# 금융권을 위한 가상화폐기반의 블록체인 플랫폼

박진주*, 정수연**, 박래현***, 한창훈***
*한신대학교 컴퓨터공학부
e-mail : alread02@naver.com

# A Study on the Block Chain Platform Used by Financial Industry

Jin-Joo Park*, Su-Yeon Jung**, Rae-Hyeon Park***, Chang-Hun Han***
*Dept. of Computer Engineering, Han-Shin University

**요 약**

블록체인 기술은 현재 다양한 분야에서 활용되는 기술로 떠오르고 있다. 특히 익명성, 공정성 등의 특징으로 인해 금융권에서의 활용이 두드러지게 나타나고 있는 현실이다. 이러한 블록체인 기반의 기술(비트코인, 이더리움, R3)들을 살펴보고, 금융권에서 어떤 식으로 활용되고 있는지에 대한 방향에 대해 알아보고자 한다.

## 1. 서론

### 1.1 연구의 배경 및 목적

거래정보를 기록하고 이를 네트워크 참가자들에게 분산하고 공유하는 분산원장(distributed ledger)을 블록 체인이라고 지칭한다.

본문에서는 소비자와의 거래가 활발하게 이루어지고 있는 금융업계에 위의 블록체인 기술을 적용하여 기존 금융거래시스템 대비 블록체인 적용 시너지에 대해 기술하고자 한다.

## 2. 금융권에서 블록체인 기술 적용 및 기술

### 2.1 기존 금융권 시스템의 특징

기존 금융권 시스템은 중앙 집중형 시스템으로 정보관리나 거래 승인 권한과 책임에 대해 특정기관에서 독점하는 구조이다. 이러한 구조는 중앙서버에서 관리할 뿐 아니라 제 3 신뢰기관(은행, 정부)과의 거래로 이루어진다.

### 2.2 블록체인 기술이 대두되는 이유와 법적 근거

기존 금융권 중앙집중형 시스템 방식은 제 3 기관의 신뢰를 확보해야 하는 문제점을 가진다. 예를 들면 다음과 같다.

① 기관의 내부의 문제로 인한 조직 내의 신뢰관계 훼손의 문제
② 기관 외부의 해킹 또는 전산오류 등으로 인한 사용자 피해 문제
③ 사용자 피해를 방지하기 위한 IT 인프라 및 보안에 많은 인력 및 자금이 소요되는 문제
④ 「금융 투자업과 자본시장에 관한 법률」 에 따른 한국예탁결제원과 「민법」 제 32 조에 따라 설립된 금융결제원 등 금융유관기관

### 2.3 블록체인 기술의 정의

중앙 집중 시스템에서 발생하는 신뢰성문제, 보안 문제에 대응하여 '블록체인 기술'의 등장으로 금융권에서는 새로운 금융권 시스템을 도입하고 있다. 블록체인 기술이란 가상화폐를 이용하여 거래를 할 때, 이용자 간에 발생할 수 있는 해킹을 막는 기술로 '공공 거래 장부'라고도 부른다.

다음으로 '중앙집중형 기술'과 '블록체인 기술'의 차이점은 아래와 같다.

| | |
|---|---|
| **중앙 집중형** | 1. 거래 내역을 중앙집중형 서버에 보관한다.<br>2. 발생한 거래내역을 제3자가 알 수 없는 구조이다. |
| **블록 체인** | 1. 거래의 모든 참여자에게 거래내역을 보낸다.<br>2. 거래가 발생할 때마다 거래에 참여한 개개인은 거래내역을 대조하여 거래위조를 방지한다. |

<표 1> 블록체인 기술 비교

## 3. 금융권에서 활용하는 블록체인 기술

### 3.1 금융권에서의 블록체인 기술구조

금융권에서는 개인의 신뢰성을 위해 블록체인의 개념을 '분산원장 시스템'에 도입하여 기관 간 거래 및 정보의 신뢰를 보장 할 수 있게 한다.

