드2의 활성값만 1, 나머지 0

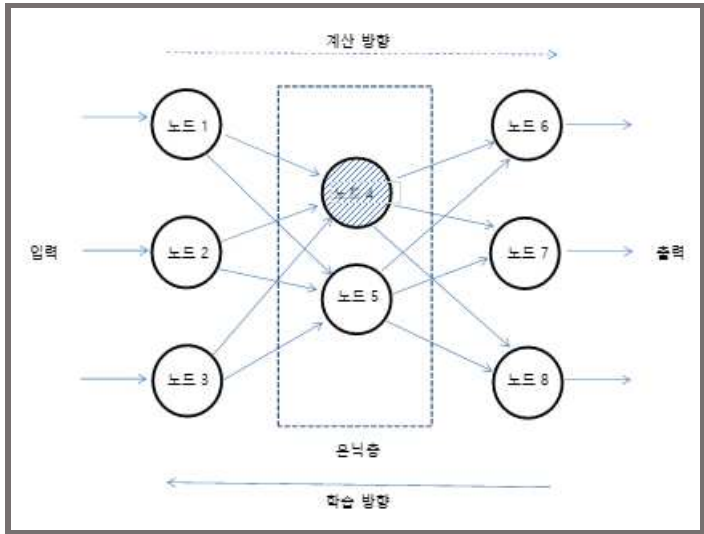


그림5. 패턴의 노이즈 인식을 최소화하는 인공신경망 역전파 알고리즘

2.2. 대체불가 디지털자산의 실물예시인 금주화에 마이크로패턴을 형성

본 논문은 대체불가 디지털자산 실물의 가장 극단적 자본주의의 예시로 화폐를 대상으로 하되, 신용화폐처럼 화폐의 기본가치 담보를 정부가 보증하는 방법 대신 재료 그 자체가 위 역할을 하도록 하기 위해 전세계가 화폐로 인정하는 ‘금’을 대체불가 디지털자산의 실물로 채택하였다. 금주화 자체가 스스로 가치를 가지는 독립적 재화이기에 정부개입과 규제를 받을 하등의 이유가 없어 이 자체로 블록체인과 별개로 물리적 탈중앙화가 실현되는 바, 가장 현실적인 ‘탈중앙화 된 금 화폐 담보성 대체불가 디지털 자산’의 대표적 실물이 될 수 있다.

1돈(3.75g)을 기준으로 실물금주화를 제작하였으며, 한 면에는 1DON 이라고 표기되어 있고, 또다른 한 면에는 위·변조 방지 고유식별패턴이 형상화되어있다.



그림6. 대체불가 디지털 자산의 금주화 실물

금주화 실물표면에 울트라쇼트 레이저를 조사하여 고유식별패턴을 회로처럼 새길 수 있다. 가장 공정이 어려운 금속표면인 금주화에 패턴을 새겼다는 것은 그 밖의 재료인 종이, 플라스틱, 유리 등에도 당연히 새길 수 있음을 증명했다고 봄이 마땅하다. 이에, 금주화 외에도 얼마든지 다른 디지털자산 실물로 확대할 수 있다.

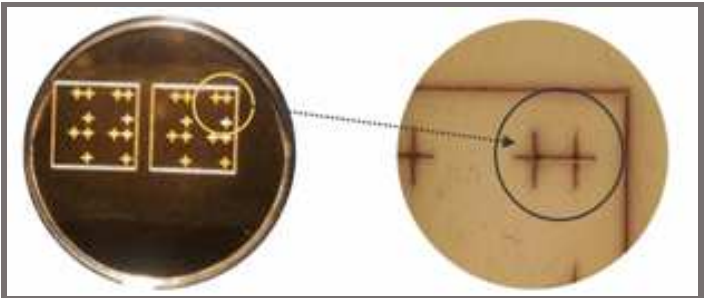


그림7. 10마이크로급으로 실물표면에 실제 십자패턴형상

대체불가 디지털자산의 저장물 데이터베이스와 실물 금주화의 패턴을 비교함으로서 동일성을 확인할 수 있게 되고, 이러한 동일성은 위·변조되지 않은 원본임을 담보하는 결과로 귀결된다.

