분산원장 기술의 현황 및 주요 이슈

2016. 12

이 자료의 내용은 공동 집필자 개인의견으로 한국은행의 공식견해가 아니라는 점을 밝힙니다.

한국은행 금융결제국

머리말

최근 국내외 금융권을 중심으로 블록체인(Blockchain) 또는 분산원장 기술(DLT : Distributed Ledger Technology)에 대한 높은 관심이 이어지고 있습니다. 금융기관과 IT기업들의 적극적인 연구와 투자에 힘입어 동 기술을 금융서비스에 적용하기 위한 방안들이 빠르게 구체화되고 있습니다. 주요국 중앙은행과 BIS 등 국제기구에서도 이같은 흐름에 큰 관심을 갖고 다양한 연구와 논의를 활발히 진행하고 있습니다.

한국은행도 2016.1월 「분산원장 기술과 디지털통화의 현황 및 시사점」을 지급결제조사자료로 발간한 바 있습니다. 하지만 이후 빠른 여건 변화를 반영하여 보다 심도 있는 후속연구를 추진할 필요성이 높아짐에 따라 한국은행은 2016년 4월부터 6개월간 IT기업, 학계, 금융권 전문가들과 함께 공동연구를 통해 분산원장 기술의 현황 및 주요 정책적 이슈를 종합적으로 짚어보았습니다.

이번 공동연구에서는 최근의 분산원장 기술 개발 현황을 상세하게 비교·소개하였습니다. 또한 국내 최초로 분산원장 기술 적용에 따른 비용절감 효과를 정량적으로 추정해 보았습니다. 아울러 한은금융망 등 주요 지급결제서비스에 분산원장 기술을 구현하기 위한 기술적 방안도 제시하였습니다. 이같은 연구 결과는 금융기관 및 정책당국들이 분산원장 기술 관련 조사연구 및 장기적인 전략 수립시 참고자료로 활용되는 한편 향후 금융기관들이 분산원장 기술 기반 시스템과 서비스를 개발하는 데도 큰 도움이 될 것으로 기대됩니다.

아직 분산원장 기술이 빠르게 발전중이고 관련 연구가 초기에 머물고 있어 이번 공동연구 이후에도 지속적인 연구 및 기술의 활용방안에 대한 노력이 필요합니다. 아무쪼록 이 책자가 분산원장 기술을 연구하거나 금융서비스에 활용하려는 모든 분들에게 유용한 기초자료가 되어 우리나라 지급결제 및 금융시스템 발전에 기여할 수 있기를 바랍니다.

2016.12월

한국은행 금융결제국장 **박 이 락**

공동연구 참가자 명단

	직·성명	소 속	비 고
한국은행	김동섭 과장	금융결제국 결제연구팀	공동연구 주관
	김형주 과장	전산정보국 신회계결제시스템팀	
학계	오세경 교수	건국대 경영	정책적 이슈(Ⅰ부) 집필
	이영환 교수	건국대 기술경영	
	김재필 교수	순천향대 IT금융경영	
	권혁준 교수	순천향대 IT금융경영	
IT기업	송주한 CSO	㈜코인플러그	기술적 이슈(Ⅱ부) 집필
	정혜경 이사		
	박승비 매니저		
은행	송상희 대리	기업은행 핀테크사업부	블록체인 워킹그룹(WG)[1]
	박문수 대리	KB국민은행 스마트전략부	
	최종윤 차장	신한은행 DI 센터	
	강명남 차장	우리은행 핀테크사업부	
	김성진 과장	농협은행 핀테크사업팀	
	전경민 과장	하나금융지주 미래금융지원팀	
유관기관	박정국 팀장	금융결제원 금융결제연구소	
	이한욱 전문연구역	금융결제원 금융결제연구소	

주: 1) 공동연구기간중 보고서 집필진과 대면회의를 통해 각 은행의 분산원장기술 활용 전략과 현황을 소개하고 주요 기술 및 정책 이슈에 대한 금융권의 입장 및 의견을 보고서에 반영

목 차

<요약>

제1부. 정책적 이슈

<제1부 그림 및 표 목차>

제2부. 기술적 이슈

<제2부 그림 및 표 목차>

<그림 1-1> 바클레이스와 시연한 코다 소개 영상 ····· 173
<그림 1-2> 하이퍼레저 익스플로러 시연 자료 ····· 174
<그림 1-3> SBI 핀테크 컨소시엄 가입 회원들 ····· 175
<그림 1-4> 이더리움 기반 크라우드펀딩 플랫폼 The DAO ····· 178
<그림 1-5> 리플의 시스템 구조 ····· 180
<그림 1-6> JP모건의 예상 블록체인 도입 4단계 ····· 185
<그림 1-7> 마이크로소프트의 블록체인 서비스 BaaS ····· 192
<그림 1-8> Overstock의 주식 거래 플랫폼 t0 ····· 194
<그림 2-1> 개방형 블록체인 ····· 198
<그림 2-2> 비트코인의 거래 절차 ····· 199
<그림 2-3> SHA-256 암호기법 ····· 200
<그림 2-4> 비트코인 통화 공급량 ····· 201
<그림 2-5> 블록 헤더의 구성도 ····· 202
<그림 2-6> 암호 화폐의 자본 규모 순위 (10월 기준) ····· 208
<그림 2-7> 컬러드 코인의 전개 ····· 209
<그림 2-8> 아브라의 개방형 블록체인 활용 구조도 ····· 212
<그림 2-9> 앵커링 구조도 ····· 213
<그림 2-10> 금융 기관의 분산 원장 활용 케이스 ····· 219
<그림 3-1> 분산데이터베이스의 예시 (Master/Standby 형태) ····· 228
<그림 3-2> 동등한 레벨의 데이터베이스 유형 ····· 229
<그림 3-3> 해시함수 동작 원리도 ····· 230
<그림 3-4> 머클 트리의 구조도 ····· 231
<그림 3-5> 공개키 암호화의 과정 ····· 232
<그림 3-6> 공개키 기술 전자서명의 과정 ····· 233
<그림 3-7> 클라이언트-서버 구조와 P2P 구조의 비교 ····· 235
<그림 3-8> PBFT 기반 합의 알고리즘 ····· 237
<그림 3-9> 토큰 기반 블록체인 지급결제시스템 흐름도 ····· 238
<그림 3-10> 토큰의 발행자와 사용자간의 블록체인의 구성도 ····· 240
<그림 3-11> 사용자 인가 및 등록 절차 ····· 241
<그림 3-12> 토큰 발행 절차 ····· 242
<그림 3-13> 토큰 사용 절차 ····· 243
<그림 4-1> RS코인의 개괄적인 구조도 ····· 258
<그림 4-2> 하위 단계 블록의 거래 승인 절차 ····· 259
<그림 4-3> 비트코인 네트워크에서 노드들의 역할 ····· 262

<표 1-1> 국내 블록체인 도입 동향 (가나다 순) ····· 186
<표 2-1> 개방형, 폐쇄형 블록체인 비교표 ····· 197

요 약

Ⅰ 정책적 이슈

(1) 기대효과 분석

(비용절감)

□ 분산원장 기술의 높은 보안성과 효율성 및 결제 신속성 등을 바탕으로 금융서비스 적용시 큰 폭의 **비용절감 효과**를 기대

분산원장 기술 비용절감 요인

구 분	절감 요인
IT시스템	응용기술 개발비용 절감
	인프라 장비조달 비용 절감
	중간구조 개발비용 절감
경영측면	회계감사 비용 절감
	종이서류 관리비용 절감
	노동비용 절감

□ 해외 선행연구(골드만삭스(2016) 등)를 참고하여 **증권부문**(거래소 및 예탁원)에서 **백오피스 비용(IT비용, 인건비 등)** 절감 효과를 **연간 1,071억원(총비용 대비 16%)** 내외로 추정 가능(2015년 기준)

— 이외에도 증권사들의 **금융비용(예치금 등에 따른 기회비용)** 절감 효과가 연간 총 100억원 규모에 이를 것으로 추정

증권부문 백오피스 비용감소 추정(2015년 기준)

(단위 : 억원)

	한국거래소	한국예탁결제원
총비용	5,508	1,188
순수 IT 비용	1,186	70
복리후생 등 인건비	2,351	605
판관비	1,971	513
비용 감소 효과	△881	△190

□ 다만 은행 등 타부문은 서비스가 광범위하고 프로세스의 구획 및 비용 구분이 명확하지 않아 비용절감 효과의 정량적 추정이 곤란

— 구체적인 송금, 인증 등 **서비스별**로 **금융기관 비용절감** 및 **소비자의 직간접적 비용절감** 효과를 세분화하여 추정할 필요

(금융인프라 변화)

□ 분산원장 기술은 **중장기**적으로 **탈중개화**, **자동화** 등을 통해 금융인프라에 **구조변화**를 초래할 것으로 예상

부문별 금융인프라 구조변화

구 분	구조변화
국제송금	■ 중개은행 및 SWIFT 등 기존 인프라를 분산원장 시스템이 대체(Ripple 등)
자본시장	■ 증권의 발행, 등록, 거래 등이 크게 효율화되고 기존 중개기관의 기능 축소
무역금융	■ 기존 수작업으로 이루어지던 무역금융 절차가 자동화되어 효율성이 높아지고 사고발생 확률이 감소
규제준수 및 감사	■ 거래데이터의 실시간 보고, 감사가 가능해지고 기관간 비교 및 통합이 용이
AML/CFT	■ 고객신원정보의 공유가 용이해지고 규제준수비용 절감
보험	■ 보험금 청구 및 지급이 자동화되고 보험사기 위험 감소
P2P대출 및 보험	■ 마이크로파이낸스 및 마이크로보험 활성화

(2) 리스크 및 규제방안

(디지털통화)

□ 디지털통화는 **익명성**, **기술적 불완전성** 등으로 **자금세탁 등 범죄에 악용**되고 있어 규제 필요성이 증대

— 최근 **미국**, **EU**, **일본** 등 주요국을 중심으로 디지털통화에 대한 규제가 도입중

국가별 규제 도입

구 분	규제 도입
미 국	■ FinCen(2013): 거래소 등에 자금세탁방지규제 적용 ■ 국세청(2014): 디지털통화에 재산세 부과 ■ 선물거래위원회(2015): 비트코인 파생상품 감독 시행 ■ 뉴욕주(2015): 비트라이센스(BitLicense) 도입
E U	■ 은행감독청(2013): 디지털통화 소비자 주의 경고 ■ 유럽위원회(2016): 거래소 등에 자금세탁방지규제 적용
일 본	■ 금융청(2016) 등: 거래소 등에 규제를 적용하고 비트코인 매매시 소비세를 비적용 검토

(분산원장 기술)

□ 분산원장 기술 적용시 **기존 금융시스템의 리스크가 상당 부분 완화**될 것으로 기대

— 금융거래가 실시간으로 안전하게 처리됨에 따라 **상대방리스크**, **운영리스크** 등이 획기적으로 축소

— 거래내역 등에 대한 실시간 파악이 가능해지고 규제준수가 자동화되는 등 **규제기술(RegTech) 적용**이 용이해짐으로써 **리스크를 보다 효과적으로 관리** 가능

□ 하지만 분산원장 기술 도입으로 새롭게 발생하거나 증대될 리스크 요인에 대한 점검이 필요

— 특히 **보안 리스크**, **법적 리스크** 등이 높아질 가능성이 크며 **스마트계약이 분산원장에 결합**되면서 발생 가능한 리스크▪에도 유의

■ 스마트계약시 프로그래밍 오류 발생 및 DDoS 공격에 의한 스마트계약 무효화 시도 등

(규제방안)

□ 금융당국의 규제는 다음과 같은 **원칙** 하에서 이루어지는 것이 바람직

① **혁신**을 저해하지 않는 동시에 **리스크**에 적절히 대처

② 디지털통화 및 분산원장 기술 **변화**에 **유연**하게 대응

③ **비즈니스 모델**에 내재하는 사업구조를 감안하여 규제체계를 마련

④ **시장교란행위**를 제재하고 관련 사업자의 **건전성**을 유도

□ 한편 분산원장 기술 상호간 연결성, 웹 애플리케이션 개발, 산업간 광범위한 활용 인프라 구축을 위해 **기술 표준화 방안**을 고민할 필요

(3) 중앙은행 디지털통화 발행

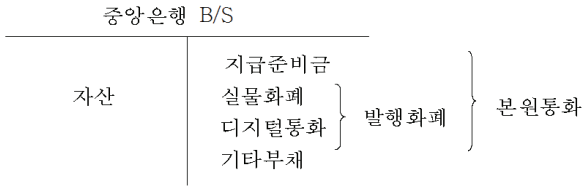
□ 최근 주요국 중앙은행에서 활발히 논의되고 있는 주제인 **중앙은행 디지털통화 발행**은 경제적 영향에 대해서는 종합적인 검토가 필요

— 중앙은행이 분상원장기술을 활용하여 직접 **개인 및 비금융기업**을 대상으로 **디지털통화**를 **발행**하는 경우

실물화폐를 대체하는 수준을 넘어 **기존 상업은행 예금과 경쟁**하면서 거시경제, 통화정책, 금융안정, 지급결제 등에 **광범위한 영향**을 미칠 가능성

— 중앙은행 디지털통화 발행시 상업은행 예금을 대체하는 규모는 **결제기능 부여 정도**, **익명성 보장여부**, **이자지급 여부** 등에 따라 결정

중앙은행 발행 디지털통화의 개념



□ 현재까지는 분산원장 기술 기반의 디지털통화 발행 사례가 없어 **시스템의 안정성 및 보안성에 대한 검증이 불완전**한 상황

— 따라서 주요국 중앙은행 개발 사례를 모니터링하면서 관련 기술에 대한 검증과 안전성을 확보하기 위한 연구와 개발을 지속 추진할 필요

— 또한 중앙은행 디지털통화 발행 대상, 발행 방식 등에 대한 다양한 시나리오별 검토와 함께 법규, 제도 등의 측면에서 다각적인 연구가 이루어질 필요

Ⅱ 기술적 이슈

(1) 기술개발 현황

(컨소시엄 등)

□ 블록체인은 **분산형 네트워크**를 기반으로 운영되는 플랫폼이기 때문에 주로 다수의 금융기관과 IT기업들은 **컨소시엄**을 구성하여 공동으로 분산원장 기술을 개발중

주요 글로벌 분산원장 기술 컨소시엄

컨소시엄	참가기관	주요 특징
R3	■ 미국 IT기업 R3사 설립 ■ 골드만삭스, UBS 등 60여개 대형 금융기관 ■ 국내 5개 은행(국민, 신한, 하나, 기업, 우리)	■ 금융기관 계약 기록관리 시스템(Corda) 개발
HyperLedger	■ 리눅스재단이 관리 ■ 금융기관 및 비금융 IT기업 등 100여개 기업 ■ 국내 기업(한국예탁결제원, 코인플러그, 삼성SDS)	■ 오픈소스 ■ 범산업용 블록체인 플랫폼을 연구 개발
SBI 핀테크 컨소시엄	■ 일본 SBI 금융그룹 주도 ■ 리플, 코인플러그 등 참여	
차이나레저	■ 중국 완샹 블록체인 랩 주도 ■ 중국 11개 대형 금융기관 참여	■ R3와 이더리움 재단 자문

□ 이와 함께 **이더리움**, **리플** 등과 같이 기존 비트코인 블록체인의 문제점을 개선한 새로운 **블록체인 프로토콜**을 개발하기 위한 시도도 활발히 진행중

주요 블록체인 프로토콜

프로토콜	특 성	현 황
이더리움	■ 스마트계약에 특화 ■ 거래체결시간 단축(12초)	■ 가상화폐(ETH) 발행 ■ 해킹사고(DAO) 발생
리플	■ 국가간 송금에 특화 ■ 실시간 결제-청산 시스템	■ 가상화폐(XRP) 발행

(부문별)

□ **금융기관**, **IT기업**, **중앙은행** 및 **정부** 등은 분산원장 기술을 활용하여 기존 인프라의 효율성을 개선하거나 새로운 서비스를 개발하기 위한 방안을 적극 추진중

부문별 주요 분산원장 기술 활용 사례

부문	활용방안	사례
금 융	■ 해외송금	■ MUFG, VISA, JP모건 등
	■ 본지점 송금	■ UBS, 도이체방크 등
	■ 자본시장 거래(장외시장 등)	■ 나스닥, Overstock 등
	■ 기록관리	■ 미즈호 등
	■ 백오피스	■ MUFG(약속어음) 등
중앙은행	■ 디지털화폐 발행	■ 영국, 네덜란드, 캐나다
정 부	■ 연금수령 및 사용내역 기록	■ 영국
	■ 주민등록 및 투표	■ 에스토니아, 러시아 등
	■ 토지소유권 등록	■ 스웨덴
IT기업 등	■ 정품 등록(귀금속, 시계 등)	■ 에버렛저(Everledger)
	■ 기반기술 개발	■ IBM, Microsoft

(2) 유형별 분산원장 기술 특성

□ 분산원장 기술은 운영방식에 따라 **개방형(Public) 블록체인**과 **폐쇄형(Private) 블록체인**으로 구분

분산원장 기술 유형별 비교

	개방형(Public)	폐쇄형(Private)
기록열람・보관 거래참여・승인	누구나 제한없이 참여 가능	필요에 따라 임의로 제한 가능
합 의	작업증명, 지분증명 등	BFT(Byzantine Fault Tolerance)
암호화폐	필요	불필요
결제완결성	네트워크 분기 가능성	시스템상 완결성 보장
확장가능성	제한적	자유로움
사 례	비트코인, 이더리움 등	R3, 하이퍼레저 등
장단점	⬆ 높은 안전성과 신뢰성 ⬆ 높은 투명성과 익명성 ⬇ 금융거래 비밀 유지 곤란 ⬇ 낮은 확장성과 효율성	⬆ 정보공유범위 설정 가능 ⬆ 높은 효율성과 확장성 ⬇ 보안성 취약
활용 분야	해외송금, 크라우드펀딩, 자산 및 정보 기록・보관	결제시스템, 신원・문서인증, 무역금융, 스마트계약 등

(3) 활용방안

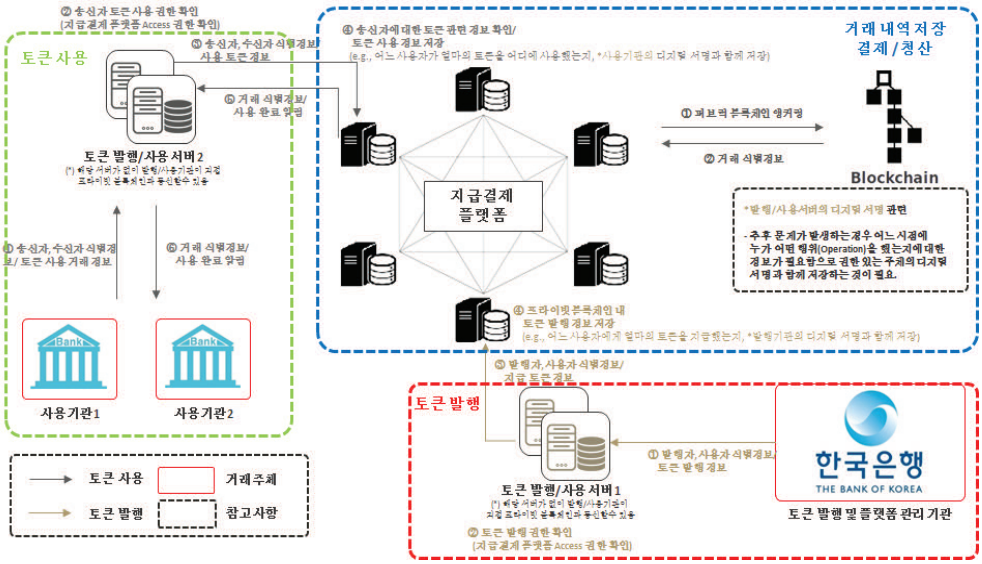
□ 분산원장 기술을 금융서비스에 활용하기 위해서는 **거래 비밀성** 유지, **권한 통제**, **신뢰 및 보안성** 유지, **확장성** 확보 등의 **기술적 과제**를 해결할 필요

— **시험적으로 신한은금융망에 분산원장 기술을 적용**하는 상황을 전제하여 각 과제에 대한 **해결방안**을 검토하고 구체적인 구현 방안을 제시

분산원장 기술의 금융서비스 활용을 위한 기술적 과제

과 제	해결방안
프라이버시	■ PKI based Key Exchange - 중앙관리자(Supernode)가 필요 - 중앙관리자 및 거래당사자만 거래정보 접근 ■ Confidential Transactions (예: Hyperledger) - 분산형 시스템에 적용 가능 - 익명성을 유지하고 거래당사자만 거래정보 접근
권한 통제	■ 중앙관리자(Supernode: Token Issuer)와 여타 참가자(Token User)로 구분
신뢰성 확보	■ 주기적으로 분산장부의 해쉬값(Merkle Root)을 개방형 블록체인(비트코인)에 기록
확장성	■ 초당 3,000건 이상의 거래 처리 가능

분산원장 기술을 이용한 지급결제시스템 구성도



제1부. 정책적 이슈

Ⅰ. 디지털통화와 분산원장 기술의 개요

1. 디지털통화의 분산원장 기술의 정의와 구분

가. 디지털통화의 정의

디지털통화는 통상적으로 가치를 전자적으로 표시한 통화를 지칭한다. 예컨대 싸이월드의 도토리처럼 법정통화로 표시되지 않았거나 혹은 페이팔 서비스에서처럼 실제 법정통화의 가치로 표시되었거나를 막론하고 전자적인 형태로 표시된 모든 화폐를 포함한다.

나. 디지털통화의 구분

디지털통화는 법정화폐 금액으로 표시된 통화와 법정화폐 금액으로 표시되지 않은 통화로 나누어지고 법정화폐 금액으로 표시되지 않은 통화를 가상통화라고 지칭한다. 2009년 비트코인을 필두로 다수의 민간 가상화폐가 등장하였다. 최근 각국의 중앙은행들은 디지털통화를 직접 발행하는 방안에 대해 활발한 논의와 연구를 진행하고 있다.

<그림 1-1>에서 보듯이 국제통화기금(IMF)은 가상통화에 대한 최근 보고서에서 빠르게 진화하는 산업의 속성상 보편적인 정의가 만들어진 적도 없고 설혹 만들어진다고 해도 가상통화의 생태계가 지속적으로 변화하는 까닭에 곧 바뀔 수 있다는 전제 위에서 다음과 같이 정의하였다.

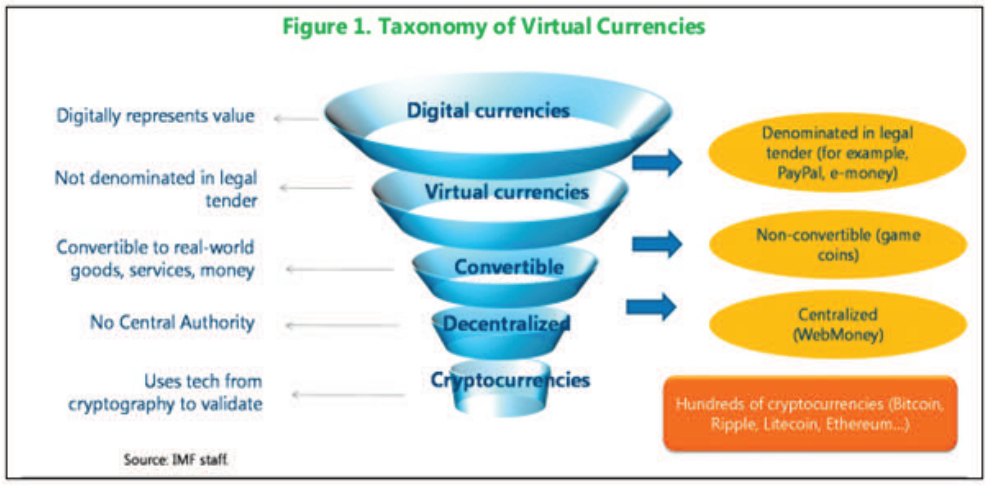
“가상통화는 민간 개발자가 발행한 그 나름의 이용방법에 맞게 정한 단위액수를 붙인 가치의 디지털 표현이다. 가상통화는 전자적으로 획득하고 저장하고 접근하고 거래할 수 있고 또한 거래당사자 동의하에 다양한 목적을 위해 사용될 수 있다. 가상통화의 개념은 인터넷 혹은 모바일 쿠폰이나 비행기 마일리지까지 포함하는 단순한 형태의 쿠폰부터 금과 같은 자산에 의해 보증되는 가상화폐 등을 포함하여 비트코인처럼 암호화통화(Crypto-currency)까지 다양한 형태를 포함한다.”

가상통화는 다시 실생활에서 실제로 상품이나 서비스 혹은 화폐로 교환될

수 있는 교환가능(Convertible) 통화와 교환불가능(Non-convertible) 통화로 구분된다. 교환 불가능한 통화는 사이버 상에서만 사용될 수 있는 도토리나 게임머니 등이 있다.

교환가능 통화는 다시 중앙집중식 통화와 탈중앙집중식 통화로 구분된다. 중앙집중식 통화는 페이팔 등 이커머스 기업들이 사용하는 이머니(e-money)가 있다. 탈중앙집중식 통화는 암호화 기술을 사용하여 유효성을 인증하게 되는데 이것이 암호화 통화(Crypto-currency)다. 암호화 통화는 대부분의 경우 흔히 블록체인(Blockchain)으로 불리는 분산원장 기술(Distributed Ledger Technology; DLT)을 활용하여 그 가치를 저장하고 유통하게 된다.

<그림 1-1> 가상화폐의 종류



자료: IMF보고서

2. 디지털통화와 분산원장 기술의 발전 단계 및 장단점

가. 분산원장 기술 설명

분산원장은 인터넷에서 서로 알지 못하는 다수의 상대방과 거래를 할 때 중개기관의 개입없이 서로 신뢰할 수 있도록 만들어주는 탈중앙화된 정보공유 저장기술(Decentralized shared-information storing technology)이다.

분산원장 기술의 혁신적인 차이점은 전통적인 중앙집중형 금융시스템과 비교하면 쉽게 알 수 있다. 기존 금융시스템은 원장(Ledger)을 집중 관리하는 신뢰할 수 있는 제3의 기관을 설립하고 해당기관에 대한 신뢰를 확보하여 금융거래를 하는 방식으로 발전해 왔다. 특히 온라인 금융시스템에서는 페이팔과 같은 제3의 사업자가 거래자에 대한 신상정보 및 잔액 등의 장부를 관리하고 이용자는 수수료를 지급했다. 하지만 신뢰할 수 있도록 제3의 기관을 설립하고 운영하는 비용이 매우 높아서 금융산업 발전의 제약 요인으로 작용해 왔다. 이러한 신뢰 비용이 사용자들의 부담으로 고스란히 전가되는 폐단이 있었다. 분산원장 기술은 사용자간 상호 신뢰를 할 수 있도록 설계된 시스템이다.

이를 위해 분산원장 기술은 모든 개인 간의 거래를 포함하는 원장을 모든 구성원이 갖고 있는 분산저장 시스템을 구현했다. 어떤 순간이고 모든 구성원이 같은 장부를 갖고 있는 것을 입증할 수 있다면 이를 조작하는 것이 사실상 불가능하여 신뢰할 수 있다. 이를 위해 특정시간 단위로 블록이라는 단위의 거래장부를 생성하고 이를 모든 구성원에게 전송하여 다수의 구성원이 거래타당성을 검증하고 전송된 블록의 유효성을 승인할 경우 모든 구성원이 각자 분산관리하는 원장 즉 기존의 블록더미에 새로운 블록을 체인형태로 연결한다. 이렇게 해서 모든 구성원이 같은 분산원장을 갖게 한다.

이렇듯 분산원장으로 설계되고 구현된 시스템은 공통의 장부를 관리하는 다수의 네트워크 참여자가 거래 타당성을 검증하고 이를 승인해야 거래가 성립된다. 이 시스템은 중앙권위기관(Central Authorized Institution)의 개입 없이 사용자 간(P2P, Peer-to-peer) 직접적인 금융거래가 가능하도록 참여자들에게 상호 신뢰를 주도록 정책적인 장치가 설계되어 있다. 그것은 원장 무결성 확보정책, 참여자간 합의정책, 화폐 발행정책, 거래장부 동기화정책으로 설명은 다음과 같다.

○ 원장 무결성 확보 정책 : 분산되어 관리되는 장부의 무결성을 확보하기 위해 분산원장은 모든 참여자(node/peer)가 같은 원장을 보관하고 새로운 거래가 일어날 때마다 똑같이 업데이트를 함으로써 무결성을 유지한다. 일단 기존의 결제기록에 새로운 결제기록이 추가되어 블록으로 묶이고 나면 되돌릴 수 없도록 비가역적으로 운영된다.

○ 참여자간 합의 정책 : 참여자들이 상호 간(間) 거래내역을 전송하기 위해 보증수단이 필요하다. 이를 위해 분산원장 시스템에는 가치 전송을 요청한 당사자를 제외한 불특정다수에게 거래에 대한 검증을 하도록 한다. 거래에 대한 검증 권한을 갖고 있는 네트워크 참여자들은 해당거래의 정당성을 검증하고 다수의 승인결과를 시스템 내에서 종합하여 정당한 거래임을 검증하게 된다. 이때 검증 권한을 가진 참여자가 다수가 되면 거래는 정당한 것으로 인정받게 되고 이것이 검증된 블록이 분산장부에 기록되면 거래가 완결된다.

○ 화폐 발행 정책 : 분산원장을 이용한 가상통화 시스템은 화폐 발행을 어떻게 얼마나 할 것인가 정책을 제정하고 이를 시행하는 것이 필수적이다. 예컨대 비트코인의 경우 참여자들에 의해 합의된 문제를 풀고 이를 증명하면 화폐를 새로 발행하여 소유할 수 있도록 허가하는 정책을 쓰고 있다. 이때 문제가 풀렸다는 것을 다수가 합의하면 블록은 공식 인정되도록 되어 있다. 이 방식은 컴퓨팅 파워가 높은 시스템을 소유한 참가자가 문제를 쉽게 풀게 되어 있으므로 소수의 채굴자가 코인을 독점할 수도 있다는 단점이 있다. 비트코인의 이런 단점을 보완하기 위해 리플코인 등 몇몇 가상화폐들은 미리 참여자에게 정해진 양의 화폐를 나누어주는 정책을 사용하기도 한다.

○ 거래장부 동기화 정책 : 탈중앙 분산장부 시스템의 정상적인 작동을 위해서는 검증권한을 가진 참여자들이 거래를 요청한 주체의 최근 거래내역 및 일련의 정보를 동일하게 가지고 있어야 한다. 그러나 여러 가지 이유로 해서 시스템들이 형태가 다른 장부를 가지고 있을 수 있다. 이를 분기(Fork)되었다고 하는데 이때 각 참여자들은 블록(노드)이 많이 형성된 가지를 많은 것을 진본으로 간주하게 된다.

나. 분산원장 기술과 시스템의 구분

분산원장 기술은 계속 진화하고 있고 수많은 가상통화가 유통되고 있는데 이를 구분하는 방법은 여러 가지가 있다. 그 중 가장 대표적인 것은 참가자들의 자격을 제한하는 정도에 따라 퍼블릭과 프라이빗 분산원장 시스템으로 나뉜다.

퍼블릭 분산원장 시스템은 다른 참가자들의 허용 없이 누구나 분산원장에 읽고 쓸 수 있기 때문에 '퍼블릭'이다. 누구도 그 권한을 부여받거나 부여하지 않는다. 반면 '프라이빗' 분산원장 시스템은 미리 정해진 참여자만이 네트워크에 접속하여 정해진 권한만을 이용하거나 행사하게 된다.

(1) 퍼블릭 분산원장 시스템

퍼블릭 분산원장 시스템은 누구나 원하기만 하면 네트워크에 접근하여 거래내역을 읽거나 제출하거나 또는 거래를 검증하고 생성할 수 있도록 한다. 이런 시스템에서의 블록체인은 경제적인 인센티브를 동반하는 작업증명(Proof of Work)이나 지분증명(Proof of Stake) 등의 수단을 사용한 암호 검증으로 안전성이 보증된다. 일반적으로 퍼블릭 분산원장은 참여자들이 익명으로 참여할 수 있도록 되어있고 거래를 검증하거나 참여자간의 합의를 도출하는 등 블록체인을 유지하기 위해 참여자들에게 통화의 발행이라는 인센티브를 제공한다. 예로는 비트코인, 이더리움 등 암호화통화가 있다.

(2) 프라이빗 분산원장 시스템

프라이빗 분산원장에는 개별 기업이 운영하는 분산원장시스템과 컨소시엄이 운영하는 분산원장시스템이 있을 수 있다. 개별 기업이 자신의 원장관리를 위해 운영하는 시스템은 중앙의 서버가 개별 참여자의 접근과 권한을 승인하는 시스템이다. 대표적인 애플리케이션으로는 항공회사의 분산 데이터베이스 관리 시스템이 있다. 항공사는 전세계의 여행사와 연동하여 고객데이터와 탑승 스케줄 등을 관리한다. 일반적으로 특정 기업이 사용하는 이러한 분산 시스템은 거래를 하거나 혹은 거래검증을 위한 시스템을 운영하거나 참여자간의 합의를 도출하거나 하는 프로세스를 만들거나 내부 화폐를 발행할 필요가 없다. 따라서 우리의 논의에서는 제외한다.

다수의 기업 혹은 컨소시엄이 운영하는 프라이빗 분산원장 시스템은 미리 지정된 개인이나 단체가 참여자간의 합의 프로세스를 검증하는 권한을 갖는다. 예컨대 금융기관의 컨소시엄 등이 운영하는 분산원장 시스템은 참여자가 제한되고 이들의 권한과 접속이 제한되는 형태로 운영된다. 따라서 부분적 탈중앙화된 시스템이다. 이 형태는 특히 금융기관들이 선호하는 시스템으로

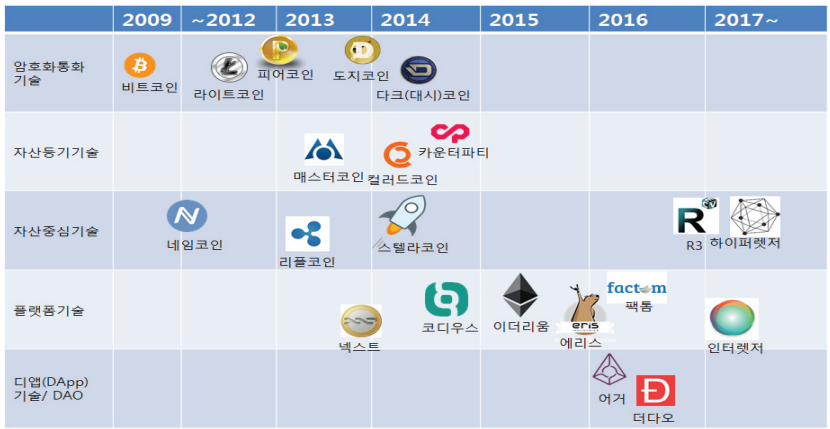
사용자들의 아이디는 고객확인제도(흔히 업무파악의무와 고객파악의무로 지칭되는 금융기관의 의무 사항)를 따르는 것이 필수 사항이 될 수 있다.

다. 분산원장 기술의 발전단계

2015년 분산원장이 기술적으로 어떻게 발전해 왔는지에 대해서는 다소의 의견이 차이가 있다. EBA는 분산원장 기술은 지난 2009년 이후 4가지 범주로 분화되어 진화해 왔다고 했고 그 범주는 암호화폐, 자산등기기술, 애플리케이션스택, 자산중심기술이다.[1] 피넥터 보고서는 분산원장 기술이 암호화폐. 자산발행기술, 자산중심기술, 응용플랫폼, 허가형분산원장의 5가지로 진화해 왔다고 했다.

본 연구자는 분산원장은 암호통화기술(Currencies), 자산등기기술(Asset Registry), 자산중심기술(Asset Centered), 플랫폼기술(Application Platforms), 디앱(Dapp; Decentralized Application; 탈중앙애플리케이션) 기술과 DAO (Decentralized Autonomous Corp.; 탈중앙자율법인)로 진화해 왔다고 본다.

<그림 1-2> 분산원장 발달과정



(1) 암호화통화기술(Crypto-currencies)

초기 분산원장 기술은 비트코인을 필두로 라이트코인(LiteCoin), 피어코인(PeerCoin), 도기코인(DogeCoin) 등 암호화통화의 가치보존과 유통을 위해

설계되었다. 분산원장은 신뢰할 수 없는 익명의 다수가 참여하는 네트워크에서 신뢰할 수 있도록 수학적 알고리즘에 의해 설계된 점은 큰 장점이었다. 또한 임의조작이 불가능하도록 고안되었고 암호화되었으므로 지급결제 수단으로서 법정화폐(Fiat Currencies)처럼 안전하게 유통시킬 수 있다. 다만 보통의 법정화폐가 갖는 법적인 지위는 갖지 않지만 동시에 규제와 감독의 대상이 아니라는 점은 장점이자 동시에 단점으로 생각될 수 있다.

아직 암호화통화의 시장규모는 미미한 정도이고 현재의 비트코인 등에 사용된 블록체인은 법정화폐를 위협할 정도의 사용량은 보이지 않고 있다. 또한 초당 처리할 수 있는 거래건수 등의 확장성 등 내재하는 기술적인 한계로 인하여 지금까지 개발된 암호화통화는 성장가능성이 다소 의문시 되고는 있다. 그러나 지속적으로 진화 발전하고 있는 암호화통화가 가져오는 혁신은 주목해야 마땅하다.

(2) 자산등기기술(Asset Registry Technology)

자산등기기술은 암호화통화인 '코인'을 활용하기 위해 분산원장을 사용하기보다는 자산을 등록하는데 사용한다. 분산원장 상의 작은 거래기록을 통해서 어떤 자산(주식, 자동차, 건물, 도메인이름 등)의 존재에 대한 증거를 남기면 중앙 기관(대부분 정부)에서 관리하는 등기소에 등록할 필요 없이 특정한 자산에 대한 소유권을 증명할 수가 있다. 공공 원장에 존재하는 개인키의 소유자가 그 특정한 자산에 대한 소유주가 되는 것이다. 자산등록기술은 규제와 감사 비용을 줄일 수 있는 개연성이 있다. 예를 들면 매스터코인, 컬러드코인, 네임코인, 카운터파티 등의 자산등록 서비스가 있다.

현재 자산등록은 기존의 분산원장에 추가 데이터를 포함하여 단순 인지하는 테크닉을 쓰고 있다. 즉 새롭게 시스템을 구성하지 않고 기존의 비트코인 블록체인 등을 이용하여 짧은 시간 안에 적은 노력으로 활성화하기에 용이하다. 하지만 기존의 네트워크에 단순히 데이터만 포함하기 때문에 기존의 네트워크 참여자는 그것이 특정 자산을 입증할 목적으로 포함되었다는 중요성을 인지하지 못할 수 있다. 즉 비트코인 블록체인 참여자가 비트코인 이외에 매스터코인이나 컬러드코인의 가치를 보호할 이유는 별로 없다. 게다가 상당량의 추가 데이터가 네트워크의 퍼포먼스에 부정적으로 영향을 줄 수

있고 거래를 입증하기 위해 추가적인 프로세싱 파워가 소비될 수 있다. 만일 원래의 분산원장 네트워크의 퍼포먼스에 걸림돌로 작용할 수 있다는 것은 치명적일 수 있다. 이 현상이 소위 "블록체인 블로우트(Blockchain bloat)"라는 것인데 대량의 금융 데이터와 함께 이 카테고리상의 애플리케이션들의 확장성에 의문을 제기하게 되는 것이다. 결론적으로 아직은 자산등록 카테고리가 금융산업을 위한 제한된 범위에서의 활용 외에는 확장되기 어렵다.

그럼에도 불구하고 주목을 해도 좋은 것은 많은 플랫폼과 서비스가 출현함에 따라서 자산등록에 집중할 서비스가 많아지고 있다는 점이다.

(3) 자산중심기술(Asset Centered Technology)

자산중심기술은 자산 존재의 디지털표현과 관리에 초점을 맞춘 기술이다. 즉, 자산등록기술과 유사하나 퍼블릭 원장에 데이터를 추가하는 방식이 아닌 고유한 기술과 프라이빗 네트워크나 컨소시엄 네트워크를 구현하여 자산의 거래나 이동을 용이하게 기술을 개발한다. 예컨대, 리플, 스텔라, 하이퍼렛저 등의 서비스는 각각 자산(통화, 금속, 주식, 채권 등) 존재의 디지털 표현과 관리에 집중하고 있다. 이 네트워크에서의 신뢰는 비트코인 식의 블록체인을 통한 마이닝이 아닌, 참여자들이 직접 제공하여 만들어낸다.

이런 방식이 성공하기 위해서는 참여자들이 '미화', '위안화' '금' '비트코인' 등의 데이터 자산을 네트워크에 출고하겠다는 약속이 있어야 가능하다. 게다가 동시에 참여자들 중 몇몇은 이러한 자산을 다른 자산으로 바꿀 수 있도록 하는 책임이 있다. 즉, 물리적 세계와 가상세계를 연결하는 게이트웨이 역할을 해야 하는 것이다. 어떤 자산을 다른 자산으로 바꾸기 위하여 마켓메이커(Market Maker)라는 기능이 이 기술에는 필수적이다. 많은 경우 마켓메이커는 외환거래 기관일 가능성이 높다.

(4) 플랫폼기술(Platform Technology)

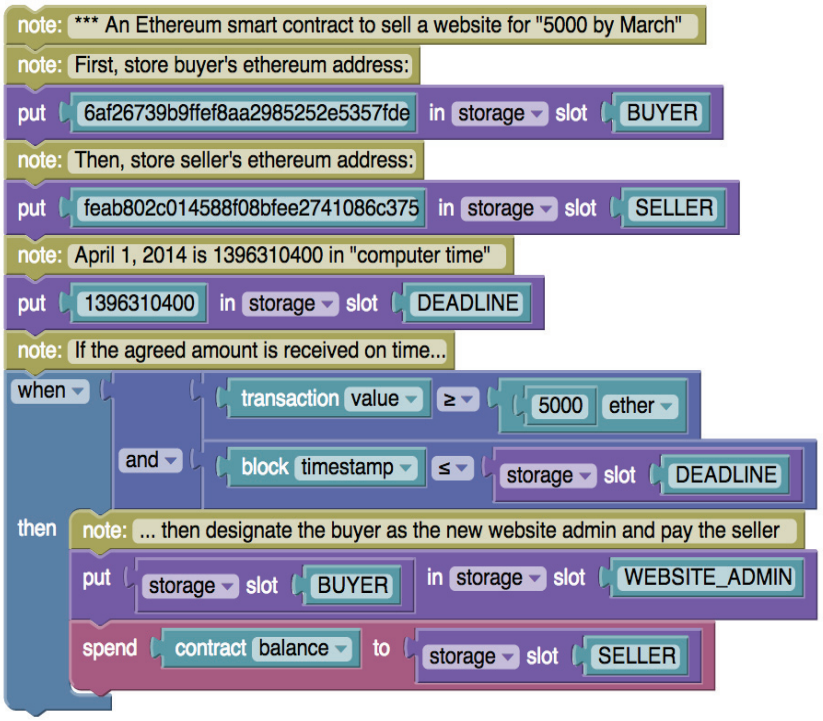
분산원장에 있어서 플랫폼기술은 암호화통화 기술을 플랫폼화하여 타 분야에 적용하는 방법을 모색하고자 하는 기술이다. 분산 네트워크상에서 완벽한 애플리케이션의 개발과 실행을 위한 플랫폼 개발이 이들의 주된 목표이다.

이더리움은 완벽한 애플리케이션 개발 플랫폼을 위하여 그들의 분산원장 플랫폼에 “튜링 완전성(Turing Completeness)”을 제공하는 강력한 프로그래밍 툴을 장착했다. “튜링 완전성”이란 수학적 시뮬레이션인 튜링머신의 수준까지 프로그래밍이 가능하다는 것이다. 이는 순차(Sequential) 프로그래밍에서 가능한 모든 기능을 장착하였다는 뜻으로 병렬처리 프로그래밍을 제외한 보통의 컴퓨터에서 실행 가능한 프로그래밍이 모두 가능하도록 설계되었다는 뜻이다.

튜링 완전성을 제공하는 이더리움과 같은 분산원장 기술은 문자 그대로 “무한대의 확장성”을 갖는다. 따라서 분산원장 기술에 전혀 새로운 산업의 지평을 여는 계기가 되고 있다. 프로그래밍 언어를 이용하여 스마트계약을 정교하고 정밀하게 설계하면 과거에는 존재하지 않았던 프로그램에 의해 운영되는 계약형태의 사업영역과 모델이 탄생한다.

따라서 이더리움의 튜링완전성이 가져다주는 확장성을 이용하여 Dapp (Distributed Application)이라는 새로운 사업 개념과 사업 영역이 탄생하였다. 이에 대한 자세한 설명은 아래 탈중앙애플리케이션(Decentralized Apps)기술과 탈중앙자율조직(Decentralized Autonomous Organization)에서 설명한다.

<그림 1-3> 이더리움을 이용한 스마트계약의 예



(5) DApp(Decentralized Applications; 탈중앙애플리케이션)기술과 DAO (Decentralized Autonomous Organization; 탈중앙자율조직)

이더리움과 같은 플랫폼기술이 무한확장이 가능한 프로그래밍 수준에까지 활용할 수 있도록 프로그래밍이 가능하기 때문에 이를 이용한 스마트계약이 최대한도로 사용될 경우 계약에 의해 실행되는 비즈니스 모델이 탄생할 수 있다. 이 프로그래밍 기능을 이용하여 애플리케이션을 개발하는 것을 DApp이라고 부르고 현재 수백개의 DApp이 개발되어 사용되고 있다.

스마트계약에 의한 애플리케이션은 기업운영의 형태까지도 띌 수 있는데 탈중앙자율조직(Decentralized Autonomous Organization)이라고 부른다. 이는 법적으로 이전에는 존재하지 않았던 새로운 사업모델의 형태로 이것이 유한책임을 갖는지 무한책임을 갖는지 조차도 불분명하다.

탈중앙자율조직의 첫 번째 케이스는 더다오라는 그룹으로 투자자(Investor)가 직접 운영하는 크라우드펀딩을 통한 벤처캐피털 펀드를 지향하고 2016년 5월 펀드모집을 했다. 더다오(TheDAO)는 이더리움 블록체인을 이용한 다수의 계약을 통해 존재하는 조직이라는 점에서 어느 국가에도 속해있지 않은 사업조직이었다. 더다오는 "프로젝트에 펀드를 나눠주는 허브 역할"을 하려고 했다. 즉, 더다오는 토큰을 투자자들에게 판매하고 거기서 만들어진 펀드를 투표를 통해 벤처투자를 하려고 했다. 더다오는 완벽하게 투명할 수 있도록 펀드매니저와 펀드디렉터를 없애고 투자자가 직접 벤처투자에 관여하도록 한 것이다. 더다오는 모든 것이 투명할 뿐만 아니라 모든 것이 프로그램 코드에 의해서 운영되도록 했다. 누구나 자세한 내용을 들여다 볼 수 있게 한 것이다. 아쉽게도 더다오는 2016년 6월 해킹을 당해 그 운영이 종료되었다.

DAO와 DApp은 개념적으로 많은 시사점이 있고 앞으로 새로운 산업의 기술적 기반이 될 정도로 혁신성이 있으나 아직도 불분명한 부분이 많고 실제적으로 어떻게 사용될 수 있는지 많은 부분이 의문점이 있다. 예컨대 이더리움은 이 보고서를 작성하는 시점에 서비스거부(Denial of Service) 공격을 받고 있는 중이다.

이렇게 심한 공격을 받는 데에는 여러 가지 원인이 있지만 그 중에서 가장 두드러진 것은 아이러니컬하게도 이더리움이 제공하는 튜링완전성, 즉 프로그래밍의 강력함에 있다. 이더리움이 지향하는 튜링완전성은 컴퓨터 이론으로 보면 비결정적(undecidable)이다. 즉, 참과 거짓을 판단할 수 없는 문제가 있기 때문에 스마트계약을 튜링완전성이 있는 언어로 써야 한다면 비결정적이다. 따라서, 이더리움이 지향하는 분산원장에서의 완전성은 불완전하다.

라. 분산원장 기술의 장단점

(1) 분산원장 기술의 장점

(가) 보안성 향상

분산원장 기술은 암호화된 데이터와 암호화된 키 값으로만 트랜잭션을 하

므로 보안성에 무결성을 가지고 있다. 또한 블록의 최초 블록과 앵커(Anker)가 되어 있어 블록 안의 데이터 변조와 탈취가 불가능한 기능을 가지고 있다.

기존의 시스템은 특정 공인기관의 시스템 오류로 인해 전체 네트워크가 마비될 수 있으며, 거래 기록 등 중요 정보가 특정 기관에 집중되어 있기 때문에 해킹과 같은 적대적 공격의 표적이 되기 쉬우나 분산원장 기술은 각 참여노드의 분산화로 해킹이 불가능하므로 보안성의 향상을 가져올 수 있다.

(나) 비용 감소

분산원장 기술은 비용의 감소를 불러올 수 있다. 인증과 데이터 트랜잭션의 증명을 위해 여러 중간 매개 또는 인증 기능이 있어야 하지만 분산원장 기술이 도입된 블록체인은 거래 정보를 은행이나 증권거래소 등의 중앙서버 그리고 공인된 제3의 기관에서 보관하는 기존 방식과 달리 모든 사용자가 거래 내역을 공유하는 시스템이다. 중앙 서버와 집중화된 시스템이 필요 없기 때문에 비용이 적게 들 뿐더러 거래 정보가 분산돼 있어 해킹 위험도 작다는 장점을 가지고 있다. 따라서 기존에 쓰였던 IT 비용의 대폭 감소를 기대할 수 있다.

(다) 거래 속도 향상

거래상의 속도를 향상시킬 수 있다. 분산원장 기술에 의한 거래는 여러 인증과 증명에서 제3자를 배제시키는 실시간 거래이므로 전체 시스템의 처리 속도나 범위가 공인된 제3자의 역량에 의해 결정되었던 과거 시스템과 달리 네트워크 내의 모든 참여자가 공동으로 거래 정보를 검증/기록/보관함으로써, '공인된 제3자' 없이도 거래 기록의 신뢰성을 확보하는 동시에, 거래의 효율성 및 속도를 가져올 수 있다. 특히 증권시장에서는 결제까지 걸리던 시간 소요를 대폭 줄일 수 있을 것으로 예상하고 있다.

또한 분산원장 기술은 거래상의 오류와 실수를 최소화시킬 수 있다. 즉 오류의 정정과 수정을 위한 시간의 소요를 제거할 수 있으므로 거래 속도의 향상을 가져온다.

(라) 가시성 극대화

분산원장 기술은 거래상의 가시성(Observability)을 극대화시킬 수 있다. 분산원장 기술은 실시간으로 분산원장의 여러 노드(Node)에 한 모니터링을 가능하게 하여 가시성을 극대화시킬 수 있다. 이러한 가시성은 분산원장 기술에 의한 가상화폐의 필수 조건으로 거래상의 가시성은 투명성과 자기부인 방지의 기능을 얻을 수 있다.

(2) 단점[1)]

(가) 검열저항성(Censorship-resistant)

블록체인에서는 이미 정해진 몇 가지 기초적인 검증 조건(총액 유지, 암호서명 포함 여부, UTXO 등)을 통과하면 모든 것이 기록될 수 있다. 따라서 해킹이 일어나더라도 해킹된 금액의 이체를 막을 수 없으며, 실수로 잘못된 계좌에 이체를 발생시키더라도 돌이킬 수 없다. 기본적으로 계좌 동결, 채권 압류, 강제 이체 등이 불가능한 것이다. 이것은 매우 심각한 문제인데, 기본적으로 인간의 실수와 해킹 등의 사고를 인정하지 않는 시스템이기 때문이다. 이러한 무관용 프로토콜은 실제 일상생활에서 대규모로 서비스를 할 경우 큰 혼란을 야기할 수 있다. 또한 이 특성은 법의 집행(law enforcement)을 기술적으로 무력화시키기 때문에 문제가 된다. 한번 분산원장으로 생성된 블록은 수정이 불가능하므로, 한번 생성된 블록은 그 상태 그대로 전체 블록체인 속에 남아 있게 된다.

(나) 익명성(Pseudonymity)

전 세계적으로 자금세탁방지(AML), 고객알기제도(KYC), 고객의 고객알기제도(KYCC) 등이 금융권의 주요 규제 이슈로 떠오르고 있다. 특히 국내 금융기관은 '금융실명제' 도입에 따라, 차명계좌 개설 및 거래나 타인의 명의를 이용한 금융 서비스 이용이 원천적으로 금지되어 있으며, '전자금융거래법'에 따라 처벌의 대상이 된다. 따라서 은행을 위한 블록체인 서비스에서 익명성을 유지하는 것은 불가능하다. 블록체인은 기본적으로 완전한 익명성을 추구

1) FINECTOR REPORT(2016.08)

하고 있기 때문에 금융권의 블록체인 도입에 문제가 된다.

(다) 투명성(Transparency)

블록체인에서는 기본적으로 모든 데이터가 모두에게 공개된다. 이체 내역, 이체 시각, 이체 금액, 이체 발신/수신 계좌, 각 계좌의 잔고 및 이체 기록 등의 모든 기록이 공개되어 있다. 이러한 부분들은 기본적으로 개인정보에 해당하기 때문에 공개되는 것은 부적합하다. 또한 자본시장에서 은행을 포함한 각 주체는 반드시 숨겨야만 하는 정보가 있는데, 이러한 부분은 내부정보나 영업기밀에 준할 수 있다. 은행이 주관하는 모든 이체내역이 외부에 공개된다면 해당 은행은 더 이상 영업을 할 수 없을 것이다.

(라) 대체가능성 문제(Fungibility problem)

분산원장 기술의 등장은 서두에서 밝혔듯이 가상화폐의 발행에 관련하여 발전된 시스템으로 가상화폐의 문제점을 같이 살펴볼 수 있는데 분산원장에 의한 가상화폐의 대체가능성이란 특정 재화나 상품 또는 화폐의 한 단위가 대체 가능한 속성을 뜻한다. 예를 들어 1만원권 지폐는 누가 소유했든, 어디에서 거래되었든 다른 1만원권 지폐와 동일한 가치를 가져야 한다. 반면에 다이아몬드는 하나하나 고유한 속성을 가지기 때문에 동일한 무게라고 하더라도 다른 다이아몬드와 대체될 수 없으며, 통상적으로 100g 크기의 다이아몬드는 1g 다이아몬드 100개 이상의 가치를 지닌다.

화폐에서는 대체가능성(Fungibility)이 매우 중요한데, 전산화된 화폐도 마찬가지이다. 전산화된 화폐의 경우, 시중 은행 어디에 있는 돈이라도 서로의 가치는 동일하다. 국민은행과 하나은행 계좌에 있는 1만원이 서로 다른 가치를 지닐 수 없다. 그러나 이러한 속성이 비트코인과 같은 블록체인 화폐에서는 그대로 적용되지 않을 수 있다.

블록체인에서는 모든 계좌와 각 계좌의 이체 기록 및 잔액이 투명하게 공개(Transparent)되고, 각 이체의 원 출처가 추적 가능(Traceable)하다. 즉 누구나 코인이 발행된 시점부터 발생한 모든 이체 기록을 열람할 수 있다. 이러한 공개성 덕분에 어떤 코인이 범죄에 연루되었는지도 알 수 있다. 범죄에

사용된 코인을 전달받게 되면 해당 범죄에 연루된 것으로 오해를 살 수도 있을 것이다. 심지어는 조사기관에 의해 소환을 당할 수도 있고, 해당 금액이 강제로 환수당할 리스크도 존재할 수 있다. 비트코인의 경우, 누구나 거래 기록을 확인할 수 있기 때문에, 불법적인 거래 기록을 가진 코인, 또는 범죄에 사용된 코인은 거래자들이 피하게 될 것이고, 시장에서 상대적으로 낮은 평가를 받게 될 수 있다.

(마) 익명의 거래 검증 주체(Anonymous Validator)

블록체인에서 거래검증의 주체는 전 세계에 분포된 컴퓨터(노드)다. 누구든지 컴퓨터만 가지고 있으면 익명으로 거래검증작업에 참여할 수 있다. 이는 인터넷 상에서 서로 신뢰할 수 없는 개인 간의 거래를 위해서 고안된 방식인데 금융기관에는 적합하지 않다.

금융기관은 직접 통제권을 가지고 각 이체를 검증해야 하기 때문에, 제3자에 검열과 그 실행을 맡기는 것은 불가능하다. 특히, 거래 조작, 이중 지불 등의 불법적인 행위에 법적인 제재를 가하거나 계좌 동결, 강제 환수 등의 긴급 조치를 취해야 하는 경우가 있으므로, 해당 기관이 온전한 거래 검증 권한을 가져가야만 한다.

(바) 확장성(Scalability)

자본시장에서는 대량의 거래데이터를 신속하게 처리하는 것이 핵심이므로 확장성과 그 속도가 매우 중요하다. 일례로 '미국청산예탁결제기관(DTCC)'의 경우, 매일 약 1억건(초당 최대 1,200건)의 이체를 처리하고 있으며, 중국의 상하이주식거래소 시스템은 최대 초당 8,000건까지도 처리한다. 이런 엄청난 처리능력은 아직 공개형 블록체인에서 구현하는 것이 불가능하다.

대표적 분산원장 기술인 비트코인의 경우, 매 거래는 10분 간격으로 블록을 통해 기록되며, 각 블록에 기록할 수 있는 데이터의 크기는 최대 1MB에 불과하다. 속도는 느리고 크기는 작다. 기존 금융시스템의 결제(Settlement) 속도보다는 훨씬 빠르지만, 지급(Payment) 속도보다는 느리다. 은행으로 이체를 하면, 이체 수령인이 거의 즉시 출금할 수 있는 반면, 현 분산원장에서는

최소 10분~60분이라는 시간을 기다려야 한다. 이는 지급과 결제가 사실상 동시에 이루어지는 블록체인의 속성에 기인한다. 초당 4~7 건의 거래를 처리하는 비트코인 네트워크의 경우, 초당 1만 건 이상의 이체를 처리하는 비자나 마스터카드 네트워크와 비교했을 때 글로벌 지급 시스템이 되기엔 부족하다.

(사) 처리비용 낭비(Waste of Computing Power)

블록체인이 가진 분산시스템은 각 자료를 부분으로 나누어 참여자들에게 배포하는 것이 아니라, 모든 자료를 모두에게 공유하는 방식이다. 전체 내용을 모든 참여자가 다운로드하여 함께 공유함으로써 제삼자가 내용을 속일 수 없게 하는 것이다. 하지만 모든 노드가 결국 동일한 작업을 하기 때문에 얼마나 많은 노드가 이체 작업에 참여하든 상관없이, 처리 효율성은 하나의 노드보다 높을 수 없다. 따라서 소진되는 처리비용을 고려한다면 전통적 처리 시스템에 비해 매우 비효율적일 수 있다.

(아) 개연적 결제의 완결성(Probabilistic Settlement Finality)

블록체인에 대해 설명할 때 좀처럼 언급되지 않는 부분으로, 결제의 완결성 문제는 블록체인의 금융기관 도입에 있어서 반드시 해결하고 가야 할 문제이다. 결제완결성(Settlement finality) 보장이란 지급결제시스템을 통해 이루어지는 지급지시, 청산, 결제가 참가기관의 파산 등의 상황이 발생하더라도 취소되지 않고(Irrevocable) 해당 지급결제시스템의 운영규칙에 따라 무조건적(Unconditional)으로 이루어지도록 하는 것을 의미한다.

즉 결제가 한번 발생하면 이것이 뒤집히지 않을 것이라는 확증이다. 원장에 기록된 내역이 갑자기 사라지거나 다른 기록으로 대체돼 버린다면 해당 은행원장에 대한 신뢰는 사라질 것이고 엄청난 혼란이 찾아올 것이다. 특히, 하나의 금융기관이 결제에 실패할 경우, 연쇄적인 금융기관들의 지급불능 사태를 촉발할 수 있다. 따라서 지급결제시스템의 경우, 한번 확정한 결제내역은 영원히 뒤바뀌지 않는다.

한국은행의 신한은금융망, 금융결제원의 CD공동망, 타행환공동망, 전자금융공동망 그리고 CLS Bank International의 CLS System 지급결제시스템은 결

제의 완결성이 법적으로 보장된다. 그러나 비트코인과 같은 블록체인의 경우 이미 한번 확정된 원장내역이 사라지거나 다른 기록으로 대체되는 일이 발생한다. 이를 블록 재조정(Block reorganization)이라 부른다.