분장원장 시스템의 개념은 거래 정보를 기록한 '원장'을 모든 네트워크상의 이용자들에게 분산

하여 기록 관리하는 시스템이다. 이러한 '분산원장 시스템' 이 가지는 가장 큰 장점은 공정성이다. 모든 참가자에게 원장이 공개되므로 정보유출이 원천적으로 봉쇄되며, 중앙 서버가 없기 때문에 내/외부의 조작으로부터 안전하다. 또한 모든 거래에 대한 기록을 공개하므로 거래에 대한 추적이 가능하다.

블록체인 기술은 알고리즘기반으로 '프로그래밍 언어' 이나 '클라우드 컴퓨팅 플랫폼' , C++, 자바(Java), 파이썬(Python), GO 등의 주요 프로그래밍 언어를 지원하여 다양한 형태로 된 대부분의 거래를 프로그래밍 가능하게 설계된 '웹 프레임워크'로 구성되어 있다.

본 연구에서는 ① '비트코인기반 블록체인 플랫폼' ② '이더리움기반의 블록체인 플랫폼' ③ 'R3 Corda 기반의 블록체인 플랫폼으로 구분하여 제시하고자 한다.

### 3.2 비트코인 기반의 블록체인 플랫폼

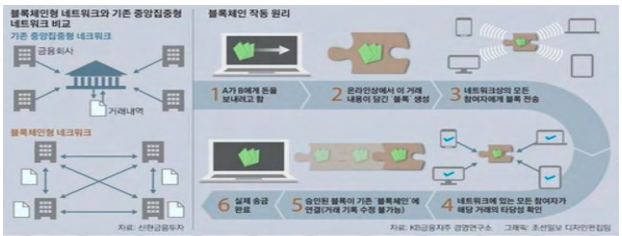
비트코인기반의 블록체인기술은 블록체인 기술을 기반으로 운영되는 '가상화폐'로부터 출발한다.

블록체인은 2008 년 사토시 나카모토에 의해 비트코인(Bitcoin)부터 처음 소개되었으며, 2008 년 10 월 암호화기술커뮤니티 'Gmane' 에 게재된 'Bitcoin: A peer-to-peer electronic cash system' 논문을 통해 제시되었고, 이 논문에서 P2P 네트워크를 이용하여 이중지불을 막는 방법을 제안하면서 블록체인 기술을 설명하였다(Nakamoto, 2008).

비트코인은 특정한 관리와 발행 주체의 부재로 운영되는데, 블록체인에 참여한 사용자들이 주체적으로 화폐를 발행하고 이체내역을 관리할 수 있는 화폐이다.

비트코인 기반의 블록체인 기술원리와 비트코인이 실제로 송금되는 과정이다.

① A 가 B 에게 송금을 시도한다.
② 온라인에서 거래내용이 담긴 블록이 생성된다.
③ 블록이 네트워크 내 모든 참여자에게 전송된다.
④ 네트워크에 속해있는 모든 참여자가 해당 거래의 타당성을 확인하게 된다.
⑤ 승인된 블록이 기존 블록체인에 연결된다.
⑥ 송금이 완료된다.

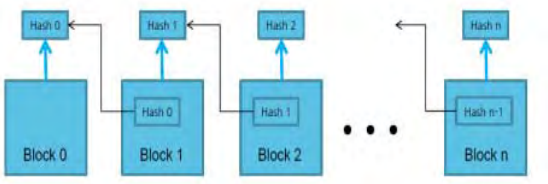


(그림 1) 송금 과정

블록체인 네트워크상에 있는 모든 이용자들에게 거래인증을 받는 원리네트워크에 있는 모든 이용자들에게 거래인증을 받는 원리이다.

① 하나의 블록에는 'Header' 영역과 'Body' 영역으로 나뉜다.
② 'Body' 영역에는 거래 내역이 암호화되어 작성되어 있다.
③ 'Header' 영역에는 아래와 같은 정보가 저장되어 있다.
- ✓ 블록버전
- ✓ N-1 번째 블록의 암호화된 Hash 값
- ✓ Body Hash 트리 루트에 대한 Hash (Merkle Root 라고 불린다.)
- ✓ 타임스탬프(Timestamp)
- ✓ 난이도 목표
- ✓ Nonce

④ 위의 'Header' 영역의 정보들 중에서 'N-1 번째 블록의 Hash 값' 이 이전 블록의 암호화 값을 의미한다. 다음 이용자는 이 값을 통해 이전 블록이 변조되지 않은 것을 알 수 있다.