2.3. 전자금화폐의 인식 및 대체불가 토큰으로의 전환

패턴인식모델에 의한 이미지프로세싱을 통해 고유식별 패턴을 인식하고, 데이터베이스의 항목 중 대체불가 토큰으로의 전환여부를 확인한다.



그림8. 실물 금주화 고유식별패턴에 대한 이미지프로세싱

```

Bitmap outImg = Bitmap.createBitmap(orgImg.cols(), orgImg.rows(),
Bitmap.Config.ARGB_8888);
Utils.matToBitmap(orgImg, outImg);
/* BlobDetector Lib */
BlobDetector detector = BlobDetector.create();
BlobDescription circle = detector.getMaxCircle(orgImg);
if (circle.mat != null){
    Mat cropped = new Mat();
    circle.mat.copyTo(cropped);
    BlobDescription blob = detector.detect(cropped);

    Bitmap outImg = Bitmap.createBitmap(blob.mat.cols(), blob.mat.rows(),
    Bitmap.Config.ARGB_8888);
    Utils.matToBitmap(blob.mat, outImg);
    LogUtil.d(TAG, blob.toString());

    if (blob.count == 12) {
        showToast("정상");
        ivResult.setImageBitmap(outImg);
    } else {
        showToast("비정상");
        ivResult.setImageBitmap(outImg);
    }
} else {
    showToast("원 검출 실패");
}
}

```

표1. 고유식별패턴 이미지프로세싱 코드 일부 발췌

인식된 고유식별패턴은 전세계 유일한 패턴이므로, 고유 금주화가 되고, 이를 디지털로 발행한 대체불가 토큰과 1:1 직결시켜주면, 그 즉시 대체불가 디지털자산으로 전환되어 전자금화폐를 발행한 것과 동일한 효과를 가지게 된다. 이러한 전환된 대체불가 토큰은 교환의 자유 법칙에 따라 제한없이 거래할 수 있다.

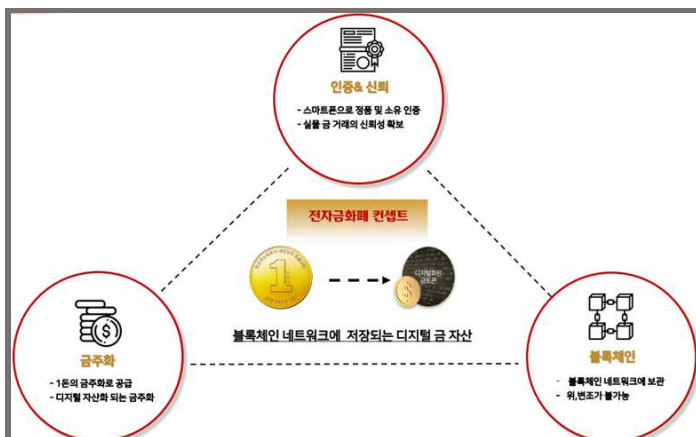


그림9. 대체불가 전자금화폐의 개념도식

3. 결 론

대체불가 디지털자산과 결합되어야 할 실물의 신뢰성을 담보함으로써, 종전의 실물이 가졌던 내재가치를 의심없이 계속 유지하면서도 디지털과의 결합으로 그 가치를 더 고도화 시킬 수 있고 거래의 편의성도 확보할 수 있다. 이로써, 유명화가의 그림을 비롯해 고가의 자동차, 부동산 등의 실물 내재가치를 그대로 흡수할 수 있는 것이다.

한편, 대체가능 토큰인 비트코인이 내재가치가 없다는 이유로 더 비싼 가격에 사 줄 또 다른 바보가 반드시 필요하다는 ‘더 큰 바보 이론(the greater fool theory)’에 직면하고, 워렌 버핏이 운영하는 투자사 버크셔 해서웨이까지 대체가능 토큰을 문명사회의 이익에 역행하는 역겨운 발명품으로 비난적 평가하는 마당에 내재가치를 가지게 된 새로운 대체불가 토큰은 이러한 평가를 시대착오적인 것으로 역전시킬 수 있다는 점에서 메타버스(meta + universe) 시대의 응답이자 소명이 될 것으로 주목된다.