블록체인은 정해진 시간 안에 특정한 난이도의 과제를 먼저 수행하기 위해 경쟁하는 시스템이다. 각 노드, 즉 네트워크 참여자들은 특정한 난이도의 과제를 수행하고 블록을 생성하여 쌓아 올린다. 과제를 수행하면 블록을 생성하여 네트워크에 전파할 수 있게 되는데, 종종 두 명 이상이 블록을 동시에 생성하는 경우가 발생한다. 이렇게 되면 각 블록 생성자는 서로 다른 블록체인 정보를 가지게 된다. 이를 '블록체인 분기' 현상이라고 칭하며 '포킹(Forking)'이라고도 흔히 불린다. 블록체인은 한 줄의 블록들로 이루어진 체인이다. 따라서 동시에 블록이 발견되었다고 해서 체인이 두 줄이나 여러 줄이 되는 것을 용납하지 않는다. 블록체인은 언제나 한 줄로 순차적으로 연결된 블록들이다. 또한 같은 네트워크에 연결된 모든 노드는 동일한 블록체인을 동기화해야만 한다. 따라서 포킹이 발생한 경우, 블록 재조정이 필요하다. 동일 네트워크에서 어떤 노드는 A블록을, 어떤 노드는 B블록을 가지는 것은 용납되지 않는다. 결국 두 노드가 네트워크상에서 만나게 되면, 더 긴 블록체인을 생성한 쪽이 이기게 되며, 더 짧은 블록체인을 가진 쪽은 더 긴 블록과 출동하는 내역들을 전부 삭제하고 더 긴 블록의 내역을 다운로드하여 대체하게 된다. 이러한 블록 재조정 과정을 통해 '동일 네트워크 동일 블록체인'이라는 원칙이 유지된다.

(자) 거버넌스(Governance)

모든 소프트웨어는 거버넌스가 필요하다. 즉, 해당 소프트웨어를 꾸준히 업데이트하고 관리하는 것이 필요하다. 잘못 생각하면 블록체인 시스템이 오직 수학적 알고리즘으로만 통제되고 인간의 규칙 제정과는 별개인 것처럼 보일 수 있다. 하지만 블록체인의 기술 규약도 결국 인간이 제정하고 유지해 나간다.

비트코인 소프트웨어는 소수의 실권자와 비공식 기관이 참여한 특수 절차를 통해 관리된다. 소프트웨어는 오픈소스이며 누구나 코드의 개선점을 제안할 수 있다. 그러나 공식 버전의 변경 사항에 대한 기술 권한은 핵심 코드를

유지, 관리하는 소수의 코어 개발팀이 관장한다. 다만 비트코인 자체가 분권화된 서비스(Decentralized service)이며 개인들이 모인 네트워크에 의해 유지되기 때문에 코어 개발자들의 결정권은 절대적이지 않다. 이 때문에 규칙에 대한 중요한 변경 사항의 경우, 커뮤니티의 폭넓은 지지와 합의가 필수적이다. 뿐만 아니라 변경 사항이 실제로 반영되기 위해선 채굴자(Miner)라고 불리는 검증인들(Validator) 과반수의 채택이 필요하다. 즉 이들이 업데이트된 소프트웨어를 설치하여 가동해야만 실제 네트워크에 반영되는 것이다. 검증인들의 발언권은 채굴에 들어가는 컴퓨터 처리 능력에 비례하여 측정된다. 따라서 일명 '채굴풀(Mining pool)'을 운영하는 소수의 사업자들이 업데이트의 비준 여부를 결정하는 강력한 힘을 갖는다.

이 합의 절차는 버그 수정처럼 논란의 여지가 없는 경우에는 쉽게 진행되지만, 주주들의 이해관계가 복잡하게 얽혀있는 경우에는 쉽지 않다. 블록체인은 공통적으로 분권화를 꿈꾸지만, 결국 이를 발명한 개발자가 존재하고 해당 소프트웨어를 관리하고 이끌어나갈 주체들이 존재한다. 그럼에도 불구하고 명확한 권한이나 의무에 대해 정의되지 않았으며 수많은 이해관계가 복잡하게 얽혀있기 때문에 의사결정은 매우 더디고 비효율적이다.

(차) 가치변동성(Volatility)

리플이나 비트코인처럼 이미 존재하는 블록체인 네트워크를 통해 자금을 이체하는 것은 가치 변동성면에서 큰 위협이 될 수 있다. 일반적으로 블록체인에서의 거래는 내부화폐를 거쳐 진행된다. A가 자신의 달러(Dollar)를 B에게 유로(Euro)로 보내고 싶을 경우, A는 보내고자 하는 금액만큼의 달러로 비트코인을 산 뒤, 해당 비트코인을 B의 계좌로 보내고 B는 국내 거래소에서 다시 유로로 환전하는 방식이다. 그러나 비트코인의 경우 거래확정 속도가 30분 ~ 1시간 정도로 느리고, 가치변동성이 매우 높다. 수수료를 아끼기 위해 비트코인 네트워크를 이용했다가, 가치변동성으로 보낼 때는 10만 원이었는데 받을 때는 7만 원이 될 수도 있는 것이다.

Ⅱ. 분산원장 기술과 금융서비스

1. 분산원장 기술의 금융서비스 적용 현황

가. 해외 현황

골드만삭스, 바클레이즈, JP모건, UBS 등 글로벌 대형은행은 컨소시엄을 결성하고 미국 핀테크 업체인 R3 CEV와 제휴하여 블록체인을 금융서비스에 활용하기 위한 플랫폼을 공동 개발 중이다[2]. 2014년 설립된 미국 뉴욕 소재 금융기술 벤처기업으로 블록체인을 이용하여 저비용으로 해외송금 및 자산관리 등에 활용할 수 있는 플랫폼을 개발 중이며, 이외에도 분산원장 기술을 기존 금융서비스 및 거래정보 기록에 활용하려는 다양한 시도가 이루어지고 있다.

<표 2-1> R3 CEV 컨소시엄 참가 금융기관

구분	컨소시엄 참가 금융기관
2015.9.15 일(9개)	· Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street, UBS
2015.9.29 일(13개)	· Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, Morgan Stanley, National Australia Bank, Royal Bank of Canada, Skandinaviska Enskilda Banken, SociéétGééale, Toronto-Dominion Bank
2015.10.28 일(3개	· Mizuho Bank, Nordea, UniCredit
2015.11.19 일(5개	· BNP Paribas, Wells Fargo, ING, MacQuarie, the Canadian Imperial Bank of Commerce
2015.12.17 일(12개)	· BMO Financial Group, Danske Bank, Intesa Sanpaolo, Natixis, Nomura, Northern Trust, OP Financial Group, Banco Santander, Scotiabank, Sumitomo Mitsui Banking Corporation, US Bancorp, Westpac Banking Corporation

자료: 한국은행(2016)

나. 국내 현황

최근 국내 은행들도 관련 핀테크 기업과의 제휴 등의 형태로 해외송금 서비스, 인증체계 개발 등에 활용하는 방안을 검토 중에 있으며, 금융권에서 블록

2) 한국은행, "분산원장 기술과 디지털통화의 현황 및 시사점," 지급결제 조사자료, 2016.1.

체인 기술에 대한 관심이 증가하고 있으며, 선도적 이미지 구축을 위해 금융회사, PG사, 핀테크 스타트업 등에서 다양한 실험적 시도를 시작하고 있다.

국민은행은 2015년 9월 코인플러그에 15억 원을 투자, 블록체인을 기반으로 한 외환송금서비스 및 개인인증서, 문서보안서비스 등 관련 제휴를 추진 중이다. 신한은행 역시 2015년 '신한퓨처스랩'(신한금융그룹의 핀테크 스타트업 육성 프로그램) 1기 업체로 선정된 스타트업 스트리미와 손잡고 블록체인 기술을 활용한 외환송금 시스템을 공동 개발하고 있다. 한편 신한은행은 스트리미의 기술력을 인정해, 직접 5억 원을 지분 투자하기도 했다. KEB하나은행은 센트비(핀테크 기업)와 업무협약을 체결하고 블록체인 기술을 활용한 해외송금서비스를 구축하고 있으며, 2015년 스타트업 육성을 위한 핀테크 '1Q랩'을 개소하고 블록체인 플랫폼을 구축하는 방안을 검토하고 있다. NH농협은행도 코빗(비트코인 거래소)과 제휴를 통해 블록체인 기술을 접목하는 방안을 검토 중이다. BNK금융그룹 부산은행과 경남은행 역시 코인플러그와 공동으로 '블록체인' 기반의 금융서비스 개발을 위한 업무협약을 체결했다.

<표 2-2> 국내 블록체인 활용 현황

구분		블록체인 연구 및 활용을 위한 주요 활동
금융	신한은행	· 외환송금서비스 블록체인 기술을 적용한 스타트업과 협업
	KB 국민은행	· 외환송금서비스, 개인인증서, 문서보완서비스 등에 국내 스타트업과 제휴를 추진하고 서비스 개발에 투자
	NH 농협은행	· NH핀테크 오픈플랫폼 사업 추진의 일환으로 서비스 모델링을 위해 핀테크 기업 20곳과 양해각서를 체결
	KEB 하나은행	· 핀테크 기업 육성센터를 통해 블록체인 기술 업체와의 협업을 준비 중
비금융	삼성전자	· IBM과 함께 블록체인을 이용한 사물인터넷(IoT) 기기가 서로 소통하는 P2P네트워크에 활용
	LG CNS	· 국내 스타트업 기업과 금융상품 유통플랫폼 파일럿시스템 구축을 위한 사업 협력 체결
	페이게이트	· 입금, 청산, 에스크로 등을 처리하는 블록체인 플랫폼을 핀테크 업체에 공개하고 블록체인을 데이터베이스 및 정산소로 활용
	코인플러그	· 블록체인 기반의 비트코인 거래소 및 전자지갑, 개인인증서 서비스 제공 · 휴대폰을 이용하여 송금하고 ATM에서 수신할 수 있는 송금 형태
	코빗	· 한국 최초로 비트코인 스타트업 회사로 국내 최대의 비트코인 거래소 운영
	스트리미	· 블록체인 네트워크를 이용한 해외송금서비스 제공
	블로코	· 블록체인을 활용한 서비스를 개발할 수 있도록 클라우드 기반의 개발 플랫폼 제공
	디바인랩	· 암호키를 분산 저장하여 거래소가 해킹당하더라도 비트코인을 보호할 수 있도록 안정성을 강화한 월렛 제공

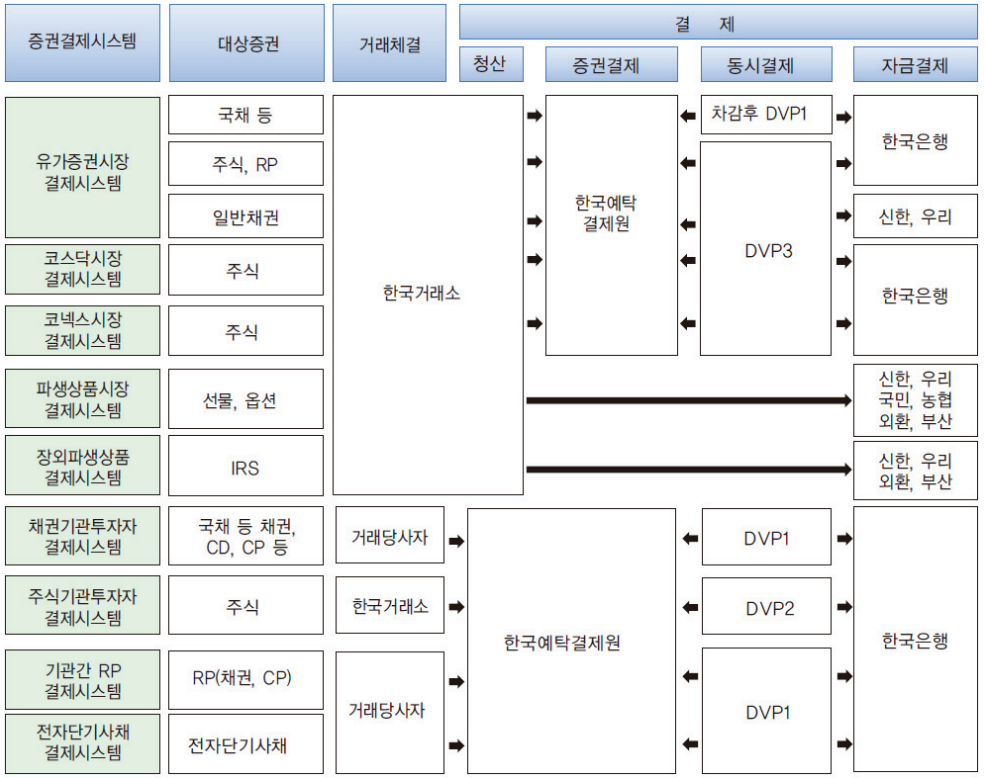
자료 : 금융보안원(2015), 국내외 블록체인 활용 동향 및 보안 기술 보고서

한편, 국내 대표적인 가상화폐 서비스업체 코인플러그는 블록체인을 이용해 공인인증서를 대체하는 본인인증 기술을 개발했다. 금융거래 등에 필수적으로 쓰이는 본인인증 기술을 더 간편하면서 안전하게 만드는 방안으로 블록체인을 활용했다. 코인플러그는 블록체인 기술과 관련해 국내 특허 12건과 해외 특허 3건을 보유하고 있는 회사로, 디지털 가상화폐인 비트코인 거래소와 비트코인 결제 솔루션 등 다양한 블록체인 관련 기술을 보유하고 있다. 이 회사는 지난해 보유한 기술력을 바탕으로 인터넷뱅킹에 사용되는 공인인증서를 별도의 인증기관을 거치지 않고, 사용자와 은행 간에서만 사용할 수 있는 방법을 공개했다. 그동안 국내에서 공인인증서 유출로 인해 심각한 문제가 발생했던 이유는 공인인증서를 통한 사용자PC-인터넷뱅킹사이트 또는 스마트폰-모바일뱅킹앱 간에 서로 믿을 수 있는지 판단하기 위해 필요한 개인키가 공개된 폴더 안에 버젓이 저장돼 있었기 때문이다. PC의 경우 액티브X, NPAPI와 같이 추가적인 플러그인을 설치해야만 했기에 해킹 위협에 노출되는 경우도 많았다. 코인플러그는 블록체인 상에서 공인인증서를 구현하는 방법의 장점을 이렇게 설명했다. 먼저 액티브X나 NPAPI와 같은 플러그인을 통한 추가 프로그램을 설치할 필요가 없으며, 자신이 소유한 개인정보를 은행 외 인증기관에 전송하는 것을 방지할 수 있다. 또 개인키와 공개키 생성 작업이 스마트폰 앱을 통해서 이루어지기에 인증기관이 없이도 공인인증서 로그인과 이체 등을 활용할 수 있다는 것이다. 은행 뿐 아니라 정부의 민원서류 발급, 조달청 입찰 등에서도 공인인증서가 활용되고 있기에 블록체인 기술은 개인정보유출 또는 해킹 등으로부터 보다 안전하고 저렴한 수단으로 재조명받고 있다.

2. 분산원장 기술의 금융서비스 적용에 따른 비용절감 효과

가. 증권업무(Capital Market) 에서의 비용절감 효과

<그림 2-1> 우리나라의 증권청산결제시스템 개요



출처 : 한국은행(2014), 한국의 지급결제제도

이미 여러 해외 보고서에서 밝혔듯이, 금융업계가 분산원장 기술을 금융업에 도입했을 경우 2022년까지 연간 20조원[3]을 절감할 수 있을 것으로 보고 있으나, 막연한 예상치이며, 아직 시행 전이기 때문에 금융권에서는 비용절감 효과를 측정하기 힘든 상황이다. 특히, 비용을 정량적으로 계산할 수 있는 방법론이 나와 있지 않는 상황에서 어떠한 비용을 변수로 놓아 계산할 것 인지도 아직 정해지지 않은 상태이다.

골드만삭스 보고서(2015)는 비용감소의 변수를 기존 시스템의 결제와 인건

3) 'The Fintech 2.0 Paper'(Santander, 2015. 6)

비 그리고 그에 따른 복리후생비를 놓고, 미국의 현 상황에서 증권시장 비용 감소를 논리적으로 추정·계산해 보았는데 본 연구는 이를 우리 금융시장(증권시장)에 적용하여 비용감소 효과를 계산해 보았다. 미국 증권시장의 비용과 한국 증권시장의 비용은 그 내용이 다르지만, 거래 청산 결제의 프로세스와 후선업무(Back office)기능이 거의 비슷하고 제3의 기관 증권시장 관여자인 미국의 DTCC와 증권예탁 결제원의 역할이 비슷하므로 비용의 절감 효과를 미국과 국내의 증권시장과 비교해 볼 수 있다.

한편 금융서비스 즉 시중은행의 분산원장 기술의 적용에 따른 비용절감 효과는 아직까지 단순 예상 추정치에만 국한되어 있어, 금융서비스 전반의 비용절감을 측정하기 어려운 상태이다. 따라서 본 연구에서는 각 금융서비스별 비용절감을 중심으로 연구하였다.

(1) 증권업무 구조와 취약점

투자자가 거래소시장에서 매매거래를 하기 위해서는 먼저 투자매매업 및 투자중개업 인가를 받은 증권회사(또는 금융투자회사, 이하 같음)에 매매거래계좌를 개설해야 하며, 동 계좌를 개설한 증권회사를 통하여 주문을 제출하여야 한다. 거래소시장에서 유가증권을 매매할 수 있는 자는 한국거래소의 회원인 증권회사에 한정되므로 일반투자자는 회원을 통하지 않고서는 거래소시장에서 매매거래를 할 수 없다.

투자자로부터 주문을 위탁받은 거래소 회원은 동 주문을 거래소에 제출(호가)하여야 한다. 한편, 외국인투자자의 주문은 금융감독원의 외국인투자관리시스템을 경유하여야 하며, 거래소의 회원이 아닌 비회원 증권회사는 투자자로부터 위탁받은 주문을 거래소 회원을 통하여 주문을 제출하여야 하는 구조를 가지고 있다.[4)]

회원으로부터 거래소에 제출된 주문은 거래소가 업무규정에서 정한 원칙에 따라 매매체결되며, 거래소는 체결결과를 회원에게 통보하고 회원은 이를 다시 고객에게 통지하게 되며 투자자는 매매체결분에 대하여 매매체결일부터 기산하여 3일째 되는 날(T+2) 회원이 정한 시간까지 매매거래를 위탁한 증권

4) KRX(한국증권거래소) 홈페이지

회사에 매수대금 또는 매도증권을 납부하여야 하며, 증권회사는 이를 거래소와 결제함으로써 매매거래가 완료되게 되는데 여기에서 여러 업무와 체계가 전체 거래에 비용과 시간의 경과를 초래하여 기회비용 및 여러 금융비용이 발생하게 된다.

세계 각국의 여러 증권거래소들은 수년에 걸쳐 거래, 청산, 결제의 간소화를 위해 수년간 노력해 왔지만, 아직까지도 앞에서 말한 여러 기관의 업무 및 시스템의 비동기화로 인해 비용 및 시간을 획기적으로 단축시키지 못하고 있다.

특히 거래소에서 거래가 진행되어, 주권이 이동한 기록의 시스템 입력을 아직도 수기로 수행하는데 한국의 증권예탁원과 같은 청산, 결제 기관인 미국의 The Depository Trust & Clearing Corporation(DTCC)은 이러한 입력과 처리를 위해 다양한 비용이 발생하고 있음을 여러 보고서를 통해 밝히고 있다.

거래소는 크게 다음 4가지의 취약점을 들어 분산원장 기술의 도입을 고려하고 있는데[5], 첫째 개별 하나하나의 주식거래가 여러 기관들과 시스템에서 개별로 중복되어 기록되면서 거래의 불확실성과 무결성 훼손 가능성이 증가된다는 측면이며 거래 체결에서 문제가 발생하는 경우 각 결제, 청산, 거래상의 참가자 각각으로부터 문제의 주식거래에 대한 수정과 동의가 이루어져야 하는 문제도 있다.

둘째, 결제 프로세스가 너무 길다는 이슈가 있다. 결제상 다양한 정보의 새로운 입력, 기존 주권명부의 갱신, 결제의 확정(Information confirmation) 등이 이루어지는 상황에서 여러 관련기관들의 후선업무 처리를 위한 절차상 또는 시스템 상 시간소요 문제가 야기된다. 주식매매 후선업무는 주식매매에 따라 거래승인, 소유권기록 변경, 주식과 대금의 교환이 이루어지는 과정으로 우리나라 증권거래소(KRX), 뉴욕증권거래소(NYSE)에서 매일 수백만 건의 거래와 수십억 주의 거래가 처리되고 있다. 거래확인에 뒤이은 후선의 청산과 결제는 완결되기까지 t+2(혹은 t+3)이 소요될 정도로 시간이 많이 필요하며, 미국 은행과 중앙대행기관 및 중개기관들은 후선업무(Back office)를 위

5) 한국예탁결제원(2014), 증권예탁 결제제도

해 90억 달러 정도의 비용을 지출하고 있다.

셋째, 계좌정보의 주식 수 및 금액 변화, 그리고 여러 주식 계좌(Account) 상의 변화 등을 수기적인 시스템을 통해 기록하는 과정에서 간섭 및 개입이 필요하기 때문에 다양한 비용과 시간소요가 발생하게 된다.

넷째, 여러 관련기관이 이러한 과정에 참가하므로 시스템 간, 또는 기록상 위험(Operation Risk)이 발생하게 된다.

상기 나열한 시간과 비용의 문제는 항상 제기된 거래소상의 문제로 앞으로의 분산원장 기술로 해결할 수 있게 된다.

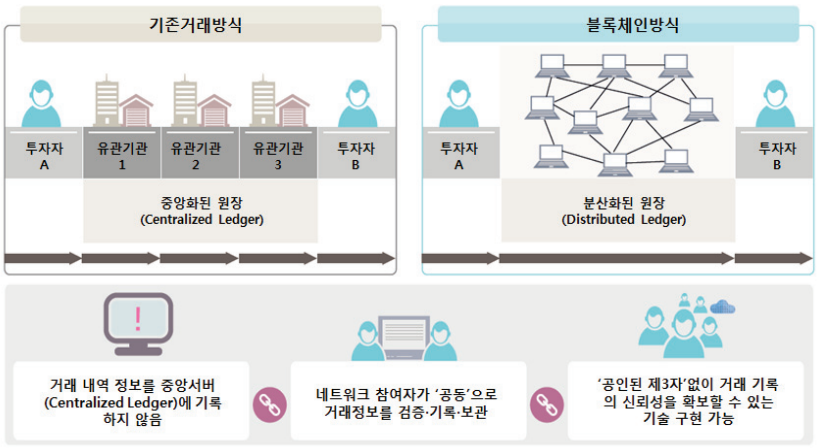
(2) 분산원장 기술 도입의 편익

분산원장 기술 도입을 통해 거래상 착오를 줄일 수 있게 된다(Reducing / Eliminating trade error). 워낙 많고 다양한 거래를 체결하는 현 증권거래소의 특성상 여러 기관들의 시스템의 유기적 연결되어 거래 주문 및 체결을 처리하면서 거래상의 착오를 발생시킬 수 있는 여러 문제점을 가지고 있다. 분산원장 기술을 도입함으로써 이러한 문제를 해결할 수 있는데 분산원장 기술로 구현된 시스템에서는 각 증권거래 기록 정보는 각각의 node들이 실시간으로 공유하게 되는데, 이에 따라 각 기록의 공증(Authentication)과 인증(Verification) 정보를 각 노드들이 분산원장을 통해 기록으로 보유하게 된다.

분산원장의 기술은 거래 기관들의 수기상의 간섭(Manual intervention)을 제거함과 동시에 거래 후 이슈(Post trade issue)와 착오체결, 계좌와 주문의 착오 등의 위험을 제거할 수 있다.

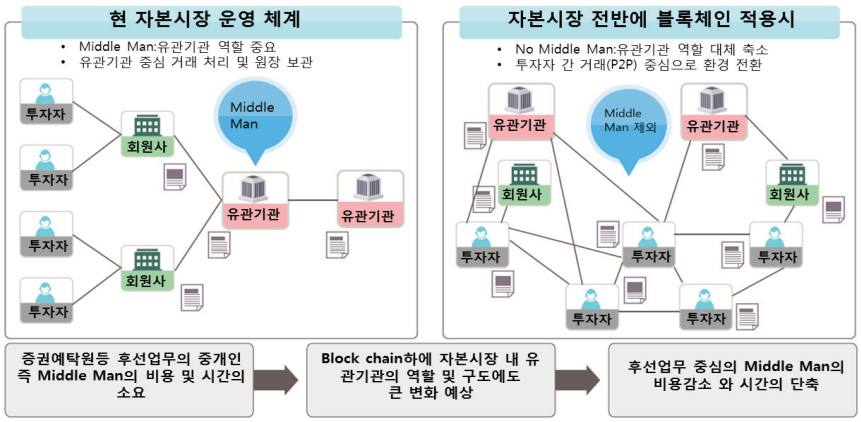
또한 현재 주식시장에서 거래확인(Affirmation and confirmation)이 다수의 관련기관들의 생태계에서 여러 차례의 확인절차를 거쳐 이루어지고 있는데 분산원장 기술은 관련기관의 등록 및 주주명부 변화 기록을 간소화시킬 수 있다.

<그림 2-2> 기존거래방식과 분산원장 기술 방식



거래체결 자료의 표준화를 통해 청산과정의 효율성 개선도 기대할 수 있다. 후선업무의 자동화와 효율성 증진으로 청산 결제가 t+1일로 감소하게 된다. 또한 주식과 거래대금의 이전에 분산원장 기술을 활용하여 기술적 혹은 수작업의 오류가 감소하게 됨으로써 결제까지의 과정에서 무결성을 달성할 수 있으며, 인증자동화로 거래상대방의 결제불이행 가능성이 감소하게 되는 편익이 발생하게 된다. 또한 투자자는 제3의 기관의 통보에 의존하지 않고 결제 통보와 모든 결제 과정을 모니터링 가능하게 된다.

<그림 2-3> 분산원장 기술 본격 도입시 자본시장 변화



자료: 코스콤

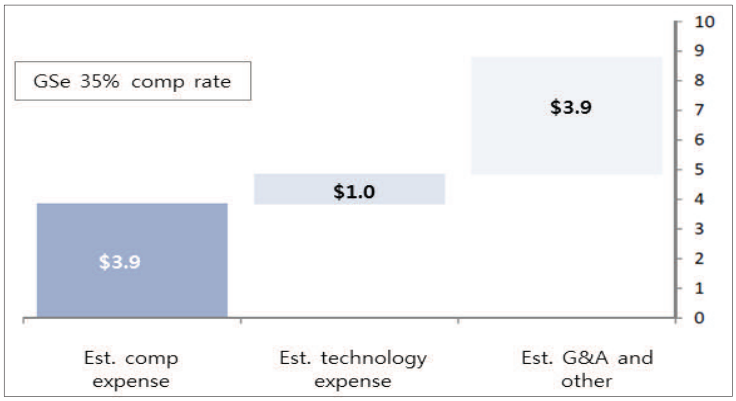
(3) 비용절감 효과 분석

분산원장 기술 도입 시 증권거래 비용절감 효과의 경우 여러 관계 기관에서 거래비용 절감을 기대할 수 있으나, 우선 증권시장 관련기관에서 발생되는 비용감소를 우선 고려하기로 한다.

미국의 골드만삭스 보고서에서는 현재 미국 거래소 등에서 총비용중 분산원장 기술을 이용하여 절약할 수 있는 비용 및 비율을 산출하였다. 특히, IT 비용과 주식 매매에 관계된 여러 기관들의 인건비 및 관리 비용을 고려하였다. 서두에서 밝힌 바와 같이 블록체인이 자본시장에 쓰이게 되면, 우선적으로 운영비 및 복리 후생비용을 줄일 수 있다고 보았다. 또한 증권 업무에 관한 비용은 직접적으로 줄일 수 있을 것으로 보고 있다. 분산원장 기술을 이용했을 때 거래와 체결이 정확하게 이루어진다고 가정하면 노동비용을 포함한 IT비용이 50%~70%의 범위(Range) 내에서 줄어들 것으로 예상하고 있다. 특히 이 보고서에서는 전체 미국의 주식거래 후선 업무에 관한 비용을 DTCC(Depository Trust Company)에서의 판관비를 기준으로 정의하고 비용감소를 추정하였으며[6], 일본의 JPX(Japan Exchange Group) 또한 최근 JPX working paper에서 증권거래소의 분산원장 기술의 이점으로 후선 업무(Reconciliation, Securities Ownership Registry)에서의 비용감소를 들고 있다[7]. 이러한 비용은 증권시장 참여기관에게는 수익이지만, 청산과 결제를 위한 비용이기 때문에, 이러한 시간과 비용의 감소를 통해 금융시장 참여자에게 효율성과 거래상의 무결성과 함께 비용 상의 편익을 줄 수 있다.

6) Goldman Sachs Global Investment Research(2016)
7) JPX(2016), JPX Working Paper

<그림 2-4> 분산원장 활용 IT 비용절감

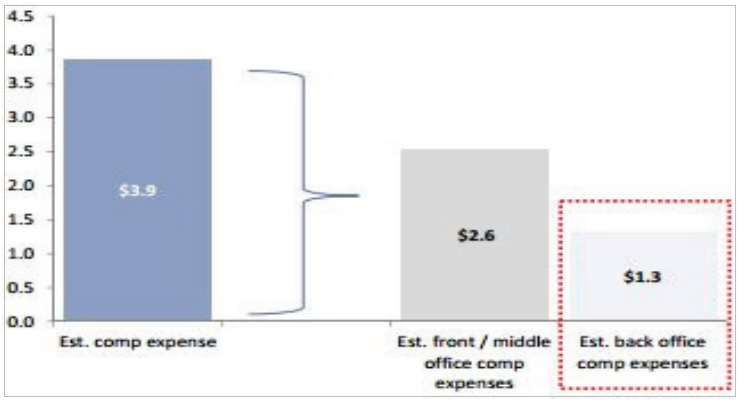


자료 : Goldman Sachs Global Investment Research(2016)

▪ 비용 절감

우리나라 주식시장의 후선업무 노동 보상비율과 IT비용을 후선업무를 담당하는 기관인 한국증권거래소(KRX)와 증권예탁원(KSD)의 재무제표를 통해 살펴보기로 한다. 먼저 한국증권거래소(KRX)의 경우, 2015년 손익계산서상 증권시장 거래에서의 총 매출이 6,085억 원이었으며 그중 총비용이 5,508억 원이었다. 이중 순수 IT비용으로 1,186억 원이 쓰였으며 복리후생, 퇴직금 인건비를 포함한 비용이 2,351억 원이고 판관비로 1,971억 원이 쓰였다. IT 비용 비중을 계산하면 총비용대비 약 22%를 차지하고 있음을 알 수 있다.

<그림 2-5> 분산원장 활용 후선업무 비용절감



한편 골드만삭스 블록체인 리포트에서 미국 증권시장의 경우 총비용 대비 순수 IT비용으로 지출되는 비중이 12% 수준이었다. 그러므로 한국증권거래소(KRX)의 IT비용 비중이 미국증권시장의 경우보다 상대적으로 높기 때문에 분산원장 기술의 핵심 편익인 IT비용 절감의 측면에서 분산원장 기술의 적용에 따른 IT비용의 절감 효과가 미국증권시장보다 한국 증권시장에서 더욱 클 것이라고 예상할 수 있다.

다만 한국증권거래소(KRX)의 IT비용 중 시스템운영비에는 서버비용과 유지보수, 보안 비용 그리고 IT자회사인 코스콤(Koscom)에 지출되는 비용이 포함되어 있으므로 미국 증권시장의 분석을 일방적으로 적용하기에는 어려움이 있으나, 본 연구는 비용절감의 개략적인 예상치를 유추하는 것을 목적으로 하므로, 이 같은 방법론을 사용하였다.

한편 한국증권거래소(KRX)의 경우 재무제표 상 전체 비용 중 후선업무(Back office)가 차지하는 부분은 청산에 국한되어 비중이 크지 않기 때문에 비용절감 효과도 미미한 수준이다. 이와 달리 한국예탁결제원은 실제 증권거래에서 후선업무의 대부분을 차지하고 있기에 이에 대해 비용절감 효과를 분석해보았다.

<그림 2-6> 한국증권거래소 연결손익계산서 (2014년, 2015년)

㈜한국거래소와 그 종속회사 (단위 : 원)

과 목	제 11 기	제 10 기
Ⅰ.영업수익	697,707,060,328	608,515,322,517
1.시장수수료 수익	275,034,532,856	221,252,950,267
2.예탁결제수수료 등 수익	168,116,983,999	133,020,764,003
3.정보 및 전산사업 수익	241,816,862,175	238,799,950,393
4.임대 및 기타영업수익	12,738,681,298	15,441,657,854
Ⅱ.영업비용	591,582,527,587	550,885,559,653
1.급여	222,870,660,242	202,961,449,485
2.퇴직급여	21,409,809,899	17,501,892,458
3.복리후생비	11,371,785,524	14,741,658,264
4.감가상각비	50,919,983,333	53,768,819,467
5.무형자산상각비	27,170,397,718	27,459,031,621
6.투자부동산감가상각비	2,117,468,353	1,808,430,633
7.대손상각비	637,482,213	652,193,377
8.지급수수료	42,506,114,160	36,760,440,487
9.광고선전비	5,355,158,141	3,826,897,443
10.교육훈련비	8,188,564,332	7,809,458,018
11.임차료	3,010,391,981	7,132,120,137
12.세금과공과	26,930,391,432	21,628,519,544
13.수도광열비	8,428,352,932	8,347,224,578
14.경상연구개발비	1,257,378,553	133,109,915
15.시스템운영비	128,890,168,625	118,606,447,994
16.기타영업비용	30,518,420,149	27,747,866,232

▪ 후선업무(Back-Office) 비용 절감

먼저 후선업무와 그에 따른 비용을 정의하고 검토해보기로 한다.

후선업무는 매매 이후의 업무로, 청산, 결제, 예탁을 의미한다.[8] 청산은 매매확인, 채권·채무의 계산, 결제이행보증을 통하여 결제일에 인도할 증권과 지급할 대금을 확정하는 절차나 기능을 말한다. 즉, 결제의 전 단계로 결제할 채권과 채무를 확정하는 과정이다.

청산은 매매나 결제기능을 수행하는 기관과는 별도로 독립적인 기관이 수행하기도 하고, 예탁결제업무를 수행하는 중앙예탁결제기관이 수행하기도 한다. 청산업무를 수행하는 시스템을 청산시스템이라고 하고, 청산업무를 수행하는 기관을 청산기관이나 청산인프라로 부른다.

결제는 증권과 대금의 최종적인 이전을 통하여 거래를 종결시키는 절차나 기능을 말한다. 즉, 결제는 확정된 채권과 채무를 해소하는 과정이다. 최종적인 소유권의 이전은 예탁결제 기관의 장부에서 계좌 간 대체를 통하여 발생한다. 결제업무를 수행하는 시스템을 결제시스템이라 하고, 결제업무를 수행하는 기관을 중앙예탁결제기관이나 결제인프라로 부른다.

예탁은 증권을 받아 집중적으로 보관하는 것이다. 예탁결제제도에서는 증권을 예탁받고, 그 증권의 권리를 나타내는 장부를 만들어서 권리의 관리가 그 장부에서 이루어지도록 하는 과정을 포함한다. 예탁이 이루어져야 이를 기반으로 장부를 형성하고 계좌간 대체를 하여 결제할 수 있다. 따라서 예탁과 결제의 기능은 분리할 수 없는 동전의 양면과 같다.

후선업무에서 가장 큰 역할을 하는 한국예탁결제원(KSD)은 앞서 밝힌 후선업무의 대부분을 책임지며, 후선업무와 기타 수익을 통해 버는 총수익은 2015년 기준 약 1,670억 원이고, 총비용은 약 1,188억 원이다. 이중 IT비용은 76억 원으로 약 6%를 차지하며, 복리후생을 포함한 인건비를 합산하여 산출해보면 약 605억 원(약 51%)임을 확인할 수 있다. 또한 판관비는 약 570억 원(약 43%)으로 구성되어 있다.

8) 한국예탁결제원(2014), 증권예탁 결제제도

분산원장 기술의 비용절감 효과를 거래시장의 IT비용과 인건비를 기준으로 분석해보았다. 이들 두 기관 즉 한국증권거래소와 증권예탁원에서 분산원장 기술을 적용하였을 때 비용감소 범위인 50% 이상 70%의 중간값(Median)인 60%가 절감된다고 가정하고, 민감도 분석을 적용해보면, 2015년 기준으로 연간 총비용 5,508억 원대비 16%인 약 881억 원을 줄일 수 있다고 추정할 수 있다.

마찬가지로 증권예탁원(KSD)의 후선업무에 대해서도 상기 민감도 60%를 기준으로 총 비용의 16%인 약 190억 원을 줄일 수 있다고 추정할 수 있다. 따라서 증권시장 전체에서 분산원장 적용 시 2015년 기준 연간 약 1,071억 원이 절감되는 것으로 추정할 수 있다.

<그림 2-7> 한국예탁결제원 손익계산서

(단위 : 백만원)

구분 (IFRS)	2011년 결산	2012년 결산	2013년 결산	2014년 결산	2015년 결산
수익(매출액)	-	128,909	125,290	133,077	168,193
순매출	-	-	-	-	-
매출원가	-	-	-	-	-
판관비	-	98,616	105,048	106,194	118,879 (70.7%)
영업이익	-	30,293	20,242	26,883	49,314
기타수익	-	1,830	1,849	1,634	1,024
기타비용	-	34,455	40,134	25,702	27,029
기타이익	-	-510	-1,135	-70	-25
금융수익	-	86,412	80,227	66,026	55,908
금융원가	-	1,761	2,165	4,157	849
지분법대상기업관련이익 등	-	-	-	-	-
법인세비용차감전순이익	-	81,809	58,884	64,614	78,343
법인세비용	-	18,802	14,084	14,108	15,501
당기순이익	-	63,007	44,800	50,506	62,842
기타포괄손익	-	5,055	127	-2,432	5,848
총포괄손익	-	68,062	44,927	48,074	68,690
매출액순이익률	-	48.88	35.76	37.95	37.36
자기자본회전률	-	14.49	13.59	13.95	16.78
이자비용	-	-	-	-	-

▪ **증권거래회원사들의 예탁 비용 절감**

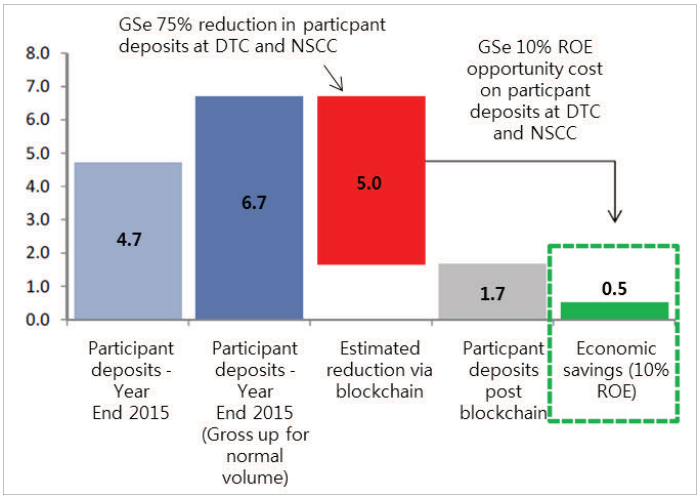
미국의 DTCC에서 증권 회원사들에게 요구하는 자본금은 총 50억불이다. 이들 회원들이 예치하는 비용은 거래상의 오류나 부정거래 혹은 주식거래에서 비롯된 사고 시 지급을 위해 필요한 예치비용으로 활용되지만[9], 이는 금융비용과 기회비용 부담으로 작용한다.

최근 예탁결제원은 주식결제 시 대금결제의 안정성을 확보하기 위해 은행에 개설한 신용한도를 증액하고 예탁결제적립금도 확대하는 등 결제유동성 재원을 확충하였다. 예탁결제원은 기존에 거래은행과 1,000억 원 규모의 신용한도를 개설하고 있었으나, 국제적 수준의 결제유동성 확보를 위해 2,000억 원으로 동 한도를 확대하였다. 즉 주식기관결제의 회원별 순채무한도가 1,000억원이므로 최대 2개의 지급채무자가 동시에 대금결제를 불이행하더라도 결제를 정상적으로 종료할 수 있도록 2,000억 원으로 증액한 것이다. 예탁결제적립금은 예탁결제원이 증권예탁결제업무와 관련하여 발생한 손실의 보전 및 자본시장법 제313조에 따른 부족 예탁증원에 대한 보전의무를 이행하기 위해 적립하는 금액을 말한다. 결제회원의 대금결제 불이행이 발생할 경우 불이행회원이 수령예정증권이나 담보증권의 처분, 결제기금의 사용으로도 손실을 보전하지 못하는 경우에는 예탁결제적립금을 통해 보전에 충당하게 된다. 현 한국증권거래소(KRX)는 각 회원사에게 예치금을 보유하고 있으며 이에 따른 회원사의 금융비용 및 기회비용이 증가하는 추세이다.

주식의 거래가 분산원장으로 거래되면, 앞에서 열거한 위험부담이 현저하게 줄어들기 때문에 예치금 적립에 따른 거래비용과 기회비용을 절감할 수 있다.

9) 한국예탁결제원(2014), 증권예탁 결제제도

<그림 2-8> 분산원장 활용 자기자본비용 절감



자료: Goldman Sachs Global Investment Research(2016)

골드만삭스 보고서의 분석에서는 분산원장 기술 적용 시 미국증권시장의 예치금액을 67억불에서 17억불로 약 75% 감소시킬 수 있을 것이라고 추정하고 있다. 이러한 예치금액의 감소 비율을 우리나라 증권시장의 예치 금액에 적용해보면 약 1,500억 원의 비용이 감소할 것으로 추정할 수 있으며, 예치금액의 감소에 따른 회원사의 금융비용 및 기회비용 상 편익이 자기자본 이익률 10%인 200억 원 정도일 것으로 환산 추정할 수 있다. 이러한 편익은 경제적 비용절감이라 말할 수 있다.

3. 은행업무에서의 비용절감 효과

가. 은행업무[10]

지급서비스(payment service)란 경제주체가 지급수단의 이전을 통해 지급행위를 할 수 있도록 금융기관 등이 제공하는 금융서비스를 말한다. 이러한 지급서비스는 인터넷뱅킹 등의 자금이체뿐만 아니라 어음, 수표, 카드, 선불전자지급수단 등 지급수단의 발행과 통신, IT기기 등을 이용한 전자지급결제대행 등도 포함한다. 지급서비스 제공기관은 서비스 제공에 따라 발생하는 금융기관간 채권·채무를 종결하기 위해 지급결제시스템에 직접 참가하거나, 직

10) 한국은행(2015), 지급결제제도

접 참가가 어려울 경우 시스템에 참가하고 있는 금융기관에 청산·결제업무의 대행을 의뢰한다.

한편, 그 동안 자금이체 등의 지급서비스는 예금수취기관이 취급하는 요구불예금에 부가된 고유업무로 인식되어 왔으나 최근 들어 카드, 전자화폐, 모바일뱅킹, 가상화폐 등 지급서비스 관련 신기술의 개발, 소비자의 금융서비스 편의성 향상, 금융기관 간 공정한 경쟁여건 조성 등의 지급결제환경 변화로 비은행 금융기관과 비금융기업도 은행과 제휴하거나 지급결제시스템에 직접 참가함으로써 지급서비스 기능을 확대하고 있다.

(1) 은행

은행은「은행법」상 환업무가 고유업무로 허용되어 있어 요구불예금을 근거로 다양한 지급서비스를 제공하고 있다. 이를 위해 국내은행은 거액결제시스템인 한은금융망은 물론 어음교환시스템, 지로시스템, 타행환공동망 등 소액결제시스템 참가를 통해 어음, 수표 등의 지급수단을 발행하고 지로, 타행환, CD/ATM, 자금관리서비스(CMS), 텔레뱅킹, 인터넷뱅킹 등의 계좌이체 및 현금 출금 등의 지급서비스를 제공한다. 또한 외국환은행의 경우 외환결제시스템에 참가함으로써 이종통화 간 매매 등에 따른 외화지급서비스를 제공한다. 외은지점은 한은금융망에는 대부분 참가하고 있으나 소액결제시스템에는 일부 외은지점만이 타행환, 전자금융 등 필요한 업무에 참가하고 있다.

(2) 비은행 예금취급기관

새마을금고, 신용협동조합, 상호저축은행 등 서민금융기관은 해당 설치 근거법에 따라 중앙회 및 연합회 등의 중앙조직 차원에서 환업무를 할 수 있도록 허용되어 있으며, 은행과 비슷한 수준의 지급서비스를 제공하고 있다.

비은행 예금취급기관은 은행과 유사한 여수신업무를 주요 업무로 취급하고 있지만 보다 제한적인 목적으로 설립되어 자금조달 및 운용 등에서 은행과는 상이한 규제를 받으며 제공하는 지급서비스도 제한적이다. 비은행 예금취급기관에는 상호저축은행, 신용협동조합·새마을금고·상호금융 등 신용협동기구, 우체국, 그리고 종합금융회사가 있다. 설립형태를 보면 상호저축은행과

종합금융회사는 주식회사, 신용협동기구는 비영리 협동조합, 우체국예금은 국영기업 등으로 다양하다.

상호저축은행 및 신용협동기구는 해당 특별법에 따라 중앙회 및 연합회 등의 중앙조직차원에서 환업무를 수행하고 있다. 이들 서민금융기관은 2002년 2월 해당 중앙조직을 대표로 금융결제원에 특별 참가하여 지로, CD, 타행환, CMS, 전자금융 등의 서비스를 제공하고 있으며 2008년부터 자기앞수표 발행이 가능해지면서 어음교환시스템에도 참가하고 있다. 그러나 결제리스크의 방지를 위해 소액결제시스템의 차액결제는 중앙조직이 선정한 결제 대행은행을 통하여 이루어지고 있다.

나. 분산원장 기술 도입의 편익

시중은행에서 분산원장 기술 도입에 따른 편익은 아직 전 세계적으로 구체적으로 제시되거나, 정량적 평가가 이루어지지 않고 있다. 자본시장(Capital market)에 대해서는, 후선업무(Back office)가 명확히 구분되어 있어 분산원장 기술을 프로세스에 적용 시 비용절감 효과를 확신하고 있으나, 은행의 경우에는 여러 가지 서비스를 복합적으로 제공하고 있어, 분산원장 기술의 적용에 따른 비용절감 효과를 현 상황에서 정확히 예상하기 힘든 상황이다. 특히, 기존의 시스템 즉 Legacy system의 무결성을 위해 시중은행들이 수십 년 또는 상당한 시간동안, 많은 투자와 노력을 기울여 왔다. 그래서 현 은행 시스템을 대체하기가 쉽지 않으며 비용감소에 대한 분석 및 연구도 미비한 상태이다.

본 연구에서는 현재 은행업의 주요 서비스와 은행권의 분산원장 기술 POC(Proof of Concept)를 기준으로 비용감소 효과를 연구하고자 한다.

다. 비용절감 효과 분석

(1) 송금

먼저 대표적인 금융서비스인 송금을 살펴보면, 국제 송금의 대표적인 송금망을 운영하는 국제은행간통신협회(SWIFT)의 보고서에서는 분산원장 기술을

이용하면 금융회사들이 기존의 막대한 전산 인력·인프라 투자비용을 상당히 줄일 수 있다고 추정하였다. 또한 분산원장 기술을 적용 시 금융 소비자들은 보다 빠르고 편리하게 거래할 수 있을 뿐 아니라 금융회사 투자비용 감소로 인한 수수료 인하 효과까지 기대할 수 있다고 보았다.

은행 내부거래를 제외하고 다른 은행 간의 거래 즉 타행송금을 살펴보면 서로 다른 은행망과의 거래를 할 때 현금을 직접 그 수취 고객의 계좌에 입금하는 것이 아닌 고객이 지급(Payment)한 후 결제(Settlement)가 완료되기 이전에 송금 받는 은행의 전산 상에 수취인의 잔고(Balance)를 먼저 증가시키는 방식을 취하고 있다. 결국 이러한 실시간 송금을 위해 수취은행은 은행 간의 정산 전까지 상대 은행의 지급 불이행이나 파산 등 리스크에 노출되게 된다. 이러한 리스크 부담을 해소하기 위한 방안은 은행 간 환거래계약(코레스 계약)을 통한 거래와 환거래 은행(코레스 은행)을 통한 거래 두 가지로 구분할 수 있다. 환거래 계약에 의한 송금 건들의 경우 은행들이 당일에 있었던 거래들을 상계(Netting) 하여 차액을 하루에 한번 하나의 이벤트로 묶어 이연차감결제 형태로 정산하게 된다.[11]

또한, 코레스 은행을 통해 받는 방법에서는 송금은행과 수취은행이 환거래 계약이 없는 경우 송금 중간에 양은행과 환거래 계약을 맺고 있는 중계은행(Intermediary Bank)이 결제를 해주는 방식을 채택하고 있다.

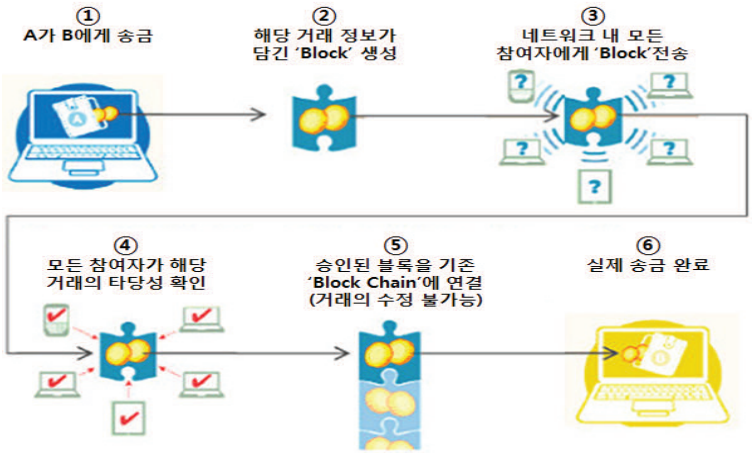
우리나라는 송금에 청산은행, 금융결제원과 한국은행이 개입하고 있는 형태로서, 청산을 위해 각각 다른 은행의 결제내역과 각종 정보가 금융결제원에 보내진다. 그리고 청산결과가 한국은행에 보내지며, 한국은행은 이러한 청산결과를 토대로 각 은행 간 결제를 완결시키게 된다. 즉 해당 은행이 아닌 기관들이 송금의 청산과 결제에 직접 개입하므로 최종송금까지 시간이 소요되며, 이 시간동안 은행들은 거래상대방 리스크 및 유동성 리스크 등에 노출되고 비용을 부담하게 된다.

특히 거래상대방 리스크와 유동성 리스크에 더욱 크게 노출되는 해외송금의 경우 분산원장 기술의 비용절감 효과가 더욱 클 수 있는데, 지금까지의 송금거래는 SWIFT라는 공통, 통일된 메시지를 보낼 수 있는 프로토콜을 쓰

11) Finector Report(2016.09)

고 있다. SWIFT 망을 통한 해외 송금 시 환거래 은행의 수와 이체금액 그리고 메시지의 수가 늘어날수록 막대한 비용과 시간이 소요되며 앞서 언급된 유동성리스크와 거래상대방 리스크도 발생할 수 있다.

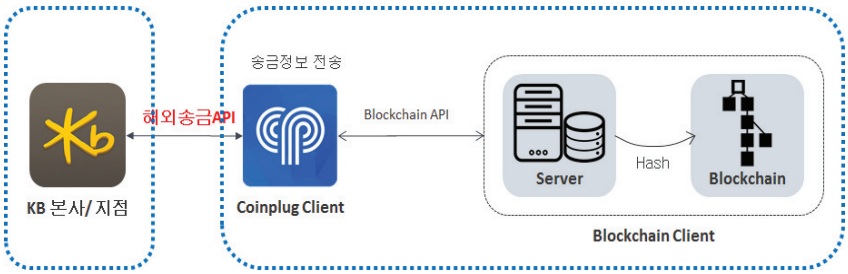
<그림 2-9> 분산원장 기술을 이용한 송금



자료: FT(2015. 11. 1)

분산원장 기술 적용 시 지급 청산 결제로 이어지는 처리가 빨라지므로 은행들의 지급금액의 시간이 단축되고 자금의 유동성 위험이 줄게 되어 유동성 리스크에 따른 비용을 줄일 수 있을 것으로 예상한다. 실제로 2016년 KB국민은행은 분산원장 기술을 이용한 송금 POC(Proof of Concept)를 분산원장 기술 전문회사인 코인플러그와 수행하여 KB은행 한국 본사에서 KB은행 동경지사로 송금하는 데 성공하였다.

<그림 2-10> KB국민은행 송금 POC

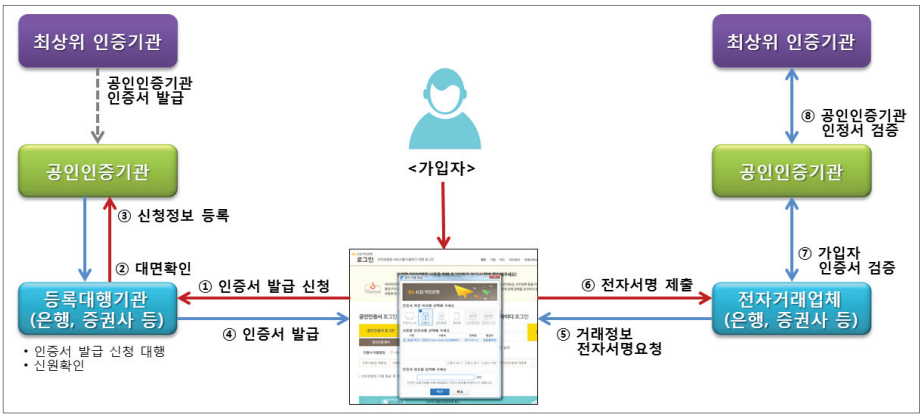


자료: (주)코인플러그

(2) 분산원장 기술을 이용한 공인 인증서

전자서명으로 대표되는 공인 인증서는 전자적인 형태로 발급되는 자신만의 인감이며 서명이다. 전자서명은 거래를 증명하거나 상대방이 누구인지 신원을 확인하는데 사용할 수 있으며, 현재 가장 보편적으로 쓰고 있는 자기 증명의 수단으로 자리 잡았다. 공인인증서가 사용되는 분야는 인터넷뱅킹·증권거래·인터넷을 통한 카드 결제·보험 등의 금융업무와 전자세금계산서·전자입찰·전자계약 등의 기업 조달업무, 정부에서 제공하는 전자민원·전자정부 업무 등이 있다.[12)]

<그림 2-11> 기존 공인인증서 방식



자료: 한국인터넷진흥원(KISA) 홈페이지

① 사용자는 은행 및 증권 등의 대행기관을 통하여 공인인증서 발급을 신청한다.

② 대행기관은 사용자 신원을 확인한다.

③ 대행기관은 공인인증기관에 사용자 신청정보를 등록한다.

④ 사용자에게 공인인증서가 발급된다.

⑤ 전자거래 업체는 사용자에게 전자서명을 요청한다.

⑥ 사용자는 발급받은 공인인증서를 통하여 전자서명을 전자거래업체에 제출한다.

⑦ 전자거래업체는 공인인증기관에 사용자가 제출한 인증서 검증을 요청한다.

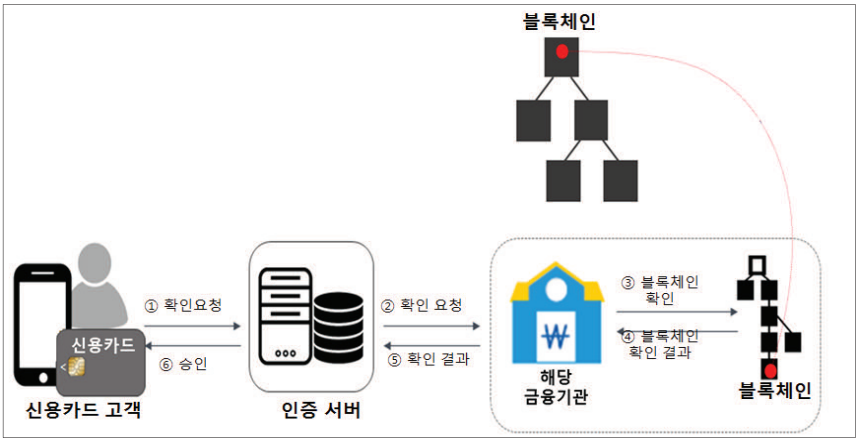
⑧ 공인인증기관은 인증서를 검증하여 전자거래업체에 제공한다.

현재 공인된 제3의 기관인 한국정보인증(주), 한국증권전산(주), 한국전산원, 금융결제원, 한국전자인증(주), (주)한국무역정보통신이 공인인증 서비스를 제공하고 있다. 이에 따라 등록비용과 인증에 대한 추가 비용이 발생하고 있으

12) 한국인터넷진흥원(KISA) 홈페이지

며, 최근에는 모바일(Mobile) 인증과 같은 본인인증이 쓰이고 있는데 이 또한 통신비와 각 통신사의 고객 데이터 접속 비용 등 추가 비용도 발생한다. 이와 같은 비용들은 공인인증서비스를 사용하고 있는 금융사와 소비자가 부담해야 하는 금액으로 일련의 인증 비용을 년 단위로 산출해보면 상당한 비용들이 드는 것이 현실이다.

<그림 2-12> 분산원장 기술을 이용한 인증서비스



자료: ㈜코인플러그

분산원장 기술을 이용하여 이러한 등록, 재등록에 있어서 각종 금융비용을 줄인 인증서비스는 제3의 기관을 배제한 인증서비스로서 KB 국민카드가 프라이빗 블록체인을 이용한 개인인증 서비스를 11월중 오픈할 예정이다. 현재는 사용자가 모바일 앱카드에 로그인할 때나 신용카드를 등록할 때 혹은 30만 원 이상 결제할 때 공인인증서를 통한 추가 인증이 필요하다. 하지만 KB국민카드는 공인인증서 대신 블록체인 기술을 활용한 '간편인증' 서비스를 추가해 이용자들이 추가 인증 방식을 선택하도록 할 계획이다. 이용자들이 간편인증 서비스를 선택하면 공인인증서처럼 유효기간이 만료될 때마다 인증서를 발급 받을 필요가 없다. 비밀번호도 6자리로 단순해 공인인증서(10자리)에 비해 사용이 간편하도록 했다. KB국민카드 입장에서도 공인인증서 발급 기관과 고객데이터를 주고받을 필요가 없기 때문에 개인인증에 들어가는 시간·비용을 절약할 수 있다. 블록체인 네트워크에서는 모든 이용자가 거래 내역을 공유하기 때문에 거래 내역을 관리하는 제3의 보증기관이 필요하지 않다. 그 때문에 거래 시간과 비용이 크게 단축되고, 데이터 위·변조가 어렵기 때문에 해킹 역시 불가능하다.[13]

4. 소결

분산원장 기술은 비트코인이라는 가상화폐로부터 시작되어 현재 특히 자본시장과 금융 산업 전체에서 활발한 논의 및 적용 움직임을 보이고 있다. 앞에서 밝힌 바와 같이 주식거래 등 증권시장에서 분산원장의 기술은 이미 여러 POC(Proof of Concept)들을 통해 적용 가능함이 밝혀졌으며, 호주 증권시장과 미국의 나스닥은 블록체인을 이용한 증권 거래시스템을 부분적으로 시작하려 하고 있다. 가장 큰 이유는 분산원장이 기존 시스템 대비 데이터의 무결성과 비용절감, 중개기관의 배제 그리고 거래시간의 단축의 이점이 자본시장에 실현될 수 있다고 보기 때문이다.

분산원장 기술의 최대 강점인, 거래승인 권한과 정보의 민주화(Democratization) 즉 다른 공인 기관이나 제3자, 중개기관의 개입을 배제하고 시스템에 의한 자율적 권한 위임이 가능해지는 것이 자본시장과 금융기관에서 두드러진다. 금융시스템에서는 관여자들의 "축소" 다시 말하면 관여자들에게 지불되는 비용들의 절감을 직접, 간접적인 긍정적인 효과로 보고 있다.

본 연구에서 밝힌 바와 같이 현재 해외경제연구소, 해외 금융컨설팅회사를 중심으로 작성된 분산원장 기술 보고서에서는, 엄밀한 정량적 분석이 아니라 비용절감 측면에서 예상과 추정만으로 분산원장 도입의 편익을 측정하고 있는 상황이다. 여러 보고서에서는 이러한 비용감소의 추정 중에서 증권시장 즉 자본시장(Capital Market)의 경우는 후선업무(Back office) 기능이 제3의 기관의 비용으로 명확히 구분되어 있어서, 비용의 추정 및 예측이 어느 정도 용이한 것으로 밝히고 있다. 하지만 시중은행들, 즉 증권시장을 제외한 금융기관들은 수행하는 서비스와 역할에 따라 차이가 있겠으나, 결제 및 지급과 기타 은행업무들 업무 범위와 내용이 광범위하고 프로세스의 구획이나 비용이 명확히 구분되지 않으므로 분산원장 기술 도입 시 비용절감 효과에 대한 정확한 정량적인 리포트가 아직까지는 없는 실정이다. 결국, 기존 시스템과 비교하여 비용감소를 명확하게 측정하기가 어려운 것이 현실이다.