(그림 2) 거래 인증 과정

비트코인 기반의 블록체인 플랫폼을 금융권의 적용 시 장단점은 다음과 같다.

| 구분 | 장점 |
|---|---|
| 자유성과 투명성 | 비트 코인은 다른 화폐에 비해서 우수한 자유성과 투명성을 가진다. 비트코인은 이해관계가 아닌 규칙적인 알고리즘에 따라 생산되고, 생산량도 정확한 예측이 가능하다. |
| 낮은 수수료 | 수수료가 저렴하다. 정해진 비트코인을 송금할 때, 비트코인의 개수와 상관없이 0.0.0.01% 미만의 수수료가 부과된다. |
| Hyper Inflation 대응 | 자국 통화가 단기간에 상승하는 물가 상승 현상에 빠진다고 해도 미리 가상 화폐로 바꾸어 놓으면 자산을 보호라 수 있기 때문이다 |
| 공통의 화폐거래 | 다른 나라에 방문을 하고 실제 화폐로 사용하기 위해서는 해당 국가의 통화로 환을 해야 한다. 비트코인은 가상화폐이기 때문에 모든 국가에서 동일하게 사용할 수 있다. |

<표 2>비트코인 플랫폼의 장점

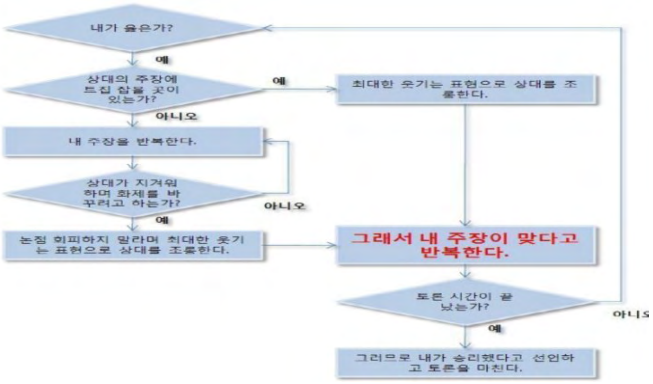
| 구분 | 단점 |
|---|---|
| 가치의 불투명성 | 비트코인의 문제점은 그것이 법정통화는 아니라는 것이다. 그렇다고 해서 실물화폐인 것도 아니다. 때문에 그 가치를 확실하게 알 수 없다. |
| 안전장치의 부재 | 법적인 틀 안에서 조치를 받기 어렵기 때문에 결제상의 실수도 보상받기 어렵다. 예를 들어 비트코인 지갑이 해킹으로 공격을 받은 경우, 이를 되찾을 방법은 없다. |
| 검증시간 | 거래 승인 시간이 상당히 길기 때문에 현금 거래를 대체하기 어렵다. 하나의 블록이 생성되는데 약 10 분의 시간이 소요되기 때문이다. 이는 검증의 수가 많아질수록 무한정 대기하게 되는 최악의 상황이 될 수 있다. |
| 자원 소모 | 비트코인의 특성상 블록체인 네트워크 상의 수많은 해시연산을 기반으로 성립한다. 이 연산은 모두 컴퓨터나 전자 회로에 기반해서 이루어지기 때문에 많은 자원을 소모하게 된다. |

<표 3>비트코인 플랫폼의 단점

### 3.3 이더리움 기반의 블록체인 플랫폼

이더리움은 비탈릭 부테린(Vitalik Buterin)이 개발한 암호화폐(2015 년 7 월 30 일)로써, '튜링완전언어'를 이용하여 조합할 수 있는 가능한 모든 형태의 거래를 프로그래밍할 수 있다. 그리고 신뢰할 수 없는 상대방과의 계약에서 '스마트 컨트랙트(Smart Contract)'의 강제적 성격으로 강력한 힘을 발휘할 수 있다.