지구의 모든 문명인은 가상의 애완고양이를 키울 권리가 있고, 그 고양이를 소유할 수 있으며, 국가권력의 개입없이 자산화하여 네트워크에서 사고 팔 수 있음은 당연하다.

[참고문헌]

[1] Burton, Amber, “Want to Buy an NFT? Here’s What to Know”, Wall Street Journal, ISSN 0099- 9660, 2021. 3. 13.
[2] Wood, Gavin. “Ethereum: A secure Decentralised generalised transaction ledger.” Ethereum project yellow paper 151.2014 (2014): 1- 32.
[3] Gencer, Adem Efe, et al. “Decentralization in bitcoin and ethereum networks.” International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2018.
[4] “Bitshares – your share in the decentralized exchange”, <https://bitshares.org/>
[5] FIPS PUB 186- 4, “Digital Signature Standard (DSS)”, 2013.7. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186- 4.pdf>
[6] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem”, ACM Transactions on Programming Languages and Systems, Vol. 4, Jul. 1982.
[7] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery”, ACM Transactions on Computer Systems, Vol. 20, Nov. 2002.
[8] Financial security institute, “Blockchain technology and security considerations”, 2017
[9] S. Nakamoto, “Bitcoin: A peer- to- peer electronic cash system”, 2008. <https://bitcoin.org/bitcoin.pdf>

2021 춘계 한국 블록체인 학술대회 블록체인의 미래 : 원천기술과 디지털 자산



The Future of Blockchain
- Fundamental Technology and Digital Asset

2021.05.21(금) 09:30-17:30
더케이호텔 서울 거문고홀(3층)



등록 | <https://onoffmix.com/event/235318>

문의 | (사)한국블록체인학회 02-701-5450 ksblockchain@naver.com
사무국장 윤석빈 seokbin7@gmail.com

주최 | (사)한국블록체인학회
한국정보과학회 소프트웨어공학 소사이어티 블록체인기술연구회

세션 1: 블록체인 실용기술 (13:50~15:00)	제1저자	제2저자	제3저자	제4저자	교신저자 소속	
블록체인을 이용한 비즈니스 모델 혁신 사례: Brave Browser	김세훈				aSSIST business school	
발전소내 사물인터넷 디바이스간 보안성 강화를 위한 블록체인 기반의 동적 암호키 기술	김정환	조수환			동서발전, 엠블럭	
블록체인 및 DID 기반 학내 신분증 발급 Eco System	김성빈	김규선	김도훈		경기대학교	
대체불가 디지털자산의 실물담보 방법 및 전자금화폐의 발행	김성진	강수연	강인준		한국전자금화폐	
DID 기반 모바일 운전면허증 PoC 구현	양희선	이규성			한국조폐공사	
세션 2: 블록체인 기반기술 (15:20~17:30)						
CDM 데이터 접근 제어를 위한 분산형 식별자 적용	정채은	강윤희	박용범		단국대학교	
샤드 기반 프라이빗 블록체인 환경에서 데이터 프라이버시 개선을 위한 매트릭스 문자 재배치 기법	이열국	고대균	서정원	박수용	서강대학교	
Leverage Sidechains to Reduce the Workload for Smart Contracts through Parallelization	M.Saetran	박수용			서강대학교	
정적 계정 할당 기반의 블록체인 샤딩 환경에서 크로스-샤드 트랜잭션 증가 비율 분석	이대현	박수용			서강대학교	
NFT Digital Asset Trading Platform for Personal Data Sovereignty	조민수				고려대학교	
Blockchain-based processing of sensitive information for GDPR compliance	이동원	인호			고려대학교	
IPFS 블록체인 환경 설계 및 2-stage 합의체 구성 제안	김주연				아주대학교	
블록체인 기반 헌혈 관리 플랫폼(A Blood Donation Management Platform based on Blockchain)	김세진	이재림	조수현		고려대학교	