앞으로 금융기관 즉 시중은행에서 분산원장 기술의 비용감소 효과를 보다

13) 매일경제신문 2016.10.24

명확하게 정량적으로 평가하기 위해서는 각 국내 금융기관들에서 시행되고 있는 POC(Proof Of Concept)를 중심으로 각 서비스 차원에서 분산원장 기술을 적용하는 경우 금융기관 비용변수, 금융소비자의 비용변수를 구별하여 비용을 측정하여야 한다. 특히 시중은행에 분산원장 기술을 적용하는 경우, 본 연구에서 “국제송금”이나 “인증 서비스” 등을 사례로 밝힌 바와 같이 금융기관의 비용과 금융소비자의 비용을 별개로 구분, 분석해야만 효과적인 비용절감을 예측할 수 있을 것이다.

분산원장 기술이 금융시스템에 적용하는 방안에 대한 논의가 시작되고 있는 현 상황에서 단순히 기존 금융 서비스 대비 비용의 감소만으로 분산원장의 편익을 측정하기 힘들다. 앞으로 분산원장 기술의 적용시 편익과 비용감소 측정을 위해서는 분산원장 플랫폼을 구축한 은행들 및 금융기관들을 중심으로 여러 은행업무들(대출, 송금, 인증, 보험, 기업금융, 무역금융, 펀드판매 및 체결 등)을 각각 세분화하여 각각의 서비스별로 효과를 측정할 필요성이 있다.

기술의 변천을 살펴보면 진보된 기술이 불필요한 비용과 업무 프로세스를 줄이는 것을 목표로 발달하고 적용되어 왔다. 인터넷이 출현했던 1980년대 이후 추가적인 규약과 프로토콜이 규정지어지면서 전 사업 분야에 급속도로 적용되어 전체 산업에 혁명을 가져왔던 것처럼, 분산원장 기술 플랫폼에 향후 여러 금융 서비스 프로토콜이 더해진다면, 금융전반에 혁명을 불러올 것을 본 연구를 통해 예측해 볼 수 있다.

Ⅲ. 분산원장 기술과 금융인프라

1. 분산원장 기술의 발전 방향

가. 분산원장 기술의 잠재적 편익과 장애 요인

분산원장 기술(Distributed Ledger Technology, DLT)의 일반적인 장점은 처리속도의 개선, 비용 절감, 보안성의 강화, 처리과정의 신뢰성 증진과 감시가능성의 확대이다. 그러나 현재까지 소개되고 있는 분산원장 기술의 활용 사례들은 일반적인 장점들을 모두 수용하기 보다는 각각 독특한 편익과 결점을 지니고 있다. 이는 아직까지 분산원장 기술이 발전 초기단계에 있고, 대규모의 성공적인 실험에는 한계가 있음을 보여주고 있다. 비록 방대한 이론적 해법과 소규모의 개념증명(Proof of Concept)이 가능성을 보이고 있지만 시스템의 호환성, 법과 규제의 강제가능성 등에서 문제를 보이고 있다.

<표 3-1> 분산원장 기술의 잠재적 편익과 장애 요인

잠재적 편익	장애 요인
거래 속도의 증가	분산원장 기술별로 환경이 달라 공개와 비공개, 가장 적절한 합의 방법과 그에 따른 에너지 소모 등에 차이 존재
정확성의 증가와 인적오류 감소	분산원장의 규모성과 현존 솔루션 간의 경합 능력이 불확실함. 특히 대규모의 빠른 응용에서는 아직까지 분산원장의 승인과정이 느림
사기의 기회 감소	분산원장 기술별이나 현존 비분산원장 기술과의 호환성이 검증되지 않아 현존 시스템의 혁신위험과 내부부서 간 승인 및 책임 문제 존재
효율성 증진과 인프라비용 감소	기업 비밀정보의 공유는 원치 않기에 산업표준의 제정에 아직 회의적임
거래의 투명성과 감시가능성 증가	기술개발 이전에 규제기관의 지원이 필요한 산업이 있으나 규제기관 간의 부조화로 개혁을 제한할 수 있음 분산원장에 탑재되는 자산의 다양성은 다수의 규제기관의 개입 개연성을 높이며, 분산원장 기술의 실패를 대비한 응급대책을 요구
악성공격에 대한 회복력 증가	디지털화된 자산에 대해 데이터의 소유자, 보유처, 국가 간 규제, 스마트계약의 코딩에러 등 대비 필요
보안성 강화	해커의 공격 가능성과 프라이버시의 인정 범위
응용가능성 확대	분산원장 기술의 비용 효율성은 요구되는 투자와 실행위험에 대비되어야 함

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

그러나 현재 분산원장은 기술적으로 이중지불이 방지되는 인증된 거래, 데이터의 추적과 투명한 거래, 해킹이 불가능한 생태계에 기반을 두어 활용되고 있다. 단기적으로 분산원장 기술은 디지털화폐를 비롯한 각종 포인트의 전달, 공유, 관리 등을 포함한 다수의 특수한 목적을 가진 서비스로 응용될 수 있으며, 더 나아가 토지등록 관리, 특허를 비롯한 각종 증명 등에도 활용이 가능하다.

이러한 서비스의 공통적인 특징은 제3자의 중개에 의존하지 않는 비즈니스 모델로 상당한 비용절감 효과를 지니고 있다는 점이다. 일례로 2016년 5월 런던시장 선거의 한 후보자는 런던시의 예산을 블록체인에 등재하여 누구든지 열람이 가능하게 한다는 'MayorsChain'을 만들 것을 공약하였고, 이를 통해 런던시 예산의 5%인 14백만 달러 정도가 절감되는 효과가 있을 것이라 주장하였다[14]. 분산원장 기술의 도입이 가져오는 비용절감 효과는 크게 IT시스템과 기업경영 측면으로 구분하여 볼 수 있다. IT시스템 측면에서는 응용기술 개발비용, 인프라 장비조달 비용, 중간구조 개발비용 등의 절감을 거둘 수 있고, 기업경영 측면에서는 회계감사 비용, 종이서류 관리비용, 노동비용 등의 절감을 가져온다. <표 3-2>에서는 이들 비용절감 요인별로 개요를 설명하고 있다.

나. 분산원장 기술의 발전 예측

분산원장 기술은 지난 3년간 2,500건 이상의 특허 출원과 140억 달러가 넘는 자금이 투자되었으며 현재 24개 이상의 국가에서 이 기술에 투자하고 있다. 또한 현재 90개 이상의 블록체인 관련 컨소시엄이 형성되어 있으며, 90개 이상의 중앙은행이 분산원장 기술에 대한 논의에 참여하고 있다. 이러한 추세를 반영하여 2017년에는 전 세계 주요은행의 80% 이상이 분산원장 기술에 대한 프로젝트를 추진할 것으로 예상되고 있다[15].

<그림 3-1>에서 보는 바와 같이 분산원장 기술에 대한 인식은 전 세계적으로 크게 증가하고 있지만 대규모 실행에는 아직까지 풀어야 할 과제들이 많

14) uk.businessinsider.com/george-galloway-blockchain-bitcoin-mayorschain-london-2015-7 참조
15) World Economic Forum and Deloitte, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, Part of the Future of Financial Services Series, 2016.8, p.14참조

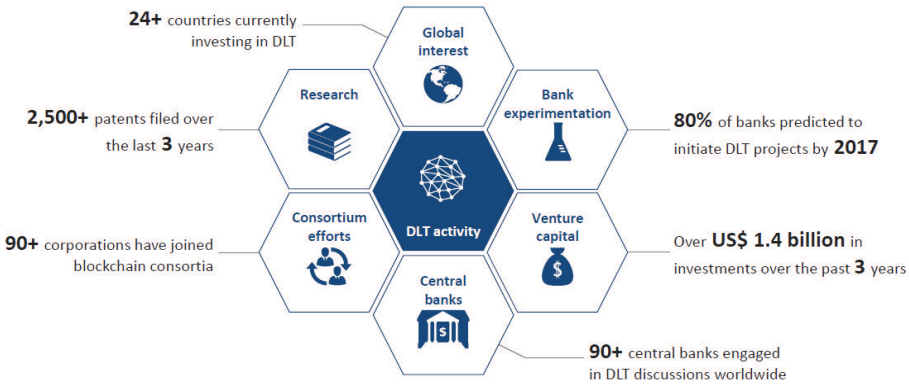
은 상황이다. 특히 규제내용의 불확실성 및 국가별 규제기관 간의 조화, 초기단계의 호환성 및 공통표준화에 대한 노력, 정당한 법적 틀의 부재 등이 장애 요인으로 자리잡고 있는 실정이다.

<표 3-2> 분산원장 도입에 따른 비용절감

구분	절감 요인	개요
IT 시스템	응용기술 개발비용 절감	· 클라우드 기반의 비공개 분산원장 환경으로 이전함으로써 비용 감소 · 백업 비용과 위기대응 비용의 감소 가능
	인프라 장비조달 비용 절감	· 위기대응과 관련한 계획, 설계, 테스트의 개인적 비용 감소 · 오픈소스로 자원의 자급자족인 경우 비용 절감 가능
	중간구조(middle structure) 개발비용 절감	· 분산원장의 개발설계가 현존 DB를 수용하는 구조일 경우 비용 감소 · 운영관리 측면의 비용 절감 가능
기업 경영	회계감사 비용 절감	· 지급보증서나 거래기록의 관리 비용 절감 · 거래 투명성과 사기의 어려움으로 인한 제3자의 회계감사 비용 감소
	종이서류 관리비용 절감	· 종이서류로 진행되는 작업의 감소로 인한 비용 절감 · 메일을 이용한 아날로그식 인증 비용의 감소
	노동비용 절감	· 원스톱 디지털 작업에 따른 노동비용 절감 · 스마트계약의 실행에 따른 운영인력 비용 절감

자료: Nomura Research Institute, Survey on Blockchain Technologies and Related Services, FY2015 Report, 2016.3

<그림 3-1> 전 세계 분산원장 기술 참여 현황



자료: World Economic Forum and Deloitte, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, Part of the Future of Financial Services Series, 2016.8, p.14

전 세계 금융기관, 규제기관, 핀테크 스타트업의 주목을 받고 있는 분산원장 기술은 향후 4단계에 거쳐서 발전할 것으로 예측되고 있다[16]. 먼저 제1단계(2016~2019)에서는 주로 단순한 응용으로 견고하고 일관된 데이터 공유에 활용될 것이다. 주로 3가지 분야에 집중될 것으로 보여 합의한 상대방과의 데이터 공유로 공용데이터에의 접근과 데이터의 이중 수집 방지, 설명과 메시지를 분산원장에 등재함으로써 데이터의 변경 기회를 줄이며, 문서화 과정의 효율성을 제고시키는 데 활용될 것으로 기대된다. 예를 들어 2차 대출시장의 문서송신과 인증에서 현재 금융인프라와 처리 절차에 분산원장에 근거한 데이터 흐름이 가미됨으로써 개선될 것이다. 분산원장 솔루션들은 마찰적(거래적) 비용을 줄여줌으로써 2차 대출시장에 대한 폭넓은 접근과 유인을 제공할 것이다.

제2단계(2017~2025)에서는 분산원장 기술과 스마트계약이 주요 거래데이터를 저장하고 공유하는데 결합되어 사용될 것으로 예측된다. 분산원장 기술은 자산관리자에게 자신들의 투자 포트폴리오를 추적하고, 상품을 개발하여 고객서비스를 제공할 수 있는 환경을 만들어 줄 수 있다. 그리고 분산원장 기술을 활용하여 실시간으로 데이터를 송신할 수 있기에 고객들은 위험과 투자실적에 대한 가장 최근의 분석을 이용할 수 있다. 즉 투자자는 직접 분산원장에 접속하거나 금융기관이 제공하는 인터페이스를 통해 자신의 거래데이터에 실시간으로 접속함으로써 셀프서비스 분석보고서를 새로운 투자분석 수단으로 제공받을 수 있다. 이러한 제2단계의 응용들은 향후 2~5년 안에 개발 활용될 수 있으며 현존하는 과정과 병행하여 고객에게 불필요한 효과를 최소화하는 방향으로 전개될 것이다. 이에 따라 전체 투자생태계와 최종사용자들이 분산원장 솔루션에 대해 신뢰를 형성함에 따라 점차 분산원장의 활용 규모가 커질 것으로 기대된다. 이에 따라 쓸모없는 후선 및 중간 오피스의 데이터 인프라는 비용절감을 위해 폐기될 것으로 전망된다.

제3단계(2020~2030)에서는 분산원장 기술이 자본시장의 주요 인프라에 본격적으로 적용될 것으로 예측된다. 자산이 분산원장에 토큰으로 등재되어 동시에 복수 자산의 거래 청산 및 결제가 가능하게 됨으로써 이전 두 단계에서 예상되었던 하이브리드나 복수 시스템을 대체하여 자산거래 사이클을 단축시키고 유동성을 제고시킬 것이다. 또한 분산원장 기술에 근거한 인프라의

16) J.P.Morgan and Oliver Wyman, Unlocking Economic Advantage with Blockchain: A guide for asset managers, 2016, p.7 참조

구축으로 새로운 투자 상품과 플랫폼의 개발이 가능하게 됨으로써 ETF(exchange trade fund)와 같이 다양한 투자 상품을 결합시킨 신상품을 출시하거나 관리비용 및 자산거래 관련 간접비를 절감하기 위한 스마트계약이 가능할 것으로 기대된다.

현재 발전 방향이 불확실한 제4단계에서는 금융시스템이 완전히 분산된 인프라를 기반으로 구축될 것으로 예상되지만 최초의 진행은 규제기관의 관리를 받는 시스템으로 추진될 수 있을 것으로 예상된다. 그러나 오픈소스 플랫폼에 의해 사적 경로로 금융인프라가 구축될 가능성도 배제할 수는 없을 것이다.

<표 3-3> 분산원장 기술의 단계별 잠재적 활용

활용 예	개요	편익	발전 단계
거래의 문서화 속도 증진	신뢰된 네트워크에서 대출 및 IPO 문서 공유와 승인	· 계약용어의 표준화 · 처리속도 증진 · 유동성 개선	1단계 (2016~2019)
조회데이터 원천의 공유	시장참가자의 일반적인 조회데이터를 분산원장에 갱신	· 이중 작업의 방지 · 자금세탁위험과 벌금부과가능성 경감	1단계 (2016~2019)
이질적 내부시스템 간의 데이터 분배	분산원장의 복수 내부시스템을 망라한 활용	· 내부조화 필요성 제거 · 정확하고 전체적인 견해 제공	1단계 (2016~2019)
비유동적 자산 정보를 위한 사적 네트워크 활용	비유동적인 장외시장 거래자산에 대한 거래상대방 발견	· 적절한 자산의 표준 정보 공유 · 중개수수료의 감소 · 큰 규모 자산풀에 제한된 접근 허용과 민감한 시장정보의 누출 방지	1단계 (2016~2019)
작업흐름과 분석을 지원하는 데이터 환경 구축	거래단계의 데이터를 암호화하여 안전한 스마트계약에 저장하고 사용자가 접속 노드를 통해 작업흐름에서 활용	· 데이터의 조화과정 제거 · 더욱 효과적인 투자분석	2단계 (2017~2025)
담보자산의 원천 및 활용 추적	분산원장을 통한 담보자산의 상태와 위치, 적격성, 재담보 설정, 초과담보 등 추적	· 복수의 마진계좌 연계 · 실시간 상태 파악 · 스마트계약과 함께 최적화 논리 지원	2단계 (2017~2025)
펀드 투자환경 개선	펀드의 이전과 소유권을 분산원장으로 추적	· 펀드가입과 상환 자동화 · 투자 사이클의 개선	2단계 (2017~2025)
규제기관의 셀프서비스 분석보고 가능	허가되고 분할된 분산원장에 대한 규제기관의 셀프서비스 분석보고서	· 규제기관의 분석보고 실패 가능성 경감	2단계 (2017~2025)
고객을 위한 분석 포탈 활용	고객이 실시간으로 직접 또는 포탈을 통해 투자포트폴리오와 실적을 분석	· 실시간으로 풍부한 정보 제공 · 개별 고객의 분석니즈에 부합	2단계 (2017~2025)
T+0 결제환경 구축	청산과 결제 과정을 단축시키는 시스템 구축	· 결제유동성 위험의 현저한 감소 · 자본의 효율적 배치	3단계 (2020~2030)
주권 관련 활동 개선	대리투표, 수익분배 등의 관리 효율화	· 관리 비용 및 수작업 경감	3단계 (2020~2030)
마진콜의 자동 실행	스마트계약을 통한 마진증거금 산출과 갱신	· 중앙거래당사자의 일중 유동성위험 제거와 전반적인 마진증거금 감소 · 관리 부담의 감소	3단계 (2020~2030)
새로운 상품 개발 활용	분산원장에 디지털화된 지분을 소유함으로써 새롭게 결합된 상품의 개발과 스마트계약의 활용	· 거래 및 관리에 수반한 간접비 경감 · 일중 유동성 제공 필요성 경감	3단계 (2020~2030)
P2P 보관과 결제 네트워크 활용	분산원장에 등재된 디지털화된 자산의 개인간 장외거래 네트워크 구축	· 중개자의 필요성 제거 · 결제 속도의 대폭 개선	3단계 (2020~2030)

출처 : J.P.Morgan and Oliver Wyman, Unlocking Economic Advantage with Blockchain, 2016, p.9

다. 분산원장 기술의 활용

현재 금융회사들은 수익성이 제한되고 있는 가운데 비용 효율성을 제고시키기 위해 분산원장 기술에 기반한 솔루션을 지급, 자본거래 후선업무, 무역금융 등의 분야에서 적극적으로 개발하고 있다. 그러나 분산원장 기술의 활용은 금융 분야를 넘어 비금융기업 및 공공부문까지 확대될 가능성이 있다.

다음의 <표 3-4>에서 보는 바와 같이 분산원장 기술은 금융, 기업, 정부, 산업연계 분야에 걸쳐 고루 활용될 것이다. 특히 금융부문의 국제송금, 자본시장, 무역금융 등과 정부부문의 신원관리, 세금, 규제감시 등에서 활용도가 높을 것으로 예측된다. 이밖에도 빅데이터, 사물인터넷, 클라우드 컴퓨팅 등 분야와 연계되어 분산원장 기술은 그 활용의 폭이 더욱 넓어질 것으로 보인다.

<표 3-4> 분산원장 기술의 활용 분류

금융	기업	정부	산업 연계
국제송금	공급사슬관리	기록 관리	재무관리 및 회계
자본시장	헬스케어	신원 관리	주주 투표
무역금융	부동산	투표	기록 관리
규제준수 및 감사	미디어	세금	사이버보안
자금세탁방지 및 고객알기제도	에너지	정부 및 비영리기구 투명성	빅데이터
보험		입법, 준수, 규제 감시	데이터저장
P2P 거래			사물인터넷

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

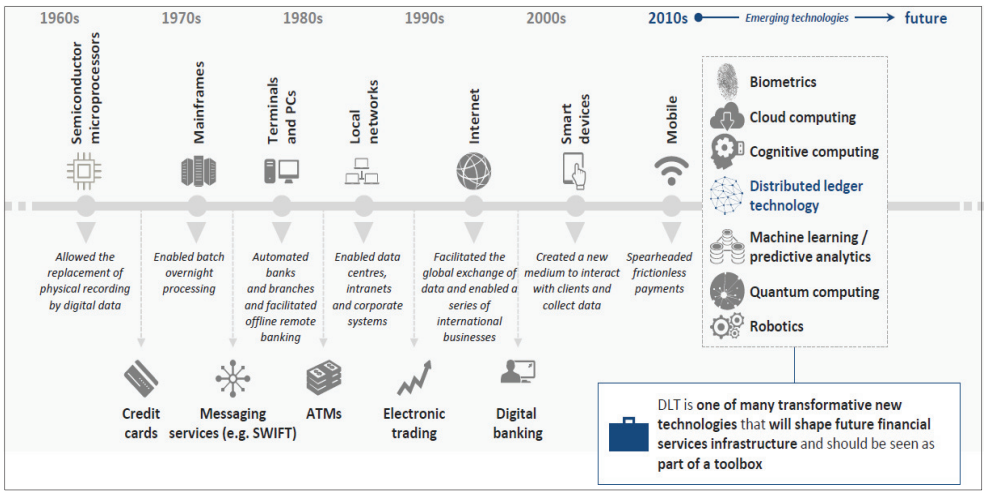
라. 분산원장 기술의 위상

분산원장 기술은 기존 금융인프라와 금융거래의 설정에서 탈피하여 새로운 설정을 구축함에 있어 단순성과 효율성을 제고시키고 있다. 이는 다음의 6가지의 중요 추진요인에 근거하고 있는데 첫째, 운영의 단순화로 합의와 논쟁 해결에 요구되는 수작업을 줄이거나 없앨 수 있으며 둘째, 규제의 효율성 개선으로 규제기관이 대상기관을 실시간 모니터하는 것이 가능하다는 것이고 셋째, 거래상대방위험의 감소로 변경이 불가능한 공유 환경에서 성문화되어

실행되는 규약에 충족되는 거래상대방만이 참여할 수 있다는 것이다. 그리고 넷째, 청산 및 결제 시간의 감소로 거래의 증명과 인증, 신속한 결제를 위한 제3자의 중개에서 탈중개화 되고 다섯째, 유동성 및 자본 요건의 개선으로 자본의 잠금이 줄어들고 투명한 유동성 관리가 가능하며 여섯째, 사기의 최소화로 자산의 증명과 거래이력의 추적이 가능하므로 자산의 신뢰성을 제고시킬 수 있다는 것이다.

이와 같이 분산원장 기술은 단순성과 효율성을 제고시킴으로써 금융서비스의 편익을 증대시켜 줄 기술로 많은 주목을 받고 있지만 실제로는 차세대 금융인프라의 근간을 형성할 여러 가지 기술 중에 하나이다. 지난 50년 동안 기술혁신은 금융산업을 변화시키는 근간을 이루어 왔는데 현재 복수의 차세대 기술들이 금융서비스의 혁신을 위해 수렴 성숙되고 있으며, 분산원장 기술은 미래 금융인프라에 변화를 주는 신기술 중의 하나이자, 이러한 기술들이 형성하는 툴박스의 한 부분이다. <그림 3-2>에 따르면 분산원장 기술은 생체인증, 클라우드컴퓨팅, 인지컴퓨팅, 인공지능, 퀀텀컴퓨팅, 로봇공학 등과 함께 미래의 금융인프라를 구축할 주요 기술로 주목받고 있다.

<그림 3-2> 기술혁신과 금융서비스의 진화



자료: World Economic Forum and Deloitte, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, Part of the Future of Financial Services Series, 2016.8

미래 금융인프라 구축에 있어 중요한 역할을 할 것으로 기대되는 분산원장 기술의 영향력을 제고하기 위해서는 금융회사, 혁신기업, 규제기관의 이해와

깊은 협업이 필요하다. 분산원장 기술을 바탕으로 금융인프라를 갱신하는 것은 상당한 시간과 투자를 요구하고 있으므로 성공적 실행을 위해서는 다음의 3가지 측면이 반드시 고려되어야 한다. 첫째는 현재의 금융인프라를 분산원장 기술로 대체하기에는 상당한 시간과 투자가 요구된다는 점이고, 둘째는 제로섬 게임으로 주요 참가자들의 이해관계 조절이 요구되며, 셋째는 새로운 금융인프라의 추진이 현재의 규제 및 관례의 변화와 새로운 법적 책임 틀을 만들어야 한다는 것이며, 특히 스마트계약의 실행은 참가자들의 지지와 관리방식에 대한 고려가 반드시 요구된다. 아직까지 이 3가지 측면을 동시에 달성하는 것이 힘들기에 고도로 규제된 시장에서 복수상대방이 있는 분산원장 기술의 대규모 실행을 어렵게 하고 있다. 그러나 향후 이것이 가능하다면 상당한 규모의 인프라 구조, 산업계 전체적인 솔루션, 표준화된 거래과정을 달성할 수 있을 것이다.

2. 분산원장 기술의 적용에 따른 금융인프라의 변화

가. 분산원장 기술의 금융인프라 적용

분산원장 기술로 새롭게 설정되는 금융인프라는 금융거래 과정을 변화시켜 현재 비즈니스모델의 근간에 의문을 제기하고 있으며, 이는 분산원장 기술의 특성인 변경불가능성, 투명성, 자율성에 그 기반을 두고 있다.

<표 3-5> 분산원장 기술의 특성과 금융시장에의 의미

현재 상태	분산된 인프라의 특성	금융시장 참가자에의 의미
· 정보저장소의 세밀한 조정 행위 필요 · 신뢰받는 단일버전의 부재와 차익거래에 대한 감사 필요	· 변경불가능성 (불가역성)	· 조정의 필요 제거 · 신뢰성 있는 단일버전의 이력 제공
· 비대칭적 정보로 인한 규제기관의 영향력 급증 · 투명성의 부족으로 금융인프라에 대한 규제 증가	· 투명성	· 시장참가자 간의 정보비대칭성 제거 · 규제기관과 대상기관 간의 협력 증대
· 거래상대방에 대한 신뢰부족으로 규제기관의 감시 요구 발생	· 자율성	· 비즈니스 결과에 대한 확실성 증대 · 분쟁해결 지원기관으로부터의 탈중개화

자료 : World Economic Forum and Deloitte, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, Part of the Future of Financial Services Series, 2016.8, p.24

(1) 변경 불가능한 분산된 기록관리

전통적으로 자산 및 거래 정보는 독립적인 저장소에 물리적으로 보관되었으나 기술이 발전함에 따라 물리적 원장은 디지털원장으로 바뀌게 되었다. 오늘날 각각의 금융인프라는 자신만의 디지털 기록관리 저장소를 보유하고 있으며, 중앙의 중개기관이 거래의 원활화를 위해 공정한 조정을 제공하고 있다. 본질적으로 분산원장 기술은 시간에 따라 거래기록을 저장하는 블록을 만들기 때문에 이전에 실행된 거래에 대해서는 변경이 불가능하다. 또한 참여 노드 간에 데이터의 복제가 실시간으로 이루어지므로 모든 참가자들에게 항상 신뢰성 있는 단일버전을 제공하고 있다.

이에 따라 분산원장 기술은 현재와 같은 중앙집중적 정보저장소의 필요성에 의문을 제기함과 동시에 기업내부의 조정 필요성도 제거하고 있다. 또한 중개기관의 개입을 없애며 생태계 내에서 차익거래의 우려를 감소시키며, 자산 및 거래의 감사에 있어 상당한 정도로 분쟁을 줄일 수 있게 해 준다.

(2) 시장참가자 간 투명성 제고

현재 금융인프라는 대부분 도입 시기와 단편화로 인해 투명성 문제를 지니고 있어 정보의 비대칭성을 야기할 수 있다. 이로 인해 금융생태계 내의 일부 참가자의 경우 경쟁의 이익을 누릴 수 있다. 결국 일부 참가자는 정보의 이득을 얻는 상태이지만 다른 참여자는 위험의 헤징과 유동성의 확보에 있어 차선의 성과와 자원의 과도한 낭비를 초래하고 있다.

분산원장 기술은 디폴트설정이 거래의 투명성을 완전히 보장하고 있으며, 사적 기록의 개념을 변화시켜 상세한 거래내역이 상대방에게 알려진다. 또한 모든 참가자들이 실시간으로 접속할 수 있는 공개된 기록 활동을 제공할 수 있다. 이에 따라 분산원장 기술은 정보의 비대칭으로 인해 야기되는 경쟁의 이득을 줄일 수 있고, 금융생태계의 불투명성으로 인해 이득을 얻는 일부 지원기관의 역할을 경감시킬 수 있다. 더욱이 금융생태계에서 투명성이 최선인가 아니면 개인 신원 데이터의 안전성과 같은 측면에서 불투명성이 필요한가에 대한 담론을 제공하고 있다.

(3) 정보비대칭성 감소로 비용절감

현재 여러 형태의 금융거래에서 신용을 얻기 위해 자산을 담보로 제공하는데 담보로 제공된 자산이 몇 차례나 더 담보로 활용되었는지 확인하는 데에는 어려움이 있다. 이처럼 자산의 담보권 파악에 대한 어려움은 동일 자산을 복수의 채무에 담보로 제공하게 하여 종종 명목가치를 초과하게 할 수 있다. 이러한 불투명으로 인해 대출자는 평판이나 신용평가기관의 평가에 의존하게 된다.

분산원장 기술은 개별자산의 출처를 공유하며 신뢰성 있는 원장에 토큰화할 수 있기 때문에 자산 및 관련 채무에 대해 가시성을 제공하여 신용거래의 효율성을 제고시킬 수 있다. 자산 및 관련 담보권과 소유권의 가시성을 높여줌으로써 위험의 계량화와 가격의 정확성을 증진시키며, 차입자가 동일한 자산을 담보로 제공하면서 여러 상대방으로부터 대출을 얻는 활동을 억제시킬 수 있다. 이는 위험을 계량화하는 신용평가기관의 역할을 줄여줄 수도 있다.

(4) 규제기관과 대상 간의 관계 개선

규제기관은 규제대상기관에게 규제가 제대로 작동되고 있는지를 확인하는데 많은 정보가 필요하다. 비록 규제대상기관이 투명성을 약속하지만, 현재의 금융시스템과 비즈니스 절차에는 상당한 규모의 비용과 위험이 내재되어 있다. 더욱이 금융생태계의 복잡성과 금융수단의 증가로 인해 투명성과 비용 간의 상관관계는 매우 중요한 문제로 대두되고 있다.

분산원장 기술은 규제기관과 규제대상기관이 서로 데이터 저장소를 공유할 수 있어 이전처럼 중앙에 데이터가 집적되는 것을 차단한다. 또한 규제기관이 실시간으로 거래데이터의 부분집합을 공유할 수 있고, 규제가 포함된 비즈니스모델을 스마트계약 형태로 가능하게 하여 규제기관이 실시간으로 거래를 확인할 수 있다.

이에 따라 규제준수에 대해서는 거래 후 모니터링에서 온디멘드(On-demand)나 즉각적인 모니터링으로 변화가 가능하다. 또한 금융시장의

적법성, 보안성, 안정성에 대한 규제기관의 명령권을 강화시키고, 장외시장이나 사적거래소(Dark pool)를 통한 거래에 대해 모니터링의 효율성을 제공할 수 있다. 이처럼 분산원장 기술은 규제준수와 관련된 비용을 상당한 규모로 줄여줄 수 있다.

(5) 자율실행으로 중개기관의 필요성 감소

현재 최소한 두 명의 시장참가자가 있는 모든 거래는 거래상대방이 반드시 지켜야 하는 협약에 의해 통제되고 있다. 이러한 협약에 대한 책임은 법과 규제의 틀에 의해 강조되어 중개기관은 복잡한 협약을 통해 협약내용에서 벗어나지 않게 당사자 간의 분쟁을 해결하고 있다.

분산원장 기술은 분산플랫폼에 협약내용을 성문화하여 상호 합의한 조건에서 금융거래가 실행되는 것을 보장함으로써 일방의 독단적 행위를 제한한다. 더욱이 금융거래 협약의 준수를 점검하는 수작업을 사라지게 하여 비즈니스를 가속화시킬 수 있다. 이에 따라 거래상대방의 협약이행 의도나 능력의 감소로 야기될 수 있는 거래상대방위험을 줄여주며, 분쟁의 중재와 비즈니스 성과 확대를 위한 중개기관의 역할도 감소시킬 수 있다.

나. 분산원장 기술과 금융인프라의 변화[17]

(1) 국제송금

(가) 현황

전 세계적으로 국제송금 규모는 매년 5%정도씩 증가하고 있으며, 2016년에는 6천10억 달러에 달할 것으로 추정되고 있다[18]. 특히 중국을 위시한 아시아지역은 브라질을 포함한 남미지역보다 큰 규모로 미국과 유로존의 뒤를 이어 세 번째를 차지하고 있다[19][20]. 국제송금 수수료는 매우 큰 편으로 평균

17) 이하 내용은 World Economic Forum and Deloitte, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, Part of the Future of Financial Services Series, 2016.8, pp. 47~127 참조
18) World Bank, Migration and Remittances Factbook 2016, 2016 참조
19) Capgemini, Top 10 Trends in Payments in 2016, 2016 참조

적으로 지급결제 규모의 7.68%를 차지하고 있다. 그리고 최근 은행을 이용하지 않는 국제송금이 전체 규모의 10%를 차지할 정도로 규모가 커지고 있다[21]. 분산원장 기술은 개인 간 또는 기업 간 소액의 국제송금이 대규모로 이루어지는 분야에서 크게 주목받고 있다.

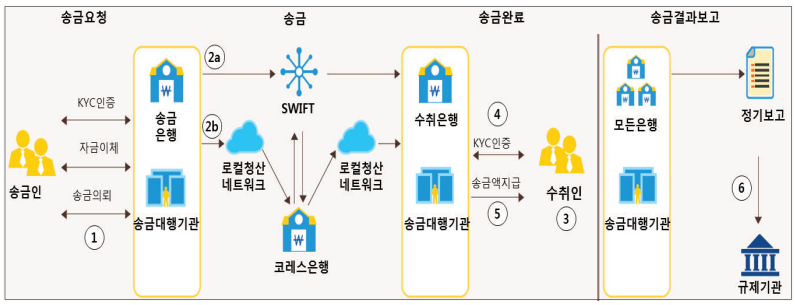
(나) 주요 참가자

국제송금 업무에서 중요한 역할을 담당하는 주요 참가자는 송금인과 수취인, 송금대행기관, 송금은행, 수취은행과 업무를 지원하는 코레스은행, SWIFT, 로컬청산은행, 규제기관이 있다.

<그림 3-3> 국제송금 주요 참가자

(다) 현재 처리 과정

<그림 3-4> 국제송금의 현재 처리 과정



① 은행이나 송금대행업자에게 국제송금을 의뢰하면 ALM/KYC 과정를 거쳐 송금액과 수수료를 수취하며 송금의뢰를 승인한다.

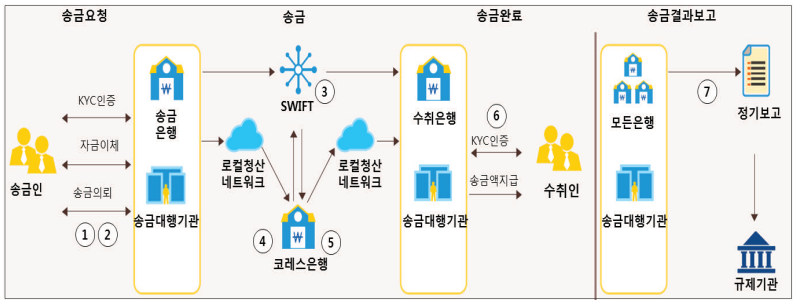
---

20) Mckinsey & Company, Global Payments 2015: A Healthy Industry Confronts Disruption, 2015 참조
21) Capgemini, Top 10 Trends in Payments in 2016, 2016 참조

② 은행이나 송금대행업자는 SWIFT망이나 코레스은행을 이용하여 자금을 이체한다.
③ 통지를 받은 수취인은 은행이나 송금업자를 찾아간다.
④ 은행이나 송금대행업자는 고객의 신원을 확인한다.
⑤ 타국으로부터 송금된 금액을 전달한다.
⑥ 은행이나 송금대행업자는 정기적으로 규제기관에 국제송금 관련거래를 상세히 보고한다(송금인과 수취인의 신원, 외환의 종류, 금액, 타임스탬프 등).

(라) 현재 처리 과정의 취약점

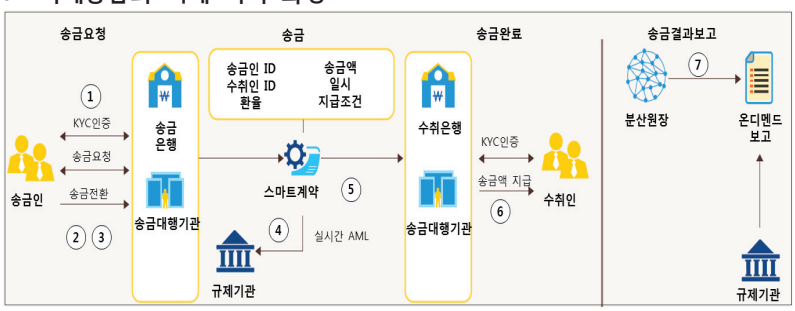
<그림 3-5> 국제송금의 현재 처리 과정의 취약점



① 송금인과 수취인에 대한 정보가 수작업과 반복적 과정을 거쳐 수집된다.
② 송금인 정보나 관련서류의 진실성에 대한 통제가 제한적이다.
③ 전달경로에 따라 지급결제 관련 비용과 시간이 많이 소요된다.
④ 은행별 또는 거래별로 정보의 승인이 거절되는 경우가 많다.
⑤ 외화타점예치계정에 자금을 넣어 두고 있으므로 기회비용과 헤징비용이 소요된다.
⑥ 수취인 정보나 관련서류의 진실성에 대한 통제가 제한적이다.
⑦ 데이터 원천과 경로의 다양성으로 인해 규제기관에 제출하는 보고서 작성에 소요되는 비용이 크고 절차가 복잡하다.

(마) 미래 처리 과정

<그림 3-6> 국제송금의 미래 처리 과정

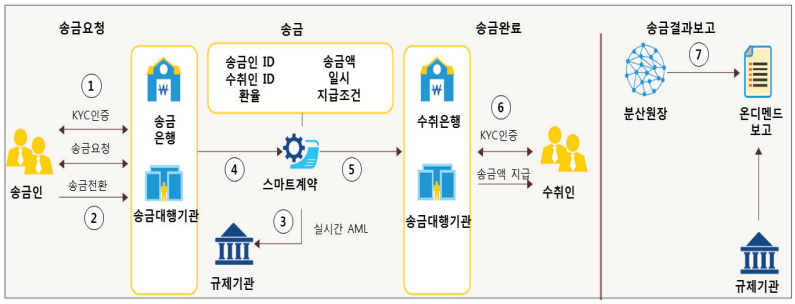


① 송금인과 은행이나 송금대행업자 간의 신뢰가 전통적 KYC나 디지털신원파일에 의해 생성된다.

② 스마트계약이 송금인과 수취인 간의 자금이체에 대한 의무를 압축 요약한다.
③ 유동성제공자에 의해 원장에서 통화가 전환된다.,
④ 규제기관이 실시간으로 거래를 모니터하고 스마트계약을 통해 AML경보를 받는다.
⑤ 스마트계약을 통해 최소수수료로 코레스은행의 개입 없이 실시간으로 자금이체를 한다.
⑥ 전달된 자금은 스마트계약을 통해 수취인의 계좌에 자동적으로 예치되거나 KYC를 거친 후 수취가 가능하다.
⑦ 규제기관은 분산원장을 통해 지속적으로 거래이력을 관찰한다.

(바) 미래 처리 과정의 이득

<그림 3-7> 국제송금의 미래 처리 과정의 이득



① 송금인은 분산원장에 저장된 자신의 디지털 프로파일로 신뢰와 인증을 받는다.
② 스마트계약을 통해 법정화폐를 송금하려는 참여자로부터 외환을 조달받는다.
③ 규제기관은 거래데이터에 접속하여 사전에 정한 조건에 근거하여 AML경보를 받는다.
④ 국제송금이 실시간으로 완결된다.
⑤ 소수 참여자의 개선된 비용구조로 인해 비용절감이 발생한다.
⑥ 수취인은 분산원장이 저장된 자신의 디지털 프로파일로 신뢰와 인증을 받는다.
⑦ 규제기관은 분산원장에 온디맨드 접속으로 거래이력을 관리한다.

(사) 필요조건 및 향후 전망

분산원장 기술을 활용한 국제송금에서 이득을 얻기 위한 핵심조건은 먼저 표준화된 KYC과정을 분산원장 참가자와 규제기관이 공유할 수 있어야 한다. 이를 통해 실시간이나 온디맨드로 AML이나 KYC에 대한 규제준수 여부를 확인할 수 있다. 그러나 은행이나 송금업자 그리고 규제기관 마다 정책이나 규제 요구조건이 상이하다는 점을 해결해야 한다.

또한 규제기관이나 중앙은행 혹은 법적 참여기관 간에 국제송금을 위한 법

적 틀을 명확히 하는데 대한 국제적 협업이 필요하다. 그러나 현재까지 이러한 협업에 대한 법적 선례가 없다는 점을 극복해야 한다. 그리고 대다수 국제지급결제 참가금융기관들이 활용할 분산원장 기술의 기본 틀에 대한 합의, 즉 상호작용성(Inter-operability)을 확보하기 위한 표준화가 이루어져야 한다. 하지만 참가자 간의 각기 다른 우선순위, 긴급 상황에 대한 견해나 예산의 차이는 국제적 합의를 도출하는데 어려움으로 작용하고 있다.

이외에도 글로벌 코레스은행이 아닌 지역은행의 경우에는 여전히 중개가 요구된다는 점, 일부 주요은행이 분산원장 기술의 채택을 주도하는 경우 이들이 표준설정에 큰 영향을 줄 수 있다는 점, 은행의 분산원장 기술을 활용한 디지털화폐 개발이 초래할 영향 등이 충분히 고려되어야 한다.

향후 분산원장 기술을 활용한 국제송금을 전망하면 2015년 12월 SWIFT는 'Global Payment Innovation Initiative'을 통해 투명한 중개수수료와 동일 일자 자금전달을 추진하고 있으나 이는 분산원장 기술에는 적용되지 않는다[22]. 북미나 유럽 지역의 도소매은행들에서 분산원장 기술의 활용에 대해 연구 및 실험을 진행하고 있으나 국제송금에 분산원장 기술을 적용하는 은행은 당분간 소수에 그칠 것이다. 그러나 규제기관에서는 분산원장 기술을 활용한 원형을 이용하여 서비스에 대한 평가와 촉진을 점검하거나 현재의 규제 틀 하에서 실행이 가능한가에 대한 검토가 진행될 것이다.

(2) 손해보험금 청구

(가) 현황

손해보험은 전 세계 보험산업에서 생명보험에 이어 2번째 큰 규모를 차지하고 있다. 2014년에는 전 세계적으로 7,286억 달러의 보험료 수입을 기록하였으며 2010년 이후로 매년 5.1%의 성장하여 2018년에는 보험료 수입이 8,951억 달러에 달할 것으로 전망되고 있다[23]. 손해보험에서 보험금청구와 처리 과정에 관련된 민원업무는 주요 마찰원인으로 수입보험료의 11%에 달

22) SWIFT는 2015년 12월 'Global Payment Innovation Initiative'를 발표하였는데 여기에는 유럽, 아시아태평양, 아프리카, 아메리카 지역을 대표하는 73개의 은행이 참여하여 현재의 국제송금과는 차원이 다른 서비스를 2017년부터 제공한다고 발표하였다.

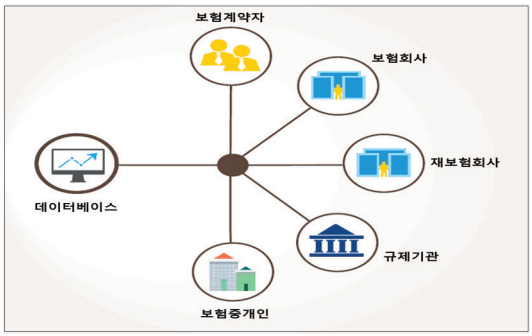
23) Finaccord, Global Commercial Non-Life Insurance: Size, Segmentation and Forecast for the Worldwide Market, 2015 참조

하는 금액을 비용으로 지출하고 있다[24]. 분산원장 기술은 손해보험에서 후선 업무 운영비용을 최적화시킬 수 있으며 특히 보험금청구의 처리에 적극 활용될 수 있다.

(나) 주요 참가자

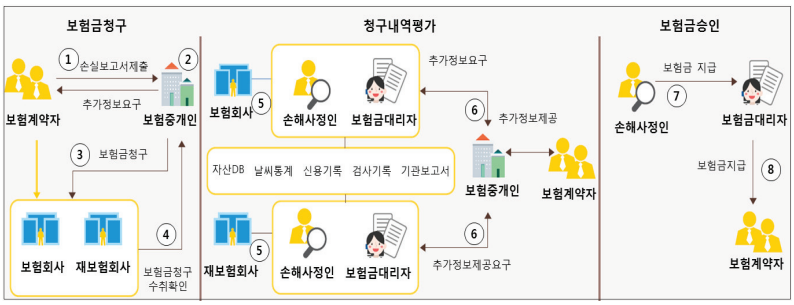
손해보험금 청구 업무의 참가자는 중요 역할을 담당하는 보험계약자, 보험회사, 재보험회사와 업무를 지원하는 규제기관, 보험중개인, 데이터베이스가 있다.

<그림 3-8> 손해보험금 청구의 주요 참가자



(다) 현재 처리 과정

<그림 3-9> 손해보험금 청구의 현재 처리 과정



① 보험계약자는 보험중개인을 통하거나 직접 보험회사에게 손해액과 보험금 보상을 요구한다.

② 보험중개인이 보험계약자에게 추가적인 정보를 요구한다.

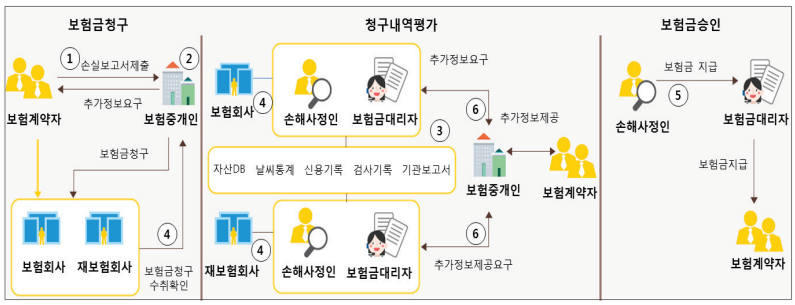
③ 보험중개인이 보험회사나 재보험회사(신디케이트보험이나 재보험의 경우)에 보험금 청구를 요청한다.

24) ISO, Verisk Analytics, 2016 참조

④ 보험회사는 보험금청구 서류 목록을 확인 후 수취확인증을 보내준다.
⑤ 손해사정사가 고객 정보, 날씨, 조사당국의 내용 및 인터뷰 등의 자료를 통하여 보험금청구의 정당성을 확인한다.
⑥ 보험회사가 추가적인 정보를 보험계약자나 보험중개인에게 요구한다.
⑦ 손해사정사가 보험금청구에 대한 평가를 마친 후 보험금지급을 승인한다.
⑧ 보험금지급 확정 후 보험회사는 보험계약자에게 확정된 보험금을 지급한다.

(라) 현재 처리 과정의 취약점

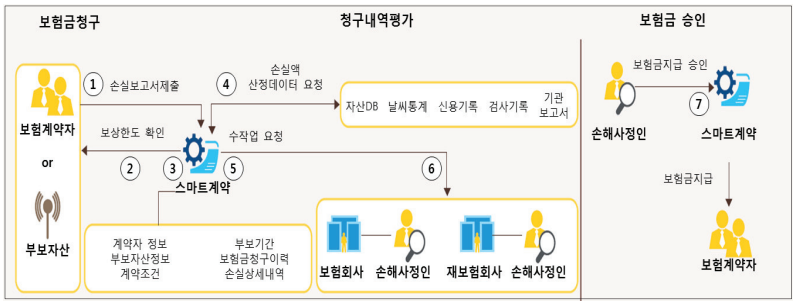
<그림 3-10> 손해보험금 청구의 현재 처리 과정의 취약점



① 보험금청구 시 보험계약자는 복잡한 청구서를 작성하고 손해규모증명서를 확보한다.
② 보험중개인은 보험금청구 과정에서 중개 역할을 하지만 이로 인해 시간과 비용이 추가된다.
③ 보험회사는 제3의 데이터제공자로부터 자산, 위험, 손실 등의 데이터를 얻기 위해 개별적인 관계를 설정한다.
④ 보험회사 간에 보험사고 평가에 대한 공유가 불가능하다.
⑤ 손해사정사가 보험금청구의 하자 여부, 추가정보 요구, 부보 및 채무 범위 확인, 손해규모 산정 등을 수작업으로 처리한다.

(마) 미래 처리 과정

<그림 3-11> 손해보험금 청구의 미래 처리 과정



① 보험계약자가 보험사고 정보를 제출하거나 부보자산에 부착된 센서 등에 의해 자동적으로 보험금청구가 가능하다.

② 보험계약자는 스마트계약에 의한 보험약관을 통해 실시간으로 부보가능범위에 대해 피드백을 받는다.

③ 보험계약자가 제출한 정보를 이용하여 보험금 실사가 스마트계약에 의해 자동적으로 완성된다.

④ 분산원장 기술이 자동적으로 2차 자료에 접속하여 손실액과 보험금 규모를 산정한다.

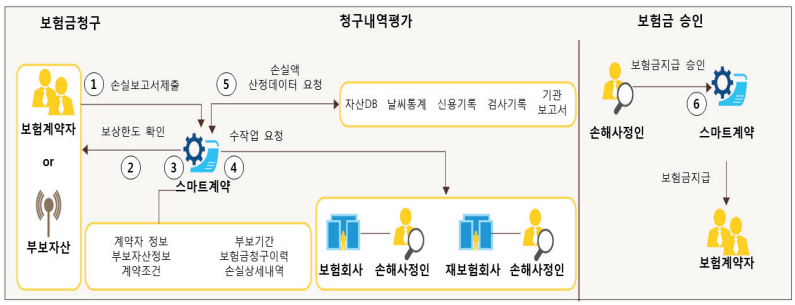
⑤ 스마트계약이 보험약관에 의해 보험회사나 재보험회사가 부담할 채무범위를 산정한다.

⑥ 미리 합의한 상황 하에서 스마트계약이 청구된 보험금에 대한 추가 보완적 평가를 하여 최종 부보금액을 산출한다.

⑦ 청구된 보험금이 승인되면 스마트계약을 통해 보험계약자에게 보험금을 지급한다.

(바) 미래 처리 과정의 이득

<그림 3-12> 손해보험금 청구의 미래 처리 과정의 이득



① 스마트계약을 활용하여 보험금청구 과정이 단순하고 완전자동화가 가능하다.

② 보험계약자로부터 손실정보를 효율적으로 전달받으므로 분산원장 기술은 중개인의 개입을 제거하여 보험금청구에 소요되는 시간을 줄여준다.

③ 스마트계약에 성문화된 약관으로 인해 손해사정사가 매번 보험금청구에 대해 확인하는 과정이 감소한다.

④ 보험회사는 보험금청구 이력과 부보자산의 출처에 완벽하게 접속할 수 있으므로 의심행위에 대한 대응력을 향상시킨다.

⑤ 분산원장 기술은 신뢰성이 확보된 다양한 데이터원천을 통합함으로써 수작업 검토를 최소화한다.

⑥ 대부분 스마트계약을 통해 후선업무 부서의 개입 없이 자동적으로 보험금을 지불한다.

(사) 필요조건 및 향후 전망

먼저 부보된 자산에 대한 기록들이 분산원장 기술을 활용한 스마트계약에 등재되어야 한다. 이는 자산의 증명이나 손실 정보가 서로 다른 참여자들이

공유하는 원장에 기록되지 않는다면 스마트계약을 이용한 보험금청구는 자동적으로 실행되지 못해 그 효과를 달성하지 못하기 때문이다. 그러나 특정 분산원장 기술을 부보된 자산의 등록메커니즘으로 활용하는 것은 여전히 도전적이며 이해당사자의 성실성을 요구하고 있다.

또한 보험회사나 규제기관은 데이터 표준의 설정과 외부의 데이터제공자들이 설정된 표준을 채택하게 함으로써 정보가 효과적으로 흐르도록 하여야 한다. 만약 데이터가 표준화되지 못하였다면 추가적인 수작업이 요구되어 비용 비효율성과 이익 감소를 초래할 것이기 때문이다. 그러나 현재 보험회사별 고유 처리과정과 데이터 형태를 표준화시켜 공유하기 위해서는 이해관계의 수렴을 통한 폭넓고 깊은 논의가 요구된다.

그리고 규제기관, 보험회사 및 관련 이해당사자는 법적 틀을 설정하여 스마트계약을 통해 보험약관을 실행하는 타당성을 확보하여야 한다. 법적 선례가 없을 경우 보험회사와 보험계약자는 거래상대방위험에 직면하거나 분쟁을 유발시킬 수 있다. 그러나 이해당사자 간에 법적 틀을 공유하는데 대한 관심사나 절박함이 서로 다를 수 있기 때문에 면밀한 협업이 요구된다.

보험에 분산원장 기술을 적용하는 것은 이제 막 초기단계이므로 현재는 불변의 보험금청구 기록 창출, 보험금청구 처리과정에서 필요한 자산증명의 개발, P2P보험 등에 관한 개념증명에 초점을 맞추고 있는 실정이다. 그러나 분산원장 기술을 활용하게 되면 규제기관이나 중개기관에게 P2P보험과 같은 신종 상품을 모니터하고 평가할 수 있으며, 보험업에서 더욱 저렴한 비용모델을 활용할 수 있는 기회를 제공할 수 있을 것이다.

(3) 신디케이트대출

(가) 현황

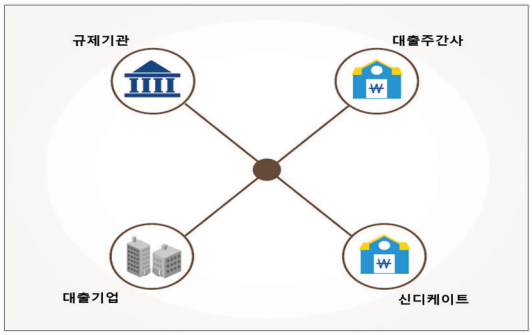
신디케이트대출 시장은 2014년 현재 4개의 미국 금융회사가 1조 9,170억 달러로 전 세계 시장의 50%이상을 차지하고 있으며, EMEA(Europe, the Middle East and Africa) 지역의 신디케이트대출 규모는 1조 2,145억 달러에 달한다. 일본을 제외한 아시아태평양 지역은 2014년에 22%의 성장을 기록하

여 총 규모는 5,242억 달러이고, 라틴아메리카 지역은 신디케이트대출 시장이 아직 성숙되지 않아 2014년에 422억 달러 수준에 그치고 있다[25]. 분산원장 기술은 신디케이트대출의 후선업무의 효율화를 꾀함으로써 신디케이트대출의 시작부터 끝까지 기존 절차와는 다른 기회를 제공할 수 있을 것이다.

(나) 주요 참가자

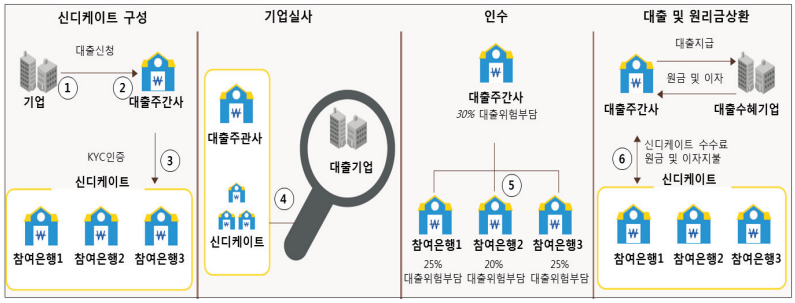
신디케이트대출 업무의 참가자는 중요 역할을 담당하는 대출주간사, 신디케이트, 대출기업과 업무를 지원하는 규제기관이 있다.

<그림 3-13> 신디케이트대출의 주요 참가자



(다) 현재 처리 과정

<그림 3-14> 신디케이트대출의 현재 처리 과정



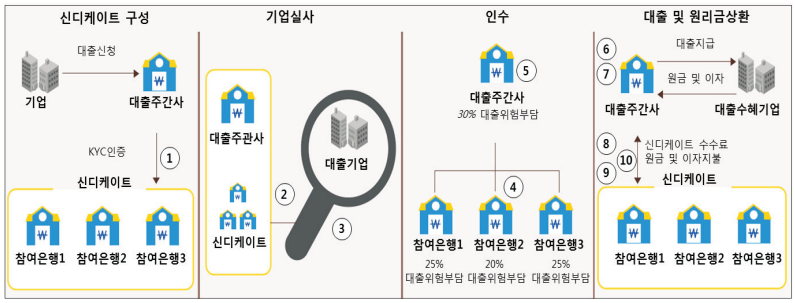
① 기업이 대출주간사에게 신디케이트대출을 요청한다.
② 대출주간사는 KYC(고객알기제도)를 통해 적격성을 판단한다.
③ 위험을 줄이기 위해 대출주간사는 신디케이트를 구성한다.
④ 대출주간사는 기업의 재무적 건전성과 대출관련위험의 수준을 조사한다.

25) Bloomberg, Global Syndicated Loans: League Tables 2014, 2014 참조

⑤ 신디케이트 참여은행은 자신이 감당할 수 있는 위험비율을 확약한다.
⑥ 대출주간사는 대출금의 분담부터 원리금의 상환에 이르는 신디케이트대출 전 과정에 걸쳐 관리책임을 부담한다.

(라) 현재 처리 과정의 취약점

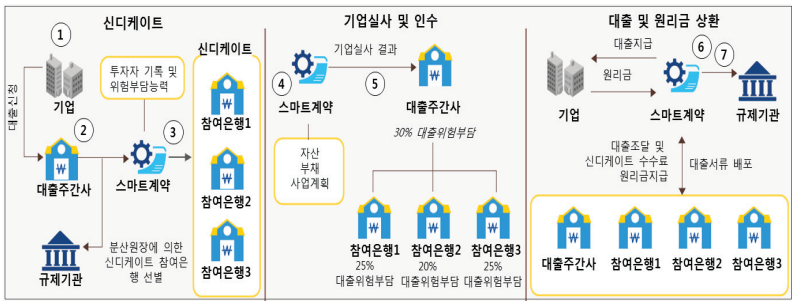
<그림 3-15> 신디케이트대출의 현재 처리 과정의 취약점



① 재무적 건전성과 사업이력을 바탕으로 신디케이트 참여은행을 선정하는 작업은 시간과 수작업을 요구한다.
② 기업의 재무정보를 분석하는 작업은 시간과 수작업을 요구한다.
③ 신디케이트 참여은행이 각기 수행하는 실사로 인해 데이터원천과 활용이 다양하므로 이를 통합하는데 시간이 소요되며 오류의 가능성이 있다.
④ 신디케이트 참여은행의 약속서명이 첨부된 서류작업은 노동집약적으로 비효율적이다.
⑤ 대출인수과정과 실사과정이 중복된다.
⑥ 대출주간사의 원리금 분배는 추가적인 비용지출이 필요하다.
⑦ 대출주간사는 대출원리금이 상환될 때까지 분배의 책임을 부담한다.
⑧ 대출금이 상환된 이후 신디케이트 참여은행들에게 분배되기까지 t+3일이 소요된다.
⑨ 제3자가 자금의 분배를 담당할 경우 추가적인 비용이 소요된다.
⑩ 신디케이트대출 제공자 간에 소통의 어려움으로 인한 이중 작업이 존재한다.

(마) 미래 처리 과정

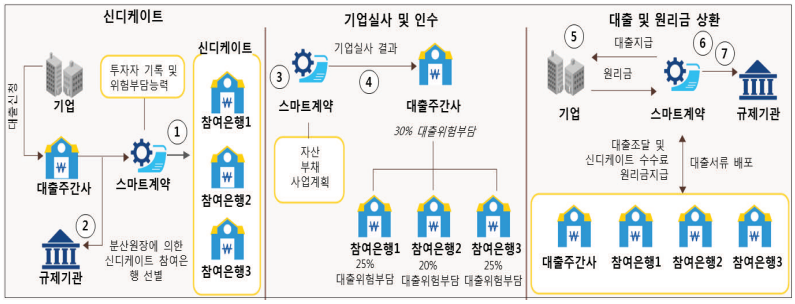
<그림 3-16> 신디케이트대출의 미래 처리 과정



① 기업은 대출주간사에 신디케이트대출을 신청한다.
② 기업의 디지털신원을 확인한 후, 대출주간사는 분산원장 기술의 기록관리 기능을 통해 실시간으로 KYC를 하고 이 과정이 규제기관에게 투명하게 제공된다.
③ 분산원장 기술에 저장된 대출가능 재원과 위험부담 능력을 이용하여 자동적으로 신디케이트 참여은행을 선정함으로써 채권단 구성에 소요되는 시간을 줄인다.
④ 기업의 재무정보와 사업계획에 분산원장 기술로 접근하여 실사를 스마트계약으로 자동화한다.
⑤ 실사과정에서 드러난 기업현황지표를 대출인수서류로 이전한다.
⑥ 스마트계약을 이용하여 대출금의 조달 및 배분, 대출관련 서비스에서 제3자의 역할을 제거한다.
⑦ 스마트계약에 포함된 규제기관이 대출관련 자료를 면밀히 검토하여 ALM에 위배되는지 파악한다.

(바) 미래 처리 과정의 이득

<그림 3-17> 신디케이트대출의 미래 처리 과정의 이득



① 스마트계약에 내재되어 프로그래밍된 선별기준에 따라 신디케이트대출 채권단이 자동적으로 구성되어 시간절감의 효과가 있다.
② 규제기관이 스마트계약에 포함됨으로써 실시간으로 ALM/KYC 자료를 제공받는다.
③ 기업의 재무정보 분석과 대출위험인수가 자동화됨으로써 시간과 자원의 절약이 가능하다.
④ 실사시스템과 인수시스템이 관련정보를 교환함으로써 절차와 시간을 단축시킨다.
⑤ 대출금의 제공이 실시간으로 이루어지며 상환대출금의 분배에 소요되던 t+3일과 대출주간사의 역할을 제거한다.
⑥ 스마트계약을 통해 대출관련업무가 이루어지므로 제3자의 중개가 사라진다.
⑦ 원리금의 분배가 자동화되므로 거래상대방위험을 경감시킨다.