튜링완전언어(Turing-Complete Language)를 이용하여 가능한 모든 문제를 계산하여 풀 수 있는 알고리즘을 생성하고, 모든 수학문제를 풀 수 있는 알고리즘을 만들 수 있는 컴퓨팅언어이다.




(그림 3) 알고리즘 흐름도

이더리움 기반의 '스마트컨트랙트'는 자기강제적 언어(Self-Enforcing Language)를 이용하여 컴퓨터언어인 '실행코드'들로 작성한 조건들이 충족이 되면, 자동으로 실행되어 계약이 이행되게 해주는 기술이다.

이더리움 기반의 블록체인 플랫폼을 금융권의 적용 시 장단점은 다음과 같다.

| 구분 | 장점 |
|---|---|
| 코드 신용 | 모든 코드와 실행되는 단계가 같은 네트워크 내에 참여하고 있는 모두에게 공개가 된다. 이로 인해 모든 참여자들은 이더리움 서버의 코드를 신용할 수 있게 된다. |
| 데이터 영구 저장 | 한 번 저장되면 영구적 저장이 가능하기 때문에 중요한 데이터를 저장 가능하다. |
| 스마트 계약 | 미리 프로그래밍된 규칙으로 인해 자동으로 계약을 진행시킬 수 있다. |
| 플랫폼을 통한 응용성(DApps) | 단일 서비스가 아닌 서비스 창조가 가능한 거대한 플랫폼이므로 무한한 응용을 할 수 있다. |
| 튜링 완전성 | 모든 수학문제 풀이 가능한 알고리즘이 가능한 컴퓨터 언어를 사용한다. |

<표 4>이더리움 플랫폼의 장점

| 구분 | 장점 |
|---|---|
| go 언어 | 대중적이지 않은 'go 언어'를 사용하기 때문에 해석에 오랜 시간이 걸린다 |
| 해킹 | DAO 해킹 사례[1]에서 볼 수 있듯이 언어표현의 자유성 보장으로 인한 여러가지 취약점이 발생한다. |

<표 5>이더리움 플랫폼의 단점

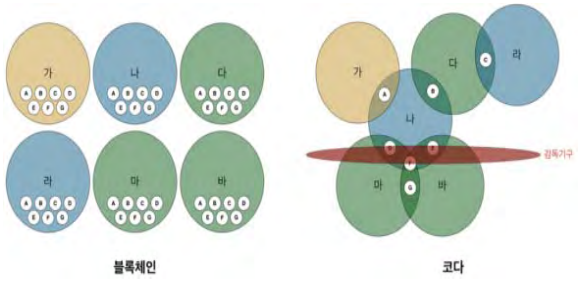
### 3.4 R3 Corda 기반의 블록체인 플랫폼

핀테크 스타트업이자 80 여 개 이상의 금융사가 참여하는 글로벌 분산원장 컨소시엄의 운영주체인 R3 의 분산원장 기술이다. R3 Corda 플랫폼의 분산원장 기술은 'Corda'라는 블록체인을 '원장'으로 활용하는 개념인 분산원장기술을 사용한다. R3 는 분산원장인 Corda 와 Corda 플랫폼을 개발하고 R3 컨소시엄간의 프로젝트를 통해 금융서비스를 개발하는 목적이다. 따라서, R3 Corda 는 가상화폐기반이 아니다. R3 Corda 기반의 블록체인 기술이 가상화폐 기술이 아님에도 불구하고, 전세계 금융권이 참여하고 있다는 점에 주목해야 한다.

기존 비트코인과 이더리움 플랫폼과는 다르게 '정보전파'를 통해 A 와 B 의 거래내역을 전혀 관련 없는 C 와 D 에게 전달하지도 않고, 거래 유효검증 요청도 없다. 즉 관련 있는 거래만 참여자에

[1] 방은주, <차세대 가상화폐 이더리움 해킹당해>. 『전자신문』. 2016년 6월 21일

한에서 공유한다.