(사) 필요조건 및 향후 전망

먼저 필요조건을 살펴보면 금융기관은 분산원장 기술로 상호간에 등급과 대출부담능력을 공유할 수 있는 틀을 개발해야 하는데 이는 대출주간사가

신디케이트를 자동적으로 구성할 수 있게 해주기 때문이다. 그러나 금융기관을 하나의 기준에 의해 순서를 매기기 위해서는 상당한 협조와 지배구조가 요구된다.

또한 금융기관은 실사를 통해 파악한 기업현황지표를 자동적으로 대출인수 서류로 이전하기 위해 표준화된 규격이 필요하다. 그러나 많은 수의 실사 및 인수 주체들을 하나의 포맷으로 통합하는 것에 어려움이 있을 수 있다. 또한 금융기관과 대출기업들은 반드시 분산원장에 신디케이트대출과 관련된 정보를 저장하여야 하는데 이는 분산원장을 통해 신디케이트 구성, 대출기업 실사, 인수양식 생성 등 세밀한 재무정보에 접근하기 때문이다. 그러나 법적 선례나 책임 모형이 없기에 분산원장에 자신의 고유 재무정보를 저장하는 위험에 참여하는 데는 현실적으로 어려움이 따른다.

신디케이트대출에서 분산원장 기술의 활용은 현재 소수의 관련금융기관들이 개념증명을 하는 단계이며 스마트계약에 의한 결제와 서비스 제공, 자동화된 인수 등에 집중되고 있는 형편이다. 또한 금융기관에게는 운영위험과 수작업을 줄일 수 있는 기회를 제공하는데 이는 주로 스마트계약을 통한 대출자금 조달 및 계좌서비스, 자동화된 인수업무를 통해 가능하다.

(4) 무역 금융

(가) 현황

현재 무역은 금융을 통해 대금결제가 이루어지며 전 세계적으로 연간 18조 달러 규모의 무역거래에는 신용 및 보험 제공, 신뢰성 보장의 형태가 포함되어 있다. 금융이 무역의 중요 인자로 포함된 이래 전 세계 시장규모는 연간 10조 달러 이상으로 증가하였다[26]. 분산원장 기술은 무역금융에서 규제 또는 운영 관련 비용을 최적화시킬 수 있다.

(나) 주요 참가자

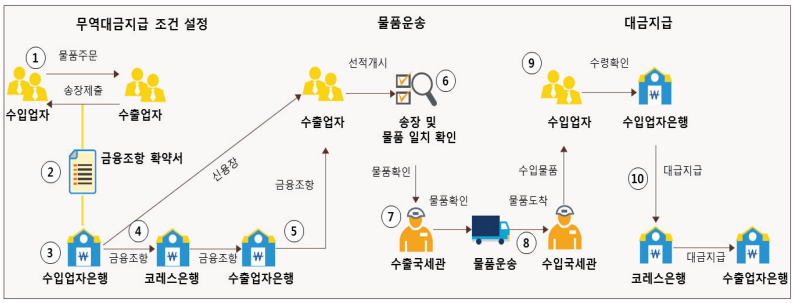
26) World Trade Organization, Improving the Availability of Trade Finance in Developing Countries: An Assessment of Remaining Gaps, 2015 참조

무역금융 업무의 참가자는 중요 역할을 담당하는 수입업자, 수입업자은행, 수출업자, 수출업자은행이 있고, 업무를 지원하는 물품확인기관, 물품운송기관, 수출입국 세관, 코레스은행이 있다.

<그림 3-18> 무역금융의 주요 참가자

(다) 현재 처리 과정

<그림 3-19> 무역금융의 현재 처리 과정

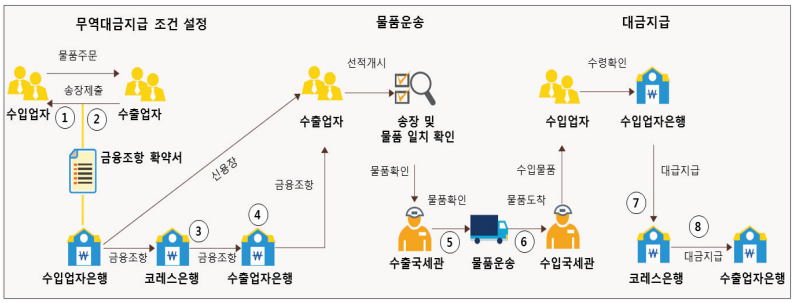


① 수입업자와 수출업자 간의 물품거래 일시를 합의한다.
② 송장에 합의된 금융조항을 첨부하고, 상품수량, 가격, 운송일정을 명기한다.
③ 수입업자는 합의된 금융조항의 복사본을 수입업자은행에 제출한다.
④ 수입업자은행은 금융조항을 검토하고 수입업자를 대신하여 수출업자은행의 코레스은행에 금융조항의 승인을 통보한다.
⑤ 수출업자은행은 수출업자에게 승인된 금융조항을 통보하고 이를 근거로 수출업자는 상품 선적을 개시한다.
⑥ 신뢰받는 제3자 확인기관이 송장과 물품의 일치여부를 검사한다.
⑦ 수출국 세관이 물품을 검역한다.
⑧ 수출물품이 운송되어 수입국 세관이 물품을 검역한다.
⑨ 검역 종료 후 물품이 수입업자에게 전달되고 수입업자는 수입업자은행에게 물품수령을 확인해 준다.

⑩ 물품수령 확인 통보 이후 수입업자은행은 코레스은행을 통해 수출업자은행으로 무역대금을 지급결제 한다.

(라) 현재 처리 과정의 취약점

<그림 3-20> 무역금융의 현재 처리 과정의 취약점



① 수입업자은행은 합의된 금융조항을 수작업으로 검토하고 코레스은행에게 승인을 통보한다.

② 수출업자는 송장을 이용하여 복수의 은행으로부터 단기자금 융자를 받는데 이는 물품의 운송이 실패하는 경우 추가적인 위험을 부담하게 한다.

③ 물품의 선적이 중개기관의 복수 점검으로 지연된다.

④ 수출업자은행은 수입업자은행으로부터 승인 통보받은 금융조항에 대해 AML을 점검한다.

⑤ 수출국과 수입국에서 각기 다른 검역 플랫폼으로 인해 잘못된 소통이나 사기의 가능성이 매우 높다.

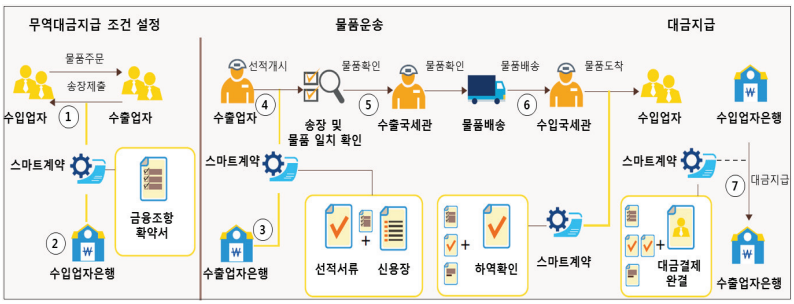
⑥ 선하증권의 정당성을 확인해주는 은행의 부재로 여러 차례 담보로 제공된다.

⑦ 금융조항의 승인이 복수의 은행을 거치기 때문에 내용이 변경되는 경우 이를 통제할 수 있어야 한다.

⑧ 무역대금의 전달을 위해 복수의 중개기관이 확인하는 과정이 필요하다.

(마) 미래 처리 과정

<그림 3-21> 무역금융의 미래 처리 과정

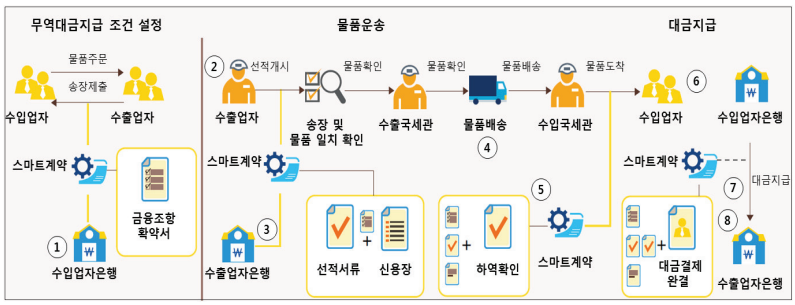


① 물품거래에 따라 합의된 금융조항이 스마트계약을 통해 수입업자은행에게 공유된다.

② 수입업자은행은 합의된 금융조항을 검토하고 신용장 초안을 작성하여 수출업자은행으로 송부한다.
③ 수출업자은행은 신용장의 용어와 조건을 검토한다.
④ 수출업자는 스마트계약 내의 신용장에 디지털서명을 하고 상품선적을 개시한다.
⑤ 제3자와 수출국 세관이 디지털서명이 첨부된 물품을 검역한다.
⑥ 물품이 운송되고 수입국 세관이 검역한다.
⑦ 수입업자가 물품수령을 디지털로 확인하면 스마트계약을 통해 수입업자은행은 수출업자은행으로 무역대금을 지불한다.

(바) 미래 처리 과정의 이득

<그림 3-22> 무역금융의 미래 처리 과정의 이득



① 분산원장 기술로 연계되어 접근이 가능한 무역금융 관련서류를 실시간으로 검토하고 승인함으로써 선적이 개시되는 시간을 절약한다.
② 분산원장 기술로 접속 가능한 송장을 이용하여 실시간으로 투명한 단기자금조달이 가능하다.
③ 수출업자은행은 위험을 부담할 중개기관이나 코레스은행이 필요하지 않게 된다.
④ 선하증권이 분산원장 기술로 추적 가능해짐으로써 이중지출의 가능성이 제거된다.
⑤ 스마트계약의 조건에 따라 진행상황이 실시간으로 분산원장 기술로 업데이트됨으로써 물품운송과정을 모니터하는 시간과 인력을 줄일 수 있다.
⑥ 분산원장 기술로 소유권을 확인함으로써 물품의 위치와 소유권에 투명성을 제공한다.
⑦ 스마트계약으로 실행되는 계약조건에 의해 코레스은행이나 추가적인 거래비용이 사라짐으로써 비용을 절감한다.
⑧ 규제기관은 실시간으로 AML을 위한 필수서류를 검토할 수 있다.

(사) 필요조건 및 향후 전망

먼저 선하증권과 송장 내용이 스마트계약으로 투명해짐으로써 거래상대방 위험을 줄일 수 있는데 이는 무역금융에서 자금융자를 받거나 이중지출을 방지하기 위해 반드시 필요하다. 그러나 이를 위해서는 금융기관과 운송회사

들이 무역금융 절차와 책임 모형을 설정하여 금융정보의 투명한 공유가 가능하여야 한다. 또한 무역금융에서 합의된 금융조항을 담은 스마트계약이 효력을 발휘하기 위해서는 금융기관과 기술회사들이 다양한 플랫폼에서도 원장의 상호작용이 가능하도록 설계하여야 한다. 이는 신용장, 선하증권, 검역서류의 생성에 있어 이해관계자들이 적법한 분산원장 기술로 통합되어야 하기 때문이다. 그러나 금융기관, 세관, 운송업자, 수입업자와 수출업자가 분산원장과 접속이 불가능할 수 있는 여러 가지 기술솔루션을 활용한다는 것이 문제점이다.

규제기관에 실시간으로 선하증권이나 신용장을 제공하기 위해서는 무역금융의 처음부터 끝까지 합의된 절차가 설정되어 있어야 하는데 이는 규제기관에서 실시간으로 스마트계약에 내포된 금융조항에 대해 규제준수를 검토할 수 있어야 하기 때문이다. 그러나 법적 선례가 부족한 상황에서 스마트계약을 통한 보고절차의 설정에 어려움이 있을 것이다.

무역금융에서 분산원장 기술의 활용은 현재 스마트계약에 봉인된 신용장, 디지털 송장 등에 대해 개념증명이 진행되는 단계이다. 또한 금융기관에게는 투명한 송장을 이용한 자금융자, 선하증권에 대한 이중지출 등의 분야에서 거래상대방위험과 사기를 줄일 수 있는 기회가 주어지고 있다.

(5) 조건부자본증권

(가) 현황

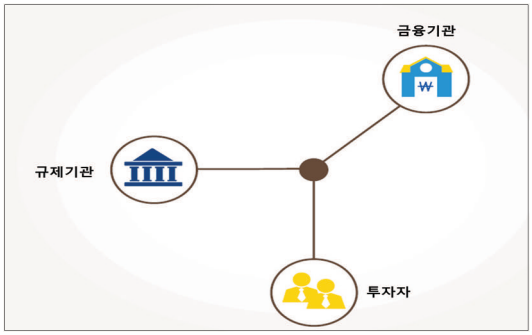
조건부자본증권(contingent convertible bonds, 코코본드)은 은행의 자본비율이 일정 수준 이하로 하락하는 경우 채권을 지분으로 전환함으로써 자본비율을 증가시키는데 활용하는 채권으로 유럽에서는 2013년 이후 두 자리 수 증가를 기록하였으나 2015년에는 크게 증가하지 않았다. 금융위기 이후 긴급 구제의 필요성을 줄이기 위한 메커니즘으로 개발된 이후 어떠한 코코본드도 지분으로 전환되지는 않았으나 여전히 불확실성이 남아있는 상황이다. 한편 수익률은 높게 형성되어 왔지만 2016년에 시행된 규제기관의 스트레스테스트로 인해 높은 수익률이 수 주 만에 모두 사라지는 극도의 가변성을 보이고 있다. 분산원장 기술은 규제를 비즈니스과정에 끼워 넣을 수 있어 코코본

드와 관련한 불확실성과 가변성을 경감시켜 향후 코코본드의 발행을 증가시킬 수도 있을 것이다.

(나) 주요 참가자

조건부자본증권 업무의 참가자는 중요 역할을 담당하는 금융기관, 투자자와 업무를 지원하는 규제기관이 있다.

<그림 3-23> 조건부자본증권의 주요 참가자



(다) 현재 처리 과정

<그림 3-24> 조건부자본증권의 현재 처리 과정

① 은행은 코코본드가 지분으로 전환되는 자본비율을 산출하여 전환옵션을 결정한다.

② 채권의 전환옵션과 만기 등 속성을 결정한 후 여러 투자자에게 코코본드를 판매한다.

③ 발행은행과 규제기관은 코코본드가 다음 중 어느 경우에 전환되는지 모니터한다.

i) 은행의 자발적 전환결정

ii) 은행과 규제기관의 시장성과 검토에 따른 결정

iii) 규제기관의 자본비율 평가를 위한 스트레스 테스트로 인한 결정

④ 모니터링에 의해 채권의 지분전환이 필요하다고 판단되면 코코본드는 사전에 정해진

전환비율로 지분으로 전환된다.

(라) 현재 처리 과정의 취약점

<그림 3-25> 조건부자본증권의 현재 처리 과정의 취약점

① 코코본드에 대한 신용등급정보가 제한적이므로 규모가 큰 투자자들의 참여가 제한적이다.

② 장부가에 의한 자본비율과 주가에 의한 자본비율 계산이 일치하지 않는다.

③ 규제기관이 자본비율의 정확한 파악과 채권의 지분전환 시기를 파악하기에 어려움이 있다.

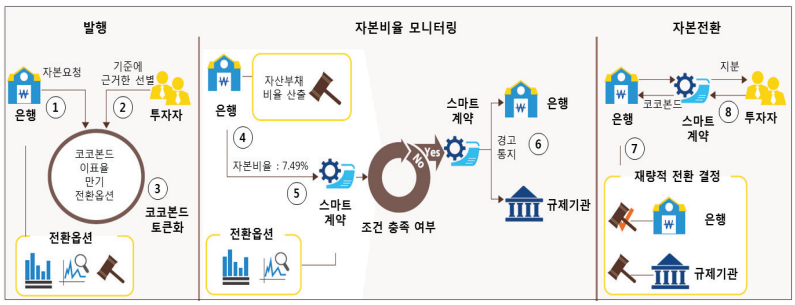
④ 규제기관이 은행과 코코본드시장의 건전성을 평가하는데 스트레스테스트에 의존할 수밖에 없다.

⑤ 투자자들이 스트레스테스트 결과에 우려를 보임에 따라 은행의 지분가치가 극도로 가변적이라고 인식된다.

⑥ 전환시기에 대한 규제가 없으므로 자본비율이 전환조건에 부합한다 할지라도 코코본드가 지분으로 즉각 전환되지 않는다.

(마) 미래 처리 과정

<그림 3-26> 조건부자본증권의 미래 처리 과정



① 채권발행은행은 자본비율을 장부가 혹은 시장가로 계산하여 전환옵션을 결정하고 채권을 발행한다.

② 은행은 분산원장 기술의 기록관리 기능을 활용하여 토큰화된 코코본드를 발행하고 자본금을 확충한다.

③ 토큰화된 코코본드에는 지분전환 시기, 발행은행, 쿠폰율, 만기를 포함한 채권의 속성이 포함된다.

④ 채권의 지분전환이 필요하면 은행은 현재 자본비율을 분석한다.

⑤ 최신 자본비율이 토큰화된 채권에 첨부되며 투자자와 규제기관에게 코코본드의 상태를 투명하게 제공한다.

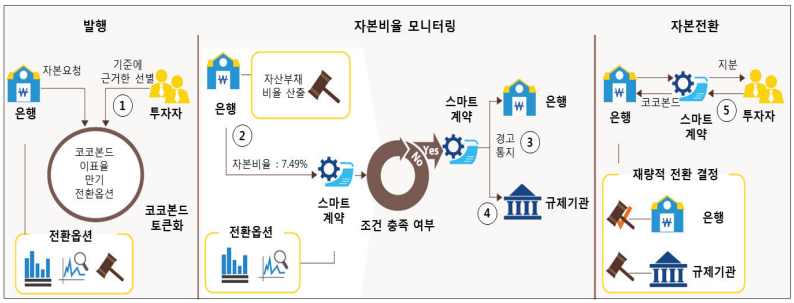
⑥ 채권의 지분전환이 필요한 시기가 도래한다면 규제기관과 은행에게 스마트계약을 통해 실시간으로 통지된다.

⑦ 은행이나 규제기관이 재량적으로 전환을 결정하면 스마트계약을 통해 채권이 지분으로 전환된다.

⑧ 사전에 정해진 전환비율이 적용된다.

(바) 미래 처리 과정의 이득

<그림 3-27> 조건부자본증권의 미래 처리 과정의 이득



① 분산원장 기술로 최신 자본비율 정보를 제공함으로써 신뢰와 함께 코코본드에 신용등급을 부여할 수 있게 되어 대형 금융기관의 참여가 가능하다.

② 자본비율의 계산이 직접 분산원장 기술에 통합됨으로써 은행은 데이터입력과 계산빈도에 대해 개선이 가능하다.

③ 코코본드의 지분전환 시기가 도래한다면 규제기관에 스마트계약을 통해 실시간으로 통보해 준다.

④ 규제기관은 은행의 자본비율을 실시간으로 파악할 수 있으므로 스트레스테스트를 할 가능성이 감소하고 이는 은행 지분가치의 가변성을 경감시킨다.

⑤ 분산원장 기술로 인해 전환시기 산출과 그에 대한 보고가 증가함으로써 코코본드의 지분전환에 소요되는 시간이 크게 줄어든다.

(사) 필요조건 및 향후 전망

먼저 규제기관과 금융기관은 코코본드의 표준 속성을 논의함으로써 투자자들에게 데이터에 근거한 의사결정이 가능하게 하여야 하는데 이는 분산원장

기술로 토큰화되기 위해 데이터 영역과 양식이 표준화되어야 하기 때문이다. 그러나 개별 시장마다 코코본드의 발행에 각기 다른 데이터를 요구하고 있으며 데이터 영역이 표준화되지 못하였다는 것은 해결되어야 한다.

그리고 규제기관은 채권의 효율적인 지분전환을 위해 전환시기 산출 방법에 표준을 부여해야 하는데 이는 전환시기 산출과정의 표준화로 인해 투자자들이 갖는 코코본드에 대한 신뢰가 증가하기 때문이다. 그러나 개별 금융기관이 독자적으로 전환이 요구되는 자본비율을 산출하고 있으며 자동 산출 정도도 각기 다른 것이 현실이다.

규제기관과 금융기관은 실시간으로 채권의 지분전환을 통보할 수 있는 비즈니스절차를 개발하여야 하는데 이는 투자자의 지속적인 투자를 이끌어 내기 위해서 코코본드의 전환가치에 대한 가변성 우려를 불식시킬 필요가 있기 때문이다. 그러나 지금까지 규제기관은 금융기관의 자본비율 분석이 요구될 때에만 스트레스테스트를 실시하였기에 채권의 지분전환에 관한 비즈니스절차에 대한 심도 있는 점검이 요구된다.

현재까지 코코본드의 발행에서 소멸까지를 분산원장에 담는 것에 대해서는 보고나 논의된 바가 없다. 코코본드 비즈니스에서 발생하는 편익과 비용이 있지만 주요 편익은 시장의 안정성을 개선시키는 것이라 할 수 있다. 규제기관에게는 금융기관에게 자본비율 산출의 표준화를 요구할 기회가 있을 것이며, 금융기관에게는 스트레스테스트로 파생되는 지분가치의 가변성을 줄일 수 있을 것이다.

(6) 규제준수 자동화

(가) 현황

규제준수는 금융기관에게 간접비 성격의 비용을 부담하게 하여 전 세계적으로 대형 금융기관이 2014년에 40억 달러를 지출하였다[27]. 또한 회계감사 역시 금융기관에게 규제준수 관련 비용을 많이 부담시키고 있어 2013년에 평균적으로 710만 달러 이상을 회계감사 수수료로 지출하였다[28]. 분산원장

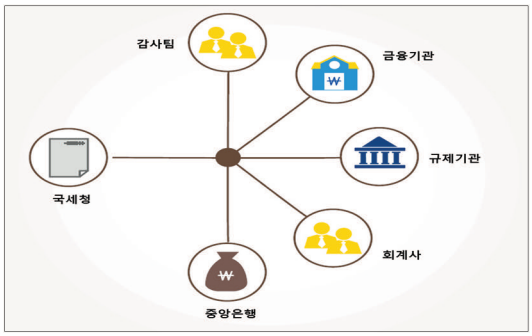
27) Financial Times, Bank face pushback over surging compliance and regulatory costs, 2015 참조

기술은 금융기관 운영의 효율성을 증진시키며 규제기관에게는 규제를 집행할 수 있는 강화된 수단이며, 재무제표 감사에 초점을 맞춘 자동화된 규제준수 솔루션으로서 기능할 수도 있다.

(나) 주요 참가자

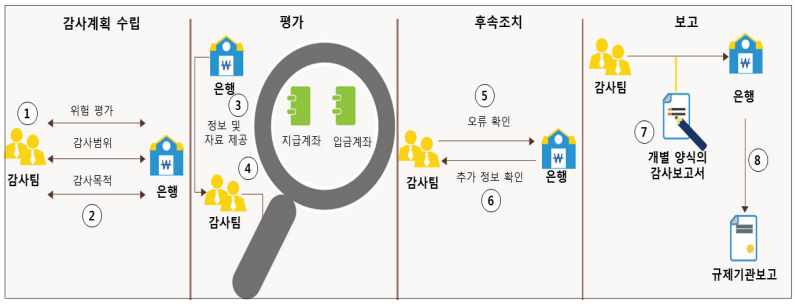
규제준수 자동화 업무의 참가자는 중요 역할을 담당하는 감사팀, 금융기관과 업무를 지원하는 규제기관, 회계사, 중앙은행, 국세청이 있다.

<그림 3-28> 규제준수 자동화 주요 참가자



(다) 현재 처리 과정

<그림 3-29> 규제준수 자동화 현재 처리 과정



① 매년 감사팀이 은행의 재무제표에 대해 감사를 계획한다.

② 감사팀이 은행과 함께 최초위험을 평가하고 감사의 범위, 목적, 시기, 필요자원 등을 결정한다.

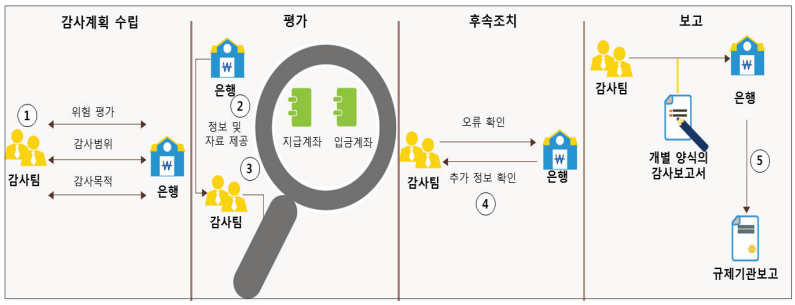
③ 은행이 감사팀에 재무제표관련 자료를 제공하고 은행시스템에 접속이 가능하게 해준다.

28) Financial Executives Research Foundation, 2015 Annual Audit Fee Report, 2015 참조

④ 회계사는 제공된 정보의 완결성을 평가하고 이와 병행하여 정확성 테스트를 실시한다.
⑤ 회계사는 데이터로부터 확인된 오류를 은행 대표에게 제시한다.
⑥ 감사 예외조항이 확인됨에 따라 감사팀은 추가적인 정보를 확보하여 감사의 깊이를 결정한다.
⑦ 감사팀은 은행의 전반적인 재무건전성에 대해 독자적 양식의 감사보고서를 제출한다.
⑧ 은행은 감사결과를 규제기관에 분기별과 연별 보고로 작성 제출한다.

(라) 현재 처리 과정의 취약점

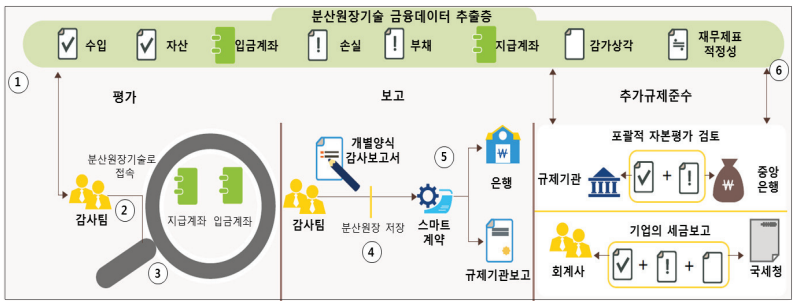
<그림 3-30> 규제준수 자동화 현재 처리 과정의 취약점



① 감사 계획을 수립하는 과정에서 다수의 업무분야에서 근로자의 업무수행이 제한된다.
② 샘플데이터를 통해 회계검토를 하는 과정에 시간이 많이 소요되며 수작업에 의존하여 비효율적이다.
③ 정보가 사본으로 전달됨으로써 실수의 가능성으로 수작업의 비효율성이 증대된다.
④ 감사 예외조항이나 실수의 후속조치로 다수의 업무분야 근로자와 추가적인 소통이 필요하므로 생산성이 하락한다.
⑤ 독자적 양식으로 제공되는 보고서로 인해 규제기관의 분기별 또는 연별 보고내용으로 전환되지 못한다.

(마) 미래 처리 과정

<그림 3-31> 규제준수 자동화 미래 처리 과정



① 분산원장 기술을 이용하여 감사팀이 실시간으로 재무정보를 추출한다.

② 감사팀에게 접속권한이 부여되어 있으므로 은행 대표가 감사 계획수립이나 데이터 배분 과정에 개입할 필요가 없다.

③ 감사팀이 분산원장 기술에서 직접 데이터를 이용하여 감사평가를 수행하여, 수작업이나 후속조치 요구로부터 발생하는 실수가 없어진다.

④ 감사팀은 독자적인 감사보고서를 작성하여 분산원장에 저장하며 은행과 규제기관은 이것에 실시간 접속이 가능하다.

⑤ 스마트계약을 이용하여 감사보고서의 내용을 재무제표로 이전시켜 이중노력을 최소화한다.

⑥ 분산원장 기술이 다음 분야에서 규제준수를 자동적으로 할 수 있도록 한다.

ⅰ) 포괄적 자본평가(comprehensive capital assessment review)

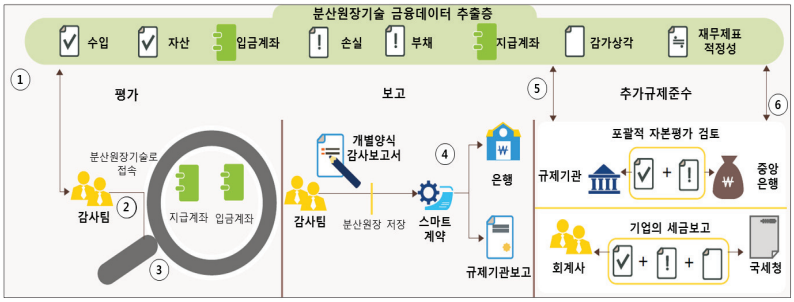
ⅱ) 기업의 세금 보고

ⅲ) 내부자거래의 적발 업무

ⅳ) 신규 규제 도입에 따른 정보처리

(바) 미래 처리 과정의 이득

<그림 3-32> 규제준수 자동화 미래 처리 과정의 이득



① 감사팀이 분산원장 기술을 이용하여 재무정보를 추출함으로써 실시간으로 업데이트된 투명하고 변경이 불가능한 정보를 제공받는다.

② 분산원장 기술로 재무정보에 접속하여 회계감사소프트웨어로 자동 점검하게 되어 시간과 자원을 절감한다.

③ 재무정보에 접속권한을 부여함으로써 수작업의 오류를 제거하고 효율적인 업데이트가 가능하다.

④ 분산원장 기술을 활용하여 규제기관에 분기별이나 연별로 보고함으로써 이중 작업의 노고가 감소한다.

⑤ 중앙은행은 분산원장 기술을 이용하여 은행자본에 대해 분석이 가능하고 그 결과를 저장할 수 있다.

⑥ 세무사가 실시간으로 재무정보에 접속하게 하여 세액 산출 및 세금 납부를 자동화할 수 있다.

(사) 필요조건 및 향후 전망

분산원장 기술 솔루션은 접속권한을 자산, 부채 등과 같은 재무상태 정보만으로 제한하여야 하는데 이는 회계감사에 필요한 자료만으로 접근을 제한함으로써 외부사용자가 발생시킬 수 있는 위험을 줄이기 위함이다. 그러나 현재 분산원장 기술은 접근을 원장의 일부만으로 제한할 수 없는 구조이다.

또한 금융기관과 규제기관은 재무정보 공유를 이행하여야 하는데 이는 규제기관이 재무정보에 실시간으로 투명하게 접속함으로써 규제준수의 이행이 가능하기 때문이다. 그러나 법적 선례가 없는 상황에서 규제기관과 금융기관 간의 공유관련 협약은 매우 도전적인 문제이다. 그리고 금융기관과 규제기관의 규제 틀은 분산원장 기술로 재무정보의 입력과 추출이 가능해야 하는데 이는 처리과정의 자동화를 가능하게 하기 위함이다. 그러나 현재 금융기관과 규제기관 간에는 분산원장에서 상호작용이 불가능할 수 있는 복수의 솔루션을 사용하고 있는 것이 지적되고 있다.

규제준수 자동화를 위한 분산원장 기술의 활용은 현재 개념증명이 진행되고 있는 상태로 지속적 회계감사, AML/KYC 확인, 자동화된 세금신고 등에 집중하고 있다. 분산원장 기술은 금융기관에게 계획과 후속조치 활동의 제거, 평가와 보고의 자동화로 인원과 수작업을 줄일 수 있는 기회가 있음을 알려주고 있다.

(7) 주권위임투표

(가) 현황

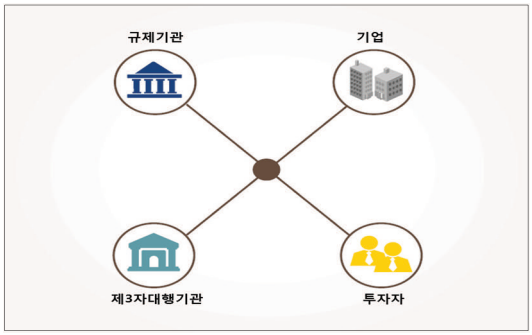
전 세계적으로 소액투자자의 주주권리 행사비율은 평균 28%로 기관투자자의 83%에 비해 낮다.[29] 그 결과 2015년 7월 1일부터 12월 31일까지 대략 240억 주에 해당하는 주권이 행사되지 않았다. 그러나 투자자의 활동이 강화됨에 따라 현재 금융기관의 대표들은 모든 주주들이 투표과정에 참여할 필요가 있음을 인식하고 있다. 따라서 분산원장 기술은 가치이전을 반박할 수 없기에 주권위임투표에 활용되면 소액투자자의 참여를 증진시킬 수 있을 것이다.

29) ProxyPulse, ProxyPulse: First Edition, 2016 참조

(나) 주요 참가자

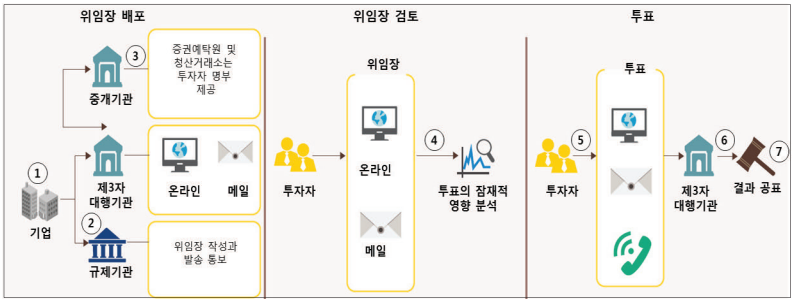
주권위임투표 업무의 참가자는 중요 역할을 담당하는 기업, 투자자와 업무를 지원하는 제3자 대행기관, 규제기관이 있다.

<그림 3-33> 주권위임투표 주요 참가자



(다) 현재 처리 과정

<그림 3-34> 주권위임투표 현재 처리 과정



① 기업은 법무, 회계를 포함하는 여러 부서의 협조로 위임장을 작성한다.

② 기업은 주주에게 발송할 서류를 제3자 대행기관에 제공하고 규제기관에 위임장 작성을 통보한다.

③ 제3자대행기관은 연락이 되지 않는 주주 정보를 파악하기 위해 중개기관에 협조를 의뢰한다.

④ 주주는 위임장을 통해 주주총회에서 요청받은 투표의 잠재적 영향을 분석한다.

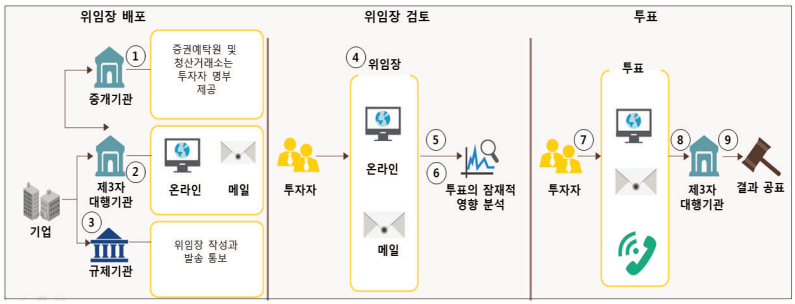
⑤ 주주는 자신의 투표를 온라인이나 메일 또는 전화로 제3자 대행기관에 전달한다.

⑥ 투표결과는 투표과정에서 다른 주주나 기업과 공유되지 않는다.

⑦ 주주총회 참석자의 투표결과와 위임투표 결과가 집계되어 발표된다.

(라) 현재 처리 과정의 취약점

<그림 3-35> 주권위임투표 현재 처리 과정의 취약점



① 중개기관의 협력 없이 한눈에 전체 주주명부를 파악하는 것이 어렵다.

② 주주의 사전 동의가 있어야만 온라인 위임장의 배포가 가능하므로 인쇄나 메일발송에 비용이 소요된다.

③ 일부 시장에 따라 위임장이 기관투자자에게 배포되지 않아 투표 참여를 제한한다.

④ 위임장에 삽입된 요약보고로 기업의 재무건전성이 호도될 수 있다.

⑤ 기관투자자의 세밀한 분석에 의해 사소한 데이터 오류가 적발된다.

⑥ 위임장의 분량과 구조화되지 못한 양식으로 인해 주주의 의사결정에 도움을 주는 정보가 수작업으로 취합된다.

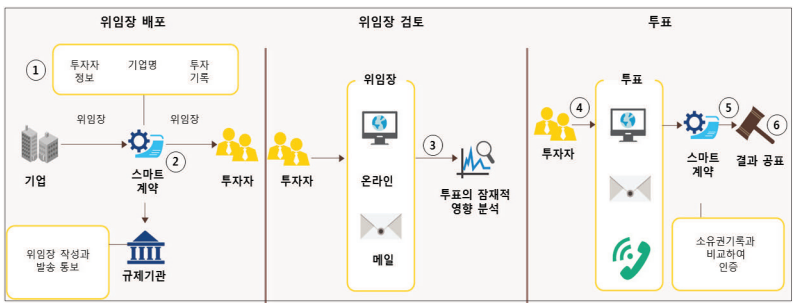
⑦ 대다수의 소액주주는 투표에 참여하지 않는다.

⑧ 제3자 대행기관이 취합하는 과정에서 기업과 주주들은 투표결과에 대해 전혀 알 수 없다.

⑨ 주식수와 투표수가 다르기 때문에 규제에 의해 투표수가 조정되거나 계산되지 않는다.

(마) 미래 처리 과정

<그림 3-36> 주권위임투표 미래 처리 과정



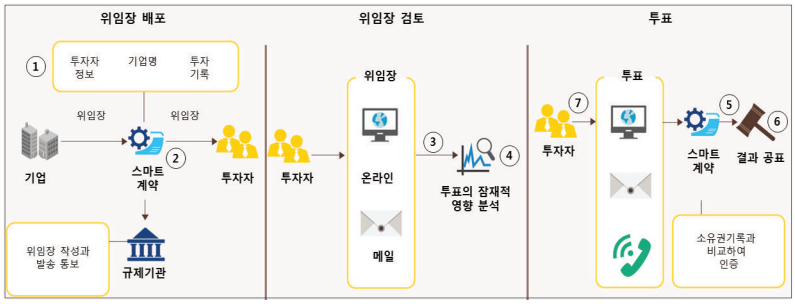
① 기업의 지분에 대한 투자주문이 실행되면 분산원장 기술은 주식수를 포함한 투자관련 기록을 저장한다.

② 기업이 위임장을 최종확정 한 후 스마트계약을 이용하여 전체 주주에게 발송하고 규제기관에 위임장의 발송을 통보한다.

③ 주주는 투표의 잠재적 영향을 파악하기 위해 분산원장 기술로 이전된 위임장을 분석한다.
④ 주주는 분산원장에 직접 투표결과를 보낸다.
⑤ 스마트계약이 투표수와 주권수를 비교하여 투표의 적법성을 보장한다.
⑥ 전체 투표결과가 실시간 혹은 주주총회에서 즉각 기업과 주주들에게 공유된다.

(바) 미래 처리 과정의 이득

<그림 3-37> 주권위임투표 미래 처리 과정의 이득



① 모든 투자기록이 분산원장 기술에 저장되기 때문에 제3자 대행기관과 중개기관의 협력관계가 필요 없으며, 스마트계약이 규제기관에 위임장의 작성과 배포를 통보할 수 있다.
② 분산원장 기술은 위임장의 인쇄와 발송에 관련된 비용을 절감한다.
③ 분산원장 기술은 위임장 접속에 활용된다.
④ 미래에 위임장 수록 정보의 분석이 개인화되고 자동화된다.
⑤ 스마트계약이 투표를 주권에 맞추어 정리한다.
⑥ 기업이나 다른 주주들이 투표결과 자료를 실시간으로 이용한다.
⑦ 분산원장 기술로 투표 참여도가 개선된다.

(사) 필요조건 및 향후 전망

기업이나 거래소는 모든 투자기록을 분산원장에 저장하여 중개기관의 개입 없이 주주명부를 확보할 수 있어야 한다. 이는 현재 제3자 대행기관이 중앙예탁기관과 협력하여 주주명부를 확보하기 때문이다. 그러나 디지털 신원증명과 함께 각종 투자관련 기록을 분산원장에 저장하기 위해서는 증권거래 후선업무 역시 분산원장 기술을 적용하는 것에 관해 업계의 논의가 필요하다.

또한 다양한 수단을 이용하여 주권을 행사하기 위해 우편이나 전화로 행사

된 투표가 토큰으로 전환되어 분산원장에 저장되어야 하는데 이는 모든 주주가 위임투표를 할 수 있게 하여 차별을 받지 않아야 한다. 그러나 투표에 따른 주주의 의사결정이 토큰으로 전환되는 과정에 정확성을 제고하기 위해 수작업의 개입이 필요 없는 창의적인 솔루션이 개발되어야 한다.

그리고 기업들이 서로 간에 파트너를 선택하여 중복개발을 최소화함과 동시에 투자자에게 신뢰받는 투표시스템을 개발하여야 한다. 이는 개별기업이 독자적으로 투표 솔루션을 개발한다면 투자자들이 표준화된 투자분석을 하는데 어려움이 있고 관심사의 충돌이 발생할 수 있기 때문이다. 그러나 스마트계약이 투표를 성공적으로 확인하여 계산하지 못할 경우를 대비한 대안 절차도 수립되어 있어야 한다.

분산원장 기술의 위임투표 활용은 현재 나스닥에서 개념증명이 진행되고 있다. 분산원장 기술은 금융기관에게 주주의 투표참여를 개선시킬 수 있는 기회를 제공하며 주주에게 위임설명서나 투표메커니즘의 이해를 증진시킬 수 있을 것이다.

(8) 자산담보권 재설정

(가) 현황

자산담보권 재설정은 금융중개기관이 후발거래에서 질권담보의 비용을 줄이기 위해 현존담보를 증권화하는 과정에서 발생한다. 자산의 담보권이 재설정됨에 따라 소유구조와 자산구성이 모호해지는데 이는 명확한 거래와 소유권 기록의 부족에 기인하여 거래상대방 위험을 악화시키고 자산가치의 불확실성을 증대시킬 수 있다.

대출을 기반으로 한 2차 거래가 아주 일반화되어 미국 대출시장에서 2014년에 이루어진 2차 거래의 규모는 6,280억 달러에 달하며, 전년대비 21%의 증가율을 기록할 정도로 빠르게 성장하고 있다[30]. 분산원장 기술은 자산담보권 재설정에 있어서 정보전달을 개선시킴으로써 규제내용을 최적화시킬 수 있을 것이다.

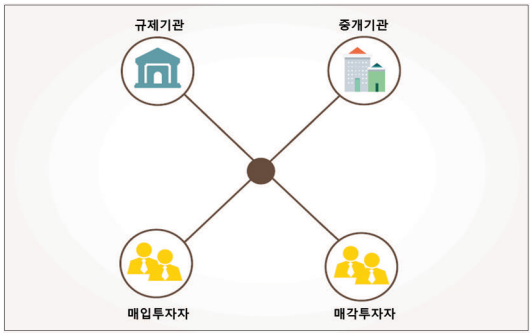
---

30) The Loan Syndications and Trading Association, *4th Quarter 2014 Secondary Trade Data Study* 참조

(나) 주요 참가자

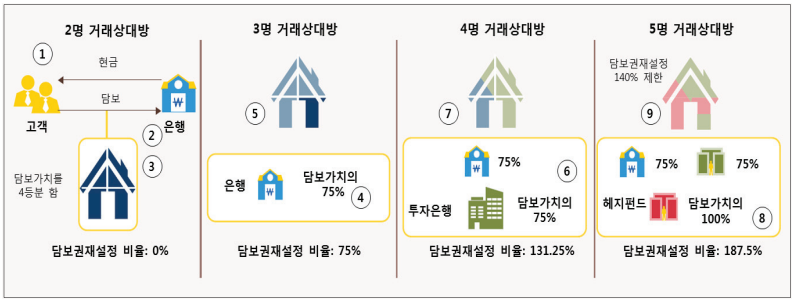
자산담보권 재설정 업무의 참가자는 중요 역할을 담당하는 중개기관, 매각투자자, 매입투자자와 업무를 지원하는 규제기관이 있다.

<그림 3-38> 자산담보권 재설정 주요 참가자



(다) 현재 처리 과정

<그림 3-39> 자산담보권 재설정 현재 처리 과정



① 고객이 주택매입을 위해 은행으로부터 대출을 받는다.

② 고객은 은행에게 주택을 담보로 제공하고 담보비율을 높일 수 있는 담보권재설정의 권한을 제공한다.

③ 모기지 상환기간 중에 은행은 담보 주택을 후발거래에 사용한다.

④ 은행은 담보주택 가치의 75%를 증권화하여 투자은행에 매각한다.

⑤ 투자은행은 은행 담보주택의 75%에 해당하는 가치를 구매하고 이를 후발거래에 사용한다.

⑥ 투자은행은 구입한 담보주택 가치의 75%를 MBS(mortgage backed security)로 만들어 헤지펀드 등에 판매한다.

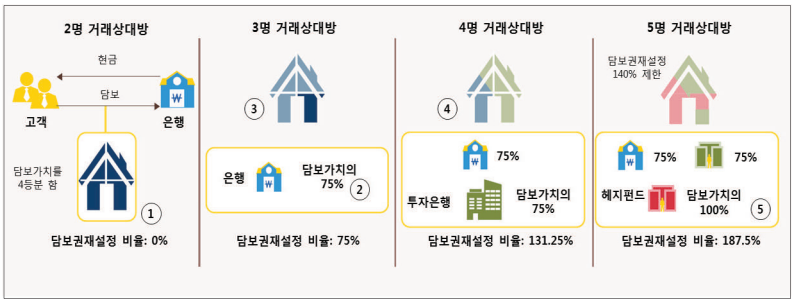
⑦ 헤지펀드는 최초 은행 담보주택 가치의 56.25%를 소유한다.

⑧ 헤지펀드는 구입한 자산가치 전체(56.25%)에 근거하여 파생상품(CDO)을 판매한다.

⑨ 소유권과 담보가치가 모호해져서 총담보가치(187.5%)가 자산가치를 초과하게 된다.

(라) 현재 처리 과정의 취약점

<그림 3-40> 자산담보권 재설정 현재 처리 과정의 취약점



① 2차 거래시장에서 보고의무가 자세하지 않아 자산의 거래나 청구권을 가진 거래상대방에 대한 기록이 충분하지 않다.

② 투자자는 자산소유 청구권을 가진 거래상대방을 제대로 파악하지 못한다.

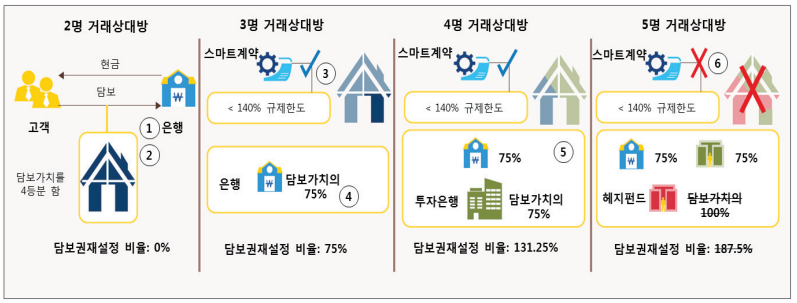
③ 규제기관은 증권화를 통해 자산담보권이 재설정되는 과정을 추적할 수 없으며 제한을 강제하는 것도 불가능하다.

④ 자세한 거래기록이 유지되지 않기 때문에 개별거래에 적용되는 담보비율은 자산의 정확한 가치를 결정하는데 어려움을 초래한다.

⑤ 시장참여자 중에서 누구라도 채무불이행이 발생하면 개별 혹은 전체 거래에 영향을 주게 되어 금융시스템에 의도하지 않은 결과를 초래한다.

(마) 미래 처리 과정

<그림 3-41> 자산담보권 재설정 미래 처리 과정



① 은행이 취득한 담보가 토큰화되어 분산원장에 기록된다.

② 스마트계약이 토큰화된 담보를 요약하고 기록유지와 가치이전을 용이하게 한다.

③ 후발거래에서 스마트계약을 통해 담보가치, 거래상대방에 대한 정보를 시장참여자에게 제공한다.

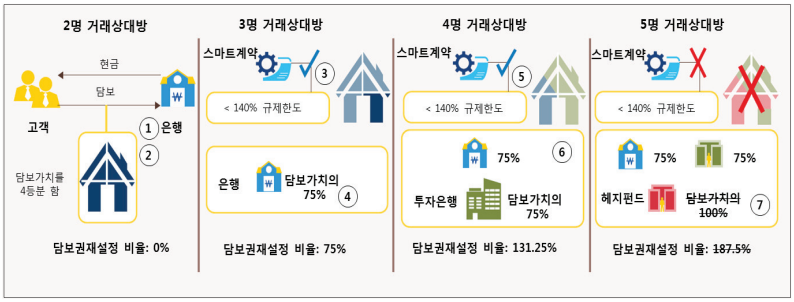
④ 투자자는 자산의 거래기록과 거래상대방 신용등급에 대해 투명한 정보를 취득함으로써 거래의사결정을 개선한다.

⑤ 규제기관은 인증된 실시간 접속으로 자세한 거래기록을 파악하고 위반 여부를 모니터한다.

⑥ 스마트계약으로 최초 설정된 담보비율을 초과하여 담보권재설정이 되지 않도록 한다.

(바) 미래 처리 과정의 이득

<그림 3-42> 자산담보권 재설정 미래 처리 과정의 이득



① 담보가치, 위험정도, 소유권기록이 투명하게 투자자에게 제공되어 투자의사결정에 도움을 준다.

② 거래기록에 의해 거래상대방의 등급이 결정되므로 투자자는 자신의 위험성향에 부합하는 거래상대방을 선별하여 위험을 해지할 수 있다.

③ 분산원장 기술은 처리과정에 효율성을 증진시킴으로써 수작업 및 관련 비용을 줄여준다.

④ 규제기관은 자산의 가치, 소유권, 위험정도에 대해 정확히 파악할 수 있어 규제통제를 강요할 수 있다.

⑤ 스마트계약으로 제한된 비율을 초과하는 자산담보비율이 설정될 수 없다.

⑥ 강제적 규제조치와 투명한 거래기록으로 채무불이행이 발생하더라도 시스템위험을 크게 줄일 수 있다.

⑦ 스마트계약으로 자금과 자산의 이전이 용이해지고 비용이 많이 소요되는 중개과정을 제거한다.

(사) 필요조건 및 향후 전망

금융중개기관과 기술회사는 담보자산을 토큰화하기 위해 공동 작업을 수행하여야 한다. 이는 자산을 추적하여 스마트계약으로 담보권재설정 비율을 산출하기 위해 필요하다. 그러나 아직까지 금융중개기관 간에 토큰화의 표준이 설정되는데 어려움이 있다. 또한 금융중개기관이 토큰화된 자산의 거래시스템에 참여하는데 동의하고 합의된 원칙과 규제를 준수하여야 한다. 이는 담

보자산이 금융시스템을 통해 이동하는 것을 정확하게 추적하기 위해 모든 금융중개기관이 분산원장 기반 솔루션에 참여하기 때문이다. 그러나 분산원장 기술의 효과성, 참여의 기본 틀, 금융서비스 공동체의 지지 등이 사전에 확보되어야 한다.

그리고 기술회사는 유연한 분산원장 솔루션을 고안하여 비표준적인 장외시장(over the counter, OTC) 거래양식까지 설명할 수 있어야 한다. 이는 미래에 장외시장까지 확장하는데 필요한 수정을 포괄할 수 있어야 하기 때문이다. 그러나 금융중개기관과 기술회사 간에 분산원장 솔루션의 유연성을 확보하기 위한 협력과 이로 인해 스마트계약에 가해질 충격을 최소화해야 할 것이다.

자산담보권 재설정에서 분산원장 기술의 적용은 현재 개념증명 단계에 있으며 주로 금시장, 환매조건부시장, 담보자산 이전 등에 집중되고 있다. 한편 분산원장 기술은 거래상대방 위험의 감소와 보다 개선된 규제조치 이행수단으로 활용될 수 있는데 이는 거래상대방 신용등급 산출시스템, 자산거래 이력저장, 투명성 확보, 스마트계약의 이행 등에 적용될 수 있기 때문이다.

(9) 주식매매 후선업무

(가) 현황

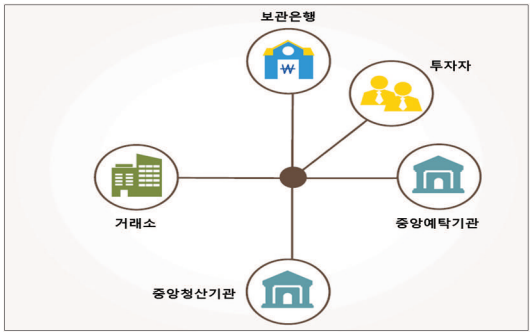
주식매매 후선업무는 주식매매에 따라 거래승인, 소유권기록 변경, 주식과 대금의 교환이 이루어지는 과정으로 뉴욕증권시장에서 매일 수백만 건의 거래와 수십억 주의 주식이 처리되고 있다[31]. 거래확인에 뒤이은 후선의 청산과 결제는 완결되기까지 t+2(혹은 t+3)이 소요될 정도로 시간이 많이 필요하며, 미국 은행과 중앙대행기관 및 중개기관에서 후선업무로 90억 달러 정도의 비용을 발생시키고 있다[32].

(나) 주요 참가자

31) NYSE, NYSE: Transactions, Statistics and Data Library, 2016 참조
32) Broadridge, Charting a Path to a Post-Trade Utility, 2015 참조

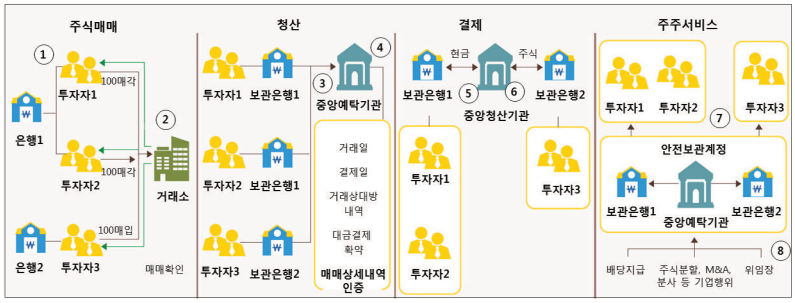
주식매매 후선업무의 참가자는 중요 역할을 담당하는 보관은행, 투자자, 중앙예탁기관, 중앙청산기관과 업무를 지원하는 거래소가 있다.

<그림 3-43> 주식매매 후선업무 주요 참가자



(다) 현재 처리 과정

<그림 3-44> 주식매매 후선업무 현재 처리 과정



① 투자자는 은행이 제공한 주식거래프로그램을 이용하여 거래소에 접속한다.

② 거래소는 주식매매주문을 체결시키고 실시간으로 확인해줌과 동시에 후선업무를 개시한다.

③ 증권거래의 결제를 위해 보관은행은 거래 상세내역(거래일, 결제일, 대금결제확약 등)을 중앙예탁기관에 발송한다.

④ 중앙예탁기관은 보관은행에서 보내온 거래 상세내역을 확인하고 모든 참여자의 거래를 체결시킨다.

⑤ 모든 참여자의 거래를 체결시킨 후 중앙예탁기관은 순거래를 확정하여 보관은행에 통보한다.

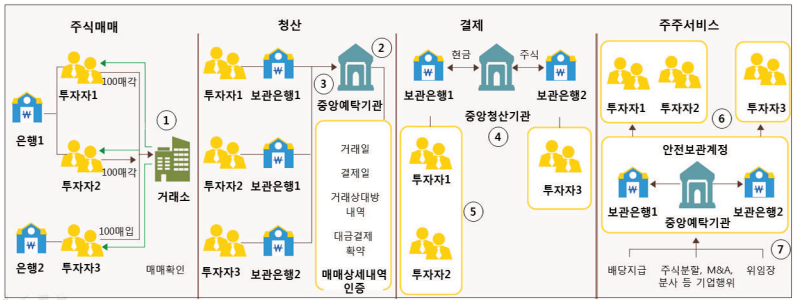
⑥ 주식과 거래대금의 동시이전이 중앙거래당사자와 투자자를 대신한 보관은행 간에 이행된다.

⑦ 주식과 거래대금이 보관은행과 중앙예탁기관의 계좌에 저장된다.

⑧ 주주 관련서비스가 투자자에게 제공된다.

(라) 현재 처리 과정의 취약점

<그림 3-45> 주식매매 후선업무 현재 처리 과정의 취약점



① 투자자는 주문을 낸 후 거래내역을 확인하지만 실제 결제는 t+2(혹은 t+3)일이 소요된다.

② 거래상대방 은행이 거래 상세내역을 빈번히 변경시킴으로써 중앙예탁기관은 청산이전에 수작업으로 이를 확인해야 한다.

③ 보관은행은 이행일에 결제가 되지 않을 가능성을 부담한다.

④ 중앙거래당사자는 결제에서 기술적 혹은 수작업의 오류 가능성을 부담한다.

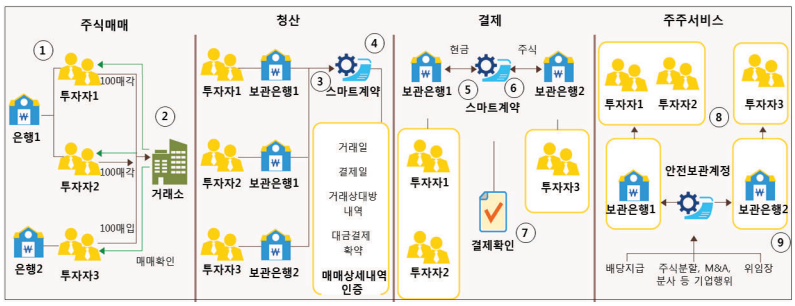
⑤ 투자자는 자신들의 거래가 결제되었는지에 대해 지속적인 통보를 받지 못한다.

⑥ 중앙예탁기관과 보관은행 간의 증권결제시스템에 계정을 저장하므로 보관은행에 유연성이 부족해진다.

⑦ 주주관련 서비스를 수행하는데 비용이 많이 소요된다.

(마) 미래 처리 과정

<그림 3-46> 주식매매 후선업무 미래 처리 과정



① 투자자는 은행이 제공한 주식거래프로그램을 이용하여 거래소에 접속한다.

② 거래소는 주식매매주문을 체결시키고 실시간으로 확인해 줌과 동시에 후선업무를 개시한다.

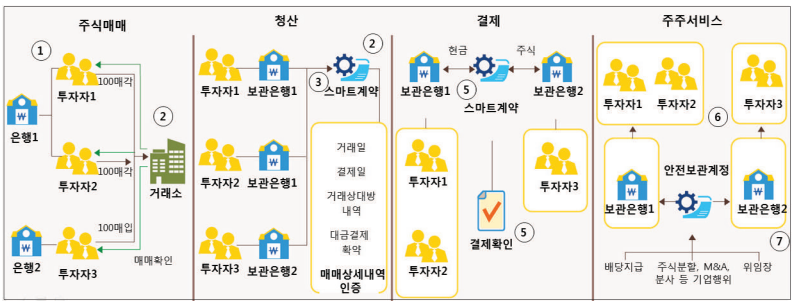
③ 보관은행은 거래 상세내역을 투자자를 대신해 분산원장에 기록한다.

④ 스마트계약으로 거래 상세내역을 인증하고 모든 참여자의 거래를 실시간으로 체결한다.

⑤ 거래체결 후 스마트계약은 순거래를 확정한다.
⑥ 스마트계약으로 보관은행 간에 주식과 거래대금의 동시이전을 보장한다.
⑦ 체결확인 내용이 다음 과정을 위해 분산원장에 저장된다.
⑧ 주식과 대금이 이전된 후 해당 내역이 보관은행의 계좌에 저장된다.
⑨ 스마트계약에 의해 주주 관련서비스가 보관은행이나 투자자에게 실시간으로 통보된다.

(바) 미래 처리 과정의 이득

<그림 3-47> 주식매매 후선업무 미래 처리 과정의 이득



① 후선업무 자동화와 효율성 증진으로 결제기간이 실시간 결제나 t+1일로 감소한다.
② 거래체결 자료의 표준화로 청산과정의 효율성 개선된다.
③ 인증자동화로 거래상대방의 결제불이행 가능성이 감소한다.
④ 주식과 거래대금의 이전에 스마트계약을 활용하여 기술적 혹은 수작업의 오류가 감소한다.
⑤ 분산원장 기술에 의한 결제확인으로 투자자는 보관은행에 의존하지 않고 결제 통보를 받을 수 있다.
⑥ 보관은행은 증권결제시스템에 통합되지 않으므로 자산의 저장에 유연성이 커진다.
⑦ 스마트계약을 통해 주주 관련서비스를 제공하므로 제3의 중개기관이 개입할 필요가 없어진다.

(사) 필요조건 및 향후 전망

보관은행과 규제기관은 협력하여 주식과 거래대금의 교환을 최소화할 수 있는 차감거래를 할 수 있어야 한다. 이는 중앙거래당사자가 실행된 거래를 종합하여 자산의 이동을 최적화함으로써 결제의 비효율성을 줄이기 위함이다. 그러나 스마트계약은 실시간으로 거래를 실행하기 때문에 사전에 정해진 간격으로 거래가 이루어질 수 있도록 맞춤화가 필요하다.

또한 규제기관, 보관은행, 거래소는 매일의 거래규모를 제어할 수 있는 솔

루션을 개발하기 위해 협력관계를 맺고 이를 통해 모든 참여자에게 규모의 경제로 인한 편익을 제공하여야 한다. 이는 후선업무가 매우 복잡하므로 규제기관, 보관은행, 거래소가 자발적으로 참여하여야 시장의 안정을 얻을 수 있기 때문이다. 그러나 분산원장 기술의 성공적 도입으로 중앙거래당사자의 중개역할이 사라진다면, 기술적 실패가 발생하는 경우 지배 및 협력 구조가 확립되어 있어야 한다는 점이 고려되어야 한다.

그리고 보관은행들은 투자자에게 익명성과 믿음을 주는 구조로 거래체결 자료를 표준화하기 위해 협력하여야 한다. 이를 표준화하지 못할 경우 수작업의 후선업무가 요구되며 이로 인해 중앙거래당사자와 중앙예탁기관의 중개역할이 여전히 필요하기 때문이다. 그러나 거래체결을 위한 전통적인 자료영역이 빈번하게 변경되기 때문에 표준화된 속성이 빈번하게 업데이트되지 않기 위해서는 초기에 상당한 협업이 가능하여야만 할 것이다.

주식거래 후선업무에서 분산원장 기술의 활용은 현재 다수의 핀테크기업이 개념증명을 하는 단계로 주로 사적 주식거래와 청산 및 결제 솔루션에 집중하고 있다. 분산원장 기술은 금융중개기관에게 비용절감과 운영효율성 개선을 제공할 수 있는데 이는 탈중개화로 인한 수수료 절감과 청산과 결제에 스마트계약을 이용함으로써 효율성을 제고함으로써 발생한다.

3. 분산원장 기술의 탈중개화와 중장기 과제

가. 분산원장 기술과 탈중개화

(1) 국제송금

현재 국제송금에 있어 자금이전의 흐름에 다수의 단계와 중개기관이 필요한데 이는 처리속도와 비용이 발생되는 원천이기도 하다. 분산원장 기술은 각 단계의 흐름을 완전히 파악할 수 있도록 투명성을 제공함과 동시에 개별기관의 원장보유 필요성을 제거함으로써 효율성을 제고시킬 수 있을 것이다. 더욱이 디지털통화는 은행들의 거래 인증을 통해 네트워크상에서 법정화폐의 거래를 촉진시키며, 해킹의 위험을 감소시킬 수 있다. 즉 송금과 외환거래를 포함한 현재의 국제지급결제는 처리속도가 늦고 비용도 많이 소요되며,

특히 통화가 다르거나 국경을 넘는 경우에는 더욱 그러하다. 분산원장 기술은 디지털토큰이나 디지털통화를 사용함으로써 이러한 문제를 해결할 수 있을 것이다.

분산원장 스타트업인 Ripple은 기업의 국제송금에 관한 솔루션을 개발하고 있다. 자체 암호화화폐(cryptocurrency) 인 'XRP'로 지급프로토콜을 만들어 비트코인 블록체인보다 더 빨리 네트워크를 통해 전달하고자 한다[33]. Ripple은 2016년 6월 뉴욕에서 가상화폐에 대한 면허를 취득하였다. Ripple과 협력하여 다수의 글로벌은행은 국가 간 지급결제시스템을 개선하는 노력을 경주하고 있다. 이에 따라 최상위 50개의 글로벌은행 중 12개가 참여하여 30개의 블록체인 프로젝트를 수행하였는데[34] 예를 들어 영국의 Santander는 영국과 21개 국가 간에 익일결제를 위해 6,000명의 직원을 대상으로 새로운 지급결제 어플리케이션을 테스트하였다. 또한 Ripple의 지급결제기술을 이용하여 오스트레일리아의 주요 은행 중 ANZ와 Westpac은 지급결제의 추적, Commonwealth는 해외지사들과의 지급결제를 테스트하였다[35].

(2) 자본시장

증권의 발행, 소유권 등록 및 거래의 경우 분산원장 기술을 기반으로 하면 발행과 소유권의 이전에 효율화를 기할 수 있다. 예를 들어 신주 발행을 통해 자본금을 확충하기 원하는 소규모 민간기업은 분산원장 기술을 통해 투자자와 직접 거래할 수 있으며, 증권의 소유자는 2차 시장에서 실시간으로 매매도 가능하다. 분산원장 기술은 개별 증권의 소유권에 대해 변경 불가능한 이력을 유지시켜 주기 때문이다. 한편 분산원장 기술이 발행 및 유통 시장에서 P2P거래를 어느 정도 가능하게 해주는가에 따라 중개기관의 역할과 중개수수료가 감소하거나 사라질 수 있다. 그러나 증권의 무결성에 대한 확신이 매우 중요하므로 발행 및 유통 시장의 P2P거래에 있어 규제받는 중개기관의 지속적인 개입이 필요할 것으로 예측된다.

또한 증권매매 후 청산 및 결제의 경우 분산원장 기술을 활용하게 되면 거의 실시간 결제가 가능하므로 결제 시간 및 위험의 감소, 거래상대방 위험

33) https://ripple.com/xrp-portal/
34) https://ripple.com/insights/seven-leading-banks-join-ripples-global-network/
35) https://cointelegraph.com/news/australias-big-four-banks-anz-westpac-test-out-ripple-payments

감소, 예치증거금이나 담보 관련 비용의 절감이 가능하다. 그리고 증권 거래 이후 브로커, 청산기관, 중앙예탁기관 등 복수 중개기관에 분산된 원장으로 인하여 거래기록 유지 개선, 복수의 개별적인 원장들을 조정하는 문제를 제거할 수 있다. 분산원장 기술이 거래의 즉각적인 결제를 실현한다면 현금으로 이루어지는 결제를 실시간으로 청산하는 중앙청산기관의 역할은 사라져 신용 및 유동성 위험이 제거될 것이다. 그러나 현금과 증권의 결제가 즉각적이지 않다면 증권거래의 청산을 위해 중개기관의 개입이 여전히 필요할 것으로 예측된다.

증권보관 및 증권 관련서비스의 경우 정해진 일자에 증권 관련서비스가 이루어지도록 구조화된 스마트계약을 활용할 수 있는데 이는 만기 원금의 상환, 채권의 이표 지급, 주식의 배당금 지급 등에 적용 가능하다. 현재 증권 관련서비스는 일반적으로 보관은행에 의해 문서화된 공표로 이루어지는데 종종 날짜 오류 등이 발생하고 있다. 증권 관련서비스에서 스마트계약은 다양하게 활용이 가능한데 자동 마진콜, 거래상대방 파산 시 자동지급 등 파생상품 업무, 신디케이트 참여은행 간의 자동화된 현금흐름이 가능한 신디케이트대출, 대출금을 상환하지 못하는 경우 개인키로 잠겨 있는 담보대출 등에 활용된다. 증권이 분산원장 기술로 등재됨에 따라 증권의 안전한 보관과 관련서비스를 제공하는 보관은행의 역할 및 수수료는 감소한다. 그러나 보관은행의 역할은 개인키의 안전한 보관과 고객친화적 분산원장 구조와 인터페이스의 개발 등으로 변화될 가능성도 있다.

또한 일부 거래의 경우는 거래참가자 간의 개선된 정보공유로부터 편익을 얻을 수 있다. 예를 들어 분산원장에 스마트계약 구조의 신디케이트론을 등재함으로써 현재 결제까지 수주일이 소요되는 작업흐름을 빠르게 할 수 있다. 대출주간사가 대출관련 조항을 프로그래밍하여 공유함으로써 필요한 경우 즉각적인 종료와 청산이 가능하기 때문이다.

이처럼 분산원장 기술은 주식, 채권, 파생상품, 환매조건부증권, 대출, 자산담보부증권 등과 같은 증권의 발행, 소유, 거래, 거래 후 청산과 결제, 보관 및 기타 관련 업무의 전 과정에서 활용될 수 있다. 참가자 간에 공유되며 동기화되는 분산원장 기술을 활용하면 각기 다른 원장들을 조화시킬 필요가 없으며, 작업흐름을 개선할 뿐만 아니라 스마트계약을 통해 수작업의 불편함을 제거할 수도 있다.

Nasdaq은 블록체인 스타트업인 Chain과 협업하여 블록체인에 기반한 자본시장 솔루션을 적극 개발하였는데 이를 통해 Nasdaq Linq 등록 기업의 IPO 이전 주식거래를 실행하고 있다. 2015년 12월에 Chain은 Nasdaq Linq의 투자자를 대상으로 민간기업의 증권거래를 성공적으로 수행하였으며, 소유권의 기록을 디지털화함으로써 결제에 소요되는 시간을 크게 감소시켰고 종이로 된 주권의 발행을 제거하였다[36]. 또한 Nasdaq은 에스토니아의 Tallinn 거래소에 등록된 기업의 주주총회에 블록체인에 기반한 전자투표 서비스를 개발하였다[37].

BOA, Citigroup, Cedit Suisse, DTCC, JP Morgan, Markit는 블록체인 스타트업인 Axoni와 협업하여 North American single-name CDS 거래를 위한 거래 후 업무처리를 성공적으로 수행하였다[38]. 여기에는 85가지에 걸쳐 기능별 업무처리, 외부시스템과의 통합, 해킹대비 회복력 및 데이터 프라이버시 등을 대상으로 하고 있다.

ICAP는 양자 간 현물환 및 선물환 블록트레이드의 후선업무를 Axoni의 블록체인과 스마트계약을 통해 성공적으로 테스트하였다[39]. 9개의 노드만 허가된 블록체인을 사용하여 블록체인이 거래를 파악하는 최적의 원천으로 데이터의 정확성과 거래 속도를 개선시키고, 사용자 서버에 기록을 제공하며 허가된 참가자만이 보안메시지를 볼 수 있도록 하여 통제와 운영과정의 개선을 확인하였다.

Overstock.com은 자회사인 TØ.com을 통해 블록체인 상의 증권 사모 및 공모에 집중하여 2015년 6월 채권을 사모하였고 이를 TØ.com에서 청산 결제하였다[40]. 더욱이 2015년 12월에는 SEC로부터 블록체인을 이용한 증권 공모를 승인받아 향후 증권 공모의 모든 과정이 블록체인을 통해 이루어지게 되었다.

---

36) http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326
37) http://ir.nasdaq.com/releasedetail.cfm?releaseid=954654
38) http://www.dtcc.com/news/2016/april/07/successful-blockchain-test-completed
39) http://newsroom.icap.com/icaps-post-trade-risk-and-information-division-announces-completion-of-a-blockchain-proof-of-technology
40) https://bitcoinmagazine.com/articles/overstock-com-offer-worlds-first-cryptosecurity-bitcoin-blockchain-1433797910

Goldman Sachs는 자체 개발한 'SETLcoin'을 이용하여 증권의 즉각적인 이전과 매매와 동시에 결제가 이루어지는 프로젝트를 진행하고 있으며[41], UBS는 Ethereum이 개발한 전 과정 자동결제 스마트채권의 데모를 진행하고 있고[42], Digital Asset Holdings는 Australian Securities Exchange의 증권 청산 및 결제를 대체하기 위한 블록체인을 개발하고 있다[43].

(3) 무역 금융

무역금융에서 수출업자, 수입업자, 관련은행, 운송회사, 항만 및 세관 등은 공유된 분산원장 기술에 접속하여 자신들과 관련된 단계를 감시할 수 있다. 무역금융의 각 단계는 수입은행의 신용장 등록, 운송회사의 물물 수령 및 전달 문서, 항만 및 세관의 선하증권 보증 등으로 분산원장 기술의 한 블록으로 네트워크상에서 인증되어 일단 물품이 수입업자에게 전달되면 스마트계약의 요구사항들이 충족, 인증되어 자동적으로 지급이 실행된다.

그리고 분산원장 기술에 의한 금융회사 간 무역금융거래의 공유는 사기위험을 줄여준다. 현재 동일한 선적에 대해 무역업자들이 복수의 은행에 신용을 신청하는 정보는 공유되지 않으나 분산원장 기술은 계약조항의 기밀을 유지한 상태로 물품의 형태와 수량, 선하증권번호, 기타 데이터를 보관하여 표시할 수 있다. 이로써 은행은 자신들이 승인하기를 원하는 무역금융 거래에 대해 이미 다른 은행이 승인하였음을 확인할 수 있어 거래의 전체 이력을 파악하는 것이 가능하며 이는 공급사슬에서 물품의 공신력을 제고시키는 것이다.

결국 분산원장 기술은 수작업으로 이루어지는 무역금융절차를 자동화시킬 수 있어 자동지급이 포함된 스마트계약에로 신용장을 이전시킬 수 있고, 메타데이터로 선하증권이나 면세증과 같은 서류를 디지털화할 수 있으며, 각 단계마다 소유권 기록을 만들어 낼 수 있다. 이를 통해 저비용, 효율성 증가, 투명성 개선, 사기위험의 감소, 인적 오류를 줄일 수 있는 것이다.

---

41) http://grillip.com/en/business-ip/2015/12/02/goldman-sachs-files-patent-application-for-securities-settlement-using-cryptocurrencies/
42) http://www.coindesk.com/new-details-ubs-blockchain-experimentation/
43) https://digitalasset.com/press/asx-selects-digital-asset.html

DBS와 Standard Chartered는 Ripple과 협업관계를 맺어 블록체인에 기반한 무역금융 시험판인 'TradeSafe'를 출시하였다[44]. 또한 싱가포르의 IT 및 통신 당국인 'Infocomm Development Authority'와 협력하여 60건의 모의 무역금융을 블록체인에 등재하였다[45].

IBM은 블록체인 상의 디지털 공급사슬과 무역금융에 집중하여 블록체인 기반의 무역금융 솔루션을 공개 출시하고, 모든 무역관련 서류를 디지털화하여 블록체인에 등재함으로써 작업흐름의 개선을 목표로 하고 있다. 즉 각종 무역관련 서류의 승인이 수입 및 수출 은행, 항구와 세관 그리고 물류회사 등에서 승인되게 하였다[46]. Barclays는 자신의 창업지원프로그램을 수료한 블록체인 스타트업인 Wave와 협력하여 선하증권의 무권화(Dematerialized) 금융을 추구하고 있다[47].

(4) 규제 준수와 감사

분산원장 기술은 거래데이터의 실시간 은행 간 조정, 보고, 감사, 규제기관과의 공유를 단순하게 해준다. 즉 분산원장 기술은 스마트계약을 통해 내부규제 준수나 외부규제 요구를 위반하였을 경우 경보를 발령하게 하고, 표준화된 회계감사양식으로 관련기관들 간의 금융데이터 비교 및 통합을 용이하게 해준다.

(5) 자금세탁방지(AML) 및 고객알기제도(KYC)

금융기관은 KYC와 AML을 위해 고객의 신원을 증명해야 하는데 이 과정은 여러 단계에서 복수의 기관들이 개입하여야 하며 종종 동일고객에 대해 한 금융기관의 다른 부서나 타 금융기관들이 중복된 정보를 확인하기도 한다. 분산원장 기술은 표준적인 KYC와 AML 데이터 환경을 조성하여 금융기관이 자신의 다른 부서나 타 금융기관과 고객의 신분 정보를 공유할 수 있게 해준다. 즉 고객이 분산원장 네트워크에 있는 한 금융기관으로부터 자신의 신

44) https://www.cryptocoinsnews.com/standard-chartered-dbs-work-on-blockchain-tech-for-trade-finance/
45) https://www.sc.com/en/news-and-media/news/asia/2015-12-17-worlds-1st-distributed-ledger-technology.html
46) http://www-03.ibm.com/press/us/en/pressrelease/50163.wss
47) http://www.coindesk.com/wave-blockchain-trade-finance-barclays/

분정보를 요청받고 KYC와 AML에 서명하게 되면, 이것으로 KYC와 AML 조사필요성이 감소하므로 새로운 금융상품과 관련된 규제준수비용이 절감될 수 있다.

(6) 보험금 지급

분산원장 기술에 등재된 보험약관은 스마트계약을 활용하여 보험회사나 신뢰받는 제3자에 의해 보험금 지급조건이 충족되었을 경우 보험금을 자동 지급하는 것이 가능하다. 임직원의 해석이 요구되지 않는 즉각적인 결정이 가능한 경우라면 보험사기나 적정 청구를 판별하는 비용은 감소할 것이다.

예를 들어 극심한 기상조건 악화로 농장물의 수확에 심각한 손실이 발생한 경우 농작물보험에서 스마트계약을 활용함으로써 농부는 분산원장 기술에 등재된 보험약관에 명기된 기상악화 조건에 따라 자동적으로 보험금을 청구하여 지급받을 수 있다. 이때 기상정보 역시 신뢰받는 기상당국으로부터 실시간으로 제공받을 수 있다. 또한 분산원장 기술에 고가 재화의 소유권을 등재함으로써 보험금의 사기청구를 줄일 수 있다. 도난당한 재화를 다시 유통시키거나 찾았을 경우 분산원장 기술에 등재된 이력은 최초 소유자를 추적할 수 있게 하여 부당한 보험금 지급을 감소시킬 수 있는 것이다.

(7) P2P 대출 및 보험

분산원장 기술은 효율적인 관리절차를 통해 P2P 플랫폼을 지원한다. 스마트계약은 특정 조건에 부합되는 경우 가치이전을 보장하는데 특히 모바일폰 사용은 많지만 금융기관이 적은 지역의 마이크로파이낸스와 마이크로보험에 유용하다. 분산원장 기술을 활용한 P2P대출 플랫폼은 스마트계약을 통해 원금과 이자 지급을 자동화시킬 수 있는데 이는 대출 여부와 대출이자율을 승인해 주는 자금제공자에게 차입자의 신용지표를 유지하게 해 준다. 또한 P2P보험 플랫폼에서 투자자는 특정 위험한도에 기반하여 보험료 납부고객과 연계될 수 있다. 즉 제시된 보험료는 투자자의 위험부담능력에 대한 역사적 데이터에 근거하여 결정되며 스마트계약은 보험료와 보험금지급을 자동화시킬 수 있다.

나. 중장기 과제

(1) 분산원장 기술의 비용편익분석

분산원장 기술을 금융산업에 적용하여 그 활용도가 제고될 수 있는가를 파악하기 위해서는 비용과 편익의 비교 분석이 필요하다. 분산원장 기술의 속도와 용량 측면을 먼저 보면 분산된 데이터베이스는 본질적으로 중앙집중 방식보다 작업수행 속도가 빠르지 않기 때문에 분산원장 기술이 빠른 속도와 대용량이 필요한 업무에 적절한가에 대해서는 아직까지 의문이 있다. 물론 현재 다양한 형태의 분산원장 기술로 속도와 수행능력을 개선시키고 있지만 금융산업에의 활용에 있어서는 개선 필요성이 존재한다.

또한 분산원장 기술 적용에 따른 높은 전환비용은 현재의 시스템을 바꾸기 어렵게 만들 수 있다. 이로써 새로운 기술의 필요를 절감하고 도입을 추진하는 의견과 수익성 악화나 현금흐름에 대한 우려로 도입에 어려움을 주장하는 의견이 상충관계를 발생시킬 수 있다. 새로운 기술로 인한 시스템의 전환에는 초기비용이 많이 들지만, 효용은 시간이 지난 뒤에 얻을 수 있기에 막대한 투자비용과 시간 그리고 이로 인한 기회비용 등을 포함하는 전환비용을 반드시 고려하여야 한다. 또한 투자수익률(ROI), 위험(risk), 영향평가(impact assessment) 등도 분산원장 기술 채택에 영향을 줄 수 있다. 그러므로 전환비용과 기대효과를 명확히 분석하는 과정이 필요하다[48].

결국 분산원장 기술에 기반한 유연한 금융솔루션을 개발하기 위해서는 전환비용 산출과 함께 모든 참가자의 협력관계를 기반으로 한 규모의 경제로 인한 편익을 고려하여야 한다. 따라서 현재 독자적으로 실행되고 있는 각종 분산원장 기술의 수렴 가능성, 분산원장 기술의 도입으로 인해 사라지는 중개기관의 역할과 그에 따른 편익, 스마트계약의 활용에 따른 순효과와 역선택, 결제시기의 단축에 따른 비용과 편익, 고객의 개인정보 공유 필요성 등에 대해 지속적인 검토가 필요하다.

48) 백종찬, 한승환, 안상욱, 김태연, 「금융기관을 위한 블록체인의 이해」, 피넥터보고서 2권, 2016.9, p.40 참조

(2) 호환성 확보와 표준 제정

분산원장 기술의 활용 분야는 향후 크게 확대되어 다양한 형태의 특수한 목적을 지닌 비공개 분산원장 기술이 개발될 것이므로 호환성 확보와 기술 표준의 확립은 매우 중요하다. 특히 복수의 분산원장 기술이 혼합되어 사용되는 경우에는 호환의 문제가 크게 대두되기 때문에 표준화되지 못하였다면 추가적인 수작업이 요구되어 비용의 비효율성 증대와 이익의 감소를 초래할 것이다.

호환성은 서로 다른 분산원장 간의 호환과 분산원장 기술과 기존 금융시스템 간의 호환을 모두 고려하여야 한다. 서로 다른 분산원장 간의 호환에는 여러 가지 기술적 방안들이 도출되고 있지만 아직까지 성숙된 기술이 없는 형편으로 분산원장 기술 간의 호환은 기술표준화와 범용화가 이루어지기 전 초기단계에서 더욱 필요하다. 또한 분산원장 기술과 기존 금융시스템 간의 호환에는 우선 기존 원장에 기록되는 화폐와 분산원장에 기록되는 화폐가 동일하여야 한다. 최종결제은행이 없이 거래은행들끼리 분산원장을 공유하는 경우 기존 금융시스템과 호환되지 않아 지급이행능력을 증명할 수 없는 신용위험이 존재하기 때문이다. 그리고 분산원장 기술은 기존 데이터베이스에 사용되는 방식으로 다루기 어려워 데이터에의 접근 및 관리에 있어 호환성 결여는 데이터분석에 어려움을 발생시킨다. 현재로서 기존 금융시스템을 한꺼번에 분산원장 기술로 대체하는 것은 비현실적이므로 기존의 업무방식을 최대한 저해하지 않으며 호환성을 확보하도록 순차적으로 시스템을 혁신해 나갈 필요가 있다[49].

분산원장 기술 활용에 있어 개별 금융거래마다 각기 다른 데이터를 요구하여 데이터 영역이 표준화되지 못하였다는 사실은 투자자들이 갖는 금융거래에 대한 신뢰 제고를 저해하는 요인으로 작용할 것이다. 즉 금융회사들이 분산원장 기술 솔루션을 중복개발 함으로써 투자자들이 표준화된 투자분석을 하는데 어려움이 있고 관심사의 충돌을 발생시킬 가능성이 클 것이다. 특히 금융거래의 효율성을 제고시키기 위해 분산원장 기술을 활용한 스마트계약에 토큰화된 자산을 등재시킴으로써 자산의 추적과 거래를 용이하게 하는 과정이 폭넓게 활용될 것이므로 금융중개기관 간에 토큰화 표준이 설정되어야 한다.

---

49) 백종찬, 한승환, 안상욱, 김태연, 「금융기관을 위한 블록체인의 이해」, 피넥터보고서 2권, 2016.9, pp.41~42 참조

(3) 거버넌스 모델의 수립

분산원장 기술로 거래상대방은 서로 간의 세밀한 재무정보에 접근할 수 있기 때문에 위험에 직면하거나 논쟁을 유발시킬 수 있다. 따라서 법적 선례나 책임 모형이 없다면 분산원장 기술에 자신의 고유 재무정보를 저장하는 위험을 부담하는 것이 현실적으로 어려울 수 있다. 또한 분산된 데이터베이스를 적용하여 거래상대방과 정보를 공유함으로써 평판관리(reputation management)의 문제가 발생할 수 있는데 이로 인한 문제는 지속적으로 기업의 평판에 영향을 주게 된다. 결국 분산원장 기술의 활용에 있어서는 이해당사자 간에 법적 틀을 공유하는데 대한 관심사나 절박함이 서로 다를 수 있기 때문에 거버넌스 모델에 대한 면밀한 검토가 요구된다.

또한 규제기관과 중개기관 역시 분산원장 기술의 활용으로 상당한 정도로 재무정보를 공유하게 되며 이를 통해 규제기관이 실시간으로 투명한 재무정보에 접근하여 규제준수를 확인하게 된다. 그러나 현재까지 법적 선례가 없으므로 규제기관과 중개기관 간의 재무정보의 공유와 관련된 협력은 매우 도전적인 문제이다.

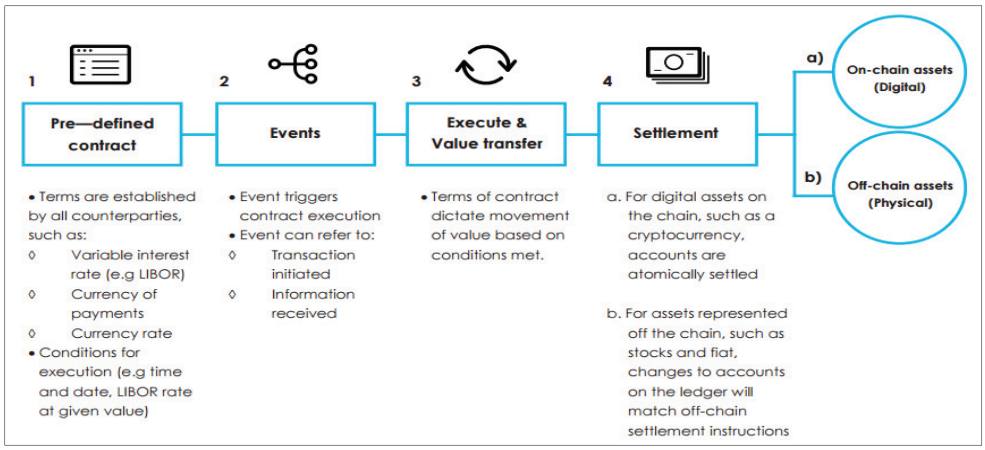
결국 현재 금융산업에 적용되는 법률이 분산원장 기술에도 적용될 수 있는 법적 근거가 준비되어야 한다. 에어비엔비(Airbnb)나 우버(Uber)와 같은 혁신기술의 경우는 '먼저 행동하고 나중에 승인을 얻는 전략(act first, seek forgiveness later)'을 활용하였지만 분산원장 기술을 활용한 금융시장에서의 혁신은 명백한 규제가 뒷받침되어 책임 있는 주체가 결정되어야 한다.[50] 특히 신원보증, 청산결제, 지급보증 문제는 규제기관이 적극적으로 개입하여 법률적인 기초를 마련하여야 한다. 이 과정에서 특히 불가역적으로 분산원장에 기록된 이체내역, 즉 결제의 완결성을 법적으로 보장할 것인가에 대한 법률적 해석은 사려 깊은 검토가 요구되는 부분이다.[51]

---

50) Euroclear and Oliver Wyman, *Blockchain in Capital Markets: The Prize and the Journey*, 2016.2, p.14 참조

51) 백종찬, 한승환, 안상욱, 김태연, 「금융기관을 위한 블록체인의 이해」, 피넥터보고서 2권, 2016.9, p.40 참조

<그림 3-48> 스마트계약의 구조



그리고 분산원장 기술의 발전에 있어 스마트계약은 매우 중요한 활용가치를 지닌 기술로 자기강제적 언어(self-enforcing language)이므로 제3자나 법집행관이 개입하지 않아도 컴퓨터가 계약을 강제로 실행할 수 있어 구조화가 잘 되어 있다면 익명의 상대방과 거래하는 것이 가능하다. 거래상대방이나 제3자를 신뢰하는 것이 아니라 컴퓨터코딩을 믿기 때문에 무신뢰거래를 가능하게 하고, 거래당사자가 복수일 때 강력한 힘을 발휘할 수 있다[52]. 그러나 법적으로 금융분야에서 스마트계약의 효력이 인정되기까지는 계약의 다양한 범위와 세부조항에 대한 심도 있는 논의가 선행되어야 할 필요가 있다.

한편 분산원장 기술과 관련된 거버넌스에 있어 규제기관의 역할은 매우 중요하다. 규제기관 스스로 다양한 분산원장에 접속하여 거래를 감사하고 실시간으로 거래추이를 분석하는 등 편익을 이끌어 냄으로써 규제 감시를 개선할 수 있다. 즉 규제기관이 분산원장 기술을 적극적으로 수용함으로써 분산원장 기술의 활용과 적용가능성이 명확해지고 해당분야의 안정성과 거버넌스가 확립될 수가 있다. 이를 위해 규제기관은 분산원장 기술과 관련된 대기업뿐만 아니라 스타트업과의 협력을 통해 기술의 이해를 증진시키고 혁신에 유연성을 제고시킬 수 있다. 더욱이 일부 규제기관이 '규제용 샌드박스(regulatory sandbox)'[53]를 설정하여 현행 규제요건을 저해하지 않는 범위에

52) 백종찬, 한승환, 안상욱, 김영진, Chris Hong, 「블록체인기술의 발전과정과 이해」, 피넥터보고서 1권, 2016.8, p.38 참조
53) 보호된 영역 내에서 프로그램을 동작시키는 것으로 외부 요인에 의해 악영향이 미치는 것을 방지하는

서 분산원장 기술 스타트업을 비롯한 핀테크기업이 자신들의 제품과 비즈니스모델을 테스트하는 환경을 제공하고 있다는 사실은 주목할 필요가 있다[54].

이밖에도 분산원장 기술의 성공적 도입으로 중개기관의 역할이 사라지는 경우 기술적 실패가 발생한다면 시장실패의 확산을 방지하기 위해 지배 및 협력 구조가 확립되어 있어야 한다. 특히 국제송금에 있어서 SWIFT의 역할, 자본시장에서 중앙청산기관과 중앙예탁기관 등의 역할에 대해서는 지속적인 검토가 필요하다.

(4) 조세체계의 확립

분산원장 기술이 지닌 변경불가능성, 투명성, 자율성의 특징을 기반으로 새롭게 설정되는 금융인프라는 기존의 조세체계에 적용되기 어려운 측면을 지니고 있다. 특히 단순성과 효율성으로 비즈니스모델의 변화를 초래해 중개기관의 역할 축소, 국내외 직접 거래의 증대, 거래 절차의 간소화, 불법 및 탈법 거래의 축소, 새로운 상품의 개발을 비롯한 확장 가능성 등이 크게 부각될 것이다.

우선 거래 단계 축소에 따른 중개기관의 역할 및 수수료의 감소는 기존 조세체계와는 달리 새롭게 형성된 시장참여자 간에 조세부담의 변화를 야기할 것이다. 스마트계약의 활용에 따라 거래의 투명성이 제고되면서 거래 절차도 간소화됨으로써 세원의 포착과 징수가 용이해지게 되면서 세율 측면의 조정 필요성이 대두될 수 있다. 세금의 징수에 있어 납세자가 분산원장 기술의 디지털통화나 디지털토큰으로 세금을 납부할 수 있다면 세금 징수의 효율화를 꾀할 수 있다. 예를 들어 자동차 등록을 분산원장에서 관리하는 경우 자동차 소유자가 신차나 중고차를 새로 구입하여 등록할 때 등록세를 분산원장 기술의 디지털통화나 디지털토큰으로 바로 납부하는 것이 가능하다. 그리고 스마트계약이 널리 활용된다면 각종 계약의 작성에 따른 인지세의 징수가 자동화될 수 있으며 이렇게 되면 인지세 전반에 대한 검토가 필요할 수 있다[55].

보안 모델로'상자'는 다른 파일이나 프로세스로부터는 격리되어 내부에서 외부를 조작하는 것은 금지되고 있다.

54) 영국, 싱가포르, 오스트레일리아의 규제기관은 블록체인에 대한 논의를 선도하며 상호간에 핀테크기업의 시장진출을 지원함으로써 핀테크 허브를 구축한다는 목표를 추진하고 있다. 또한 영국과 싱가포르는 각각 규제용 샌드박스의 운용을 발표하였다.
Moody's Investor Service, Credit Strategy-Blockchain Technology: Robust, Cost-effective Applications Key to Unlocking Blockchain's Potential Credit Benefits, 2016.7, p.10 참조

그리고 기술, 데이터, 거래관행 등의 표준화로 호환가능성과 복잡성이 증대됨으로써 새로운 금융상품의 생성과 기존 금융상품의 퇴출이 자유롭게 발생할 것이므로 조세체계 역시 이에 상응하는 유연성을 확보할 필요가 있을 것이다. 결국 모든 시장참가자가 이해하기 쉽게 설정된 법에 기반한 조세체계 확립에 대한 검토가 요구된다.

4. 소결

분산원장 기술은 금융인프라 기술로써 높은 활용가능성, 불가역성, 저렴한 비용의 회복력이라는 매력적인 특성을 지니고 있다. 이러한 특성을 바탕으로 금융인프라를 새롭게 설정함으로써 관리의 단순화, 결제시간의 단축, 규제의 효율성 개선, 유동성 및 자본요건의 개선 등을 통해 단순성과 효율성을 제고시킬 수 있다. 그리고 향후 인공지능, 사물인터넷, 클라우드컴퓨팅 등과 함께 차세대 금융인프라의 근간을 형성할 것이다. 따라서 분산원장 기술을 금융산업 전반에 활용하게 되면 금융인프라 및 서비스의 혁신으로 인한 편익과 함께 큰 폭의 비용절감 효과를 거둘 수 있다. 앞서 살펴본 바와 같이 자본시장의 경우 증권의 소유권을 분산 저장할 수 있을 뿐만 아니라 실시간으로 업데이트 할 수 있다. 또한 주주권 행사와 배당금의 지급을 비롯한 주식관련 서비스에 효과성을 배가시킬 수 있기에 심지어 중개기관의 필요성도 향후에는 검토의 대상이 될 수 있다.

결국 분산원장 기술은 금융서비스의 디자인에 유연성을 제공할 수 있기 때문에 금융산업의 다양한 분야에서 활용될 것이며, 그 편익 역시 다양한 범위에서 발생하게 되어 일률적으로 전체 편익규모를 측정하는 것은 쉽지 않다. 아직까지 실용의 측면과 규제의 관점에서 검토되어야 할 부분이 있지만 분산원장 기술은 금융서비스 관련 조정과정이나 데이터의 공유로 인해 자동적이면서 효과적인 비즈니스 운영을 가능하게 하여 비용을 크게 절감시켜 금융시장 참가자들의 편익을 증진시킬 수 있다. 따라서 분산원장 기술이 금융인프라에 미치는 긍정적 효과를 확대시키기 위해서는 금융회사와 핀테크기업 그리고 규제기관의 이해 깊은 협업이 필요한 것이다.

---

55) Nomura Research Institute, Survey on Blockchain Technologies and Related Services, FY2015 Report, 2016.3, p.72 참조

그러나 향후 분산원장 기술을 활용하여 금융인프라를 새롭게 설정하기 위해서는 상당한 시간과 투자가 지속적으로 필요하고, 주요참가자들의 이해관계 조절과 협력이 반드시 전제되어야 하며, 현재의 규제 및 관례 변화와 새로운 법적 책임 틀이 만들어져야 할 것이다. 특히 스마트계약의 실행은 참가자들의 지지와 관리방식에 대한 철저한 검토가 반드시 사전에 고려되어야 한다.

분산원장 기술은 아직 발전의 초기단계이지만 현존하는 금융인프라와 금융비즈니스에 커다란 혁신을 가져올 수 있기 때문에 금융기관, 규제기관, 스타트업을 비롯한 관련업체 모두의 참여와 협업을 요구하고 있다. 현재의 작업관행과 이익에 집중하다가 기술발전의 편익을 간과하여서는 안 될 것이다.

IV. 디지털통화 및 분산원장 기술과 규제

1. 디지털통화 규제의 필요성과 방안

가. 주요국의 디지털통화 규제현황

해외 각국의 금융당국과 국제금융기구들은 디지털통화는 금융산업의 급속한 변화를 초래할 것이라는 데에 주목하고 있다. 디지털통화는 상당한 성장 잠재력을 갖고 있으나 그에 상응하는 위험이 변수로 작동할 수 있다는 점에서 당국으로서는 큰 도전이다. 지금까지 비트코인 등의 디지털통화는 상대적으로 낮은 규제 속에 낮은 수수료, 빠른 처리시간 등 장점이 부각되어 왔다. 하지만 금융당국에게는 금융의 자유와 프라이버시를 최대한 보장하는 동시에 자금세탁방지(AML; Anti-money Laundering)나 테러자금유입방지(CFT; Counter Financial Terrorism)를 제공하는 금융무결성(Financial Integrity)과 함께 소비자 보호, 과세 등의 기능을 제대로 확보할 수 있는지가 중요하다.

또한 디지털통화의 규제는 ① 디지털통화 거래소, ② 지갑서비스 제공 사업자, ③ 사용자에 대한 규제로 나누어 생각할 수 있는데 사용자에 대한 규제는 실질적일 수 없으므로 제외된다. 디지털통화 규제를 선도하고 있는 미국의 규제는 주로 거래소에 집중되어 있다. 반면 유럽은 거래소와 지갑서비스 제공 사업자 양자에게 분산되어 있다.

(1) 미국

비트코인 등의 디지털통화에 대한 규제는 미국이 선도하고 있는 중이다. 미국에서는 재무성소속 핀센(FinCEN; Financial Crimes Enforcement Network)과 뉴욕 주가 거래소를 위한 라이선스인 '비트라이선스'를 세계 최초로 제정하면서 중심역할을 하고 있고 나머지 기관들과 주정부는 핀센과 뉴욕 주의 규제에 준해서 각기 법규제를 입법하거나 검토하는 중이다.

(가) 미국 핀센(FinCen)의 규제 안내 해설서

2013년 3월 핀센은 가상통화를 발행, 취득, 분배, 교환, 수금, 송금하는 사람들에 대한 은행비밀법 실행 규제적용 여부를 분명히 하기 위해 안내 해설서를 발행하였다. 디지털 가상통화의 사용자는 규제받지 않으나 거래자(exchangers)와 관리자(administrator)는 자금서비스사업자로서 제재대상이다. 따라서 이들은 법에 정한 대로 정부에 등록할 의무가 있고 그에 맞는 규제의 준수가 요구된다는 것이 디지털통화 사업자에 대한 미국정부의 정리된 입장이다.[56][57] 이에 의하면 디지털통화거래소는 화폐서비스사업자(MSB; Money Service Business)로 등록하고 고객확인(Know Your Customers, KYC)규정을 준수하고 자금세탁방지 프로그램을 설치하고 의심거래행위보고(Suspicious Activity Report)를 권고하였다.

(나) 미국 상원 청문회

2013년 미국상원은 세계 최초로 비트코인에 대한 청문회를 개최하였다. 청문회에 나온 FinCEN 대표는 비트코인의 장점에 대해서 인정하면서도 상당한 정도의 위험성이 있다고 지적하였고 연방정부 대변인은 현재 규제가 적당하다고 증언했다.

(다) 미국 국세청

2014년 미 국세청은 비트코인과 기타 디지털통화에 대해 세금보고 주의사항을 발표했다. 이 발표에 따르면 비트코인 등 디지털통화는 재산(property)이지 화폐가 아니다. 따라서 재산세부과 대상이라는 미 세무국의 공개적인 입장을 밝혔다.

---

56) FINCEN. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. Aug. 2015.

57) Buterin, Vitalik. FINCEN: Bitcoin Users Not Regulated, Exchanges Are. Bitcoin Magazine. http://bit.ly/2dxxL9M. 2016.10.17. 접속.

(라) 미국 선물거래위원회

2015년에 미국 선물거래위원회(Commodity Futures Trade Commission)는 코인플립이라는 스타트업이 제공하기 시작한 비트코인관련 옵션 상품에 대해 금지 조치를 내렸다. 그 이유는 비트코인이 화폐가 아니고 규제가 필요한 상품(Commodity)인데, 교환가치가 있는 상품으로서 비트코인 옵션을 등록하지 않았다는 것이다. 이는 미국 정부 당국의 디지털화폐에 대한 시각을 확실하게 해주는 것으로 이를 계기로 선물거래위원회는 비트코인 관련 모든 파생상품에 대한 감독을 강화하기 시작했다.

(마) 미국 증권거래위원회

2015년에는 증권거래위원회가 디지털통화 채굴과 관련 있는 폰지 사기단을 증권거래법 위반으로 제소하는 사건이 있었다. 그 내용은 다음과 같다.

비트코인의 가격이 상승함에 따라 이를 채굴하려는 경쟁이 점점 치열해져서 강력한 컴퓨팅 파워가 없으면 채굴에 성공하는 것은 매우 어렵다. 성공적인 채굴자는 특별히 제작한 ASIC 칩을 장착한 컴퓨터가 수백 대가 연결된 채굴장(이를 농장이라고 부른다)을 축조했다. 이렇듯 채굴이 어려우니 자기들이 농장을 만들고 농장의 지분을 팔 테니 지분인 '해쉬렛(Hashlet)'을 구입하면 채굴된 코인을 지분에 따라 분양하겠다는 사기꾼들이 생겨났다. 이들은 '해쉬렛'을 2천만 달러 어치를 발행했다. 하지만 채굴 농장 같은 것은 존재하지 않았다. 이에 대해 미국 증권거래위원회는 비트코인 채굴 회사인 것처럼 조작하고 폰지사기 형태로 판매한 사기판매 회사와 그 대표를 증권법 위반으로 기소했다. 증권거래위원회는 모든 채굴 계약이 증권법의 대상은 아니지만 특별히 '해쉬렛'은 증권법의 규제대상이 된다고 해석했고 따라서 증권거래위원회의 규제에 저촉되는 사기행위라고 보았다.[58][59]

(바) 뉴욕 주

비트코인 등 디지털통화와 관련된 범죄가 반복되면서 2015년 뉴욕 주는 디

58) BBC. Bitcoin scam charges made against companies in US. http://bbc.in/1YJeT7p. 2016.10.17. 접속.
59) UNITED STATES DISTRICT COURT DISTRICT OF CONNECTICUT. SECURITIES AND EXCHANGE COMMISSION vs. HOMERO JOSHUA GARZA. http://bit.ly/2epGVTq. 2016.10.17. 접속.

지털통화 거래 서비스에 대해 라이선스(소위 비트라이선스; Bitlicense)를 발급하기 시작했다. 비트라이선스 사업자는 자금세탁방지제도와 테러자금조달금지제도를 준수하기 위해 고객확인(Know Your Customers: KYC) 의무를 부과받고 있고 소비자 거래 내역을 최소 7년간 보관할 의무가 있다. 또한 하루 1만 달러를 초과 거래한 고객 명단을 24시간 내 규제 당국에 보고할 의무가 있다. 게다가 모든 직원은 지문을 뉴욕 정부에 제출해야한다. 이렇듯 엄격한 비트라이선스는 작은 사업자들에게는 상당한 재정적 행정적 부담을 준다. 따라서 다수의 서비스 사업자가 뉴욕에서의 서비스를 포기하는 현상이 나타났다.[60] 비트라이선스는 뉴욕 주에 거주하는 소비자나 사업자들 상대로 서비스를 하는 모든 사업자에 적용된다는 점이 뉴욕 주의 비트라이선스를 강력하게 한다. 즉, 뉴욕 주에서 발행한 비트라이선스가 없다면 뉴욕 주에 주거하는 고객에게 서비스를 제공하지 못한다.

뉴욕 주는 디지털거래소가 비트라이선스에 의한 규제가 아닌 한정목적수탁회사(Limited purpose trust company)로서 은행법에 의해 규제 받는 방법도 제공하는데 이런 종류의 회사는 수신과 여신 서비스는 제공할 수 없고 여타 사업도 극도로 제한된다. 예컨대 비트라이선스를 받은 사업자는 단순하게 고객의 비트코인을 관리할 수가 있지만 한정목적수탁회사는 은행법에 따른 고객에 대한 신탁업무수행자로서만 업무수행을 제한받는다. 2015년 5월 뉴욕소재 itBit는 최초로 한정목적수탁회사로 등록한 비트코인 거래소가 되었다.[61] itBit 관계자에 의하면 한정목적수탁회사로 등록하는 절차가 비트라이선스나 머니 송금 라이선스를 받는 것보다 훨씬 더 까다로워서 이 종류의 회사는 비트라이선스를 받는데서 면제되었다고 한다.[62]

당초 뉴욕 주의 비트라이선스를 시작점으로 미국의 타 주들도 비슷한 법을 제정하리라고 전망되고 있으나 소규모 비트코인 사업자들의 저항에 의해 지연되고 있다. 예컨대 캘리포니아는 가장 먼저 뉴욕의 선례를 따를 것으로 전망되었으나 2017년에 다시 논의하기로 하며 연기되었다. 현재 법안을 만들고 있거나 상정한 주는 캘리포니아, 코넷티컷, 펜실베니아, 뉴햄프셔, 노스 캐롤라이나. 뉴저지 등으로 알려져 있다.

60) Parker, Luke. Mass Exodus of Bitcoin Exchanges from New York State Triggered by BitLicense Deadline. http://bit.ly/1HEt4PG. 2016.10.17. 접속.
61) Higgins, Stan. ItBit Nets $25 Million, Launches NYDFS-Approved Bitcoin Exchange. CoinDesk. http://bit.ly/1PsclE0. 2016.10.17. 접속.
62) Metz, Cade. NY Backs Bitcoin Exchange. But It May Not Fly in California. Wired. http://bit.ly/2dpIq3m. 2016.10.17. 접속.

(2) EU 및 기타 국가

(가) EU

EU는 비트코인 등의 디지털통화에 대해 별도의 규제를 하고 있지 않고 있으나 2012년 10월 유럽중앙은행(European Central Bank; ECB)는 디지털(가상)통화인 비트코인과 세컨드라이프의 린든달러에 대해 분석하고 가상통화가 중앙은행의 업무에 주는 영향에 대해 조사했다. 이 조사 보고서는 고객에게 금융혁신 제공을 통해 추가적인 결제수단을 주는 긍정적인 면이 있지만 사용자들에게 상당한 위험이 있다고 결론지었다.[63]

2013년 12월 은행감독청은 비트코인과 같은 디지털가상통화를 사거나 보유하거나 거래하는 것은 심각한 리스크가 있고 법적인 규제를 통하여 소비자가 보호되지 않고 돈을 잃을 위험이 있음을 경고했다. 추가적으로 통화가치가 안정적으로 남아있을 지에 대한 보장도 없어서 감독청이 규제와 감독이 필요한지 평가하기까지 경고를 발행한다고 하였다. 익명성으로 인하여 자금세탁 등의 범죄에 사용될 수 있으므로 법집행시 갖고 있는 자금이 묶일 수도 있고 세금의 의무가 발생할 수 있으므로 이런 점을 충분히 이해하고 잃으면 안되는 "진짜" 머니는 사용하지 말도록 경고하였다.[64]

2015년 EU의 유럽사법재판소는 "비트코인을 위해 전통적 통화(즉, 법정통화)와 교환하는 것은 부가가치세(Value Added Tax; VAT) 면제대상"이라고 판결했다. 또한, "EU에 속한 국가들은 법정통화처럼 사용되는 통화, 은행채권, 코인 등에 대해서 일어나는 거래에 대해 세금을 면제해야한다"고 판결했다. 이는 미국에서 화폐가 아닌 상품으로 해석하는 것과는 달리 적어도 EU에서는 디지털통화가 상품이 아니고 화폐라는 점을 시사하고 있다.[65] '

2016년 7월 유럽위원회(EC)는 디지털(가상)통화가 쉽게 거래되고 누가 거래하는지 알 수 없기 때문에 문제가 생기고 있다고 간주하고 디지털통화거래소와 지갑관리(Custodial Wallet) 서비스 제공자에게 자금세탁방지법 규제를

63) Eurosystem. VIRTUAL CURRENCY SCHEMES. European Central Bank. ISBN: 978-92-899-0862-7. 2012.10.
64) EBA. EBA warns consumers on virtual currencies. http://bit.ly/2evJnsV. 2016.10.17. 접속.
65) Court of Justice of the European Union. Judgment in Case C-264/14. PRESS RELEASE No 128/15.

확대 적용하는 지침서 초안을 제출했다. 2017년부터 적용될 지침서 초안은 EU의 모든 디지털통화 거래소들은 자금세탁방지법과 고객확인(Know Your Customers, KYC)규정을 준수하도록 되어있다. 이는 거래소와 지갑관리서비스 제공사에게 지속적으로 거래를 관찰하게하고 이상한 움직임에 대한 보고 규정으로 체크포인트를 만들겠다는 EU의 계획이다.[66]

EU는 개인의 프라이빗키와 이를 단순 보관하는 서비스는 대상이 아니지만 월렛 관리서비스 제공자들은 법적 규제 대상이다. 이는 당연히 월렛 제공서비스제공자 중 고객의 프라이빗키를 가지고 전적인 콘트롤을 할 수 있는 서클(Circle)이나 자포(Xapo) 등 월렛사업자들을 포함한다. 또한 그린어드레스(GreenAddress)나 블록트레일(Blocktrail)과 같이 다중서명 키 중에 하나만 갖고 있는 서비스는 고객을 대신하여 지출하는 것이 불가능하다고 하더라도 법의 규제 대상이 된다. 거래소를 포함하여 이들 규제 대상 사업자는 아무리 사소한 액수라고 하더라도 자금세탁방지법과 고객확인규정을 준수해야 하며 이는 논의나 협상의 대상이 될 수 없다.

익명성과 관련하여 EC는 디지털통화의 범죄사용을 방지하기 위하여 사용자와 비트코인주소가 연결이 될 수 있어야 한다고 규정했다. 이에 대해 EU의 초안은 다음과 같이 기술하고 있다.[67]

> "가상화폐 환경은 대부분 익명으로 남아있으므로 가상화폐 플랫폼과 지갑관리(서비스) 제공자는 가상화폐거래에서 익명성을 (장점 등의) 이슈로서 언급하면 안 된다. 왜냐하면 사용자는 거래소 플랫폼이나 지갑관리(서비스)를 사용하지 않고도 거래를 할 수 있기 때문이다. 익명성과 관계된 위험들에 맞서 싸우기 위해서는 각국의 금융정보기관(Financial Intelligent Unit)은 가상통화의 주소와 그 소유자의 아이디를 결부할 수 있어야 한다. 게다가 유저들이 당국자들에게 자발적으로 자기선언(Self declaration)할 수 있는 가능성을 열어놓고 추후 평가할 가능성을 열어야 한다."

즉, 익명성이 보장되는 분산원장 아이디를 쓸 때 유저가 원한다면 자신의 실제 신분을 자발적으로 공개하도록 한다. 자기선언(Self-declaration)을 하는

66) Wirdum, Aaron. E.U. Representatives Clarify the Proposed Anti-Money Laundering Directive. Bitcoin Magazine. 2016.10.17. 접속.
67) 전게서 11.

것은 강제규정이 아니므로 자발적으로 할 수 있도록 열어놓고 추후 장점을 평가하겠다는 뜻이다. 정확하게는 2019년으로 예정된 차기 보고서에 권고안으로 선택할 가능성을 열어놓겠다는 장기적 포석이다. 가상통화를 사용할 때 자신의 실제 신분을 연결해 놓고 신용점수가 누적될 수 있게 한다면 익명성은 신용도를 저해하는 것으로도 생각될 수 있다. 그렇다면 언제고 자발적으로 자기선언을 하는 것이 유행처럼 사용될 수도 있지도 않을까 하는 바람이 여기에 숨겨져 있다.

이 초안은 현재 EU에서 논의 중으로 네덜란드의 안은 지갑서비스 제공자들에 대한 고객확인(KYC)과 자금세탁방지(AML)규정을 삭제하는 것을 제안하고 있다.

(나) 독일

독일은 2013년 8월 세계최초로 비트코인 등의 디지털화폐를 가치단위를 지닌 "개인화폐(Private Money)"로 은행법의 금융상품에 대한 가이드라인에서 금융상품(Financial Instrument)으로 규정했다. 이에 따라 비트코인 사업체는 금융서비스를 제공하는 회사로 규정되어 엄격한 운영 기준을 적용하도록 되었다. 예컨대 비트코인사업체는 최소 73만유로(악 9억 원)의 자본금이 있어야 한다.[68]

2013년부터 비트코인이 화폐의 지위를 얻으면서 시세차익을 자본이득(Capital gain)으로 25%의 세금을 내게 되었는데 독일 정부가 이에 대해 면세하는 조치를 1년간 단행했다. 예컨대, 2012년에 100비트코인은 550유로가 시세였는데 1년 후에 7,600유로로 뛰어올라서 약 7,000불의 차익이 생겼다면 세금은 1,750불이다. 이를 감면한 것이다. 또한 독일 정부는 채굴로 생기는 세금은 가치를 창조하는 것이므로 보통의 소득세의 대상에 속한다고 해석했다.[69]

2013년 8월, 독일 소재 비트코인 거래소인 Bitcoint.de는 피도르은행과 파트

68) Spaven, Emily. Germany officially recognises bitcoin as "private money". CoinDesk. http://bit.ly/1aYSGb0 2016.10.17. 접속.
69) Gilson, David. German government relieves capital gains tax on bitcoin positions. CoinDesk. http://bit.ly/2eIa9lH. 2016.10.17. 접속.

너십을 체결하고 고객들이 은행계좌를 이용해 실시간으로 비트코인 매매를 할 수 있게 했다.[70]

(다) 기타 국가

덴마크는 2014년 디지털통화 거래에 대해서 세금면제(Tax-free) 결정을 내렸다. 세무국의 결정은 디지털통화가 물리적으로 존재하지 않고 실제 통화로 생각될 수 없다는 이유다. 비트코인의 거래는 "순전히 개인적(Purely private)인 것의 결과"로 거래가 파생된 것으로 해석한다. 비트코인에 대한 거래를 주업무로 하는 업체는 이 해석의 대상에서 제외되고 수입과 지출에 대해서 보고해야 하는 의무는 진다는 것이 덴마크 당국의 해석이다.[71]

영국 등 대부분의 EU국가는 아직까지는 별다른 규제가 없다. 영국은 규제를 도입하기 보다 새로운 프로그램을 도입했다. 영국은 Project Innovate라는 스타트업과 창업자가 쉽고 빠르게 적절한 고객 보호에 관한 규제를 준수하면서 시장에 진입할 수 있도록 만들어주는 프로그램을 도입했다. 이는 혁신적인 스타트업 기업이 초기에 규제를 쉽게 따라갈 수 있도록 만들어주는 프로그램이다.

일본은 비트코인 등 디지털통화를 일반상품(Commodity)으로 간주해서 이를 교환할 때 8퍼센트의 소비세와 다른 세금을 함께 부과해 왔다. 마운트곡스 디지털통화거래소의 파산이후 12만명 이상 피해자가 생긴 것에 충격을 받아 일본 금융감독청은 디지털통화 관련 사업자들에게 현장 검증을 수행하고 있고 사업자들에 고객파악의무를 요구하고 있다. 현재 일본은 디지털통화가 거래 시 재화로 간주되는 일반상품임에도 불구하고 면세를 검토하고 있는 것으로 알려졌다.[72]

---

70) Spaven, Emily. Marketplace Bitcoin.de registers with Germany's financial regulator BaFin. CoinDesk. http://bit.ly/2enDrT8. 2016.10.17. 접속.
71) Sharkey, Tom. Denmark Declares Bitcoin Trades are Tax-Free. CoinDesk. http://bit.ly/1gWSOcw. 2016.10.17. 접속.
72) The Mainichi. Japan looks to end sales tax on bitcoin in spring. Minichi Japan. http://bit.ly/2eapUT2. 2016.10.17. 접속.

나. 디지털통화 발행에 따른 리스크 분석

(1) 전통적 결제시스템에서 일어나는 리스크의 변화

전통적 결제시스템에서 일어나는 리스크의 유형은 신용 리스크, 유동성 리스크, 운영 리스크, 법률 리스크, 시스템적 리스크 등이 있다. 이러한 전통적 시스템에서의 리스크가 분산원장을 도입하여 디지털통화를 발행하고 금융네트워크 참가기관의 결제가 실시간으로 이루어질 수 있다는 전제위에 어떻게 변화하는지 살펴보자. 금융시스템에 분산원장이 도입될 경우 다음과 같은 최소한의 기능이 포함될 것을 가정한다.

- 금융시스템의 안정적 운영을 위해 프라이빗 분산원장 사용

  * 분산원장을 도입한 스마트계약 기능(즉, 이더리움 분산원장과 유사하나 튜링완전성은 다소 제한된 형태. 튜링완전성에 대한 위험은 아래 '분산원장 기술의 금융서비스 적용에 따른 리스크 분석' 섹션에서 다룰 것임.)

○ 신용 리스크 : 금융시장인프라 참가기관이 파산 등으로 결제시점에 지급채무를 완전히 이행하지 못할 경우에 발생하는 손실위험이다. 이는 결제시차 등으로 인해 생기는 리스크로 분산원장이 도입될 경우 실시간 결제가 되는 효과가 있으므로 전통적인 형태의 신용 리스크는 대부분 해소될 것으로 예측된다. 동시에 분산원장 도입 시 투명성에 의해 금융거래 기관에 대한 신용분석이 실시간으로 행해지므로 리스크 노출이 최소화된다.

○ 유동성 리스크 : 금융시장인프라 참가기관이 단기적인 자금부족으로 정해진 결제시점에 결제의무를 이행하지 못하는 경우 발생하는 리스크이다. 즉, 금융건전성 자체에는 별문제가 없지만 해당 금융기관이 예정된 시간에 자금을 지급하지 못하고 대체자금도 조달하기 어려워 일시적으로 결제를 이행하지 못하는 경우 발생한다. 이 경우 역시 리스크가 최소화된다.

○ 운영 리스크 : 정보시스템이나 내부프로세스의 결함, 운영인력의 실수 또는 외부사건 등으로 인해 금융시장 인프라가 제공하는 서비스의 축소, 질적 저하 혹은 장애가 발생할 위험이 있다. 분산원장 도입 시 운영인력의 실수나 외부의 사건 혹은 전산의 결함으로 발생하는 오류로부터 회복력이 뛰어나기 때문에 서비스의 축소나 질적 저하가 발생할 우려가 대폭 줄어든다.

○ 법률 리스크 : 법률이나 제도가 제대로 정비되어 있지 않거나 법적 불확실성으로 인하여 결제가 완결되지 못하는 경우 발생하는 리스크다. 지급 결제와 관련하여 국내외, 법률, 운영기관의 규칙 또는 참가기관 간 협약 등이 미비한 경우나 새로운 법률이나 제도의 도입에 따른 예상치 못한 책임이나 상황에 대한 대응이 미흡한 경우 발생할 수 있다. 분산원장 도입 시 자산거래나 소유권확인이 실시간 가능할 뿐만 아니라 스마트계약이 가능할 수 있도록 튜링완전성을 갖도록 설계된 시스템을 도입할 경우 법률적인 리스크가 최소화 될 수 있다.

○ 시스템적 리스크 : 금융시장인프라에서 특정 참가기관의 결제불이행이 다른 참가기관으로 확산되어 연쇄적인 결제불이행을 유발함으로써 금융시장 전체의 안정성에 악영향을 미치는 리스크이다. 다른 리스크와 마찬가지로 전통적인 형식의 시스템적 리스크는 분산원장의 제공하는 투명성에 의해 대폭 완화될 것이다.

다. 디지털통화 발행에 따른 규제와 방안

(1) 디지털통화 규제의 필요성

분산원장 기술을 사용한 디지털통화는 통상 전자화폐나 기타 유사 전자 결제 매체들이 갖는 위험과 유사한 형태의 범죄관련 위험에 직면하게 된다. 단지 디지털통화는 기존의 전자화폐보다 더욱 많이 범죄에 사용되는 현상을 보이고 있어서 일반 소비자가 투자처로 사용하기에는 여러 가지 문제가 있을 수 있다. 디지털통화가 범죄에 많이 이용되는 이유는 다음과 같은 네 가지 이유로 생각할 수 있다.

(가) 익명성 보장

디지털통화는 탈중앙화된 화폐이며 글로벌하게 사용될 수 있고 상당한 정도의 익명성이 보장되어 거래의 추적이 쉽지 않다. 예컨대, 2014년 세계 최대 비트코인 거래소중의 하나였던 실크로드는 마약과 자금세탁 등에 관여한 이유로 미국 FBI에 회사의 대표가 체포되었고 가석방 없이 종신형이라는 선고를 받고 복역 중이다.[73] 실크로드가 범죄에 이용된 가장 큰 이유는 익명성이 상당한 정도 보장되기 때문이다.