(그림 4) Corda 와 블록체인의 비교

R3 Corda 기반의 블록체인 플랫폼은 동일한 분산원장 기술에서 공동으로 처리와 독립적으로 운영하는 금융업무에 기본적인 자산(증권 및 현금 등)발행/기록, 고객인증, 타임스탬핑, 규제(AML), 레퍼런스스테디어(Reference Steadier) 등의 블록체인 참여자들 간 공동으로 처리되는 플랫폼이다.

R3 Corda 기반의 블록체인 플랫폼을 금융권의적용 시 장단점은 다음과 같다.

| 구분 | 장점 |
|---|---|
| Transaction | 거래 속도의 증가 |
| 거래검증 | 정확성의 증가와 인적 오류 감소 |
| Fraud | 사기의 기회 감소 |
| 인프라 | 효율성 증진과 인프라비용 감소 |
| 투명성 | 거래의 투명성과 감시가능성 증가 |

<표 6>R3 Corda 플랫폼의 장점

| 구분 | 장점 |
|---|---|
| 알고리즘 상이 | 분산원장 기술 별로 환경이 달라 공개와 비공개, 가장 적절한 합의 방법과 그에 따른 에너지 소모 등에 차이 존재 |
| ROI | 분산원장의 규모성과 현존 솔루션 간의 경합 능력이 불확실 |
| 호환성 | 분산원장 기술 별이나 현존 비 분산원장 기술과의 호환성이 검증되지 않아 현존 시스템의 혁신위험과 내부부서 간 승인 및 책임 문제 존재 |

<표 7>R3 Corda 플랫폼의 단점

## 참고문헌

[1]허세영 외 2 명 / 비트코인 후 블록체인

[2] Moody's Investor Service, Credit Strategy-Blockchain Technology: Robust,Cost-effective Applications Key to Unlocking Blockchain's Potential Credit Benefits,2016.7

[3]네이버 지식백과

## 출처

[1]https://www.posri.re.kr/files/file_pdf/63/14417/63_14417_file_pdf_1480992336.pdf

[2]https://ko.wikipedia.org/wiki/%EC%9D%B4%EB%8D%94%EB%A6%AC%EC%9B%80

[3] https://blog.iwanhae.ga/introduction_of_bitcoin/

[4]http://biz.chosun.com/site/data/html_dir/2016/08/25/2016082500393.html

[5]http://www.seunghwanhan.com/2015/06/ethereum-introduction_3.html

[6]http://cafe.daum.net/_c21_/bbs_search_read?grpid=1X3I5&fldid=G2cb&datanum=5&q=%BA%F1%C6%AE%C4%DA%C0%CE%C3%A4%B1%BC%B7%AE&_referer=V7kfJwkeLEGMZxGlgqZEmapjMR25_wbDRn4r.WZEI6ctm3ShzX-OCLQn6XEXVVZJTz1Idm4evg88ZbRsafiT_g00

[7]http://www.mobiinside.com/kr/2017/06/21/blockchain-part2

[8] https://brunch.co.kr/@jeffpaik/27

[9]https://blog.theloop.co.kr/2017/01/26/%EC%99%9C-%EA%B8%88%EC%9C%B5%EA%B6%8C%EC%97%90%EC%84%9C%EB%8A%94-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%97%90-%EC%A3%BC%EB%AA%A9%ED%95%A0%EA%B9%8C/, https://blog.theloop.co.kr/

[10]https://blog.theloop.co.kr/2017/01/26/%EC%99%9C-%EA%B8%88%EC%9C%B5%EA%B6%8C%EC%97%90%EC%84%9C%EB%8A%94-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%97%90-%EC%A3%BC%EB%AA%A9%ED%95%A0%EA%B9%8C/, https://blog.theloop.co.kr/

[11]http://terms.naver.com/entry.nhn?docId=2838482&cid=43667&categoryId=43667

[12] 국무총리훈령 제 661 호 '금융규제 운영규정'

[13] https://brunch.co.kr/@jeffpaik/22