여기서 상당한 정도라 함은 분산장부는 익명성이 보장되는 대신 한 번 만들어진 거래기록은 영구성을 갖고 지워지지 않는다는 점 때문이다. 장부 거래에서 익명의 거래자를 찾아서 실존 인물과 연결하기는 쉽지 않지만 일단 하나라도 연결이 되면 모든 거래자가 고구마 줄기 뽑히듯이 따라 나오게 되어있다. 예컨대 FBI는 실크로드 서버를 특정하기 위해 6개월 동안 작업을 했다.[74][75] 서버를 특정할 수 있었던 우연히 발견한 서버의 환경설정 오류 때문인 것으로 알려져 있다.[76] 어쨌거나, 서버가 일단 특정되고 나면 범죄에 사용된 거래가 특정된다. 그와 함께 범죄와 연결된 모든 거래자와 거래내역이 밝혀지게 됨으로써 특정 거래와 연결된 범죄자들의 일망타진이 가능해진다.[77]

(나) 법적 지위 불확실

비트코인 등의 디지털통화는 국가 혹은 중앙정부의 개입 없이 P2P 환경에서 작동하도록 되어있고 이를 매개로하는 거래소 등은 금융사업자로 정의되어 있지 않은 경우 사업자를 규제할 법률이 마땅치 않다. 국제적으로 많은 국가들이 상이한 입장을 보이고 있는 가운데 대한민국 정부는 2013년 "화폐, 전자화폐, 금융상품으로 인정할 수 없다"고 결론을 내린 바 있다.[78] 즉 디지

---

73) Reuters. Two Bitcoin exchange operators charged in money laundering scheme. http://cbsn.ws/2eyhlAv. 2016.10.17. 접속.
74) Cubrilovic, Nik. Analyzing the FBI's Explanation of How They Located Silk Road. http://bit.ly/1w59fAz. 2018.10.17. 접속.
75) Graydon, Carter. How the FBI Likely Illegally Hacked Silk Road Servers to Find Alleged Pirate Ross Ulbricht. http://bit.ly/2dmK2uH. 1016.10.17. 접속.
76) Greenburg, Andy. FBI's Story of Finding Silk Road's Server Sounds a Lot Like Hacking. Wired, http://bit.ly/2eo4GMM. 1016.10.17. 접속.
77) Bohannon, John. Why Criminals can't hide behind Bitcoin. AAAS. 2016.3.9.

털통화는 발행기관이 모호하다는 점 등으로 현행 법령상 화폐 및 전자화폐는 물론 금융상품으로서의 요건도 충족하지 못한다.

디지털통화가 법적지위가 불확실하기 때문에 법외에 있고 적절한 규제가 없다는 것은 치명적이다. 이 말은 누구나 비트코인 등 디지털 사업을 시작할 수 있고 이에 따라 디지털통화 거래소는 쉽게 탈법적 범죄에 노출될 가능성이 있다. 게다가 법적인 지위가 불분명하여 범죄에 노출되더라도 소비자 보호 등을 위해 적용할 규제법이 마땅치 않다.

예컨대, 2014년 2월 일본 소재 비트코인 거래소 마운트곡스는 시가 약 4억 5천만 달러의 비트코인을 분실했다고 주장하며 법정에 파산신청을 했다. 2010년 설립된 마운트곡스는 2013년에는 세계 비트코인 거래의 70%를 장악할 정도로 성장해 있던 세계최대의 거래소였다. 후에 이 '분실'은 내부자의 소행으로 의심되었고 마운트곡스의 대표인 마크 카펠라스는 2015년 8월 거래소의 데이터 조작과 공금횡령 혐의로 체포되었다. 하지만 고작 10개월 복역한 후 보석되었다. 이렇게 적은 형량만을 받은 이유는 당시 대표인 마크 카펠라스 등 마운트곡스 관련자들은 입출금을 기록한 장부가 없었다고 주장하고 있기 때문이다. 기록된 장부가 없는 상태에서 일반 소비자 고객의 피해액을 산출하거나 횡령액을 산출하는 것은 거의 불가능하다. 따라서 대부분의 범죄는 카펠라스 등이 저지른 내부자의 범죄로 보이지만 증거가 불충분하다. 국가의 규제 내에 있는 금융회사라면 도저히 일어날 수 없는 일이 일어났지만 사실상 법적인 지위도 없는 비금융자산의 거래로 간주된다면 장부기록의 의무도 지울 수 없고 장부가 없으니 증거도 없다. 이미 앞에서 설명한 대로 일본은 마운트곡스 디지털통화거래소의 파산이후 12만 명이상 피해자가 생긴 것에 충격을 받아 일본 금융감독국은 디지털통화 관련 사업자들에게 현장 검증을 수행하고 있고 사업자들에 고객파악의무를 요구하고 있다. 하지만 마운트곡스는 범죄행위를 제외하면 기술인프라도 제대로 없고 기업으로서의 기본적인 회계 원칙조차도 지켜지지 않던 형편없는 기업이었다. 웹사이트를 만들면서 운행사이트에 대한 시험운전 조차도 없었던 것으로 알려지고 있다.

유사하지만 또 다른 파생되는 문제 중의 하나는 장물의 문제다. 비트코인의 경우 2009년부터 2015년까지 해킹당한 거래소가 3분의 1이고 그 중 반이 손

78) 신현규. "비트코인 화폐 아니다"…정부, 모니터링 강화키로. 매일경제. http://bit.ly/2egJVqz. 2016.10.17. 접속.

해를 견디지 못하고 사업을 폐쇄했다. 이 말은 현재 판매되고 있는 비트코인의 많은 수가 장물일 확률이 높다는 뜻이다. 비트코인에 투자하는 소비자는 자신도 알지 못하는 사이에 장물취득을 할 수도 있다는 점은 비트코인 시장에 치명적인 장해가 될 수 있다.

(다) 기술적 경험적 미숙에서 오는 오류로부터 취약

디지털통화 산업은 지금까지 기술적인 노하우를 가진 해커 커뮤니티에 의해서 주도되어 왔다. 혁신적인 성향을 가진 이들 해커들은 안전과 보안이라는 보수적인 금융시스템의 본질적 성격을 이해하지 못하는 경향이 있다. 일반적인 금융기관은 오랜 기간 검증을 거치지 않은 시스템은 실무에 적용하지 않는다. 반면 디지털통화를 주도하는 혁신 시스템은 단기간의 검증만을 거치기 때문에 내부의 프로그램 오류로 인하여 크게 실패하게 될 수가 있다. 그 뿐만이 아니라 해커들의 공격대상이 되고 약점이 수시로 노출된다.

2016년 8월 약 7천만 달러의 비트코인을 도난당하여 마운트곡스 이후 최대의 도난사건으로 기록된 비트피넥스도 역시 유사하다. 비트피넥스는 2012년 서비스를 시작하여 해킹이 일어나기 전 가장 큰 비트코인 거래소였지만 시스템 오류가 자주 발생하여 "Bugfinex"라는 이름으로 불릴 정도로 불안정했다고 한다.[79] 이와 같이 디지털통화 거래소는 내부 오류와 해킹에 의해 지속적으로 문제를 야기해왔다. 2009년부터 2015년까지 비트코인 거래소의 3분의 1이 해킹에 피해를 봤고 그 중 반은 손해를 만회하지 못하고 폐업을 한 바 있다는 점은 결코 우연이 아니다. 많은 젊은 창업자들은 오랜 기간 완벽하게 검증을 거친 보안체계의 중요성을 이해하지 못한 채 창업을 하기 쉽다.

튜링완전성을 제공하는 이더리움은 비트코인이 제공하지 못하는 영역까지 활용될 수 있도록 강력한 기능을 제공하기 위해 튜링-완전(Turing-completeness), 가치 인지능력(value-awareness), 블록체인 인지능력(blockchain-awareness), 상태(state)개념 등을 포함하여 설계되었다. 즉 적용성이 뛰어나게 하도록 디자인된 것이다. 그러나 적용성이 뛰어나다는 것은 곧 보안에 취약하다는 말과 같다. 즉, 보안은 공격 가능한 경우의 수를 제한하여 경로를 차단할 수

79) Higgins, Stan. Bitfinex Examined: Inside the Troubled Bitcoin Exchange's History. CoinDesk. http://bit.ly/2aJMeNj. 2016.10.17. 접속

있어야 하는데 경우의 수가 많아지면 해킹으로부터 취약할 수 밖에 없다. 실제로 이로 인한 해킹사고도 계속되고 있다.

이미 1장에서 설명했듯이 이더리움 블록체인 상에서 구현된 탈중앙어플리케이션(DApp)을 기반으로 만들어진 TheDAO는 전세계에서 약 1억 2천만 달러가량 투자를 끌어 모으며 사상 최대의 크라우드 펀딩으로 화제를 모았다. 그러나 TheDAO가 제공했던 기능중의 하나인 리펀드 기능에 치명적인 결함이 발견되면서 이를 이용한 해킹 공격에 당시 가치로 약 750억 원 가량을 도난당한 후 서비스가 중단되었다. TheDAO 케이스는 튜링완전성을 유지하면서 동시에 보안성을 유지할 수 있는지에 대한 근본적인 문제에 대한 질문을 던지고 있는 중이다.[80]

이더리움의 경우 설계와 개발상에는 오류가 발견되지 않았으나 실제 운영상에서 다소의 결함이 발견되고 있다. 예컨대 2016년 9월부터 10월 중순까지 이더리움은 약 한 달간 해커그룹의 DoS(서비스거부; Denial of Service)공격에 의해서 그 처리 속도가 60초 이상으로 늦어지는 현상을 겪고 있다. 공격자는 처리수수료(일명 '가스값' 혹은 '연료값')를 낮게 부과하는 블록 서버들에게 명령어를 5만 번 반복되도록 요청하는 식으로 공격을 했다. 이로 인해 해당 블록들의 검증이 이뤄지지 않으면서 전체 처리 속도가 늦어지게 되었다. 다행하게도 과부하로 인한 합의 실패나 과부하 등 다른 오류로 전이되지는 않았으나 설계상의 완벽함이나 프로그램 개발상의 오류가 아닌 실제 운영에서 일어난 일이라는 점에서 튜링완전성에 대한 적용성과 확장성에 대한 믿음이 의구심으로 변하고 있는 중이다. 창의적이고 탁월한 아이디어가 아쉽게도 단순한 경험부족에서 비롯된 실수와 해킹에 의해서 빛을 잃어버린 것이다.

문제는 이러한 해킹이 일상화되면서 일반 소비자 고객들의 피해가 막심하나 그 피해가 구제된 사례는 거의 찾아보기 힘들다. 일반 금융권에서는 단 한 번의 사고라도 생기지 않도록 이중삼중의 소비자 보호책이 제도화되어 있다는 점이 크게 다른 점이다.

80) 피넥터. "블록체인 기술의 발전과정과 이해," 2016/8. 피넥터 보고서.

(라) 범죄 전력자들에 대한 신분 조사 없음

세계 어느 국가건 은행 등 금융기관에서 종사하는 종업원은 신분확인을 하게 되어있다. 금융기관 내부에서 사고가 나는 것을 미연에 방지하기 위해서다. 반면 디지털통화 거래소는 종업원에 대한 범죄 신분확인뿐만이 아니고 사업체 소유주나 대표에 대한 범죄 신분확인 조차 되고 있지 않다는 점은 치명적이다. 예컨대, 마크 카펠레스는 2010년 프랑스 정부의 서버를 "해적질한"죄로 징역살이를 1년이나 했던 자로 2011년 마운트곡스의 대표가 되었다. 그가 훗날 마운트곡스와 관련하여 횡령혐의로 유죄판결을 받은 것은 결코 우연이라고 할 수 없다.

(마) 결론 : 법적지위 및 규제기준 필요

이렇듯 디지털통화에는 기존의 금융서비스 및 금융기관이 경험하던 리스크는 상당부분 줄어드는 대신 새로운 종류의 리스크가 존재하는 까닭에 이에 대한 대응책으로서 규제가 필요하다. IMF는 최근 보고서에서 금융조치태스크포스(FATF)가 국가 연합 차원에서 금융무결성, 탈세대책, 소비자 보호 등에 대한 규정과 해석이 현재 불분명하므로 이를 명확히 할 필요가 있다고 보았다.[81]

- 금융 무결성(Financial Integrity) : 디지털통화의 익명 거래 기능은 자금세탁이나 테러자금의 유입을 초래한다. 특히 국경의 개념이 모호해지는 사이버세상에서는 다국가 간 거래와 사이버 범죄의 활동이 문제가 된다. 디지털통화가 법정통화로 변환되는 거래소 규제 및 지속적인 모니터링이 필요하다. 가상통화를 이용한 서비스 사용자들을 상시 모니터링하고 지갑 서비스 제공자에게 직접적 규제, 즉각적인 불법 자산의 몰수 추진을 할 수 있어야 한다.

- 소비자 보호 : 규제의 불확실성과 투명성의 부족은 소비자 보호의 취약점을 만들고 있다. 이는 가상 통화 시스템의 장애로 인한 프로토콜 마비와 거래 플랫폼, 지갑 서비스 제공자, 지불결제 게이트웨이의 장애는 소비자

81) He, Dong, Karl Habermeier, Ross Leckow, and Vikram Haksar. "Virtual Currencies and Beyond: Initial Consideration," International Monetary Fund, 2016.

보호를 어렵게 한다. 또한 중앙화 된 거래소의 해킹과 온라인 폰지 등의 사기 문제, 거래를 되돌릴 수 없는 문제 등으로 국가적인 소비자 보호 입법 추진 및 수정적용이 필요하다.

- 과세 : 가상 통화들은 탈세 수단으로 이용될 가능성이 높다. 익명으로 국가를 넘으며 거래가 이루어지기 때문에 효과적인 과세 집행의 수단 개발이 필요하다. 일부 국가는 이미 과세와 관련한 상당한 진보적 조치가 만들어져 있으나 전 세계적인 국제적 일관성을 가지기 위해 치밀한 분석과 토론이 필요하다.

- 거래소의 통제 및 자본 흐름 관리 : 디지털 통화는 자본 통제의 회피에 사용되는 것이 대부분이며 익명성을 가지고 인터넷을 통해 빠른 속도에 비해 낮은 거래 비용으로 국가 간 거래가 이루어져 전통적인 결제시스템의 비용과 규제가 높은 정부 하에서 세금 회피자나 범죄 조직들에게 매우 매력적이다. 이런 점에서 디지털통화 거래소의 통제와 자본 흐름의 지속적인 모니터링이 중요하다.

- 금융 안정성 : 디지털통화들은 아직은 작은 규모이며 또 금융 시스템과의 제한된 연결로 인하여 아직은 시스템 수준의 금융안정성을 위협하지는 않는다. 그러나 거래소의 파산문제, 보안 침해의 취약성, 신용위험, 유동성 위험이 존재하므로 분산원장기술의 확장에 맞추어 증권, 주식 거래와 같은 모니터링의 강화와 감독이 필요하며 국제적으로 합의된 규제 원칙 및 국가기관 사이의 협력이 강조된다.

- 통화정책 : 현재는 디지털통화가 통화정책에 대해 어떤 종류의 영향을 끼칠 정도로 중요한 의미는 없지만 널리 사용되게 되면 몇 가지의 우려가 예상된다. 먼저 경직된 공급규칙 때문에 구조적인 디플레이션의 위험이 존재하므로 최종대부자 역할(lender of last resort : LOLR)의 어려움이 예측된다. 즉 경제성장과 함께 통화의 공급을 지속적으로 유지할 수 있도록 설계 되어야 하는데 현재 유통되고 있는 디지털통화는 글로벌 금융위기와 같은 공황 상태에서는 중앙은행의 LOLR를 대처할 수 없다. 통화정책 신뢰가 낮은 국가에서는 가상통화는 법정통화를 대처할 수 있는 매력적인 옵션이 된다는 점은 중요하다.

이와 유사한 맥락에서 금융조치태스크포스(FATF)는 모든 디지털통화는 FATF가 규정한 표준에 맞도록 AML/CFT 프레임워크가 적용되어야 한다는 가이드라인을 출간한 적이 있다.[82][83]

어쨌거나 디지털통화는 잠재적인 혜택이 있으나 동시에 금융 무결성, 소비자 보호 등에서 다소의 문제를 야기할 것이며 탈세 목적의 사용자가 모일 뿐만이 아니고 통화 관리에도 문제가 될 수 있다. 이런 저런 문제에도 불구하고 결국 광범위하게 사용될 것이라는 점은 자명하다. 따라서 혁신의 속도와 맞추어 규제도 세심하고 유연한 대응이 필요하며 국제기구 등을 통한 국제적 커뮤니티 협력도 강화되어야 하며 장기적 관점에서 국제 표준 및 규제에 가장 적절한 지침을 제공하는 모범사례를 개발하고 다른 분야에도 적용시키는 것이 필요하다고 보았다. 현재 가장 중요한 포인트는 지속적인 모니터링과 분석을 통해 기술 혁신에 따른 위험을 지속적으로 분석하고 적절할 때에 적당한 규제로 응답하는 것이다.

(2) 디지털통화 규제 방안

디지털통화에 대한 규제는 소비자보호, 상대 참여자에 대한 건전성과 조직의 규칙, 지불 방법으로서 운영규칙(예컨대, EU내에서 결제완결성) 등 세가지 분야를 커버해야 한다. 디지털통화의 본질을 생각할 때, 온라인과 그에 따른 국가적인 통치구역의 한계가 불분명하다는 점에서 완벽하게 효과적이기 위해서는 글로벌 수준의 공조가 대단히 중요하다.

BIS는 최근 보고서에서 CPMI(Committee on Payments and Market Infrastructure) 멤버들이 글로벌 수준의 공조가 없더라도 단일 국가 수준에서 선택할 수 있는 다섯 가지 조치를 디지털통화에 대한 규제 방법으로 제시하고 있다.[84]

- 홍보 및 도덕적 권고 : 디지털통화에 직접적으로 개입하는 것보다는 당국은 사용자들과 투자자들에게 적절한 수준의 위험성을 환기시킴으로서 시장에 영향을 줄 수 있는 도덕적 권고를 사용할 수 있다.

82) FATF. Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014/6. FATF Report.
83) FATF. Virtual Currencies: Guidance for a Risk-based Approach. 2015/6. FATF.
84) BIS. Digital Currencies. BIS Committee on Payments and Market Structure Report. 2015/11.

- 사업체에 대한 규제: 제도적 접근 방법으로서 당국은 구체적인 형태의 업체에 대해(예컨대, 디지털화폐와 전통적인 지급수단이나 실제 화폐를 바꾸는 사업체) 제한적인 규제를 지정할 수 있다. 업체는 중개거래업을 포함하여 사용자들에게 디지털화폐를 저장하거나 거래할 수 있게 해주는 디지털 화폐 관련 서비스를 제공하는 교환소나 디지털 화폐를 받는 상점, 그리고 디지털 지갑 애플리케이션 서비스 제공자는 모두 다 대상이 될 수 있다.

- 이미 존재하는 제도의 해석: 어떤 당국자들은 이미 존재하는 규제 제도가 디지털 화폐와 중개 거래업자에게 적용이 되는지 평가할 수 있다. 예컨대 당국자는 조세법에서 디지털통화 제도가 세법에 어떻게 적용되는지 규정하는 등에 대한 것이다.

- 규제의 범위 확대: 법적인 규제 영역이 문제가 될 소지는 있다고 하더라도 당국자는 전통적인 결제방법과 중개사업자에게 적용되는 규제 범위를 확대하는 방법을 통해 디지털통화와 중개사업자들에게 적용하는 방안을 찾을 수 있다. 예컨대, 당국은 AML/CFT 요건을 디지털통화 거래와 거래상대방에게 적용하거나 소비자보호 관련 규정이 디지털통화에 똑같이 적용되도록 한다.

- 금지: 당국은 디지털통화의 사용을 그 법적 관할권 안에서 금지하는 것을 고려할 수 있다. 실제적으로 이는 디지털통화기반 금융활동과 디지털통화거래나 소매상들의 디지털화폐 사용을 금지하는 것을 의미할 수 있다. 이런 종류의 규제에는 일반적 프레임워크에 대해서 국가 당국자의 광범위한 분석이 선행되어야 할 것이다.

<그림 4-1> Digital Currencies에 대한 규제 분류

Broad classification of the main types of regulatory action — Table 1

Main options	Type of actions / Country examples
Information/moral suasion	• Public warnings • Investor/buyer information • Research papers *Most countries have issued these types of warnings, research or information notes.*
Specific stakeholder regulation	• Regulation of digital currency administrators (record-keeping, reporting, AML/TF). *Example: United States.* • Regulation of digital currency exchangers (record-keeping, reporting, prudential measures, AML/TF). *Examples: United States, France, Canada, Singapore, Sweden.* • Consumer protection measures (payment guarantee, redeemability etc).
Interpretation of existing regulations	• Application of regulation based on "interpretation" of how existing framework (eg tax law treatment) may be applied to digital currencies or digital currency intermediaries. *Example: United States.*
Overall regulation	• Dedicated regulation, covering all three aspects (consumer protection, prudential/organisational rules for stakeholders, and specific operating rules as payment systems).
Prohibition	• Ban (or amount cap) on retail Bitcoin transactions. • Ban on digital currency acceptance by retailers. • Ban on digital currency-based financial instruments. *Examples: China, Belgium.* • Ban on digital currency exchangers. • Ban on Bitcoin transactions between banks. *Examples: China, Mexico.*[11]

자료: BIS 보고서

2. 분산원장 기술 규제의 필요성과 방안

가. 분산원장 기술의 금융서비스 적용에 따른 리스크 분석

(1) 분산원장 기술에 의해 추가되는 리스크

분산원장기술은 전통적인 금융시스템의 리스크를 상당부분 완화시켜준다는 점을 이미 설명했지만 분산원장기술에 의해 새로이 추가되는 리스크 또한 간과할 수 없다. 이에 대해 논의하기 위해서는 튜링불완전성을 갖는 비트코인식 분산원장과 튜링완전성을 갖는 이더리움식 분산원장을 나눠서 생각할 필요가 있다.

튜링완전성을 갖는 분산원장은 풍부한 상상력을 가진 스마트 계약을 가능하게 하므로 과거와는 전혀 다른 새로운 형태의 사업모델과 새로운 산업의 탄생이 가능할 만큼 장점이 크다. 그러나 이미 지적한 대로 이더리움의 경우 튜링완전성이 있는 강력한 프로그래밍 언어를 설계했다는 것이 일방적으로 장점만이 있는 것은 아니다. 그에 따른 리스크도 함께 증가한다. 이런 점에서 튜링완전성이 포함된 분산원장 기술의 리스크에 대해서 따로 논의한다.

(가) 튜링불완전성 분산원장 기술에 의해 추가되는 리스크

분산원장 기술을 금융서비스에 적용할 때 발생할 수 있는 리스크는 전통적인 금융시스템에 존재하는 리스크와는 확연히 다르다. 분산원장 기술을 사용하면서 추가되는 리스크는 다음과 같다.

○ 보안 리스크: 분산원장이 구조적 해킹이 불가능하도록 설계되었고 아직까지 어떤 취약성도 노출된 적이 없는 안전한 구조를 가지고 있다. 그럼에도 불구하고 분산원장관련 서비스가 수없이 해킹을 당해왔다는 점은 주목할 만하다. 지금까지 해킹된 것은 분산원장 기술 자체가 해킹당한 것은 아니라는 점은 중요하다.

피넥터는 최근 보고서에서 분산원장 유관 서비스만 해킹을 당했고 사용자의 PC도 해킹당한 것이 아니라는 주장을 하였는데,[85] 그것은 사실과 다르다. 해커가 서비스 제공자와 소비자, 공급자를 가려가면서 해킹하는 것은 아니다. 개인의 지갑이 털리는 것은 상대적으로 작은 사건이기 때문에 뉴스거리가 안되는 것일 뿐 개인 지갑도 상당수가 쉽게 해킹당하는 중이다.[86] 이와 관련하여 FBI는 다음과 같은 사실을 보고하고 있다.[87]

- 2011년 6월 유저들의 컴퓨터의 비트코인 월렛을 터는 "Infostealer.Coinbit"라는 이름의 맬웨어를 발견했다. 이 맬웨어는 유저의 컴퓨터를 감염시킨 뒤 유저의 비트코인 지갑에서 폴란드

85) 피넥터. "블록체인 기술의 발전과정과 이해," 피넥터 보고서. 2016.8. 43쪽.
86) Thomas Fox-Bewster, "How Hackers Abused Tor To Rob Blockchain, Steal Bitcoin, Target Private Email And Get Away With It," 포브스 잡지. 2015/2/24. (2016/9/17일 액세스)
87) 전게서 14.

에 있는 서버로 전송할 수 있었다.

- 2011년 6월 한 비트코인 사용자는 암호화되지 않은 월렛에서 2만 5천개의 코인이 도적맞았다는 글을 게시했다. 당시 가격으로 50만 달러에 해당하는 금액이다.

- 이 외에도 FBI 보고서는 ZeuS 맬웨어를 이용하여 컴퓨터를 비트코인을 채굴하도록 한다든지 하는 등의 사례를 예시하고 있다.

사실 아래 표에서 보듯이 2009년부터 2015년 사이에 총 비트코인 거래소의 삼분의 일이 해킹을 당했고 그 중의 반은 문을 닫았다. 이렇게 많은 수의 거래소가 문을 닫을 정도로 해킹이 성행했다는 말은 법적으로 미묘한 문제를 야기할 수 있다. 비트코인이 많은 국가에서 법정통화의 지위를 가지지 않고 법적으로 가치 있는 재화로 간주되고 있는 현실을 감안할 때 현재 시장에서 거래되는 많은 수의 비트코인이 장물일 가능성이 높다는 것이다.

장물을 사고 팔 때 대부분의 국가에서는 네모닷(Nemo dat; Nemo dat quod non habet)[88] 원칙에 따라 장물의 취득은 불법이고 법적인 소유권을 인정하지 않고 있다는 점을 주목해야 한다. 시장에서 구입한 비트코인이 원래 존재하지 않는 권한을 소유한 것처럼 오해하고 있을 수 있다는 것이다.[89]

88) 가지지 않은 것은 아무에게도 줄수 없다는 라틴어 법언으로 재산법에서 구매자가 물권을 지니지 않은 판매자로부터 물건을 구입하였을 경우 물권을 취득하지 않는 법률 원칙을 말한다. 선의의 구매자가 비록 모르고 장물을 구매하였다고 하더라도 소유권은 원소유자에게 귀속된다.

89) 이동규, "최근 비트코인 동향의 주요 특징 및 시사점", 2015/2/9, 한국은행 금융결제국

<표 4-1> 비트코인 관련 해킹 피해 사례

시기	서비스명	서비스 종류	피해금액
2011. 6월	Mt.Gox	거래소	875만달러
2011. 8월	MyBitcoin	거래소	80만달러
2012. 9월	Bitfloor	거래소	25만달러
2013. 4월	Instawallet	지갑서비스	460만달러
2013.10월	Inputs.Io	지갑서비스	100만달러
2013.10월	Global Bond Limited	거래소	500만달러
2014. 2월	Mt.Gox	거래소	4억5천만달러
2014. 3월	Flexcoin	은행(비트코인 보관)	65만달러
2014. 3월	Polenix	거래소	5만달러
2014. 8월	BTER	거래소	165만달러
2015.10월	Blockchain.info/ LocalBitcoins사용자	개인	25만불(추정)
2015.11월		개인	
2015. 1월	Bitstamp	거래소	500만달러
2015. 2월	BTER	거래소	175만달러
2015. 2월	Cavirtex	거래소	0달러, 거래소 폐쇄
2015. 3월	Coinapult	거래소	4만3천달러
2015. 5월	Bitfinex	거래소	43만달러
2015. 6월	Scypt.CC	클라우드 마이닝	미상
2015. 10월	Purse.io	비트코인(아마존연결 쇼핑)	30만달러
2016. 6월	The Dao	크라우드 펀딩	5천5백만달러
2016. 8월	Bitfinex	거래소	7천만달러

원 자료: 한국은행(2015년이후 자료 추가)

○ 범죄기술 발달에 따른 리스크: 분산원장은 투명성이 최대화되고 해킹이 불가능하다는 것이 잘 알려져 있고 아직까지는 분산원장 자체가 해킹된 적은 없고 앞으로도 그럴 것이다. 그러나 양자컴퓨터를 사용한다면 분산원장 기술에서 자랑하는 해킹불가능은 무용지물이 될 것이다.

○ 결제 완결성 리스크: 각 분산원장의 설계에 따라 달라질 수 있지만 대부분의 분산원장은 검증이라는 단계를 거치게 된다. 분산원장 시스템에서 어떤 거래가 발생하였을 경우 거래자는 이를 공지하게 되고 채굴자가 채굴된 블록에 넣어서 발행할 수 있게 되는데 이때 해당 거래내역 확인(Confirmation)은 1이 된다. 그리고 해당 블록의 해시를 이용하여 차기 블록이 생성되면 해당 거래내역 확인은 1이 가산된다. 비트코인

블록체인 시스템에서는 거래가 이런 확인이 6번 일어나야 정상적인 재거래가 가능하도록 설계되어 있다. 즉 60분 정도 소요되어야 재사용이 가능한 것이다. 그런데 이것을 일반적인 소액결제의 현장인 POS에서 사용될 수가 없으므로 많은 사업자는 자신이 리스크를 지고 필요에 따라 1~2번의 확인만으로 재거래가 이루어질 수 있도록 하고 있다. 일반적인 디지털통화 거래소의 경우 이체내역 확인(1번 확인)만으로도 인정해주고 있다. 일반적으로 소액결제 현장에서 리스크가 내재함에도 불구하고 이체내역 확인을 하고 이를 기반한 추가 거래 혹은 재거래를 가능하게 하는 이유는 편리함에 비하여 위험성이 매우 낮기 때문이다. 이는 마치 소액결제에 대해서 신용카드 지불시 서명 없이 신용카드 지불을 승인하는 것과 유사하다. 신용카드에 대한 고객신용 거절의 위험성은 거래 지연에 따른 비용이 상대적으로 크다. 하지만 소액이 아닌 고액에 대해서는 값비싼 물품을 구매할 경우 이중으로 지불할 소지가 있다. 이를 이중지불(Double payment 또는 spending) 공격이라고 하는데 공격자는 두 가지 방법을 사용할 수 있다. 하나는 거래가 승인되기 전에 또 다른 거래를 하는 것이고 다른 하나는 공격자가 블록체인 분기를 이용하여 본인의 거래를 무효화시키는 방법이다. 이와 같은 리스크 노출을 줄이기 위해 프라이빗 분산원장을 설계할 때 결제완결성을 보장하는 것이 가능하다. 문제는 이것이 바람직한 기능인지에 대한 검토와 함께 애플리케이션 분야에서 최적화된 안정성을 추구할 수 있는지에 대한 연구가 바람직하다.

○ 결제 불가역성 리스크: 분산원장의 기본적인 설계 기능 중의 하나인 불가역성은 잘못된 결제가 일어났을 경우 되돌릴 수 없도록 만들어졌다는 점인데 이로 인해 기존의 금융시스템에 도입하기 어렵게 된다. 특히 어떤 경우라도 우발적 거래가 취소되지 못한다는 점은 금융시스템에서 분산원장 도입을 설계할 때 신중히 개선을 검토해야 할 것이다.

(나) 튜링완전성 분산원장 기술에 의해 추가되는 리스크

앞에서 설명했듯이 튜링완전성으로 이더리움을 실행하는 가상 머신의 스마트계약 처리능력은 병렬처리가 아닌 일반 범용 컴퓨터와 동급일 만큼 강력하다. 이런 강력함은 기본적으로 고려해야 할 문제와 함께 오류에 대한 리스크를 동반한다.

○ 근본적으로 고려해야 할 문제에 대한 리스크 - 정지문제: 가장 근본적으로 계산복잡도 이론의 고전적인 문제인 “정지문제(Halting problem)”에 맞닥뜨리게 된다. 어떤 프로그램이 정지할지 혹은 정지하지 않을지(즉, 영구 반복에 빠질지) 판정할 수 있는 일반적인 알고리즘을 찾는 문제다. 1936년 튜링은 이 문제에 대한 알고리즘은 없다는 것을 수학적으로 증명한 바 있다. 분산원장이 튜링완전성을 갖는다는 것은 정지문제에 대한 해답이 있어야 한다는 말이다. 이더리움을 디자인한 비탈릭 부테린은 이에 대해 인지하고 있었던 것으로 보인다.[90] 이더리움은 이를 “연료값”을 부과함으로써 해결하고자 했다. 스마트계약에서 거래가 있을 때마다 “연료값”을 빼도록 한다면 밸런스는 0로 수렴하므로 어떤 계약이든 종국에는 정지된다. 그러나 이는 정지문제에 대한 근본적인 해결책이 아님은 자명하다.(“연료값”은 거래를 보낸 사람이 가격을 정하면 참여자(채굴자)가 원하면 이를 받아들일지 정하게 되어있다. 즉 시장이 결정하는 것이다.)

○ 근본적으로 고려해야 할 문제에 대한 리스크 - 비결정문제: 비결정문제(Undecidability problem)는 어떤 프로그램을 보고 그 프로그램이 어떤 일을 하는 지 알 수 없다는 이론이다. 보통 비결정이슈는 모두 정지문제로 환원되고 그렇다면 “연료값”으로 풀 수가 있을 것으로 생각될 수도 있다. 그런데 임시방편인 “연료값”이 근본적이 해결책이 아니므로 비결정문제가 불거진다.

비결정문제를 스마트계약에 대입해 생각해보면 스마트계약으로 쓰여진 프로그램이 어떤 의미인지(혹은 어떤 결과를 내는지) 알 수가 없다. 스마트계약의 의미는 프로그램을 실행하고 나서야 알게 된다는 말이다. 일반 선의의 스마트계약 참여자들이 계약을 복잡하고 공격적으로 만들 필요는 없을 것이다. 그러나 도둑이 복잡하고 공격하기 위해 만든 스마트계약에 대해서는 그 악의를 미리 읽거나 필터할 수 없다. 그래서 일단 시스템(Ethereum Virtual Machine)에 의해서 자동으로 실행되고 나서 백만 달러나 천만 달러를 훔쳐간 후에야 결과를 알 수 있는 상황이 올 수 있다.

90) Ethereum Community. White Paper. http://bit.ly/1dUsoip. 2016.10.17. 접속.

○ 스마트계약 상의 프로그래밍 오류로 인한 리스크: 공격자가 아니라고 하더라도 스마트계약 프로그램 상의 오류로 인한 리스크는 여전히 존재한다. 스마트 계약을 아무리 잘 작성을 한다고 하더라도 비결정적이므로 미리 결과를 예측하는 것은 불가능하다. 따라서 스마트계약에 오류가 있다면 미리 필터하기가 이론적으로는 불가능하고 실제적으로도 매우 어렵다. 스마트계약 상의 프로그래밍 오류는 코드 정합성을 테스트하는 툴이라도 잘 발달되어 있다면 어느 정도 줄일 수 있을 수 있다. 그러나 이더리움 언어들은 새로 나온 프로그래밍 언어라서 개발 도구가 아직은 잘 발달해 있지 않다.

○ DoS 공격에 의한 스마트계약 무효화 시도: 이더리움은 2016년 9월 18일 이후 거의 한달 간 Dos(Denial of Service) 공격을 받는 중이다.[91] 그 이유는 연료값이 낮게 책정된 거래가 있어서 이를 이용하여 저렴한 거래를 발생시켜서 전체 이더리움 시스템에 대해서 공격하는 중이다. 이러한 공격은 간단하게 연료값을 올려서 해결할 수는 있다. 그러나 지금까지 알려지지는 않았고 상상하기 어렵지만 만에 하나 개별 스마트계약에 대해서 공격하는 기법이 나온다면 스마트계약 자체를 무력화해버리는 공격도 가능할 수 있다.

나. 분산원장 기술과 모니터링 방안

금융시스템에 분산원장을 도입한다는 것은 기본적으로 금융시스템에 내재하던 리스크를 극단적으로 줄일 수 있고 장점이 단점에 비해 훨씬 크다는 것은 이미 강조하여 설명한 바 있다. 그와 동시에 분산원장의 종류에 따라 다소 새로운 종류의 리스크가 소개되는데 크게 튜링불완전 분산체인과 튜링완전 분산체인에 따라서 나뉜다.

튜링완전성을 가진 분산원장은 그것이 가져다 줄 국가적 이익이 상상도 못하게 크지만 위험도 적지 않고 이를 도입하기 위한 방법에는 여러 가지가 있을 수 있다. 따라서 분산원장 기술은 금융시스템에 신중하고 조심스럽게 일관된 로드맵을 가지고 도입해야 한다. 그러나 그와 동시에 국가적인 이익

91) Wilke, Jeffrey. “The Ethereum network is currently undergoing a DoS attack.” Ethereum Blog. http://bit.ly/2et5EHm. 2016.10.17. 접속.

을 생각하여 신속하고 적극적인 자세로 도입하는 것이 필요하다.[92] 다시 강조하지만 신중하되 신속하게 도입하는 것이 필요하다.

분산원장을 도입하면서 분산원장 기술을 통해서 도입할 수 있는 것은 금융산업의 규제전반에 적용될 수 있는 소위 RegTech라고 부르는 규제 기술이다. 본 장에서는 그에 관해 토론한다.

(1) 규제기술(Regulation Technology)의 역할

금융서비스가 혁신을 거듭하고 변신하는 동안 새로운 기술에 의해 경쟁은 심화되고 있는 중이다. 클라우드 컴퓨팅, 블록체인, 인공지능 등의 기술의 접목과 함께 보안기술을 강화하면서 동시에 신기술과 서비스를 가능하게 하는 새로운 벤처기업이 속속 출범하는 중이다. 이러한 와중에 핀테크와 디지털 통화를 중심으로 자금세탁/테러자금(ML/TF) 등의 범죄조직에 의해 남용되는 것이 발견됨에 따라 법규제 준수에 대한 요구가 급속히 증가하고 있는 중이다. 이에 따라 금융서비스 사업자들은 규제 의무를 되도록 저렴하고 빠르게 만족시키는 것이 우선순위가 되고 있다. 또한 금융 규제 및 감독 관청 역시 금융에 관한 규제가 혁신을 살리는 동시에 규제를 효율적으로 감독하는 방안을 찾는 중이다. 이런 시장의 요구를 만족시키고자 시작된 산업이 RegTech(Regulation Technology)이다.

(가) 금융기관의 규제 준수 자동화

모든 금융기관은 다수의 규제를 준수하고 그에 맞는 요구사항을 보고할 의무가 있다. 이런 활동은 내부 부서나 외부 기관이 실행하게 된다. 이는 감사, 세금 보고, 종합 자본 분석 검토(CCAR; Comprehensive Capital Analysis and Reviews), 증권거래위원회 보고 등은 금융기관의 연중 예산에 비용으로 추가되는 규제 준수관련 소요비용의 몇 가지 예일 뿐이다.

- 미국의 대형 금융기관들은 약 40억 달러를 규제준수관련 비용으로 사용하고 있다.[93]

92) 이 부분은 피넥터 보고서(2016년 9월호)를 참조했음을 밝혀둔다.
93) Financial Times. "Banks face pushback over surging compliance and regulatory costs, 2015. (WEF. The Future of Financial Infrastructure에서 재인용)

- 감사비용은 가장 큰 금융기관의 경우 가장 큰 규제 준수 비용이 되고 있다. 2013년 상장 기업들은 감사소요비용으로 연간 평균 710만 달러를 사용하였다.[94]

이러한 문제에 대한 해결책으로 분산원장은 운영의 효율성을 증가시킬 수 있는 잠재력이 있고 규제기관들에게 강화된 제재 수단을 제공할 수 있다. 분산원장을 이용할 때 재무제표 감사 프로세스 규제 준수 솔루션을 사용하여 자동화할 수 있다.

(나) 규제 기술(Regulation Technology; RegTech)을 이용한 AML/CTF

RegTech은 법규제(Regulation)와 기술(Technology)의 합성어로 기업들에게 법규제 준수의 필요사항을 효과적이고 효율적으로 제공하도록 연구 개발되고 있는 기술이다. 최근 데이터에 대한 중요성과 함께 이를 이용한 규제 수준에 대한 요구사항과 보고사항이 증가함에 따라 이에 대한 관심도 높아지고 있다.

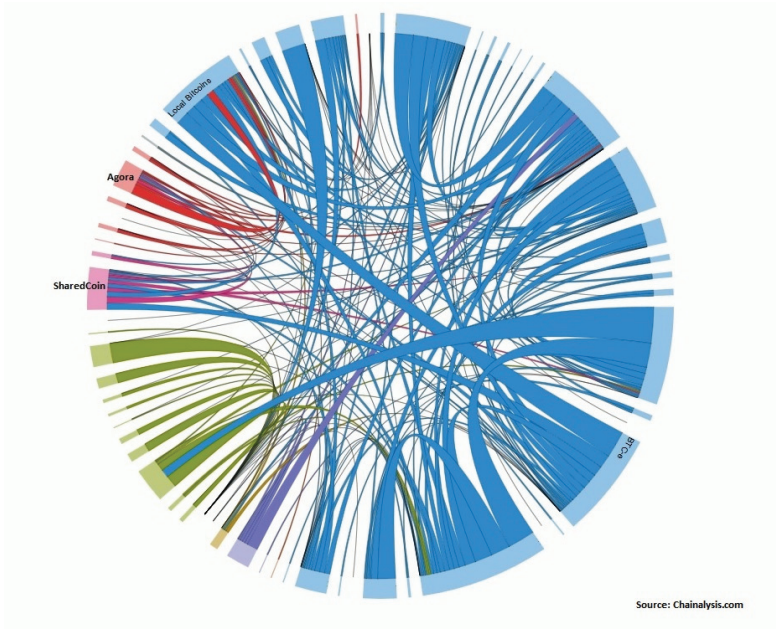
블록체인의 투명성을 이용하여 디지털화폐의 움직임을 분석하여 AML/CFT에 사용할 수 있다. 예컨대 이미 기술한 바와 같이 비트코인은 많은 경우 범죄나 세금회피를 목적으로 사용되고 있다는 것은 잘 알려져 있다. 이를 차단하기 위해 매우 자세한 모니터링이 진행될 수 있다. 아래 그림은 2015년 비트코인의 움직임으로 시각화를 위해 단순화하고 색채로 나타낸 것이다.[95]

범례는 아래와 같다.

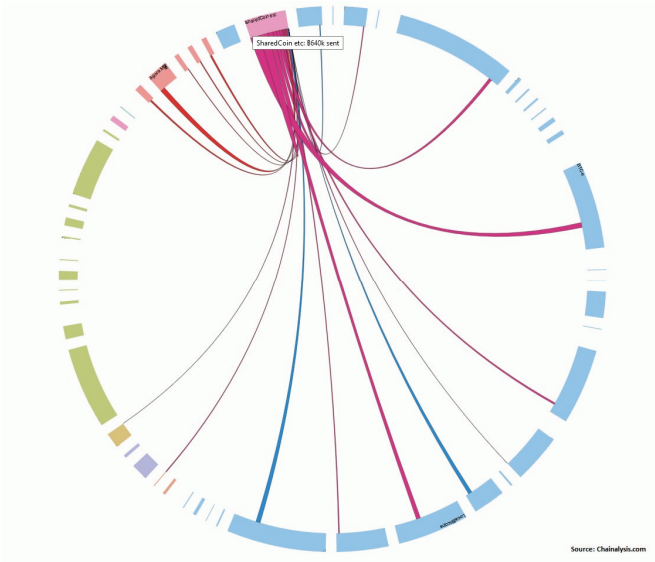
Blue: virtual currency exchanges
Red: darknet markets
Pink: coin mixers
Green: mining pools
Yellow: payment processors

94) Financial Executives Research Foundation. Annual Audit Fee Report. 2015.
95) ofnumbers.com. http://bit.ly/1ncsHty. 2019/6/9 복사.

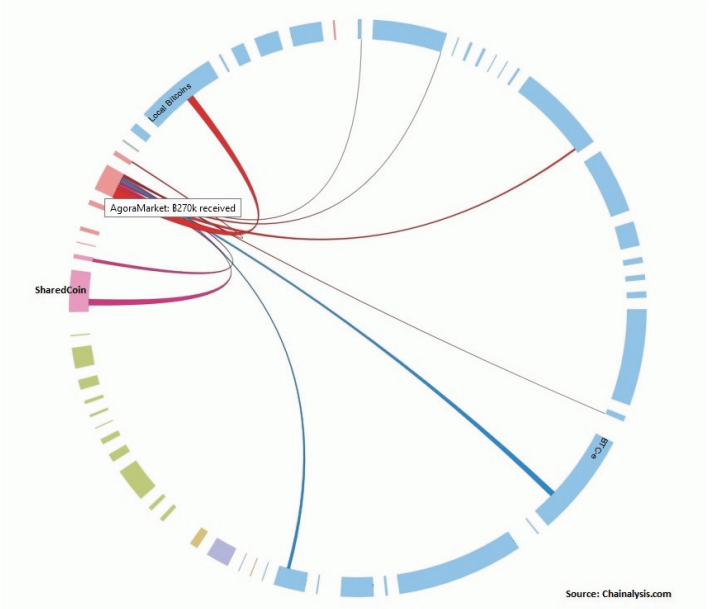
<그림 4-2> 2015년 비트코인의 움직임 시각화 그래프



위의 그림에서 SharedCoin 서비스를 이용한 자금세탁의 의혹이 있는 움직임만을 도시하면 다음과 같다.(SharedCoin은 유저들의 코인을 섞어서 보내주는 서비스를 하는 사이트로 비트코인의 출처와 역사를 지워주는 일을 하는 서비스다.)



2013년 설립된 아고라는 암시장에서 범죄자들의 자금이 움직일 수 있도록 IP 주소를 지워주는 서비스를 하는 곳이다. 이를 사용한 돈의 움직임으로 추적하면 아래의 그림과 같다.



3. 디지털통화 및 분산원장 기술의 표준화 분석

가. 디지털통화 및 분산원장 기술의 표준 도입의 필요성

표준화는 생산. 소비, 유통 등 관련 분야에서 능률을 높이고 경제성을 향상시키는 한편 제품의 품질을 개선하는데 도움을 주고 업무의 단순화를 가져온다. 분산원장 기술은 다수의 기술이 난립하고 있고 디지털통화는 더욱더 많은 수가 시장의 혼란을 가져오고 있는 중이다. 이런 점에서 디지털통화와 분산원장 기술 표준 도입은 이들 기술 발전을 돕고 활성화하는데 많은 도움이 된다.

분산원장 기술에서 표준이 필요한 부분은 다음과 같다.

(1) 분산원장 기술 측정기준 표준화

분산원장 기술은 다양하고 많은 경우 서로 다른 활용 목적을 충족하기 위해서 제안되어 만들어지고 있다. 이런 점에서 블록체인에 대해 어떤 표준화된 측정기준을 갖고 설명할 수 있다면 가장 현명한 시작점을 제공할 수 있을 것이다. ISITC(International Securities Association for Institutional Trade Communications; 기관무역 통신 국제증권협회)는 분산원장 기술의 활용을 위해 측정기술표준화가 필요하다고 보고 다음과 같은 10개 분야의 측정기준을 도입할 것을 주장하였다.

"복원성(Resilience), 확장성(Scalability), 보안성(Security [including: Trust, Identification, Authentication]), 대기시간(Latency), 데이터(Data [including: Structure, Audit, Privacy, GDPR]), 거버넌스(Governance), 법제(Legal [including: Jurisdiction, Dispute Resolution]), 규제(Regulatory), 소프트웨어(Software [including: Version Control, Code, External interfaces, Development & Bug Fixes]), 네트워크(Network)"

(2) 분산원장 기술 상호 연결 표준화

분산원장 기술의 잠재력은 아무리 강조되어도 지나치지 않다. 그런데 전세계의 분산원장이 어떤 방식으로든 서로 연결될 수 있다면 실시간으로 원장 동기화를 할 수 있다. 이를 위해 분산원장 간의 상호연결을 위한 표준화가 중요하다. 즉 비트코인, 리플코인, 이더리움 등 기존의 분산원장 간의 연결 표준과 향후 창안될 블록체인에 대한 상호 연결성을 제공하는 것이 중요하다. 또한 분산원장끼리의 연결뿐만이 아니라 SWIFT와 ISO, FIDO 등의 금융 관련 국제송금, 지급결제, 바이오인증 등 기존의 표준 프로토콜과의 매끄러운 연계를 통한 관련 산업의 활성화 유도를 위한 연결 표준화는 적극 추진되어야 할 것이다.

(3) 분산원장 기술 기반 "스마트 웹"기술 표준화

분산원장 기술은 "스마트" 기술과 연결되는 것이 필요하다. 특히 스마트 기술 중 스마트 웹 기술의 연동성을 추진하는 것이 필요하다 할 것이다. 그 중 웹지불결제, 웹암호화, 웹애플리케이션 보안, 미디어 확장을 위한 분산원장,

프라이버시 등에 대한 표준화가 필요하다.

(4) 광범위한 산업의 분산원장 기술 활용 인프라를 위한 표준화

금융서비스 제공자뿐만 아니라 사물인터넷 등 다양한 사업자들의 광범위한 협업을 제고하고 스마트 계약 등 블록체인에 내재하고 있는 비즈니스 모델의 창의적 발전을 도모하는 동시에 포괄적이고 투명한 자동 규제 감독 체계를 통하여 연관 산업의 동시 다발적 발전을 촉진하는 인프라를 위한 표준을 제공하는 것이 필요하다.

나. 표준 도입시 고려사항 및 방안

(1) 진화하는 기술로서 표준 도입

과거 공인인증서가 표준으로 채택되면서 가장 실패한 부분은 공인인증서가 지속적으로 또 점진적으로 진화해야 하는 시스템임을 인지하지 못한 데에 있다. 디지털통화나 분산원장 기술이 어떤 형태로든지 표준화되어 도입이 된다면 표준은 되도록 기술진화와 독립적이면 좋을 것이다. 그러나 분산원장 기술은 지속적으로 진화할 것으로 보인다. 따라서 기술진화의 가능성이 있다고 하면 주저없이 진화할 수 있는 표준과 그 모델을 반영하고 이를 위해 깊이 고민되어야 할 것이다.

(2) 국제 공조를 통한 규제 효율성 최대화

자금세탁(AML)과 테러자금 조달방지(CFT)를 위한 비용이 현재 2014년 기준 100억 달러가 들어가고 있다. 또한 고객파악(KYC)에 드는 거래지연과 KYC지침을 위반하여 내는 벌금액수도 상당하다. 이를 분산원장 기술이 해결해 줄 것으로 기대한다. 암호화된 아이디(주소)를 실제 ID로 전환한다면 KYC지침을 쉽게 준수할 수 있을 뿐 아니라 AML/CFT를 획기적으로 줄일 수 있다. 그러나 또한 이를 더욱더 강력하게 하기 위해서는 국제적인 공조가 필요하다. 국제적으로 연결할 수 있는 기술의 표준화를 통해서 인프라를 연결할 수 있다면 더욱 강력해진다.

예컨대, 현재 스위프트가 관할하는 전세계 7,000여 개 은행으로 연결되어 원장이 모든 은행에 실시간으로 동기화된다면 중복된 KYC와 오류를 감소시킬 수 있다. 이런 개인 식별 기술은 이미 암호화된 개인키와 공개키로 검증되었으나 정확한 개인식별을 위한 좀더 강력한 기술이 요구(생체인식 기술 등)된다. 이렇듯 표준화된 KYC 기술을 준수하는 은행만 분산원장에 참여시키는 것으로도 AML/CFT를 훨씬 더 낮은 비용으로 더 효율적으로 수행할 수 있도록 해준다. 따라서 국제사회와 지속적으로 공조하면서 진화시킬 수 있는 방안이 중요하다 할 것이다.

(3) 해킹위험으로부터의 보호

일반적으로 분산원장 기술이 안전하다고는 하지만 분산원장 관련기술이 수없이 해킹당해 왔다는 사실은 변하지 않는다. 세계의 금융기관이 분산원장으로 연결된다면 이를 노리는 해커들은 취약한 부분을 찾아다니며 공격할 것이다. 이들로부터 네트워크를 보호하면서 지속적으로 네트워크의 안전을 점검하는 국제공조체제 등이 가동되어야 할 것이다.

4. 소결

미국의 FBI는 2012년 4월 비트코인 등 디지털통화가 불법적인 행위를 막는 법집행에 뚜렷이 도전하고 있다는 보고서를 발표하면서 이들 혁신적인 신기술이 불법적인 행위에 이용되는 것을 경계한 바 있다. 특히 이 보고서는 디지털통화는 주조, 작동, 배분까지의 과정이 맬웨어(Malware)나 봇넷(Botnet) 등의 사용을 통해 쉽게 불법적인 송금이나 조작이 가능하여 불법적인 행위에 특히 취약하다는 점을 지적하였다. 따라서 비트코인 등의 디지털통화가 중앙기관이 없다고 하더라도 비트코인을 취급하는 서비스 기업은 고객들에게 신분증이나 은행 정보를 제시하도록 하여 본인확인을 하도록 권고한 바 있다. 또한 송금서비스 기업들은 FinCEN에 등록하고 자금세탁방지 프로그램을 의무적으로 설치하도록 권고하고 있다.

디지털통화는 범죄자와 해커 등 많은 범죄자들의 지속적인 공격대상이 되어 왔고 피해자들을 양산해 왔다. 따라서 법규제를 통해 첫 번째 소비자를 범죄로부터 보호하고, 두 번째 비트코인 등 디지털통화가 범죄에 악용되는

것을 차단하고, 세 번째 혁신적 창업자들에게 해킹 등에서 자신들을 보호할 수 있도록 가이드라인을 제시할 수 있다는 점에서 혁신성과 창조성을 해치지 않는 한도 내에서 적절히 규제하는 것이 필요하다.

이와 같은 맥락에서 미국의 뉴욕 주를 선도로 많은 국가와 지방정부가 디지털통화 사업자를 규제하는 움직임을 보이고 있는 것은 의미 있는 일이다.

또한 IMF는 최근 보고서에서 금융무결성, 탈세대책, 소비자보호 등에 대한 규정과 해석이 현재 불분명하므로 국가연합차원에서 이를 명확히 하고 디지털통화의 규제에 국제공조가 중요함을 강조한 것 또한 의미가 있다. 왜냐하면 디지털통화가 많은 혜택을 가져올 잠재력이 있으나 동시에 금융 무결성, 소비자 보호 등에 문제를 야기할 수 있고 탈세 목적의 사용자가 모일 수 있으며 통화 관리도 문제가 되기 때문이다.

그럼에도 디지털통화와 분산원장 기술은 결국 광범위하게 사용될 것이고 혁신의 속도에 맞추어 규제도 세심하고 유연한 대응이 필요하며 국제기구를 통한 국제적 커뮤니티 협력도 강화되어야 하며 장기적 관점에서 국제 표준 및 규제에 가장 적절한 지침을 제공하는 모범사례를 개발하고 다른 분야에도 적용시키는 것이 필요하다. 현재 가장 중요한 것은 지속적인 모니터링과 분석을 통해 기술 혁신에 따른 위험을 지속적으로 분석하면서 창조성을 해치거나 혁신성을 저해하지 않는 범위 내에서 적절한 규제로 응답하는 것이다. 특히 대형 금융기관이 아닌 소규모의 신기술 창업자들이 규제 내에서 자유롭게 창업하면서 규제를 잘 준수할 수 있도록 규제 기술(RegTech)의 적극적인 도입을 통해 규제 보고와 관리를 자동화할 수 있도록 해야 할 것이다.

규제는 다음과 같은 원칙위에서 이루어지는 것이 바람직하다.

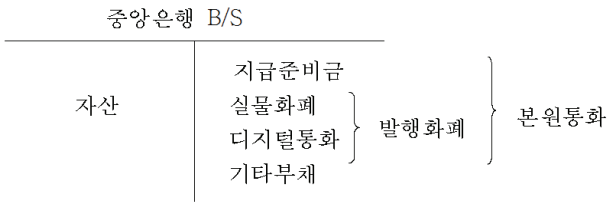
- 규제는 혁신을 옥죄지 않는 동시에 리스크에 적절히 대처해야 한다.
- 규제는 디지털통화의 변화에 유연하게 적응해야 한다.
- 규제는 디지털통화의 비즈니스 모델에 내재할 수 있는 사업구조에 기초해야 한다.
- 규제는 시장에서의 교란 행위(AML/CFT, 사기 등)를 제재할 뿐만 아니라 디지털통화 거래소 등 중개업의 건전성까지도 유도해야 한다.

V. 중앙은행의 분산원장 기반 디지털통화 발행

1. 중앙은행 발행 디지털통화의 개념과 특징

중앙은행이 발행하는 디지털통화는 법정화폐(Fiat money)로서 실물화폐와 달리 전자적 형태로 저장되고, 실물화폐나 지급준비금과 함께 본원통화(Monetary base)를 구성한다. 그러나 중앙은행의 채무라는 점에서 은행예금이나 기존의 전자화폐와 구별된다.

<그림 5-1> 중앙은행 발행 디지털통화의 개념



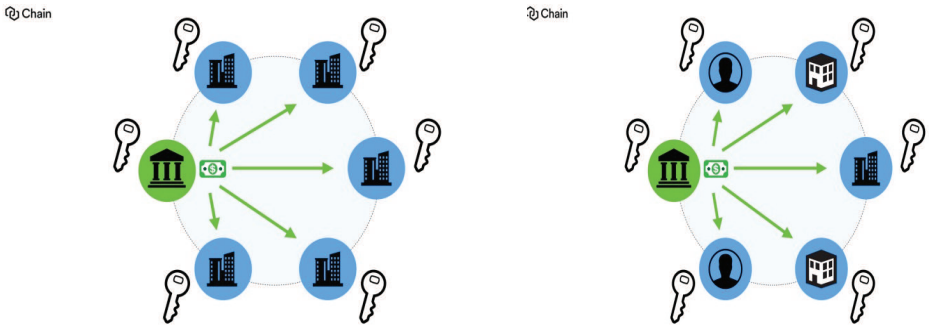
이는 그동안 은행만이 가졌던 중앙은행 예금계좌에 대한 접근이 개인이나 기업까지 확대되는 것을 의미하고, 또한 상업은행 예금의 대체제로서 일반인들에게 제공되는 것을 의미한다. 이때 중앙은행 발행 디지털통화의 상업은행 예금과의 대체 정도는 중앙은행 발행 디지털통화에 결제기능 부여정도(자금이체+상업은행의 대금결제+자동이체 등), 익명성 보장여부, 이자지급 여부 등에 따라 달라질 것으로 예상된다. 따라서 중앙은행은 디지털통화의 발행에 앞서서 이들에 대한 신중한 검토를 수행해야 할 것이다.

체인(Chain)사의 루드윈(Ludwin)이 2016년 6월에 미국의 연방준비제도에서 행한 연설 내용을 보면 루드윈은 중앙은행 발행 디지털통화 방식을 대 은행 발행모형과 대 일반 발행모형으로 구분하고 있다(<그림 5-2> 참조). 대 은행 발행모형은 중앙은행이 은행 간 네트워크에 참여할 뿐만 아니라 해당 네트워크에 디지털통화를 직접 발행하는 방식으로서, 이 경우 디지털통화는 지폐나 동전처럼 하나의 새로운 거래수단(new medium)이기 때문에 실질적인 것이고 따라서 실물화폐로 바꿀 필요가 없다. 뿐만 아니라 중앙은행이 발행한 것이기 때문에 정부의 신용과 완전한 믿음에 기초한다. 이러한 구조에서는 디지털 자산의 거래가 디지털통화로 인해 매우 간단해질 수 있다. 디지털 자

산을 보유한 은행과 디지털통화를 보유한 은행 간에 거래는 양자가 동의하고, 그들이 네트워크상에서 통제하는 자산에 해당하는 개인키로 서명하면 끝난다. 청산이나 결제 없이 언제든지 엄격한 보안과 완벽한 투명성 하에서 실시간 자산 교환(real-time DvP)이 이루어질 수 있다.

대 일반 발행모형은 중앙은행이 모든 기관과 사람에게 디지털통화를 직접 발행하는 방식으로서, 이 경우 모든 사람이 은행지폐를 보유할 수 있고 또한 모든 사람이 개인키를 보유할 수 있기 때문에 모든 사람은 디지털 은행지폐를 보유할 수 있다. 이때 스마트폰은 개인키를 담을 수 있는 안전한 도구가 될 수 있다. 중앙은행이 두 가지 모형 중 어떤 방식을 취하느냐에 따라 경제와 금융산업에 미치는 영향이 다를 것으로 예상되고, 대 일반 발행모형의 경우 훨씬 더 큰 영향을 미칠 것으로 예상되기 때문에 보다 신중해야 할 것이다.

<그림 5-2> 대 은행 발행모형과 대 일반 발행모형

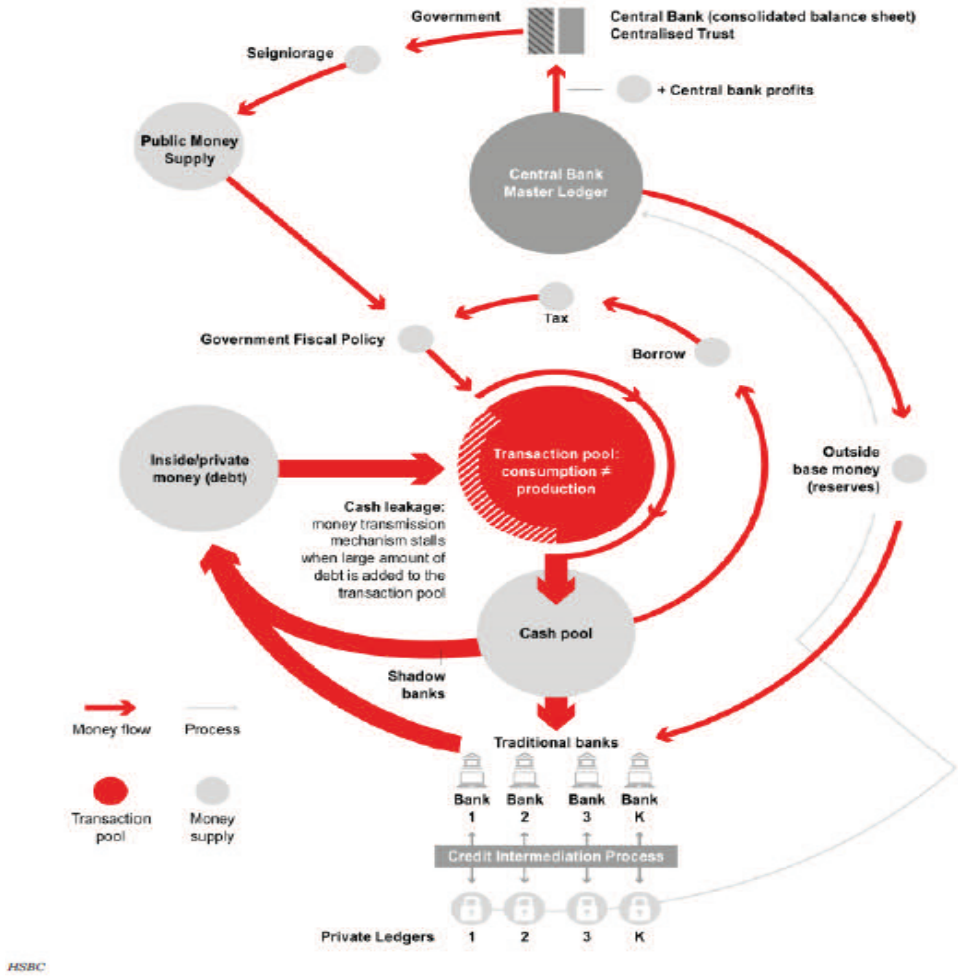


자료: Chain.com

한편 HSBC는 2016년에 발간된 내부보고서에서 현행 은행체제를 통해 공급되는 방식을 내부통화(inside money) 방식이라 하고, 이 방식은 은행의 선택에 의해 결정되기 때문에 정확히 실물경제에 어느 정도의 화폐가 공급될지 알 수 없는 한계점이 있다고 하고 있다. 특히 비생산적 사업을 위해 은행의 부채가 과다하게 생성된다면 과다한 부채는 성장 자체를 낮출 수도 있다고 한다. 반면 분산원장 기술에 기반한 화폐의 직접 공급방식(outside money)은 온라인 판매업자들이 고객들의 상품 구매와 지불 흐름을 모두 파악하고 있기 때문에 담보물 없이 대출을 해 줄 수 있는 것처럼, 분산원장을 통한 실시간 빅데이터 분석에 기반한 화폐전송시스템에 의해 정부나 중앙은행이 경제

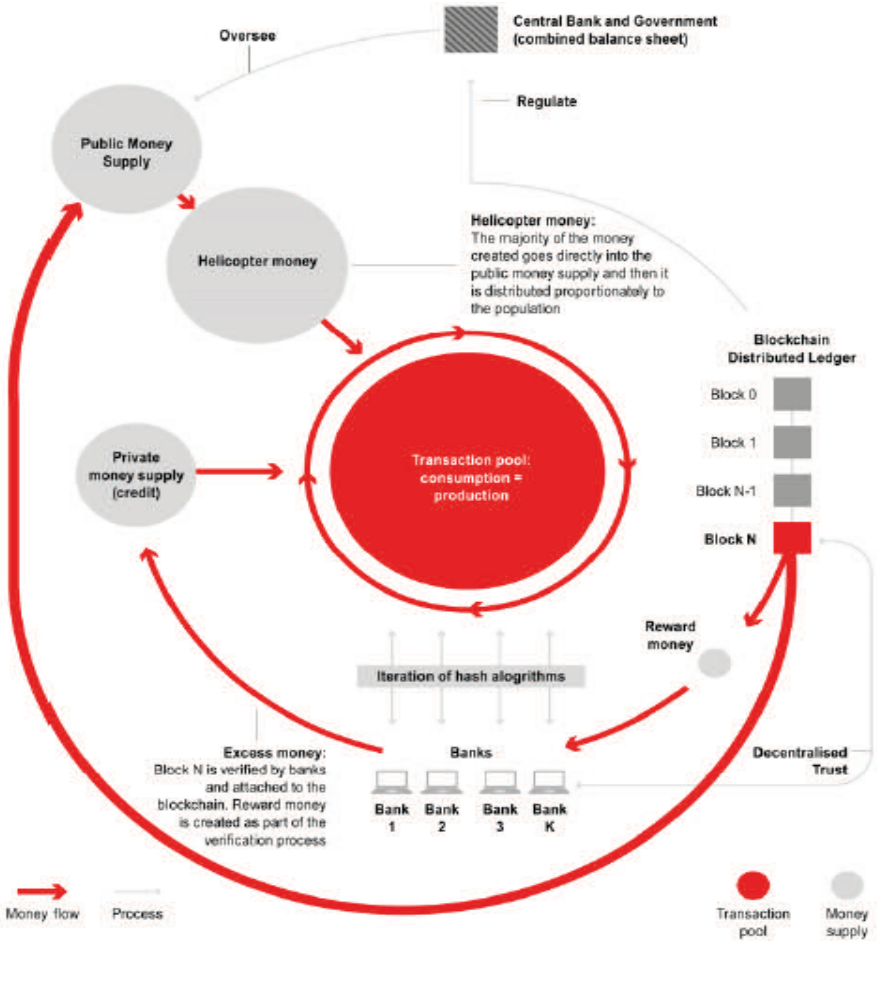
를 보다 효율적이고 체계적으로 균형을 이루도록 할 수 있다고 한다. 즉 분산원장을 사용해서 '헬리콥터 머니'[96]를 가능하게 할 수 있다고 한다.

<그림 5-3> 현행 은행 시스템



96) '헬리콥터 머니'는 노벨경제학상 수상자인 밀턴 프리드만이 최초로 사용한 말로 중앙은행이 민간 신용 시스템을 통하지 않고 대중들에게 직접 화폐를 공급하는 것을 의미한다.

<그림 5-4> 중앙은행이 디지털통화를 발행할 경우

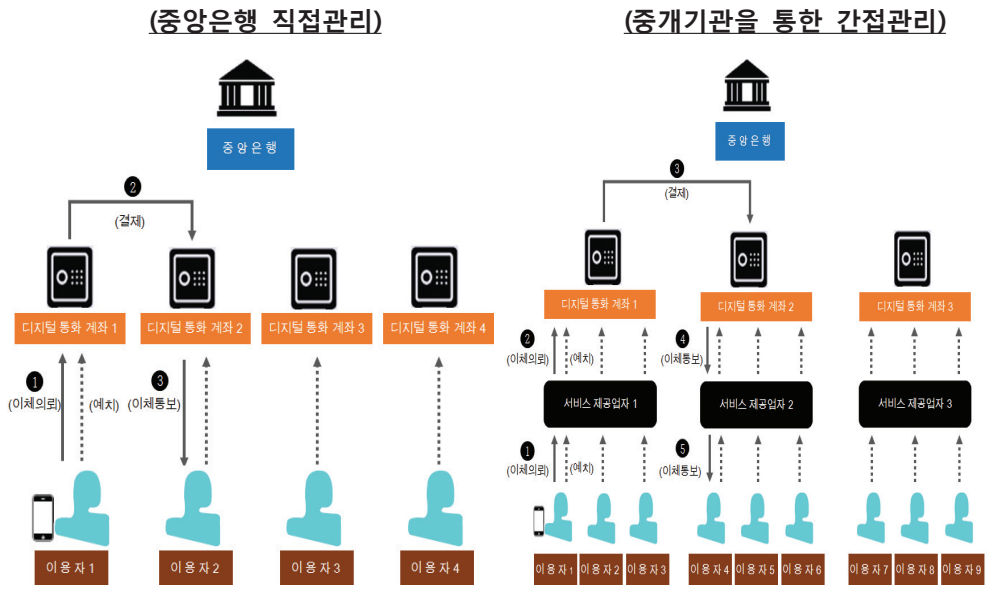


HSBC

2. 디지털통화의 발행 방법

중앙은행은 은행뿐만 아니라 모든 사람(법인 포함)이 중앙은행에 '디지털예금계좌'를 보유하도록 함으로써 디지털통화를 제공하게 된다. 중앙은행이 '디지털예금계좌'의 관리를 직접 하느냐 또는 중개기관을 통해 하느냐에 따라 계좌 직접관리방식 대 중개기관을 통한 계좌 간접관리방식의 두 가지로 구분될 수 있다.

<그림 5-5> 중앙은행의 계좌 직접관리방식 대 중개기관을 통한 계좌 간접관리방식



자료: Dyson and Hodgson, "Digital Cash: Why Central Banks Should Start Issuing Electronic Money,"PositiveMoney, Jan. 2016.

<그림 5-5>에서 우측 그림의 경우 서비스 제공업체들은 계좌정보, 지급카드, 잔액확인, 분류코드, 계좌번호, 인터넷/모바일은행업무, 전화나 이메일을 통한 고객지원 등을 제공할 책무를 진다. 또한 정상적인 지급결제 네트워크를 통한 지급결제 서비스 기능을 디지털통화계좌를 보유한 자들에게 제공할 책무가 있다. 서비스 제공업체들에게 지급된 모든 자금은 중앙은행 계좌에 전액 전자적으로 예치되기 때문에 서비스 제공업자들은 언제나 100% 유동성을 확보하게 되며, 현행 제도에서 은행이 잘못될 때 은행 예금자의 일부에게만 예금지불이 가능한 것과 대조를 이룬다.

계좌에 있는 디지털통화는 법적으로 서비스 제공업체가 아닌 계좌보유자에게 속하게 되는데 이는 디지털통화가 서비스 제공업체의 대차대조표가 아니라 중앙은행의 별도 고객계좌에 있기 때문이다. 반면, 현행 제도에서 개인들이 입금한 실물화폐는 은행의 자산이 되고(은행 소유) 실물화폐를 입금한 자에게는 은행 부채인 은행예금이 주어지게 된다.

또한 서비스 제공업체는 고객의 디지털통화를 대출해 줄 수 없고 중앙은행 계좌에 자금이 있기 때문에 서비스 제공업체의 신용리스크나 운영리스크가

발생하더라도 고객에게는 전혀 손해가 발생하지 않는다. 반면, 현행 은행들은 고객의 돈을 대출하는데 사용하기 때문에 은행이 부실화되거나 사건이 발생할 경우 고객들은 손실을 볼 수 있는 구조이다. 한편 디지털통화계좌에 있는 자금은 중앙은행의 부채가 되며 이는 정부에 의해 발행된 무이표 영구채 자산으로 담보화하면 어떤 리스크도 없다, 이러한 정부채는 이자지급도 없고 만기도 없기 때문에 회계 상 정부의 부채로 잡히지 않는다.

지금까지 살펴 본 디지털통화계좌 간접관리방식과 은행계좌 간접관리방식을 비교 요약하면 다음 <표 5-1>과 같다.

<표 5-1> 디지털통화계좌 간접관리방식과 은행계좌 간접관리방식의 비교

비교 항목	디지털통화계좌 간접관리방식	은행계좌 간접관리방식
계좌관리서비스	서비스 제공업체	상업은행
계좌제공자	중앙은행	상업은행
계좌자금	중앙은행의 부채	상업은행의 부채
법적 통화 소유권	고객	상업은행
유동성	100% 확보	일부 확보
신용리스크	없음	있음
예금보험제도	필요없음	필요함
바젤자본규제	필요없음	필요함
서비스혁신	가속화	더딤

디지털통화는 분산원장 기술에 기반하여 발행할 수도 있지만 중앙집중형으로 발행할 수도 있다. 그러나 현재 대다수 중앙은행의 디지털통화 발행은 분산원장 기술을 기반으로 진행되고 있다. 두 방식을 간략히 비교 요약한 내용이 <표 5-2>에 주어져 있다.

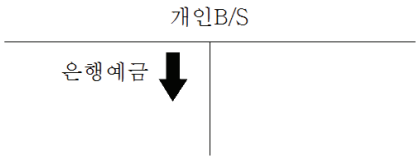
<표 5-2> 분산원장 기술 기반 발행방식과 중앙집중형 발행방식의 비교

비교 항목	분산원장 기술 기반	중앙집중형
거래의 안정성과 투명성	높음	높음
지급과 결제	이체 즉시 동시 완료	이체 즉시 동시 완료
비용구조	저렴	과다
거래검증 및 원장관리	소수의 인가기관 및 중앙은행(permissioned blockchain)	중앙은행
인가기관	기존의 금융기관	없음
통화발행규모	중앙은행이 결정	중앙은행이 결정
구현방법	이용자가 인가기관에서 공개키와 개인키를 부여받아 사용	현재 방식

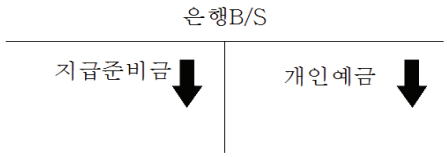
3. 디지털통화의 발행 관리 프로세스

<그림 5-6>을 통해 디지털통화가 발행되어 관리되는 프로세스를 구체적으로 번호 순서대로 살펴보기로 하자.

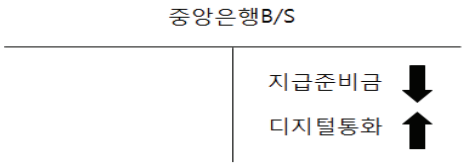
① 개인이 서비스 제공업체에 디지털계좌를 개설하고(최초잔액 '0') 은행에 자금이체 요청: 개인의 은행예금이 감소하고 서비스 제공업체의 해당 개인에 대한 계좌에 디지털통화 이체



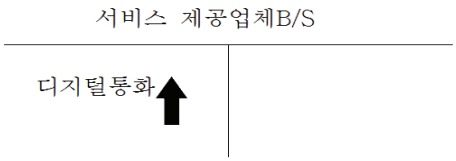
② 은행은 자신의 중앙은행 지준계좌에서 서비스 제공업체의 디지털계좌로 자금이체 요청: 은행의 지급준비금과 해당 개인의 예금이 동시에 감소



③ 중앙은행은 해당 은행의 지준계좌의 자금을 서비스 제공업체의 중앙은행 디지털계좌로 이체

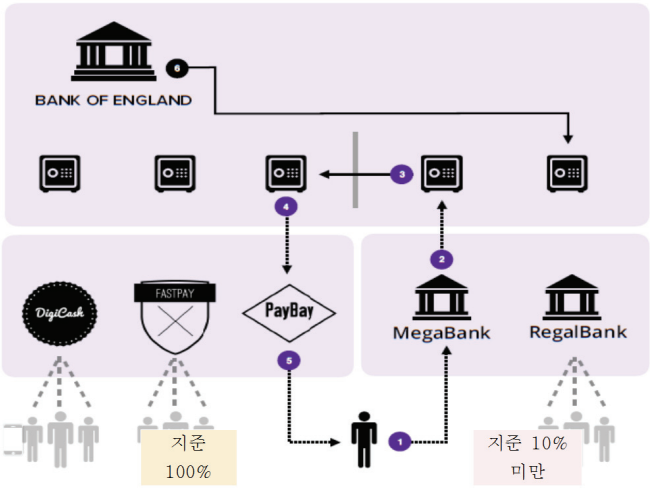


④ 중앙은행은 서비스 제공업체에게 고객의 자금이체가 이루어졌음을 통보



⑤ 서비스 제공업체는 입금되었음을 고객에게 통보

<그림 5-6> 디지털통화의 발행 관리 프로세스



자료: Dyson and Hodgson, "Digital Cash: Why Central Banks Should Start Issuing Electronic Money,"PositiveMoney, Jan. 2016.

4. 거시경제에 미치는 영향

가. 긍정적 영향

(1) GDP 성장률 제고

Barrdear and Kumhof(2016)는 분산원장 기술에 기반하여 GDP의 30%에 해당하는 금액만큼 중앙은행 디지털통화를 발행하여 국채를 인수한다면 실질이자율, 세금왜곡 및 통화거래비용의 감소로 인해 GDP를 최대 3%씩 영속적으로 증가시킬 것으로 전망하였다. 그들은 전통적인 동태확률 일반균형모형(DSGE model)을 글로벌 금융위기 이전의 미국경제에 적용하였으며, 중앙은행 발행 디지털통화가 은행예금의 불완전한 대체재이고, Jakab and Kumhof(2015)에서처럼 은행예금이 여신이나 자산 취득을 통해 만들어진다고 가정하였다.

(2) 실질이자율 하락

국가 채무의 증가에 따라 국채에 대한 실질 이자율이 증가하는 상황에서 중앙은행 발행 디지털통화에 의한 국채 인수는 균형 실질이자율을 낮출 것으로 예상된다. 중앙은행이 통화를 발행해서 국채를 보유할 경우 다음과 같은 두 가지 결과가 예상된다.

(가) 중앙은행의 순이자마진으로 인해 생긴 이익을 정부로 재송부할 경우 정부의 이자부담을 줄일 수 있고 따라서 부채 수준을 보다 지속 가능하게 만든다. 이때 중앙은행 발행 디지털통화의 보유가 거래 목적상 보다 유용함에 따라 비금전적 이익이 보다 크기 때문에 순이자마진은 평균적으로 양(+)이어야 하기 때문이다.

(나) 중앙은행이 보유한 국채는 사실상 부도 가능성이 없는데 이는 정부의 부도로 인해 생기는 손실은 정부에 의한 중앙은행 자본금의 대체를 유발하기 때문이다. 또한 민간 부분의 관점에서 볼 때, 중앙은행이 발행한 디지털통화와 같은 중앙은행에 대한 청구권은 중앙은행에 대한 다른 청구권의 형태로는 상환될 수 없기 때문에 결국 민간 부문이 보유하는 부도가능 부채의 스톡을 줄이고, 관련 신용리스크에 대한 인식을 낮춰, 결과적으로 국가 부채에 대한 이자율을 낮추게 된다. 국채 이자율의 하락은 일반적으로 민간 차입자의 차입비용을 낮추기 때문에 결국 이는 자본 축적과 경제 성장의 이익을 가져올 수 있다.

(3) 재정수입 증가

중앙은행 발행 디지털통화가 공개시장조작이나 리포(Repo)거래를 통해 국채와의 교환형식으로만 스톡 공급과 회수가 이루어지는 것으로 가정할 경우, 중앙은행 발행 디지털통화는 순이자비용의 감소를 가져오기 때문에 정부와 중앙은행의 결합 재정수입의 영속적인 증가를 가져온다. 이는 정부 예산과 부채의 변화 없이 정부가 재정지출을 늘리거나 세율을 낮출 수 있도록 한다. 이러한 비용절감을 중앙은행과 재정당국이 어떻게 나누느냐에 따라 통화정책과 재정정책이 달라질 수 있다.

(4) 거시경제의 안정성 증가

분산원장 지급시스템의 장점 중 하나는 전체 거래기록이 실시간으로 모든 거래증명자에게 뿐만 아니라 정책수립자들에게도 제공된다는 것이다. 따라서 충격이나 정책변화에 대한 경제의 반응을 거의 즉각적으로 관찰할 수 있기 때문에 거시경제의 안정성 관리에 도움을 줄 수 있다.

(5) 탈세와 탈법의 감소

현금통화는 익명거래가 가능하기 때문에 탈세, 탈법, 탈규제의 목적으로 악용된다. 대부분의 국가에서 50% 이상의 통화가 거래를 숨기기 위해 사용되는 것으로 조사된다. 미국의 경우 통용 통화의 78%가 $100짜리 지폐, 유럽의 경우 1/3은 50유로짜리, 1/3은 500유로짜리, 일본은 87%가 10,000엔짜리 지폐이며, 미국의 경우 $100 짜리 고액권의 증가는 GDP 성장의 3배에 이르고, 지하경제의 규모는 전체 GDP의 7-10%에 이르고, 탈세규모는 2006년 기준 $4,500억에 이르는 것으로 추산된다(Rogoff, 2014). 중앙은행 발행 디지털통화로 대체된다면 이러한 지하경제가 양성화될 수 있다.

(6) 주조차익(seigniorage)의 재창출

은행들은 실물화폐가 필요할 때 중앙은행에 예치된 자신의 지준을 줄이거나 중앙은행과 리포계약을 체결한다. 지준을 줄이는 경우에는 지준에 대한 지급이자가 줄고, 리포계약을 체결하는 경우에는 리포 이자수입의 형태로 주조차익이 발생한다. 만약 전체 실물화폐가 디지털통화로 바뀐다면 주조차익의 변화는 없으나(실물화폐든 디지털통화든 이자지급이 없기 때문), 은행예금 중 일부가 디지털통화로 바뀐다면 주조차익은 증가한다.

(7) 금융포용(financial inclusion)의 증가

Ecuador 정부는 모든 국민들이 중앙은행에 계좌를 갖게 하는 지급시스템 인프라를 구축하였다. 해당 중앙은행 계좌를 통해 국민들은 실물화폐를 맡기고 전자 잔고(electronic balance)를 통해 전자적으로 돈을 쓸 수 있다. Ecuador 정부는 미국 달러를 확보하는 것 외에도 은행의 혜택을 받지 못하

는 많은 국민들에게 디지털 은행계좌를 제공하기 위해 이러한 시스템을 구축한 것이다.

우리나라의 경우에는 대다수의 국민들이 은행계좌를 가지고 있는 상황이기 때문에 위와 같은 금융포용의 증가는 기대하기 어려울 것이다. 그러나 많은 사람들이 기존의 은행서비스에 대해 불만을 가질 수 있기 때문에, 중앙은행 발행 디지털통화의 공급은 이들에게 새로운 금융포용으로 작동할 수 있다.

나. 부정적 영향

(1) 전환 리스크의 발생

중앙은행이 새로 디지털통화를 발행할 시 새롭고 검증되지 않은 통화 및 재정 환경으로의 전환으로 인해 발생할 수 있는 리스크를 면밀히 검토해야 할 것이다. 새로운 중앙은행 발행 디지털통화 계정 상품에 대한 디자인과 시장검증을 시행해야 하고, 사이버 보완 및 해킹에 대한 보호를 비롯하여 철저히 검증되고 신뢰할만한 디지털 인프라를 구축하여야 한다. 또한 시스템 운영자들에 대한 적절한 사전 훈련을 실시하고, 디지털통화 발행 시 법적 제도적으로 필요한 사항들을 사전에 준비하여 대비하여야 한다. 아울러 외국 중앙은행과의 충분한 교감을 통해 전환 리스크를 최소화할 필요가 있다.

(2) 비용 발생

현존하는 민간 디지털 통화에서와 같은 완전 무허가 시스템(fully permissionless system)의 경우 거시경제적으로 의미 있는 규모에 도달하기 위해서는 상당한 사회적 비용의 추가가 필요할 것으로 보인다. 그러나 허가가 필요한 분산구조(distributed but permissioned architecture)를 채택한다면 새로운 시스템 구축에 따른 사회적 비용은 그리 크지 않을 것이다.

5. 통화정책에 미치는 영향

가. 긍정적 영향

(1) 추가적인 통화정책 수단 확보 가능

(가) Barrdear and Kumhof(2016)

중앙은행 발행 디지털통화는 다른 유형의 금융자산과 불완전 대체재(imperfect substitute)이기 때문에 중앙은행은 전통적인 금리정책 이외에 또 다른 정책수단을 보유하게 된다. 이에는 GDP 대비 중앙은행 발행 디지털통화의 양을 고정시키는 양적 정책과 정책금리와의 스프레드를 고정시키는 가격정책 두 가지가 있을 수 있다. 인플레이션이 목표치에서 벗어난 경우 경기확장기(경기수축기) 동안 GDP 대비 중앙은행 발행 디지털통화량을 줄이거나(늘리거나) 또는 정책금리와의 스프레드를 늘림으로써(줄임으로써) 경기역행적(counter-cyclical) 수단으로 사용할 수 있다.

그런데 추가적인 통화정책 도구로서의 효과성은 다음과 같은 요인들에 의해 결정된다.

① 충격의 성질: 통화거래 잔액의 양이나 가격의 관리가 해당 잔액의 수급에 영향을 주는 충격에 대한 반응일 때 효과적

② 다른 유형의 통화거래 잔액과의 대체성: 은행예금이 중앙은행 발행 디지털통화를 쉽게 대체할 수 없을 때 효과적

③ 재정정책과의 상호연관성: 중앙은행 발행 디지털통화의 발행이나 회수의 예산에 대한 영향이 세율이나 정부지출의 경기역행적 변화를 초래하지 않을 때 효과적

(나) Rogoff(2014), Dyson and Hodgson(2016)

실물화폐(physical cash)가 존재하는 한 음의 금리정책을 수행하기가 어려운데(Zero Lower Bound Constraint), 중앙은행은 실물화폐 대신에 디지털통화를 발행함으로써 음(-)의 금리에서도 전통적인 통화정책을 운영할 수 있다. 현금통화는 디플레이션의 압박 하에서 중앙은행이 음(-)의 금리정책을 수행하는 것을 어렵게 만든다. 일반적으로 현금을 보유하는 것(hoarding cash)은 불편할 뿐만 아니라 위험한데, 금리가 음이 될수록 보유할만한 가치가 커진다. 중앙은행의 모든 부채가 전자적인 것으로만 구성된다면 지준(reserve)에 대해 음의 이자를 지급하는 것(실질적으로 수수료를 부과하는 것)은 쉽다.

(2) 양적완화 정책 수행 시 보다 효과적

(가) Barrdear and Kumhof(2016)

현 체제에서 중앙은행은 상업은행을 통해서만 양적완화를 수행할 수 있다. 즉 중앙은행이 중앙은행의 지준을 이용하여 민간부문의 자산을 취득하기 위해서는 상업은행의 중개를 필요로 하며 이 과정에서 상업은행의 대차대조표의 금액이 증가하게 된다. 만약 상업은행들이 양적 완화에 의해 자신들의 대차대조표 금액이 늘어나는 것을 상쇄하려는 다른 의도가 있다면 해당 정책의 실효성이 떨어질 수밖에 없다. 그러나 중앙은행 발행 디지털통화에 의한 자산 취득은 자산과 중앙은행 돈의 직접적인 교환에 의해 이루어지므로 상업은행의 관여를 필요로 하지 않는다. 따라서 이 경우 양적완화 정책이 보다 더 실효성을 가질 수 있다.[97]

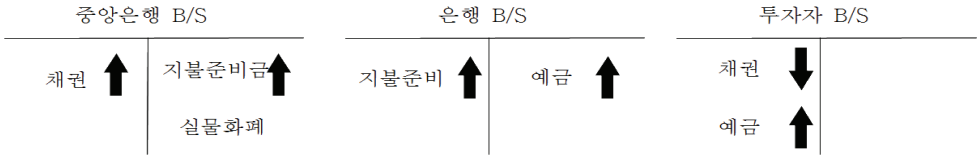
(나) Dyson and Hodgson(2016)

양적완화는 채권이나 주식과 같은 금융자산의 취득을 통해 이루어지기 때문에 금융자산 가격의 상승을 유발하고, 일반 대중들보다는 일부 부유한 자산가들에게만 유리해서, 실제 총수요를 증가시키는데 한계가 있다.

---

97) Sunil(2016)에 의하면 인도의 경우 현재 은행시스템 하에서는 중앙은행이 리포금리를 125bp 내릴 때 상업은행들은 고객들에게 60bp만을 내린다고 한다.

<그림 5-7> 현행 양적완화 통화정책의 한계



만약 '헬리콥터 머니'가 가능하다면 국민들의 소비를 증가시키거나 부채상환을 가능케 할 수 있다. 그러나 '헬리콥터 머니' 방식을 사용하기 위해서는 중앙은행에게 화폐를 분배할 수 있는 배분통로가 필요한데, 현재 시스템에서는 곤란하고 디지털통화시스템이 필요하다. 따라서 중앙은행 발행 디지털통화는 '헬리콥터 머니'와 같은 새로운 통화정책 수단의 사용을 가능하게 한다.

(3) 실물화폐의 자연적 감소에 대비

만약 신용카드나 직불카드가 실물화폐를 완전히 대체한다면, 실제 사용할 수 있는 화폐는 은행예금밖에 남지 않는데, 이러한 추세가 실제로 가속화되는 상황에서 중앙은행은 디지털통화를 발행할 필요성이 커진다.

나. 부정적 영향

(1) 새로운 통화정책 체제로의 전환 리스크

중앙은행이 디지털통화를 발행하면서 새로운 통화정책 체제로 전환할 경우 발생할 수 있는 리스크에 대한 적절한 관리가 요망된다. 예를 들어 중앙은행 발행 디지털통화의 이용증가로 현금뿐만 아니라 상업은행 예금이 감소할 경우 상업은행의 지준 규모에 영향을 주기 때문에 은행의 신용창출과 통화량에 영향을 미치게 되는데 아직까지 이런 영향이 불확실하다. 또한 상업은행의 지준감소로 결제자금이 부족해져 유동성 리스크가 발생하고 시장금리가 상승하는 등 새로운 리스크가 발생할 가능성이 생긴다.

(2) 현금수요의 감소 가능성

중앙은행 발행 디지털통화의 결제편의성, 현금의 보관 및 소지에 따른 불편

성, 은행의 현금교환 시 수수료 부과 가능성 등을 고려할 때 장기적으로 현금수요가 감소할 가능성이 있다.

(3) 신규 통화창출의 축소

은행대출의 경우에는 차입자의 신규예금을 의미하기 때문에 신규 통화창출이 이루어지는 반면, P2P 대출의 경우 한 사람의 예금계좌에서 다른 사람의 예금계좌로 단순히 이전하는 것이기 때문에 신규 통화창출이 없다.

(4) 신용창출 축소 가능성

디지털통화 계좌 제공자들이 등장하더라도 이들이 고객의 디지털통화를 대출에 사용할 수 없기 때문에 당분간 은행 대출영업에 대한 영향은 없을 것으로 예상된다. 그러나 고객의 허락을 얻고 법이 허용한다면 고객의 디지털통화를 자금원으로 하여 이들도 대출을 할 수 있을 것이다.

지준은 위험가중치가 0%이기 때문에 은행예금의 디지털통화로의 대체는 자본요구량에 변화가 없고 따라서 이에 따른 신용공급의 변화는 없을 것으로 예상할 수 있다. 그리고 실제로 지준 수준에 따라 신용창출이 이루어지는 것이 아니라 손실흡수 자본량에 따라 신용창출이 이루어지기 때문에 디지털통화의 발행으로 인한 은행의 지준 감소는 은행의 신용창출에 영향을 미치지 않을 것으로 보인다.

현재 은행시스템에서는 은행의 대출 시 대출금만큼 지준이 줄지 않는데 해당 대출금이 다른 은행들을 거쳐 다시 해당 은행으로 예금됨에 따라 지준이 늘어날 수 있기 때문이다. 따라서 실제 지불해야 하는 지준은 해당 대출금의 일부에 해당하게 된다. 그런데 만약 은행 대출 시 차입자가 은행이 아닌 디지털통화 계좌 서비스업체에게 지불한다면 전체 지급금액에 해당하는 지준이 줄기 때문에, 결과적으로 부족한 지준을 빌려야 하는 문제가 발생할 수 있다. 때문에 대출비용이 증가하여 신용창출이 줄어들 여지가 있다(물론 반대로 디지털통화 보유자가 은행계좌로 오는 경우에는 지준이 늘어난다). 장기적으로 은행신용이 계속 공급되면서 동시에 디지털통화 서비스업체들로부터 신용공급이 동시에 이루어진다면 오히려 신용공급은 증가할 것이다.

6. 금융안정에 미치는 영향

가. 긍정적 영향

(1) 금융시장의 리스크 감소

현재 일반 소비자들은 은행계좌를 통해서만 전자적으로 현금 지급결제를 할 수 있다. 그런데 은행들은 예금을 이용해서 리스크가 있는 대출을 시행하기 때문에 예금은 리스크에 노출될 수밖에 없는 구조이다. 그러나 중앙은행이 대중들에게 디지털통화를 발행하면 이는 정부에 의해 보증되기 때문에 전혀 리스크가 없으며, 대중들은 은행의 도움이 없이도 전자지급결제시스템에 직접 연결될 수 있다.

(2) 은행의 도덕적 해이 문제 해결

현재 예금보험제도는 은행들의 잘못에 대해 정부가 대신 책임지는 구조이고, 공공정책을 수행하는 은행들의 도덕적 해이 문제는 심각한 문제가 아닐 수 없다. 중앙은행 발행 디지털통화에 대해서는 정부가 보증을 설 이유도 없고 손해보는 일도 없다. 또한 예금보험제도의 혜택을 받을 수 없는 연금이나 보험사 등의 경우에도 중앙은행 발행 디지털통화를 사용해서 직접 결제할 수 있기 때문에 전체 금융시장의 유동성 리스크와 신용리스크를 감소시킬 수 있다.

(3) 거래상대방 신용리스크의 감소

분산원장에 기반한 중앙은행 디지털통화가 결제에 이용될 때 지급결제가 안전하게 될 뿐만 아니라 거래당사자간에 직접적인 거래가 가능하게 되고, 금융시스템은 훨씬 더 적은 수의 거래상대방으로 운영될 수 있기 때문에 중앙은행이나 감독기구는 주요 금융기관들의 거래상대방 신용노출(counterparty credit exposure)에 대한 가시성 결여의 문제를 해결할 수 있다. 따라서 이 경우 해당 리스크에 대비한 담보의 필요성이 없어지게 되므로 양질의 담보부족으로 인해 발생하는 문제를 없앨 수 있어 거시경제적인 안

정과 금융안정에 상당한 기여를 할 수 있다. 특히 분산원장 기술은 실시간으로 컴플라이언스에 대한 모니터링을 가능하게 만들기 때문에 거래당사자들의 담보소유 현황과 재담보 현황을 실시간으로 파악할 수 있도록 해 준다.

(4) 시스템 운영 효율성 제고

현 체제하에서 중앙은행은 시스템의 유지보수를 위하여 운영시간을 일정시간으로 제한하고 있기 때문에 은행들은 거래상대방 리스크에 노출되게 된다. 그러나 분산화된 지급결제시스템에서는 전체 시스템의 운영에 어떤 거래증명자도 별다른 영향을 미칠 수 없기 때문에 유지보수를 위한 시스템의 중단이 불필요하다.

(5) 그림자금융의 안정성과 건전성의 개선

정책당국은 점점 더 중요성이 커지고 있는 예금수신기관 밖에서 작동하는 자본시장(그림자 금융)의 유동성에 영향을 끼칠 수 있는 새로운 도구를 확보할 수 있어야 하는데, 분산원장에 기반한 중앙은행 디지털통화는 이를 파악하는데 도움을 줄 수 있다.

나. 부정적 영향

(1) 상업은행의 자금 수급구조 불안정성 증가

(가) Dyson and Hodgson(2016)

은행예금과 중앙은행 발행 디지털통화는 전자적으로 사용되고 결제된다는 점에서 완전 대체제이기 때문에 은행의 지급결제서비스에 경쟁체제가 도입되는 것을 의미한다. 상업은행들은 최선의 지급서비스를 고객에게 제공하기 위해 디지털통화 계좌 제공자와 경쟁을 해야 한다. 그러나 상업은행은 예금을 기반으로 수익성 높은 대출을 할 수 있는 반면, 디지털통화 계좌 제공자들은 그럴 수 없고 또한 디지털통화 계좌 제공자는 고객에게 서비스 수수료를 부담시켜야 하는 불리한 입장이다. 그러나 은행예금은 신용리스크에 노출

되는 반면, 디지털통화계좌의 경우 100% 안전하고 고객이 원하는 새로운 서비스를 개발 제공할 수 있는 장점이 있다.

(나) Broadbent(2016)

상업은행의 경우 디지털통화로의 자금유출로 예금이 감소하면 대출재원 부족에 따라 자금중개기능이 위축되고, 시장성수신 및 기관자금 의존도 심화로 인해 자금조달의 안정성이 약화되는 등 자금 수급구조상 불안정성이 커질 가능성이 있다.

(2) 상업은행 차입이자율의 상승

중앙은행 디지털통화의 발행 시 소매거래 잔액의 상당 부분이 은행예금으로부터 중앙은행발행 디지털통화로 전환될 것으로 예상되기 때문에, 은행들이 높은 이자율의 도매금융에 더욱 의존하게 되고 고객 유치를 위한 다양한 혜택을 제공해야 하는 등 은행의 수익성이 악화될 가능성이 높다.

Barrdear and Kumhof(2016)는 중앙은행 발행 디지털통화 도입 시 양적 규율(quantity rule) 하에서 중앙은행은 수요증가에 대해 통화의 양을 늘리기보다는 대신 민간 부문이 요구하는 이자율을 낮추도록 함으로써 시장이 청산되도록 하는 방법을 제안하고 있다. 이때 중앙은행 발행 디지털통화에 대한 이자율이 음이 될 가능성을 포함하여 어느 정도 움직일지는 은행예금과의 대체 탄력성과 상대적 선호 충격의 크기에 따라 달라질 것이다. 또한 그들은 중앙은행 발행 디지털통화 시장의 가격발견 메커니즘이 충분히 융통성을 갖도록 함으로써 은행의 예금금리가 너무 변하지 않도록 하는 것이 필요하다고 한다.

한편, 가격 규율(price rule) 하에서 중앙은행은 중앙은행 발행 디지털통화에 대한 이자율을 정하고 대신 민간 부문이 통화량을 결정하도록 하는데 이때 발행방식을 어떻게 하느냐가 관건이 된다. 그들은 중앙은행이 오직 국채를 사는 방식으로 중앙은행 디지털통화를 발행하는 것으로 가정하고 다음의 두 가지 시나리오를 제시하고 있다. 만약 중앙은행이 디지털통화를 은행에 직접 공급하지 않는다면, 은행예금을 디지털 통화로 바꾸기 원하는 민간 부문은

국채를 사서 중앙은행에 줘야 하는데, 이때 예금은 전체 은행시스템을 떠나는 게 아니라 국채 매도자로 이전할 뿐이기 때문에 은행의 자금조달 비용은 크게 변하지 않을 것이다. 만약 중앙은행이 디지털통화를 은행에 직접 공급한다면, 예금보유자는 은행과 직접 교환할 것이기 때문에 예금에 의한 자금조달은 줄지만 은행의 전체 자금조달은 줄지 않는다. 이때 중앙은행에 의한 자금조달이 정책금리에 의해 이루어진다면 은행의 평균 조달비용은 상승할 수 있지만 정책금리보다 낮은 금리의 은행예금에 의해서 계속 자금을 조달할 수 있으므로 크게 상승하지는 않을 것으로 전망하고 있다.

(3) 평상 시 유동성비율의 감소와 금융위기 시 뱅크런 가속화 가능성

평상시 상황에서 은행예금의 디지털통화로의 전환은 예금의 감소를 의미하기 때문에 상업은행의 경우 결제자금의 부족에 따른 유동성리스크가 커질 수 있다. 이때 예금의 감소는 지준의 감소를 동반하기 때문에 자본계정과 자본요구량에는 영향을 주지 않을 것으로 보인다. 그러나 지준의 감소로 인해 유동성 비율(지준/예금)이 하락하는 일이 발생할 수 있는데, 이때 중앙은행은 은행으로부터 채권을 매수하여 지준을 공급함으로써 문제를 해결할 수 있다. 또한 금융위기 시에 디지털통화의 존재는 은행들의 부도 사태(Bank runs)를 가속화시킬 수 있는데 상업은행 예금은 건전성규제, 예금보험제도 등이 있어 금융시스템 전반에 뱅크런이 발생할 위험은 크지 않을 것으로 예상된다.

7. 지급결제에 미치는 영향

가. 긍정적 영향

(1) 지급결제시스템에서의 경쟁과 혁신의 증진

디지털통화를 모든 국민에게 발행함으로써 중앙은행은 새로운 기업들이 은행을 통하지 않고 지급결제 계좌와 서비스를 제공할 수 있도록 하여 은행과의 경쟁을 촉진시킬 수 있다. 중앙은행 디지털통화에 자동이체나 온오프라인 간편결제 지원 기능이나 서비스가 보강될 경우 경쟁은 더욱 촉진될 것이다.

(2) 지급결제시스템의 안정성 제고

새로운 기업들이 디지털통화계좌에 있는 중앙은행 통화를 사용해서 직접 결제를 할 수 있기 때문에 일부 은행들의 부도나 기술적 실패 시에도 지급결제시스템에 문제가 생기지 않을 뿐만 아니라 기존 대형 금융기관에 집중된 결제리스크를 크게 완화할 수 있다. 또한 금융기관 간 거래의 복잡한 상호연계성을 쉽게 파악할 수 있어 지급결제시스템의 복원력을 높일 가능성이 커질 것으로 예상된다.

(3) 결제효율성 증가

기존 예금과는 달리 계층화된 중앙집중형 지급결제시스템에 의존하지 않기 때문에 기술적인 측면에서 결제효율성이 높아질 수 있다. 또한 영국의 거액결제시스템(CHAPS)에서와 같이 계층화된 참가구조 하에서 간접참가기관은 직접참가기관에 비싼 수수료를 지불하는 대신 중앙은행 발행 디지털통화를 통해 거래할 유인이 커진다.

나. 부정적 영향

(1) 시스템의 안정성 및 보안성에 대한 검증 불가능

중앙은행과 소수의 거래검증기관 중심으로 운영되는 제한적인 분산원장 방식에서는 시스템의 안정성과 보안성을 확보하는 것이 매우 중요한데, 아직까지 분산원장 기반의 중앙은행 디지털통화가 발행된 사례가 없어 시스템의 안정성과 보안성에 대한 검증이 불가능한 상황이다.

(2) 잠재적 리스크의 존재

현 시스템은 회원은행이 일시적으로 또는 영원히 그 기능을 멈출 때 중앙은행으로 하여금 운영리스크와 그와 관련된 평판리스크에 직면하도록 만드나, 분산원장 시스템은 어떤 한 거래증명자라도 모든 거래에 대해 그 타당성을 확인해 줄 수 있는 설계로 인해 이러한 위험으로부터 안전하다고 할 수

있다. 그렇지만 중앙은행 발행 디지털통화가 중앙집중화된 기술로 만들어진다면 사이버 공격이라는 훨씬 더 큰 리스크에 노출될 수도 있다.

8. 해외사례 분석

가. 영란은행

영란은행은 전 세계 중앙은행 중에서 분산원장 기술 기반 디지털통화 발행과 관련하여 가장 적극적인 연구와 논의를 진행하고 있다. 2015년 2월 금융환경 및 제도변화, 기술혁신 등에 대응한 중장기 정책방향 설정을 위한 조사연구 비망록에서 디지털통화 발행을 주요 검토과제로 설정한 바 있다.

(1) Barrdear and Kumhof(2016) 연구모형

2016년 7월에 발표된 Barrdear and Kumhof(2016)의 연구자료에서는 분산원장 기술에 기반 하여 GDP의 30%에 해당하는 금액만큼 중앙은행 디지털통화를 발행하여 국채를 인수한다면 실질이자율, 세금왜곡 및 통화거래비용의 감소로 인해 장기 균형 GDP를 최대 3% 영속적으로 증가시킬 것으로 전망하였다. 또한 그들은 중앙은행이 디지털통화 발행량과 금리 조절을 새로운 정책수단으로 활용하여 경기사이클을 안정시키는 역량을 크게 개선할 수 있다고 보고하였다.

그들은 전통적인 동태확률 일반균형모형(DSGE model)을 글로벌 금융위기 이전의 미국경제에 적용하였으며, 중앙은행 발행 디지털통화가 은행예금의 불완전한 대체재이고, Jakab and Kumhof(2015)에서처럼 은행예금이 여신이나 자산 취득을 통해 만들어진다고 가정하였다. 그들은 중앙은행 발행 디지털통화를 '중앙은행이 허용하는, 보편적이고, 전자적이고, 24×7의, 국가통화기반의, 이자를 지급하는 중앙은행 당좌계정'[98]으로 정의하였다. 대부분의 거래잔액은 상업은행의 예금 형태로 유지되고, 현재의 예금보호장치가 필요 시 적용된다고 가정하였다. 또한 신용공급은 현재 금융기관의 권한 아래에 그대로 존속하고, 상업은행은 여전히 화폐의 한계 단위 제공자의 역할을 수행한

98) central bank granting universal, electronic, 24×7, national-currency-denominated and interest-bearing access to its balance sheet

다. 중앙은행 발행 디지털통화의 운영을 위해 분산원장의 사용이 반드시 필요한 것은 아니지만, 경제의 재무안정성에 절대적으로 중요한 시스템의 탄력성(Resiliency)을 보장하기 위해 필요하다고 가정하였다. 중앙은행의 정책수단으로 첫째, 발행 디지털통화에 대해 지급하는 이자율을 설정하고, 민간부문으로 하여금 잘 정의된 자산을 대가로 중앙은행 발행 디지털통화를 얼마나 사거나 팔지를 결정하도록 하는 것과 둘째, 디지털통화 발행량을 정하고 민간부문으로 하여금 시장이 청산될 때까지 중앙은행 발행 디지털통화에 대한 이자율을 올리거나 내리게 하는 두 가지를 상정하였다.

(2) RSCoin(Danezis and Meiklejohn, 2016)

2016년 2월 런던대학의 Danezis and Meiklejohn는 비트코인과 유사한 암호화화폐로서 분산원장 기술을 활용하여 중앙은행이 발행하고 관리할 수 있는 디지털통화인 RSCoin을 발표하였다. 이는 거래원장의 유지관리로부터 통화공급의 창출을 분리한 암호화화폐 프레임워크에 해당한다.

(가) 장점

RSCoin의 장점으로는 통화정책을 투명하게 만들고, 지급 및 가치 이전 수단에 대해 직접적인 접근을 가능하게 하고, 익명성을 보장하고, 분산원장 및 디지털통화의 혁신적 사용으로부터 이익을 창출할 수 있다는 것을 들 수 있다.

(나) 확장성(scalability) 문제의 해결

중앙은행은 거래를 확인하는 권한인 민테트(mintettes)를 기관들에 위임하고, 민테트를 받은 기관들은 비트코인의 채굴자들과는 달리 알려지고 궁극적으로 잘못된 행동에 대해 책임을 질 수 있기 때문에, RSCoin은 이중지불 감지를 위한 간단하고 빠른 메커니즘을 지원할 수 있다. 이러한 민테트의 역할은 실제 중앙은행과 연결되어 있는 상업은행이 맡을 수 있다.

(다) 채굴자들의 도덕적 해이 문제 해결

채굴자들은 그들이 담고 있는 모든 거래를 완전히 확인하지 않고 블록을 생성할 인센티브가 존재하는데, 양질의 서비스를 제공하는 민테트들은 그 대가로 수수료를 받고, 불량하거나 게으른 민테트들은 받지 못하도록 하는 것이다.

(라) 중앙은행들간의 상호운영성(interoperability) 문제 해결

이종 통화 간 교환의 투명성과 감사가능성, 안전이나 지정학적인 이유 등에 의해 서로 지지하지 않는 중앙은행들간의 문제 등을 해결할 수 있다.

<그림 5-8> RSCoin의 구조

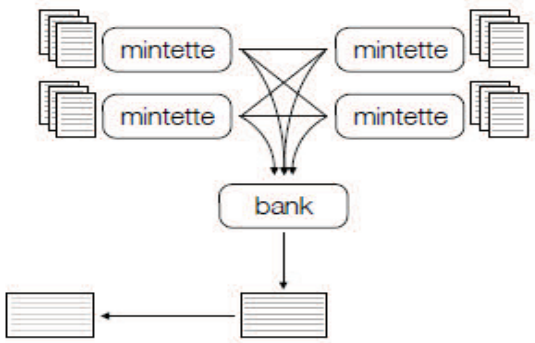


Fig. 1: The overall structure of RSCoin. Each mintettes maintains a set of lower-level blocks, and (possibly) communicates with other mintettes (either directly or indirectly). At some point, the mintettes send these blocks to the central bank, which produces a higher-level block. It is these higher-level blocks that form a chain and that are visible to external users.

<그림 5-8>은 RSCoin의 기본 구조를 설명하는 그림이다. 중앙은행은 민테트들에게 PKI-형태 기능성(민테트의 공개키 서명)의 권한을 부여하고, 낮은 수준의 블록은 이런 서명 중 하나를 포함할 때 타당한 것으로 간주된다. 민테트들에 의해서 블록이 생성되는 시간 구간을 epoch라 하고, 이들은 주 분산원장에 포함되지 않기 때문에 낮은 수준의 블록이라고 한다. period라고 불리는 미리 정해진 시간 구간 끝에 민테트들은 그들의 블록을 중앙은행에 제공하게 되고, 중앙은행은 이들을 합해서 새로운 블록의 형태로 일관된 기

록을 형성하게 된다. 이러한 높은 수준의 블록만이 주 분산원장에 통합되기 때문에 RSCoin의 사용자는 높은 수준의 블록만 추적하고 있으면 된다. 이와 같이 RSCoin은 2단계 실행(Two-Phase Commit)의 변종 방식으로서 2층 구조의 분산원장 방식(Factom)과 상호합의 메커니즘(Certificate Transparency)을 주요 특징으로 한다.

나. 중국인민은행

중국인민은행은 2014년 디지털화폐연구팀을 설립하여 2015년 초부터 디지털통화의 핵심기술, 발행 및 유통환경, 관련 법률문제 등을 연구하기 시작한 것으로 알려져 있다. 인민은행은 2016년 1월 20일 개최한 디지털화폐 세미나에서 향후 중앙은행 주도로 디지털통화 발행을 추진할 것이라고 발표하였다. 인민은행은 분산원장 등 지급결제 관련 기술진보와 경제발전에 따라 디지털통화가 개발되는 것은 자연스러운 현상이나 보안 및 인증 관련 기술적 문제와 자유태환 등의 문제점을 해결해야 할 것이라고 강조하였다.

인민은행은 디지털통화 발행을 통해 실물화폐 발행 및 유통비용 절감, 지급결제시스템의 효율성 개선, 경제 거래활동의 편리성과 투명성 제고, 탈세 및 자금세탁 방지, 통화관리능력 강화, 금융포용 촉진 등을 도모할 수 있을 것으로 기대하고 있다. 그러나 인민은행의 디지털통화 발행 목적에 대해서는 대내외적으로 의견 차이가 있다. 금융권에서는 2015년 중 3차례의 금리인하와 위안화 가치절하에 따른 해외 자본유출 및 환율 불안정을 해결하기 위한 방편으로 보는 경향이 강하다. 특히 2015년 3월 당시 시점으로 중국내 비트코인 거래량이 전 세계 거래량의 80%에 달한 점은 환율정책의 불안요소에 대한 대응방안으로 중국 당국이 디지털통화의 발행을 고려하게 된 직접적인 원인이라는 시각도 있다. 디지털통화 도입 시 투기자본의 유출입 동향 파악이 용이하기 때문에 중앙은행이 위안화 가치하락과 국외 자본유출에 적극적으로 대응할 수 있기 때문이다.

다. 캐나다 중앙은행

캐나다 중앙은행은 디지털통화 관련 연구를 활발히 진행하고 있으며 2016년 6월 캐나다 지급결제 컨퍼런스에서 자국 내 대형은행들과 제휴를 통해

분산원장 기술 기반 디지털통화인 CAD-COIN의 개발을 추진하고 있는 것으로 보도되었다.[99] 캐나다 중앙은행의 수석부총재인 Carolyn Wilkins는 "중앙은행의 여러 핀테크 관련 연구 프로젝트 중의 하나로 지급결제 캐나다, R3, 캐나다은행들과 함께 분산원장을 활용하여 은행 간 지급결제시스템 POC를 진행 중이다"리고 하였다. 그는 "이번 프로젝트의 목표는 먼저 기술을 이해하는 것이다. 그러한 시스템이 실제로 사용되기 위해서는 먼저 해결해야 할 장애물들이 아직 많다. 우리의 실험 중에는 일반인들에 대한 중앙은행 발행 디지털통화 계획은 들어 있지 않다. 이는 아직까지 많은 중앙은행들이 검토하고 있는 개념적인 연구주제일 뿐이다."라고 강조했다.

첫 번째 프로젝트는 가상환경에서 국가 통화를 발행하고, 해당 분산원장 회원들인 은행들 간 거래에서 이를 사용하고, 가상환경에서 직접 지급결제를 수행할 수 있는 능력을 시험해 보는 것이다. 현재도 가상환경에서 주식이나 부동산 권리증 등을 거래할 수 있지만 언젠가는 거래당사자들이 가상환경에서 나와 (원장 밖에서) 실제 돈을 이체하여야 한다. 이번 실험을 통해 우리는 분산원장에서 가치를 실제 이체할 수 있도록 만드는 것이다.

재스퍼 분산원장 결제 플랫폼(Jasper Distributed Ledger Settlement Platform)의 프로세스는 다음과 같다. 먼저 플랫폼에 참가하는 자는 현금담보를 중앙은행의 특별계좌에 저당물로 잡힌다. 그러면 중앙은행은 해당 가치를 CAD-CAIN으로 전환해서 해당 참가자의 계좌로 전달한다. 회원 승인을 먼저 받아야 하는 네트워크의 회원들은 CAD-COIN을 서로 교환하며, 만약 다른 통화로 교환하고자 할 때에는 CAD-COIN을 주고 현금담보물을 받을 수 있다. 중앙은행은 해당 CAD-COIN만큼 파괴함으로써 프로세스가 종결된다. 캐나다 중앙은행은 먼저 대형은행들과 공동으로 실험을 진행 중이지만 이는 궁극적으로 CAD-COIN은 진정한 의미의 중앙은행 발행 디지털통화가 될 것으로 예상된다.

라. 호주 중앙은행

호주 중앙은행인 호주연방은행도 디지털통화 연구에 박차를 가하고 있다.

99) Shin, Laura, "Canada has been experimenting with a digital fiat currency called CAD-COIN," Personal Finance, June 16, 2016.

호주연방은행은 2015년 리플랩스(Ripple Labs)와 제휴를 맺고 Ripple Coin을 도입하고 분산원장 기술 연구에 박차를 가하고 있다. 호주연방은행의 최고정보관리책임자 Whitening은 디지털통화와 분산원장 기술을 미래의 수단이라고 일컫고 분산원장 기술을 결제 인프라에 적용할 계획이라고 밝혔다.

마. 기타 국가

러시아 중앙은행은 2016년 4월 분산원장 기술 기반의 중앙은행 디지털통화 발행 가능성을 언급하였으며 네덜란드 중앙은행은 2016년 6월 자체 개발한 디지털통화인 DNBCoin을 여러 조건 하에서 시뮬레이션 중이라 밝혔다.

9. 소 결

2009년 비트코인을 필두로 민간 가상통화가 다수 등장하면서 최근 각국 중앙은행들은 분산원장 기술을 기반으로 디지털통화를 직접 발행하는 방안에 대해 활발한 논의와 연구를 진행 중이다. 특히 BIS(2015)와 영란은행은 민간 가상통화의 성장으로 중앙은행의 역할이 축소될 가능성에 대비하여 분산원장 기술 기반 중앙은행 디지털통화를 발행할 필요성을 제기하고 있다.

중앙은행 발행 디지털통화는 단순히 실물화폐를 대체하는 수준을 넘어 기존 상업은행 예금과 경쟁하면서 거시경제, 통화정책, 금융안정성 및 지급결제에 광범위한 영향을 미칠 수 있음을 살펴보았다. 그런데 상업은행 예금을 대체하는 규모는 다양한 결제기능 부여정도, 익명성 보장여부 및 이자지급여부 등에 따라 상이할 것으로 예상된다. 중앙은행 발행 디지털통화가 단순한 자금이체 기능뿐만 아니라 상업은행 예금계좌와 같이 상거래 대금결제, 자동이체 등 다양한 결제기능을 제공한다면 상업은행 예금을 상당폭 대체할 수 있을 것으로 예상된다. 익명성 보장여부와 정부나 사법당국의 거래주체 확인 요구 시 허용여부 등에 따라서도 대체 정도가 달라질 것으로 예상된다. 또한 디지털통화에 대한 이자지급여부도 영향을 미칠 것으로 보이는데, 만약 디지털통화에도 이자를 지급한다면 중앙은행이나 정부의 추가적인 부담이 되고, 지준금리가 은행예금 금리보다 높으면 은행예금이 디지털통화로 대체될 가능성이 커질 것이기 때문에 이를 신중히 검토해야 할 것이다.

그런데 아직까지 분산원장 기술 기반의 중앙은행 디지털통화가 발행된 사례가 없기 때문에 시스템의 안정성 및 보안성에 대한 검증이 불가능한 상황이다. 주요국 중앙은행의 개발 사례를 지속적으로 모니터링하면서 분산원장 기술 기반 중앙은행 디지털통화 발행을 위한 기술을 검증하고 안정성을 확보하기 위한 연구와 개발을 계속 추진해야 한다. 이때 중앙은행 발행 디지털통화의 기능, 발행대상 및 발행방식 등에 대한 다양한 시나리오 하에서 다양한 기술을 비교 검토할 필요가 있다.

중앙은행 발행 디지털통화는 완전히 새로운 형태의 화폐로서 기존의 법, 제도, 기술 등으로 포괄하지 못하거나 상충될 수 있기 때문에 이에 대한 다각적인 연구가 장기적으로 수행될 필요가 있다.

VI. 결 론

분산원장 기술로 인한 편익을 추정한 기존의 연구들을 보면, 정교한 정량적 분석이라기보다는 기술로 인한 비용절감 측면만을 대략적으로 추정한 정도이다. 이중 자본시장(Capital Market)의 경우는 후선업무(Back office) 기능이 제3의 기관의 비용으로 구분되어 있어 비용의 추정 및 예측이 어느 정도 가능하나, 자본시장을 제외한 금융기관들은 서비스가 광범위하고 프로세스의 구획 및 비용이 명확히 구분되지 않아 분산원장 기술의 도입에 따른 비용감소 측정이 어려운 현실이다.

보다 명확한 정량적 평가를 위해서는 국내 각 금융기관들에서 시행중인 POC(Proof Of Concept)를 고려하여 분산원장 기술을 적용할 때 각 서비스별로 금융기관 비용변수와 금융소비자의 비용변수를 구별하여 측정할 필요가 있다. 본 연구에서는 "국제송금"과 "인증 서비스" 분야에 대해 금융기관의 비용과 금융소비자의 비용을 별개로 구분하여 분산원장 기술 도입에 따른 비용절감을 예측하는 방안을 제시하였는데, 이 같은 방법을 다른 분야에도 적용할 수 있을 것으로 기대한다. 향후 분산원장 기술 적용에 따른 편익과 비용감소를 정확하게 측정하기 위해서는 분산원장 플랫폼을 구축한 은행 및 금융기관들의 여러 업무(대출, 송금, 인증, 보험, 기업금융, 무역금융, 펀드판매 및 체결 등)를 각각 세분화하여 측정할 필요가 있다.

분산원장 기술은 금융서비스 디자인에 유연성을 제공할 수 있기 때문에 금융산업의 다양한 분야에서 활용될 수 있으며, 그 편익 역시 다양한 범위에서 발생하게 되는 만큼 전체 편익규모를 일률적으로 측정하는 것은 쉽지 않다. 아직까지 실용의 측면과 규제의 관점에서 검토되어야 할 부분이 있지만, 분산원장 기술은 금융서비스 관련 조정과정이나 데이터의 공유를 통해 자동적이면서 효과적인 비즈니스 운영을 가능하게 하여 비용을 크게 절감시키고, 금융시장 참가자들의 편익을 증진시킬 수 있을 것이다. 따라서 분산원장 기술이 금융인프라에 미치는 긍정적 효과를 확대시키기 위해서는 금융기관과 핀테크기업 그리고 규제기관의 이해와 깊은 협업이 필요하다. 현재의 작업관행과 개별 기관의 이익에만 집중하다가 기술발전의 편익을 간과해서는 안 될 것이다.

미국 FBI는 비트코인 등 디지털통화가 주조, 작동, 배분까지의 각 과정에서 맬웨어나 봇넷 등을 통해 쉽게 불법적인 송금이나 조작이 가능하기 때문에 불법적인 행위에 매우 취약하다는 점을 지적하고, 비트코인을 취급하는 서비스 기업에게 고객들의 신분증이나 은행 정보를 확인하도록 권고하고, 송금서비스 기업들은 FinCEN에 등록하고 자금세탁방지 프로그램을 의무적으로 설치하도록 권고하고 있다. 소비자를 범죄로부터 보호하고, 디지털통화가 범죄에 악용되는 것을 차단하면서도, 혁신적 창업자들의 혁신성과 창조성을 해치지 않는 한도 내에서 적절한 규제를 마련하여 시행하는 것이 필요하다.

이와 같은 맥락에서 미국 뉴욕 주를 선도로 많은 국가와 지방 정부가 디지털통화 사업자를 규제하는 움직임을 보이고 있는 것은 의미있는 일이다. 또한 IMF는 최근 보고서에서 현재 금융무결성, 탈세대책, 소비자보호 등에 대한 규정과 해석이 불분명하여 이를 명확히 할 필요가 있으며 디지털통화의 규제에는 국제공조가 중요함을 강조한 것 또한 의미가 있다.

그러나 새로운 기술의 혁신 속도에 맞추어 규제도 세심하고 유연하게 대응해야 하며, 장기적 관점에서 국제 표준 및 규제에 가장 적절한 지침을 제공할 수 있도록 모범사례를 개발하고 적용할 필요가 있다. 중요한 것은 지속적인 모니터링과 연구를 통해 기술 혁신에 따른 위험을 꾸준히 분석함으로써, 창조성이나 혁신성을 저해하지 않는 범위 내에서 적절한 규제로 응답하는 것이다. 특히 대형 금융기관이 아닌 소규모 신기술 창업자들이 규제 내에서 자유롭게 창업하면서 규제를 잘 준수할 수 있도록 규제 기술(RegTech)의 적극적인 도입을 통해 규제 보고와 관리를 자동화할 필요가 있다.

2009년 비트코인을 필두로 민간 가상통화가 다수 등장하면서 최근 각국 중앙은행들은 분산원장 기술을 기반으로 디지털통화를 직접 발행하는 방안에 대해 활발한 논의와 연구를 진행 중이다. 중앙은행 발행 디지털통화는 단순히 실물화폐를 대체하는 수준을 넘어 기존 상업은행 예금과 경쟁하면서 거시경제, 통화정책, 금융안정 및 지급결제에 광범위한 영향을 미칠 수 있음을 살펴보았다. 상업은행 예금을 대체하는 규모는 다양한 결제기능 부여정도, 익명성 보장여부 및 이자지급여부 등에 따라 상이할 것으로 예상된다. 중앙은행 발행 디지털통화가 단순한 자금이체 기능뿐만 아니라 상업은행 예금계좌와 같이 상거래 대금결제, 자동이체 등 다양한 결제기능을 제공한다면 상

업은행 예금을 상당 폭 대체할 것이고, 익명성 보장여부와 정부나 사법당국의 거래주체 확인요구 시 허용여부 등에 따라서도 대체 정도가 달라질 수 있다. 또한 디지털통화에 대한 이자지급여부도 영향을 미칠 것으로 보이는데, 만약 디지털통화에도 이자를 지급한다면 중앙은행이나 정부의 추가적인 부담이 되고, 지준금리가 은행예금 금리보다 높으면 은행예금이 디지털통화로 대체될 가능성이 커질 것이기 때문에 이에 대한 신중한 검토가 필요하다.

아직까지 분산원장 기술 기반의 중앙은행 디지털통화가 발행된 사례가 없기 때문에 시스템의 안정성 및 보완성에 대한 검증이 불가능한 상황이다. 주요국 중앙은행의 개발 사례를 지속적으로 모니터링하면서 분산원장 기술 기반 중앙은행 디지털통화 발행을 위한 기술을 검증하고 안정성을 확보하기 위한 연구와 개발을 계속 추진할 필요가 있다. 이때 중앙은행 발행 디지털통화의 기능, 발행대상 및 발행방식 등에 대한 다양한 시나리오 하에서 여러 기술을 비교 검토할 필요가 있다. 아울러 중앙은행 발행 디지털통화는 완전히 새로운 형태의 화폐로서 기존의 법, 제도 등으로 포괄하지 못하거나 상충될 수 있는 만큼 이에 대한 다각적인 연구가 꾸준히 이루어져야 할 것이다.

제1부 참고문헌

금융결제국, “분산원장 기술과 디지털통화의 현황 및 시사점,” 지급결제 조사자료, 2016.1.

금융결제원, “중국 인민은행, 디지털화폐 조기 발행 검토,” KFTC 지급결제동향 제257호, 2016.04.

백종찬, 한승환, 안상욱, 김영진, Chris Hong, 「블록체인기술의 발전과정과 이해」, 피넥터보고서 1권, 2016.8

백종찬, 한승환, 안상욱, 김태연, 「금융기관을 위한 블록체인의 이해」, 피넥터보고서 2권, 2016.9

신현규. “비트코인 화폐 아니다“…정부, 모니터링 강화키로. 매일경제. http://bit.ly/2egJVqz. 2016.10.17.

오광진, “중, 인민은행판 비트코인 발행으로 자본유출 대응…법정 디지털화폐 검토,” 조선비즈닷컴, 2016.1.22.

이병찬, “중국, 세계 첫 디지털화폐 발행국가 될까,” 머니투데이, 2016. 03.11.

피넥터. “블록체인 기술의 발전과정과 이해,” 「 피넥터 보고서」 2016/8.

Angela Watch, “The Bitcoin Blockchain as Financial Market Infrastructure: a Consideration of Operational Risk,” Legislation and Public Policy vol 18, NYU, 2015

Aggarwal, Sunil, “Central Banks Face 3 New Dilemmas in the Era of Bitcoin and Digital Currencies,” Bitcoin Magazine. May 25, 2016.

Barrdear, John and Michael Kumhof, “The Macroeconomics of Central Bank Issued Digital Currencies,” Staff Working Paper Series No. 605, Bank of England 2016.

BBC. “Bitcoin scam charges made against companies in US,” BBC News. http://bbc.in/1YJeT7p. 2016.10.17.

Bird, Mike, “HSBC says the Blockchain could be used for ‘Helicopter Money,” Business Insider, 2015-11.

BIS. Digital Currencies. BIS Committee on Payments and Market Structure Report. 2015/11.

Ben Dyson and Graham Hodgson, Digital Cash: Why Central Banks Should Start Issuing Electronic Money, PositiveMoney, 2016.1

Bohannon, John. “Why Criminals can’t hide behind Bitcoin,” AAAS. 2016.3.9.

Buterin, Vitalik. “FINCEN: Bitcoin Users Not Regulated,” Exchanges Are. Bitcoin Magazine. http://bit.ly/2dxxL9M. 2016.10.17.

Chiu, J. and T-N Wong, “E-money: Efficiency, Stability and Optimal Policy,” Bank of Canada, Working Paper, 2014-16. April.

Court of Justice of the European Union. Judgment in Case C-264/14. PRESS RELEASE No 128/15.

Committee on Payments and Market Infrastructures, "Digital Currencies," Bank for International Settlements, Nov. 2015.

Crosman, Penny, "The Anti-Bitcoin-A Centralized Digital Currency-Takes Root," Payment Source, May 19, 2016.

Cubrilovic, Nik. "Analyzing the FBI's Explanation of How They Located Silk Road." http://bit.ly/1w59fAz. 2018.10.17.

Del Castillo, M. "The DAO: Or How A Leaderless Ethereum Project Raised $50 Million," TechCrunch. 2016/10/17

Denezis, George and Sarah Meiklejohn, "Centrally Banked Cryptocurrencies," NDSS '16, 21-24 February 2016.

Dyson, Ben and Graham Hodgson, "Digital Cash, Why Central Banks Should Start Issuing Electronic Money," Positive Money, 2016.

Euroclear and Oliver Wyman, Blockchain in Capital Markets: The Prize and the Journey, 2016.2

EBA. "EBA warns consumers on virtual currencies." European Banking Authority(EBA). http://bit.ly/2evJnsV. 2016.10.17.

Eurosystem. VIRTUAL CURRENCY SCHEMES. European Central Bank. ISBN: 978-92-899-0862-7. 2012.10.

EY Global Financial Services Institute, "Trends in Cryptocurrencies and Blockchain Technologies: a Monetary Theory and Regulation Perspective," The Journal of Financial Perspectives: FinTech, Winter 2015, Vol 3- Issue 3.

EY Global Financial Services Institute, "Financial Regulation of Fintech," The Journal of Financial Perspectives: FinTech, Winter 2015, Vol 3- Issue 3.

EY Global Financial Services Institute, "FinTech in China: from the Shadows?" The Journal of Financial Perspectives: FinTech, Winter 2015, Vol 3- Issue 3.

Evry, Blockchain: Powering the Internet of Value, White Paper, 2015.12

FATF. Virtual Currencies Key Definitions and Potential AML/CFT Risks, FATF Report. June 2014.

FATF. Virtual Currencies: Guidance for a Risk-based Approach. FATF Report. June 2015.

FinCen. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. Aug. 2013.

Fung, Ben and Hanna Halaburda, "Understanding Platform-Based Digital Currencies," Bank of Canada Review, Spring 2014.

Gilson, David. "German government relieves capital gains tax on bitcoin positions." CoinDesk. http://bit.ly/2eIa9lH. 2016.10.17.

Gareth Lodge, Breaking the Payments Dam: External Forces Transforming the Payments Ecosystem, Celent, 2015.11

Goldman Sachs Global Investment Research, Profile in Innovation: Blockchain, Putting Theory into Practice, Equity Research, 2016.5

Government Office for Science, Distributed Ledger Technology: beyond blockchain, A Report by the UK Government Chief Scientific Adviser, 2015.12

Graydon, Carter. “How the FBI Likely Illegally Hacked Silk Road Servers to Find Alleged Pirate Ross Ulbricht.” http://bit.ly/2dmK2uH. 1016.10.17.

Greenburg, Andy. FBI’s Story of Finding Silk Road’s Server Sounds a Lot Like Hacking. Wired, http://bit.ly/2eo4GMM. 1016.10.17.

He, Dong, Karl Habermeier, Ross Leckow, and Vikram Haksar. Virtual Currencies and Beyond: Initial Consideration, International Monetary Fund, 2016.

Higgins, Stan. “ItBit Nets $25 Million, Launches NYDFS-Approved Bitcoin Exchange.” CoinDesk. http://bit.ly/1PsclE0. 2016.10.17.

Higgins, Stan. “Bitfinex Examined: Inside the Troubled Bitcoin Exchange’s History.” CoinDesk. http://bit.ly/2aJMeNj. 2016.10.17. 접속

HSBC, Getting Value from Blockchain, 2016.5

IBM, Blockchain: A new disruption in financial services?, 2016.7

John Barrdear and Michael Kumhof, “The macroeconomics of central bank issued digital currencies,” Staff Working Paper No. 605, Bank of England, 2016.7

J.P.Morgan and Oliver Wyman, Unlocking Economic Advantage with Blockchain: A guide for asset managers, 2016

Kiviat, Trevor, “Beyond bitcoin: Issues in regulating Blockchain Transactions,” Duke Law Journal, Vol.65, 2015

Ludwin, Adam, “Why Central Banks Will Issue Digital Currency?”, http://medium.com/chain-inc

Marc Rysman and Scott Schuh, “New Innovations in Payments”, Innovation Policy and the Economy, vol 17, NBER, 2016

Maras, Elliot, “Digital Currency Technology Nabs Investment, Makes Inroads with Central Banks,” CCN.LA, 2015.10.12.

Metz, Cade. “NY Backs Bitcoin Exchange. But It May Not Fly in California.” Wired. http://bit.ly/2dpIq3m. 2016.10.17.

Michael Mainelli and Alistair Milne, “The Impact and Potential of Blockchain on the Securities Transaction Lifecycle,” SWIFT Institute Working Paper No. 2015-007, SWIFT Institute, 2016.5

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

Nomura Research Institute, Survey on Blockchain Technologies and Related Services, FY2015 Report, 2016.3

Parker, Luke. “Mass Exodus of Bitcoin Exchanges from New York State Triggered by BitLicense Deadline.” BraveNewCoin. http://bit.ly/1HEt4PG. 2016.10.17.

Ponsford, Mattew, “A Comparative Analysis of Bitcoin and other Decentralized Virtual Currencies: Legal Regulation in the Republic of China, Canada, and the

United States," Jolt Digest, Harvard Journal of Law and Technology, Nov 14, 2015.

Reuters. "Two Bitcoin exchange operators charged in money laundering scheme." Reuters News. http://cbsn.ws/2eyhlAv. 2016.10.17.

Rogoff, Kenneth, "Costs and Benefits to phasing out Paper Currency," working paper presented at NBER Macroeconomics Conference, May 2014.

Spaven, Emily. "Germany officially recognises bitcoin as 'private money'." CoinDesk. http://bit.ly/1aYSGb0 2016.10.17.

Sharkey, Tom. "Denmark Declares Bitcoin Trades are Tax-Free." CoinDesk. http://bit.ly/1gWSOcw. 2016.10.17.

Shin, Laura, "Canada Has Been Experimenting with a Digital Fiat Currency called CAD-COIN," Personal Finance, June 16, 2016.

The Mainichi. "Japan looks to end sales tax on bitcoin in spring. Minichi Japan," The Mainichi News. http://bit.ly/2eapUT2. 2016.10.17.

US DISTRICT COURT DISTRICT OF CONNECTICUT. "SECURITIES AND EXCHANGE COMMISSION vs. HOMERO JOSHUA GARZA." http://bit.ly/2epGVTq. 2016.10.17.

UNSW Digital Financial Services Research Team, "Regulatory Handbook: The Enabling Regulation of Digital Financial Services," UNSW, Dec. 2015.

Wirdum, Aaron. "E.U. Representatives Clarify the Proposed Anti-Money Laundering Directive." Bitcoin Magazine. 2016.10.17.

World Economic Forum and Deloitte, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, Part of the Future of Financial Services Series, 2016.8

제2부. 기술적 이슈

Ⅰ. 블록체인 기술 개발 및 연구 현황

본 장은 주요 사례들을 중심으로 각 분야에서 현재 추진중인 블록체인 기술의 연구 및 개발 방향과 대표적인 활용 분야에 대해 서술한다.

1. 블록체인 컨소시엄

블록체인 컨소시엄은 블록체인에 대한 활용 방안을 찾고자 하는 기업 및 기관들이 블록체인을 연구하고 최종적으로는 여러 기업 및 기관들이 함께 사용할 수 있는 공동의 블록체인망을 개발하는 모임을 의미한다. 주로 블록체인 기술을 기반으로 하는 스타트업이 중심이 되고, 블록체인 시스템을 연구 또는 활용하고자 하는 기업들이 모이면서 구성된다. 최근에는 금융기관뿐 아니라 블록체인 활용 방안을 찾고자 하는 비금융기관들도 컨소시엄에 참여하는 추세이다. 블록체인은 기본적으로 분산형 네트워크이고 중앙의 통제자 대신 여러 서버가 노드를 담당하고 네트워크를 분할해서 운영하는 시스템이다. 따라서 특정 기업이 단독으로 개발해서 상용화하는 경우 오히려 블록체인 네트워크를 활성화하고 효율적으로 활용하는데 제약이 될 수 있으며, 많은 기업들이 블록체인 네트워크를 함께 구성해서 사용하는 것이 규모의 경제를 구축하고 블록체인의 효율성을 높이는데 더 적합하다. 이러한 이유로 많은 기업이 컨소시엄을 구성해 공동으로 활용할 수 있는 블록체인 플랫폼을 만들기 위해 연구하고 있다.

가. R3 CEV

블록체인 컨소시엄의 대표적인 사례 중 하나는 R3 CEV이다. R3 CEV 컨소시엄은 블록체인 기술 기업인 R3가 중심이 되어 은행 등 금융기관이 활용할 수 있는 블록체인을 연구 및 개발하는 것을 목표로 하는 컨소시엄으로 현재 60개 이상의 금융기관이 참여하여 연구를 진행하고 있다. 국내 은행 중에는 하나은행이 최초로 R3 CEV에 가입했으며[100], 신한은행, KB국민은행, 우리은행, IBK기업은행이 가입을 마무리했거나 진행중인 등 다른 국내 금융기관들도 참여에 관심을 보이고 있다.[101] R3 CEV의 가장 두드러진 성과는 지난 3월 금융 기관에 특화된 블록체인 서비스인 코다(Corda)를 개발하여 발표한

100) http://www.hanafn.com/pr/news/newsDetail.do?seq=3317&page=0
101) http://www.ddaily.co.kr/news/article.html?no=147909

것이다. 비트코인, 이더리움 등과 달리 유통되는 내부화폐가 없는 코다는 금융기관의 계약을 관리하고 기록하기 위해 만든 블록체인 플랫폼으로 블록체인의 특징인 분산화된 메커니즘을 유지하는 동시에 금융기관에서 활용하기 더 편리하도록 설계한 서비스이다. R3 CEV는 코다에 거래 당사자와 조정기관만이 거래 내역을 확인할 수 있는 정보 공개 권한 범위 설정, 합의 메커니즘의 다양화 및 스마트 계약(smart contract) 기능 등 기존 블록체인 대비 여러 기능을 추가 및 조정했다고 발표했다.[102] 이후 금융 기업 바클레이스와 함께 코다를 기반으로 한 스마트계약 탬플릿 시연회를 개최하기도 하는 등 금융기관용 블록체인 컨소시엄 가운데 가장 많은 협력 기업을 가지고 있고 대외적으로 많이 알려져 있다.[103]

<그림 1-1> 바클레이스와 시연한 코다 소개 영상

자료: Barclays

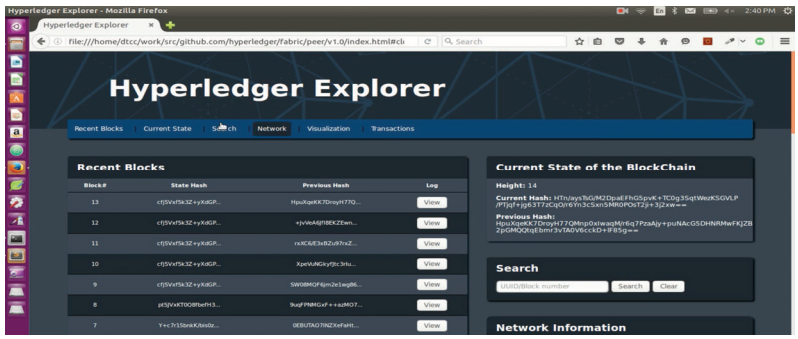
올해 10월 R3 CEV는 코다의 코드를 오픈소스화하여 11월 30일에 범산업 블록체인 컨소시엄인 하이퍼레저(Hyperledger)에게 제공한다고 발표했다. R3 측은 각 기관이 다른 블록체인 플랫폼을 만들어 각자가 섬처럼 소통할 수 없는 결과를 초래하지 않도록 표준화하는 방법으로 코다의 코드를 하이퍼레저에 제공하기로 결정했으며 코다가 금융산업 블록체인의 표준이 되기를 바란다고 밝혔다.[104]

102) http://www.coindesk.com/r3cev-blockchain-regulated-businesses/
103) https://www.youtube.com/watch?v=1UhrmsTZNvc
104) http://www.reuters.com/article/us-banks-blockchain-r3-exclusive-idUSKCN12K17E?feedType=RSS&feedName=technologyNews

나. 하이퍼레저 프로젝트 (Hyperledger Project)

R3 CEV가 금융기관이 활용할 수 있는 블록체인 구성을 목표로 결성된 컨소시엄이라면, 하이퍼레저 프로젝트(Hyperledger Project)는 비금융기관까지 참여해 공동으로 사용하는 범산업용 블록체인 플랫폼 구성을 목표로 하는 컨소시엄이다. 리눅스 재단(Linux Foundation)이 주도하는 오픈소스 블록체인 컨소시엄인 하이퍼레저 프로젝트에는 현재까지 100여개의 기업이 가입하였으며 인텔, IBM 등 대형 IT 기업, R3, 코인플러그 등 블록체인 기술 기업, JP모건 등 금융 기업 및 제조사, 컨설팅 업체 등 다양한 분야의 기업들이 참여하고 있다. 한국에서는 한국예탁결제원과 삼성SDS가 하이퍼레저 프로젝트에 가입하였다.[105][106] 다양한 기업군들이 모인 컨소시엄인만큼 컨소시엄 내에서 협업 및 개발을 통해 다양한 블록체인 활용 방안을 연구하고 있고 이와 관련한 신규 플랫폼들도 발표하고 있다. JP모건에서 발표한 스마트 계약 기반 블록체인 플랫폼 Juno[107], 컨설팅 기업인 엑센츄어(Accenture)에서 제안한 블록체인 기반 약품 정품 인증 플랫폼[108] 등 하이퍼레저 프로젝트 내에서 다양한 블록체인 활용 방안이 연구되고 있다. 또한 IBM, 인텔, DTCC 등이 공동으로 하이퍼레저 참여 기업들이 자유롭게 블록체인을 활용할 수 있는 내부 오픈소스 서비스인 하이퍼레저 익스플로러(Hyperledger Explorer)를 개발하는 등 참여 기업간 자유로운 협업을 통해 블록체인 활용 방안을 연구하고 있다.[109]

<그림 1-2> 하이퍼레저 익스플로러 시연 자료



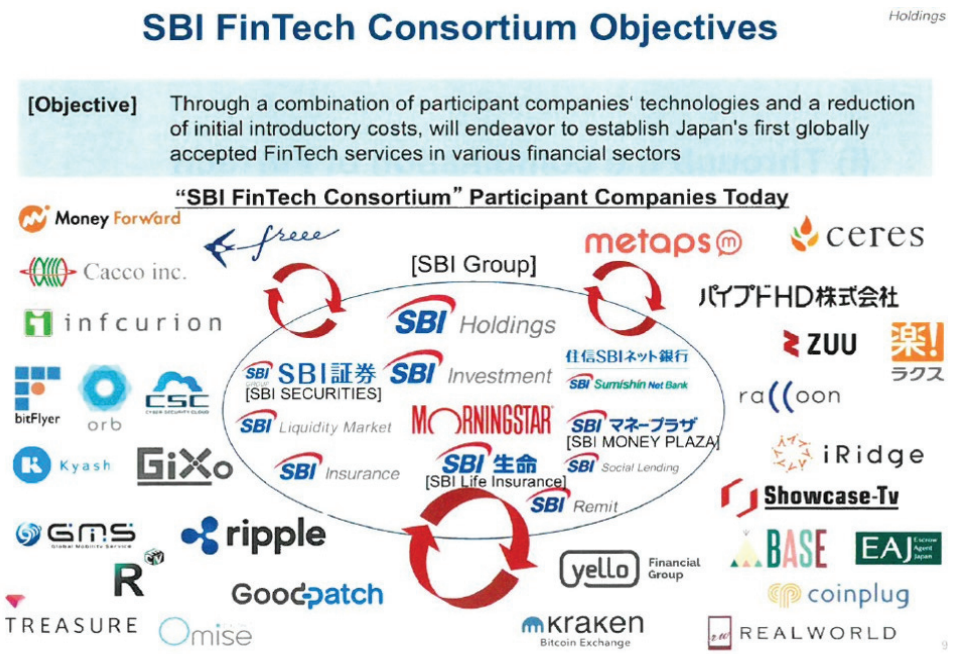
자료: Coindesk

105) https://www.hyperledger.org/announcements/2016/08/30/hyperledger-project-grows-170-percent-in-six-months
106) https://www.hyperledger.org/announcements/2016/07/27/hyperledger-project-has-welcomed-more-than-60-members-since-february
107) https://bitcoinmagazine.com/articles/jpmorgan-unveils-juno-prototype-at-hyperledger-meeting-1457629074
108) http://www.coindesk.com/hyperledger-counterfeit-drugs-blockchain/
109) http://www.coindesk.com/hyperledger-first-blockchain-explorer/

다. 아시아 지역의 블록체인 컨소시엄

아시아 시장에서도 시장 특성을 고려한 블록체인 개발을 목표로 하는 컨소시엄이 다수 구성되고 있는데, 일본의 SBI 핀테크 컨소시엄과 중국의 차이나레저(Chinaledger)가 대표적인 사례이다. SBI 핀테크 컨소시엄은 일본의 SBI 금융그룹이 주축이 되어 만든 컨소시엄으로, 블록체인을 기반으로 사물인터넷 등 금융권과 핀테크 분야의 활용법을 모색하고 있다. 빅데이터, 사물인터넷, 인공지능 등 신기술을 금융 분야에 적용할 수 있는 핀테크 생태계 구축을 목표로 만들어진 컨소시엄으로, 이같은 신기술을 적용할 수 있는 근간 시스템을 블록체인으로 보고 이에 대한 연구 및 개발을 추진중이다. SBI 금융그룹의 계열사 이외에도 금융기관용 블록체인 프로토콜인 리플, 코인플러그 등이 동 컨소시엄에 합류하였으며, 아시아에서 활용할 수 있는 블록체인 플랫폼 및 이를 활용한 핀테크 상품을 만드는 것을 목표로 한다.[110]

<그림 1-3> SBI 핀테크 컨소시엄 가입 회원들



일본에 SBI 컨소시엄이 있다면, 중국의 대표적인 블록체인 컨소시엄으로는 차이나레저(Chinaledger)를 들 수 있다. 차이나레저는 올해 5월 중국의 완샹

110) https://www.sbigroup.co.jp/english/investors/disclosure/presentation/pdf/160519presentations.pdf

(Wanxiang) 블록체인 랩을 주축으로 중국의 대형 금융기관들이 참여한 블록체인 연구 컨소시엄이다. 구체적인 기업의 리스트와 프로젝트 내용이 공개되지 않았지만, 중국내 약 11개의 대형 금융기관이 프로젝트에 참여했다고 발표했으며, R3 CEV와 이더리움 재단이 자문위원으로 참여했다. 차이나레져는 중국 내 금융기관 간 통용할 수 있는 오픈소스 블록체인 플랫폼 개발을 목표로 연구 및 개발을 진행할 예정이다.[111] 특히 완샹 그룹은 블록체인에 대해 공격적 투자를 하고 있어 컨소시엄 성장에 긍정적인 영향을 줄 것으로 예상된다.

2. 블록체인 프로토콜

블록체인 컨소시엄을 통해 여러 기업 및 기관들이 협업하여 공동으로 사용할 수 있는 블록체인 네트워크를 만들기 위한 시도와 함께, 블록체인의 활용 방안을 확장하고 새로운 대안 블록체인을 개발하고자 하는 프로토콜 개발도 진행되고 있다. 이더리움(Ethereum), 리플(Ripple) 등이 대표적인 사례인데, 이들 프로토콜은 블록체인을 기반으로 비트코인 이외의 다른 서비스에 블록체인을 활용할 수 있는 플랫폼으로서 블록체인의 기존 장점을 유지하면서도 비트코인 블록체인 등이 가지는 한계들을 극복하기 위한 대안이다.

가. 이더리움(Ethereum)

이더리움은 2013년 해커인 비탈릭 부테린(Vitalik Buterin)이 차세대 분산 어플리케이션 플랫폼이라는 이름으로 백서(Whitepaper)를 발표하면서 알려지기 시작한 블록체인 프로토콜이다. 개발자인 비탈릭 부테린은 이더리움 프로토콜로 2014년 World Technology Award에서 페이스북 창업자인 마크 주커버크를 제치고 IT Software 부문을 수상자가 되었다.[112]

이더리움 블록체인 프로토콜이 가진 가장 큰 특징은 블록체인의 응용 범위를 넓게 확장시켰다는 것이다. 우선 기능이 제한적이던 기존의 블록체인과 달리 이더리움은 프로그래밍 언어 단위를 잘게 분할하여 응용하는 사실상의 튜링 완전 언어(Turing Complete Language)를 구현한 블록체인 프로토콜이다. 언어단위를 잘게 쪼갠 블록체인 프로토콜이기 때문에 이더리움 위에서는

111) https://bitcoinmagazine.com/articles/china-joins-the-blockchain-race-with-chinaledger-alliance-1462204569
112) http://www.wtn.net/summit-2014/2014-world-technology-awards-winners

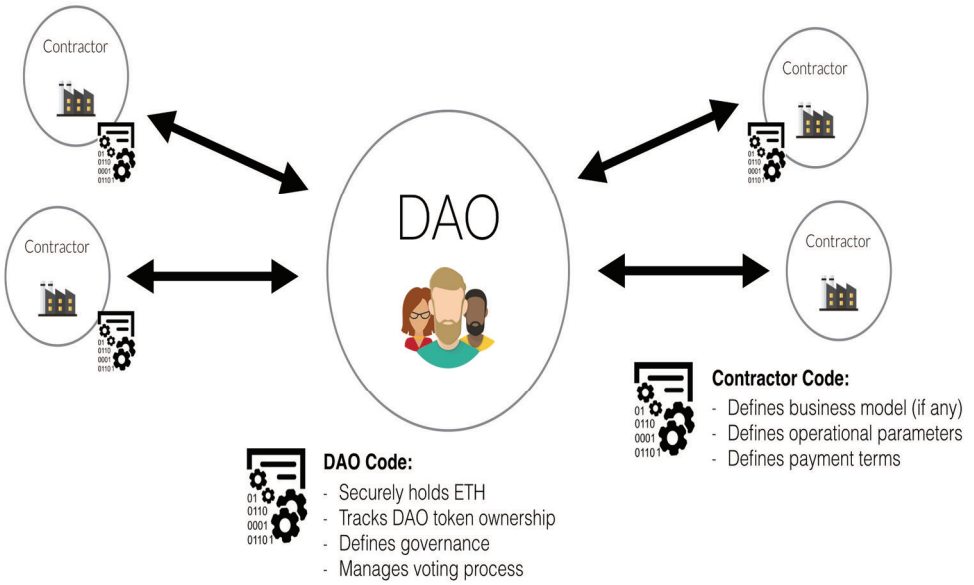
다양한 경우의 수를 가진 프로그램을 개발할 수 있다는 장점이 있다. 하지만 그만큼 구현할 수 있는 프로그램의 경우의 수도 늘어나기 때문에 다양한 보안상의 공격에 대비해야 한다는 과제 또한 존재한다.

또한 이더리움이 가장 각광을 받는 블록체인 프로토콜로 꼽히는 이유는 스마트 계약(Smart Contract) 시스템에 특화하여 개발된 블록체인 프로토콜이기 때문이다. 스마트 계약은 법적 거래 혹은 계약을 컴퓨터 코드로 짜놓은 프로그램으로 거래 내용, 유효 기간, 거래 당사자 등 코드별로 분류된 계약 요소들을 채우고 이 조건이 충족되면 자동으로 계약이 실행 및 종료되는 시스템이다. 기존에 법적 중재자나 집행인이 필요했던 방식과 달리 서로의 합의 하에 내용을 채우면 자동으로 만들어지는 자기 강제적 언어 기반의 플랫폼이기 때문에 계약 내용의 구성이 잘 되고 신뢰할 만한 기반을 가진다면 익명의 사람들이 서로에 대한 신뢰나 중개기관이 없이도 시간과 비용을 절감하며 계약을 체결할 수 있는 시스템을 구축할 수 있다. 현재 비트코인 방식 블록체인의 경우 분산원장 데이터베이스로서 비용, 보안, 속도 등의 측면에서 기존 시스템을 개선할 수 있는 기술로 주목받고 있지만, 비트코인 이후 기술을 활용할 만한 두드러진 대표 컨텐츠가 나오지 않은 상황이다. 스마트 계약은 데이터베이스를 저장하는 플랫폼으로서의 블록체인의 기능을 상당 부분 확장할 수 있고 활용도를 높일 수 있기 때문에 만약 블록체인 위에 스마트 계약을 구동할 수 있는 시스템이 갖춰진다면 금융 거래, 무역, 계약, 인증 등 수많은 분야에서 블록체인의 활용도를 획기적으로 높일 수 있다. 아직은 초기 단계로 완전하게 구현된 것은 아니지만 이미 기초적인 스마트 계약 시스템이 개발되었고, 향후 스마트 계약을 구현하는 프로토콜로 발전될 것으로 전망된다. 또한 비트코인 블록체인에서 거래를 처리하는데 소요되는 약 10분이라는 시간 제약을 극복하고 12초 내외에 거래가 처리되도록 시스템을 구성하는 등 비트코인 블록체인의 거래의 확장성 문제도 일정 부분 극복했다.

이더리움은 현존하는 블록체인 프로토콜들 중 활용 가능 범위가 넓기 때문에 마이크로소프트 등 많은 기업들이 이의 활용에 관심을 보이고 있고, 다수의 블록체인 스타트업들도 이더리움의 화폐 단위인 이더(Ether) 거래소부터 스마트 계약까지 이더리움을 활용하는 프로그램 및 서비스 개발을 진행중이다. 최근 화제가 된 분산형 자치 조직 DAO(Decentralized Autonomous Organization)는 이더리움이 적용된 대표적인 사례다. DAO는 이더리움을 활

용하여 중앙 운영주체가 없이도 분산과 자율을 바탕으로 운영되는 크라우드 펀딩 플랫폼으로서 최고경영자, 대표, 이사회 등이 없이 다수가 자유롭게 이더리움 프로토콜을 통해 익명으로 펀딩에 참여할 수 있다. 이 플랫폼에는 이더리움의 내부 화폐인 이더(Ether)를 보유하고 있으면 누구라도 참여해 투자를 할 수 있는데, 이더를 소유한 사람은 DAO에 참여하기 위해 보유한 이더를 DAO의 주소로 전송하고 동일한 가치의 DAO코인을 받게 된다. 아이디어를 가지고 있는 사람은 누구든지 DAO에 자신의 아이디어를 게시할 수 있고, DAO 토큰을 가진 사람은 원하는 아이템에 자유롭게 투자할 수 있으며, 투자한 토큰의 수만큼 투표권이 주어지고 수익 또한 투자한 토큰 지분만큼 할당받게 된다. 투자를 받고자 하는 사람은 이더리움의 스마트 계약 코드에 따라 투자 유치 신청서를 제출하고 투자자들은 그 코드를 확인하고 투자하며, 코드에 따라 계약이 자동적으로 실행된다. 약 한 달간의 투자자 및 투자금 모집에서 DAO는 크라우드 펀딩 역사상 가장 많은 금액인 약 1억 6천만 달러의 투자를 유치하면서 가장 성공적인 블록체인 적용 사례로 평가받고 있다.

<그림 1-4> 이더리움 기반 크라우드펀딩 플랫폼 The DAO



자료: The DAO

그러나 DAO는 최근 해킹 공격을 받아 안정성에 대한 의심을 받기도 했다. DAO에는 투자를 위해 전환한 DAO 토큰을 다시 이더로 바꾸는 스플릿

(Split) 기능이 있는데, 해커는 이 스플릿 기능의 취약점을 공격하여 같은 토큰을 여러 번 인출하도록 함으로써 약 5,500만 달러의 금액을 추가로 인출하였다. 이 사태를 해결하기 위해 이더리움 재단과 커뮤니티는 논의와 투표 끝에 DAO와 연관된 이더 자금에 대해 또 다른 블록체인 프로토콜을 만들어 새 블록체인에 가치가 유지되도록 하는 이른바 하드 포크(Hard Folk)를 시행하기로 결정했다. 하드 포크는 성공적으로 실행되어 해커가 해킹을 통해 획득한 이더는 가치가 없게 되었다. 하지만 이같은 결정에 반발한 소수의 사용자 및 개발자들이 기존 이더리움 프로토콜에 잔류를 선언했고, 그 결과 이더리움 시스템은 하드 포크로 새롭게 생성된 이더리움과 기존의 이더리움 프로토콜에 잔류해 있는 이더리움 클래식(Ethereum Classic)으로 이원화되어 존재하고 있다. DAO 해킹 사건의 사례는 이더리움 플랫폼 자체의 결함보다는 이를 적용한 DAO라는 어플리케이션의 맹점을 공격한 사례이기 때문에 이더리움은 여전히 차세대 블록체인으로서 주목을 받고 있지만, 이더리움 개발을 담당하는 이더리움 재단 측에서는 이번 사태를 통해 발견된 문제점들을 바탕으로 이더리움의 확장성과 보안성 향상을 목표로 지속적으로 이더리움 개발을 진행중이다.

최근 많은 기업들은 이더리움의 높은 활용도에 주목해 단순한 이더리움 기반 서비스 개발을 넘어서 이더리움 기반 폐쇄형 블록체인(Private Ethereum) 플랫폼을 개발하고 있다. 올해 10월 세계 최대 금융기관 중 하나이자 하이퍼레저의 참가 기관인 JP모건은 Quorum이라는 이름의 이더리움 기반 자체 폐쇄형 블록체인 네트워크를 개발했다고 발표했다.[113][114] 또한 미디어기업이자 최근 하이퍼레저에 가입한 톰슨 로이터도 이더리움을 기반으로 하는 블록체인 플랫폼인 BlockOne을 발표하는 등 이더리움을 블록체인 플랫폼으로 활용하여 개발하는 사례가 증가하고 있다.[115][116]

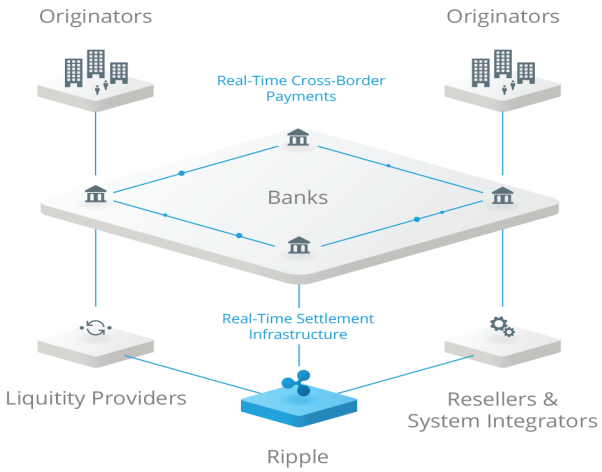
나. 리플(Ripple)

리플(Ripple)은 블록체인 프로토콜 중 국가 간 혹은 금융기관 간 송금 및 결제에 초점을 맞추어 개발한 블록체인 프로토콜이다. 블록체인 기술은 송금 분야에서 기존 시스템의 비효율적인 요소를 해결할 수 있는 기술로 평가받

113) http://www.coindesk.com/jpmorgan-ethereum-blockchain-quorum/
114) https://www.cryptocoinsnews.com/jp-morgan-joins-ethereum-developing-private-blockchain-quorum/
115) https://blockone.thomsonreuters.com/
116) http://www.coindesk.com/thomson-reuters-blockchain-ethereum-devcon2/

는다. 특히 해외송금 시스템의 경우 송금을 위해 여러 중개은행들이 개입하고 SWIFT 등 국제송금 전용 전신망을 사용하는 등 다수의 제3기관의 개입으로 많은 수수료 비용이 발생하고, 결제 요청 통신, 완료 통신 등 각 과정마다 결과가 따로 생성되는 등 복잡한 절차가 필요할 뿐 아니라 결제 완료 시점까지 결제 리스크에 노출되기도 한다. 또한 다른 금융기관들이 각자의 시스템을 통해 결제 및 청산을 하기 때문에 해외송금이 완료되기까지 1주일 이상이 걸리기도 할 정도로 비효율적인 시스템을 가지고 있다. 리플은 현재의 복잡한 송금 시스템을 극복할 대안으로 블록체인의 분산된 네트워크를 이용해 중개기관을 최대한 배제하는 신속한 송금과 실시간 결제 및 청산 시스템 구축을 시도하고 있다. 기존에 여러 단계를 통해 이루어졌던 복잡한 송금 및 결제를 분산원장이라는 하나의 플랫폼을 만들어 빠르고 간단한 결제 시스템을 구축하는 것이 리플의 목표이다.

<그림 1-5> 리플의 시스템 구조



자료: Ripple

리플 프로토콜에서는 XRP라는 이름의 화폐단위를 사용한다. XRP는 총 1천억개 정도가 이미 발행되어 있으며 한 번 거래가 이뤄질 때마다 0.00001XRP가 수수료로 지불된다. 리플 네트워크에 참여하는 금융기관이 일반적인 이체나 환전을 할 때는 XRP를 활용할 필요없이 리플의 블록체인 시스템을 활용하여 송금 및 결제를 할 수 있지만, XRP를 매개로 활용하면 마일리지, 카드 포인트 등 다른 종류의 화폐나 유가물도 교환할 수 있게 된다. 지난 7월 리플에서 발간한 보고서에서는 현재 은행 시스템은 매우 거대하기 때문에 당장 모든 은행이 전 분야에서 블록체인을 송금 플랫폼으로 적용할 수는 없겠

지만, 현재의 고비용의 비효율적인 송금시스템을 개선할 수 있는 방안으로서 블록체인 기반 송금 시스템의 적용 분야를 조금씩 넓혀간다면 금융기관들은 획기적인 비용절감과 효율성 증가의 효과를 기대할 수 있을 것이라고 밝혔다.[117]

리플은 송금 및 결제에 초점을 맞춘 블록체인 프로토콜인 만큼 금융기관과의 협업에 적극적인 행보를 보이고 있다. 장기적으로는 SWIFT를 대체하는 송금 및 결제 플랫폼을 만들기 위해, 다수의 금융기관이 참여하는 블록체인 기반 지불결제 네트워크 구성을 목표로 하고 있다. 지난 5월에는 산탄데르(Santander) 은행 영국 지부와 일본의 미즈호 은행이 리플의 블록체인을 기반으로 하는 Payment 시스템 개발 계획을 발표했고 이를 금년중 출시하는 것을 목표로 테스트 중이라고 밝혔다.[118] 지난 7월에는 다국적 기업용 소프트웨어 기업인 SAP가 두 은행과 합작하여 블록체인 기술을 활용한 국가 간 송금 및 결제 시스템의 기술검증을 진행할 계획이라고 발표했다.[119]

올해 9월에는 리플과 여섯 개 은행이 함께 분산원장 기술을 기반으로 은행간 해외 송금 및 결제 시스템을 개발하는 Global Payments Steering Group(이하 GPSG)을 결성했다. GPSG은 금융기관과 협업을 통해 기존 플랫폼보다 더 신속하게 송금할 수 있는 분산원장 시스템을 개발하고 이와 동시에 분산원장 기반 송금 및 결제에 대한 표준과 운영 방식에 대한 합의안을 만들어 은행들이 활용할 수 있는 블록체인 플랫폼을 만들 계획이다.[120] 이외에도 리플은 다양한 금융기관과 마이크로소프트, MIT 등과의 공동 연구를 진행하는 등 다양한 기업들과의 협업을 통해 자사의 프로토콜을 활용하여 결제시장에서 블록체인을 활용할 수 있는 방안을 모색중이다.

다. 디지털 에셋 홀딩스(Digital Asset Holdings)

디지털 에셋 홀딩스는 JP모건 임원 출신인 Blythe Masters가 설립한 블록체인 기업으로 자본시장을 위한 분산원장을 개발중이다. 자본시장에서 활용할 수 있는 디지털 자산 모델링 언어(Digital Asset Modeling Language, 이하

117) The journey to Real-time cross border commercial payments using distributed ledger technology, Ripple and Accenture, 2016
118) http://www.coindesk.com/santander-uk-payments-app-ripple/
119) https://bitcoinmagazine.com/articles/sap-and-ripple-collaborate-on-cross-border-payments-trial-using-blockchain-technology-1468862163
120) https://ripple.com/insights/announcing-ripples-global-payments-steering-group/

DAML)라는 이름의 분산원장용 스마트 계약 언어를 개발하고 있다.

디지털 에셋 홀딩스는 이더리움과 달리 DAML을 튜링 불완전 언어로 설계했다. 튜링 불완전 언어는 기능적으로 제한되어 있어 활용도가 떨어질 수 있지만, 튜링 완전 언어로 프로그램을 설계했을 때에 비해 고려해야 할 오류와 변수를 최소화할 수 있는 장점이 있다. 디지털 에셋 홀딩스는 기능을 어느 정도 희생하더라도 자본시장에 더 최적화된 안정적이고 높은 보안성을 가진 분산원장 플랫폼을 제공하는 것을 목표로 한다.

디지털 에셋 홀딩스는 자본시장 블록체인 플랫폼 도입을 목표로 설립된 기업인만큼 주로 자본시장 관련 기업 및 기관과 협업을 통해 분산원장 기술을 적용하는 방안을 개발하고 있다. 올해 3월에는 미국 예탁결제원(Depository Trust & Clearing Corporation)과 블록체인 기반의 Repo 결제 및 청산 시스템 개발에 합의했으며,[121] 호주 증권거래소(Australian Stock Exchange)에서는 디지털 에셋 홀딩스에 추가 투자를 하는 등[122] 자본시장에서 블록체인 도입을 목표로 협력이 진행중이다.

3. 금융기관 및 기업의 블록체인 활용 현황

이더리움, 리플 등 프로토콜이 전반적인 금융 시스템이나 서비스를 다루는 하나의 플랫폼으로 블록체인을 개발한다면, 금융기관 등의 기업들은 각 기관이 내부적으로 가지고 있는 시스템의 비효율적인 요소들을 제거하고 새로운 서비스를 개발하기 위한 시스템으로서 블록체인에 접근하고 있다.

우선 다수의 금융 기관들이 블록체인 시스템을 기반으로 하여 자체적으로 유통하는 디지털 화폐를 개발하는 방안에 대해 연구하고 있다. 금융기관들이 블록체인의 분산형 네트워크를 통해 디지털 화폐를 유통할 수 있게 되면 고객들의 거래 내역을 쉽게 확인하는 등 고객관리와 자산 관리가 용이해지고 기존 화폐 관리비용을 절감할 수 있을 뿐만 아니라, 해외 지점과 연동하여 다른 화폐로 환전이 쉬워지는 등 많은 장점들을 바탕으로 시스템을 효율적으로 운영하고 추가적인 서비스도 개발할 수 있기 때문이다. 이전까지는 디지털 화폐를 유통하고 관리할 수 있는 안전한 시스템이 없었기 때문에 이를

121) https://digitalasset.com/press/dtcc-digital-asset-repo-poc.html
122) https://digitalasset.com/static/documents/30_22Jun_ASX%20Increases%20Investment%20in%20Digital%20Asset%20Holdings.pdf

구현하기가 쉽지 않았지만, 비트코인이라는 가상 화폐를 성공적으로 유통하고 있는 분산형 네트워크인 블록체인 기술이 디지털 화폐 생태계를 만들 수 있는 기술이라 판단됨에 따라 많은 금융기관들이 블록체인 기반 화폐를 발행하는 방안을 연구 및 개발 중이다.

또한 금융기관들은 비트코인으로 증명된 바와 같이 중개기관 없이 실시간으로 송금이 가능하다는 블록체인의 장점을 바탕으로 블록체인 기반의 해외송금 플랫폼 개발도 진행중이다. 현재 SWIFT망 등의 전신료와 중개은행에 지불하는 수수료 등으로 은행들의 송금 서비스 관련 시간적, 비용적 부담이 높은 상황에서 중개기관 없이 바로 송금을 처리할 수 있는 블록체인 플랫폼은 낮은 비용으로 빠른 시간에 송금을 할 수 있는 대안으로서 각 금융사가 큰 관심을 갖고 있다. 이외에도 금융기관들은 결제청산 시스템, 스마트 계약 기능을 활용한 거래 플랫폼 등을 개발하고 있다.

대표적인 사례는 일본의 MUFG코인이다. 일본 최대 금융기관중 하나인 미쓰비시 UFG 금융그룹(이하 MUFG)는 블록체인 활용방안을 활발히 연구중인 아시아의 대표적인 대형 금융기관으로, R3 CEV의 회원이기도 하다. MUFG는 내부적으로 송금, 가상화폐, 결제시스템 등 다양한 블록체인 기술 기반 플랫폼을 실험 중인데 이중 가장 주목받는 연구 분야가 자체 코인 발행이다. MUFG는 블록체인을 활용한 자체 가상화폐인 MUFG 코인을 개발하고 있는데, 은행 계좌 잔액을 MUFG 코인으로 전환하여 모바일 앱 등을 통해 은행 서비스에 간편하게 사용할 수 있고, 향후 ATM을 통해 MUFG를 엔화로 전환하여 출금하는 서비스도 구상중이다. 아직까지 구체적인 실행 여부는 정해지지 않았지만 MUFG 코인의 발행이 확정된다면 2017년 말 출시를 목표로 하고 있다. 또한 MUFG는 블록체인 스타트업과의 협업을 통해 블록체인 기반 약속어음 교환 플랫폼의 기술검증을 진행 중이다.[123] 일본의 또 다른 대형 금융기관인 미즈호 금융그룹 또한 여러 블록체인 기업들과의 협력을 통해 블록체인 활용 방안을 찾고 있다. 올해 2월에는 컨설팅기업과 협력을 맺고 미즈호 금융그룹 전체에 블록체인을 기반으로 한 기록관리 시스템을 연구할 것이라고 발표했고, IBM과 협력을 통해 블록체인 기반 송금 및 결제 시스템에 대한 테스트도 진행 중이라고 밝혔다.[124][125]

123) http://www.coindesk.com/chain-mufg-blockchain-promissory-notes/
124) https://www.cryptocoinsnews.com/mizuho-cognizant-develop-blockchain-solutions-record-keeping/
125) https://www.cryptocoinsnews.com/mizuho-ibm-digital-currency-test/

은행 간 자체 컨소시엄을 구성해 결제를 위한 디지털 코인 개발에 착수한 사례도 등장하고 있다. UBS, 도이체방크, 산탄데르, 뉴욕 멜론 은행 (BNY Mellon) 등 4개 대형 은행은 송금 및 결제 시스템에 적용되는 블록체인 기반 가상화폐인 Utility Settlement Coin을 개발 중이며, 이를 2018년 초에 출시할 계획이라고 발표했다.[126] 4개 은행 중 UBS 주도로 이루어지는 이 시스템은 금융기관들이 주식, 채권 등 금융상품을 거래할 때 은행 간 상이한 시스템을 통합하여 블록체인을 기반으로 거래 즉시 결제가 완료되는 자체 디지털 화폐 플랫폼으로서 거래시점과 결제시점 사이의 상대방 리스크 노출 위험을 극복할 수 있다. 현재는 2018년 출시를 앞두고 각국 규제 당국의 승인과 중앙은행의 협조를 얻기 위해 노력중이다.[127]

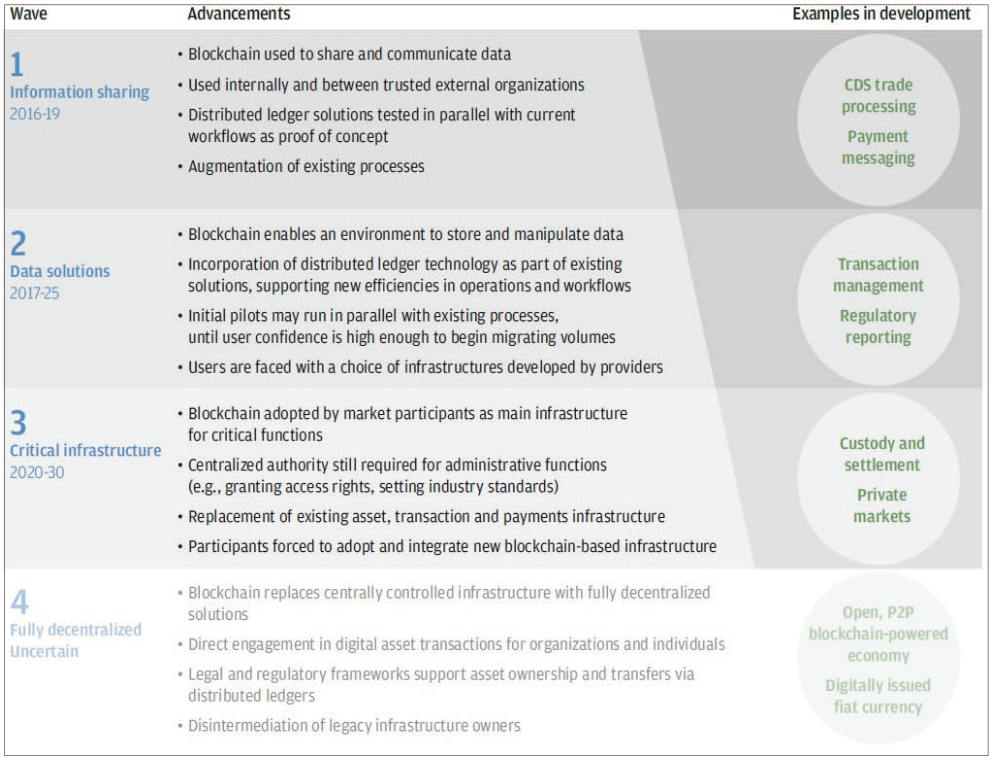
금융 회사인 VISA도 블록체인에 대해 활발히 연구 및 투자를 하고 도입 방안을 모색하고 있다. 올해 10월에는 블록체인 스타트업과 협업을 통해 비자 네트워크를 이용한 블록체인 기반의 실시간 결제 플랫폼을 2017년 출시를 목표로 개발할 것이라고 발표했다.[128] 또한 VISA 유럽지부에서 새로운 시스템과 혁신적인 서비스에 대한 연구를 담당하고 있는 VISA Europe Collab에서는 현재 블록체인을 새로운 송금 플랫폼을 개발할 수 있는 기반기술 중 하나로 보고 이에 대한 연구를 진행중이다. 지난 9월에는 블록체인 관련 스타트업과 협력하여 블록체인 기반 송금 플랫폼에 대한 기술 검증을 약 100일간 진행할 것이라고 발표했다. VISA 측은 블록체인 기반의 새로운 송금시스템은 기존 SWIFT망을 기반으로 하는 송금 시스템보다 최대 80% 가까이 비용을 절감할 수 있을 것으로 추산하며 VISA의 네트워크와 블록체인 기술을 결합하여 기존 송금 시스템의 비용을 절감하고, 송금 및 결제 시스템 기반이 취약한 개발도상국에서 VISA의 네트워크와 시장을 확장할 수 있는 발판이 될 것으로 기대하고 있다.[129]

미국의 대표적인 금융기업인 JP모건도 지난 2월 약 2,200여명의 고객을 대상으로 블록체인 기반 시스템을 통해 런던에서 도쿄로 달러를 송금하는 테스트에 성공했다고 밝혔다. JP모건은 지난 7월 자산관리 산업에서의 블록체인 활용법에 대한 보고서를 발표했는데, 향후 5~10년간은 블록체인 기술을 내부자료 공유 등 간단한 어플리케이션을 통해 주로 활용해 보고, 새로운 기

126) https://bitcoinmagazine.com/articles/major-banks-developing-utility-settlement-coin-an-industry-standard-for-digital-central-bank-cash-1472140867
127) https://www.ft.com/content/1a962c16-6952-11e6-ae5b-a7cc5dd5a28c
128) http://www.coindesk.com/visa-blockchain-payments-service/
129) https://www.cryptocoinsnews.com/visa-test-blockchain-payments-among-banks-swift-rival

술의 리스크를 고려해 기존의 시스템과 연동 혹은 병행하면서 다양한 실험을 진행할 것이라고 밝혔다.[130]

<그림 1-6> JP모건의 예상 블록체인 도입 4단계



자료: Unlocking Economic Advantage with Blockchain

많은 글로벌 기업과 금융기관들이 블록체인 도입을 검토하고 연구를 진행하는 가운데 국내에서도 블록체인에 대한 관심과 도입 시도가 이루어지고 있다. 삼성전자는 지난해부터 IBM과 함께 사물인터넷 등을 통해 블록체인을 활용할 수 있는 방안을 연구 중이다. 각 금융기관들도 R3 CEV나 하이퍼레저 등 블록체인 컨소시엄에 가입하고 있으며, 일부 금융기관들은 스타트업과 협력하여 인증, 송금, 전자 자산 등의 분야에서 블록체인 기반 플랫폼을 테스트하는 등 도입을 준비하고 있다.

130) Unlocking Economic Advantage with Blockchain, JP Morgan & Oliver Wyman, 2016

<표 1-1> 국내 블록체인 도입 동향 (가나다 순)

기업명	블록체인 도입 현황
삼성전자	• IBM과 함께 블록체인 활용 방안 검토 중 131)
삼성SDS	• 블록체인 업체 블로코에 투자 132) • 블록체인 컨소시엄 Hyperledger 가입
신한은행	• 블록체인 컨소시엄 R3CEV 가입 • 블록체인 기반 골드바 구매 교환증 및 보증서 서비스 출시133)
우리은행	• 코인플러그와 블록체인 관련 업무협약 체결 134)
전북은행	• 블록체인 기반 간편 로그인 서비스 개발 135)
하나은행	• 블록체인 컨소시엄 R3CEV 가입
한국예탁결제원	• 블록체인 컨소시엄 Hyperledger 가입
한국조폐공사	• 코인플러그와 블록체인 기반 사업협력 MOU 체결 136)
BNK금융	• 코인플러그와 블록체인 기반 서비스 업무협약 체결 137)
IBK기업은행	• 코빗과 블록체인 기반 서비스 업무협약 체결 138)
KB국민카드	• 코인플러그와 블록체인 기반 개인인증 서비스 구축 139)
KB국민은행	• 블록체인 컨소시엄 R3CEV 가입 • 코인플러그와 블록체인 기반 해외송금 플랫폼 개발 140) • 코인플러그와 블록체인 기반 비대면 실명인증 플랫폼 개발141)
NH농협은행	• 블록체인 업체 코빗과 제휴 142)

4. 정부 및 공공기관의 블록체인 활용 현황

블록체인은 공공 분야에서도 활용 가능성이 높은 기술이다. 거래내역이 투명하게 공개되고 거래내역이 추적가능하며 중앙집중이 아닌 분산형 네트워크로 구성되는 블록체인은 세금, 토지, 여권, 신분증, 보조금 등 정부가 관리하고 분배하는 모든 자산을 쉽게 등록하고 내역을 추적하는 서비스를 만드

131) http://www.hankyung.com/news/app/newsview.php?aid=2016082351841
132) http://www.yonhapnews.co.kr/bulletin/2016/07/14/0200000000AKR20160714026300017.HTML?input=1195m
133) http://www.yonhapnews.co.kr/bulletin/2016/08/17/0200000000AKR20160817102400002.HTML?input=1195m
134) http://www.fntimes.com/paper/view.aspx?num=162024
135) http://www.ddaily.co.kr/news/article.html?no=142206
136) http://www.ebn.co.kr/news/view/849764
137) http://www.yonhapnews.co.kr/bulletin/2016/01/15/0200000000AKR20160115145100051.HTML?input=1195m
138) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20160310163334&type=det&re=
139) http://www.ddaily.co.kr/news/article.html?no=140988
140) http://www.etnews.com/20151201000427
141) http://www.g-enews.com/ko-kr/news/article/news_all/20160429131201210615 1_1/article.html
142) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150826155406&type=det&re=

는 데 활용될 수 있다. 또한 블록체인 기술은 같은 내용의 원장을 여러 네트워크 참가자가 나눠서 가지고 있기 때문에, 기존 중앙집중 방식으로 운영되는 경우 외부의 공격에 취약하고 이에 따라 보안 시스템에 많은 비용을 지불해야 했던 문제점을 극복할 수 있을 것이라고 보고 있다.

정부 혹은 공공기관의 서비스는 시민들의 정보를 안전하게 보관하고 편리하게 제공하는 것을 목표로 한다. 일반 기업도 고객에 대한 정보 관리를 중요시하지만 공공기관은 상대적으로 보유하는 정보의 양이 많고 대상이 거주하는 시민 전체에 해당하기 때문에 이같은 개인정보들을 철저히 보관해야할 책임이 있다. 이에 더하여 정부 및 공공기관의 정보 관리는 시민들에게 편리한 공공 서비스를 제공하는 것을 목표로 지향해야 한다. 블록체인 개발도 이러한 방향성을 갖고 진행되고 있으며, 특히 가상화폐, 소유권 등록 등의 분야에서 활발하게 연구되고 있다.

우선 주요국 중앙은행들은 블록체인을 기반으로 디지털 화폐를 발행하여 유통하는 방안에 대해 다양하게 연구하고 있다. 위에서 언급한 사례와 같이 일반 금융기관도 블록체인 기반의 가상화폐 개발을 진행하고 있지만, 민간 금융기관은 화폐의 역할을 대신하는 블록체인 기반 코인을 만드는 데 관심이 있는데 비해, 중앙은행은 법정화폐를 발행하고 유통하는 주체로서 디지털 화폐를 블록체인을 통해 직접 발행하고 유통하는 방안을 연구하고 있다는 점에서 차이가 있다. 현재 중앙은행이 실물 화폐를 발행하고 유통하는 데는 많은 비용이 든다. 특히 동전의 경우 액면 가치가 실제 금속으로서의 소재 가치와 큰 차이가 없고 분실이 잦기 때문에 유통과 관리에 드는 비용에 비해 효율성이 떨어진다는 평가를 받고 있다. 또한 현재 화폐 시스템은 탈세를 추적하기가 용이하지 않다는 문제점이 있다. 블록체인 기반 디지털화폐 시스템은 거래내역을 실시간으로 확인할 수 있고 빠른 결제 및 청산이 가능하며 분실에 대한 우려가 없다는 장점을 갖는다. 세계경제포럼에 따르면 800명의 조세 전문가 중 약 73%가 2025년 이전에 블록체인을 기반으로 조세를 걷는 사례가 나타날 것이라고 예상했다.[143] 중앙은행은 블록체인이 향후 디지털 화폐를 유통하고 관리할 수 있는 플랫폼이라 보고 개발을 진행하고 있다. 관련 분야에서 가장 활발한 연구를 진행하고 있는 곳은 영란은행이다. 지난 3월 영란은행은 University College London의 교수진과 함께 영란은행에서 발행하는 디지털 화폐인 RSCoin을 보고서를 통해 발표했고, 이후 7월에는

143) http://www.coindesk.com/world-economic-forum-governments-blockchain/

디지털 화폐 발행이 거시경제학적으로 미칠 영향에 대한 보고서를 발표했다. 영란은행은 디지털화폐가 가져다 줄 긍정적 영향력이 크고 장기적으로는 필요성도 있지만 단시일 내에 디지털화폐를 발행하기로 결정한 것은 아니며 우선 디지털화폐의 잠재적인 편익과 부작용 등을 고려하여 향후 구체적인 방안을 정해야 한다는 입장이다.

네덜란드 중앙은행도 지난 2월 중앙은행이 통제하는 블록체인 기반 디지털 화폐인 DNB 코인에 대한 아이디어를 발표했고, 이후 오픈소스인 비트코인 소프트웨어를 기반으로 실험을 진행하였다고 밝혔다. 동 실험에서는 비트코인과 같은 가상화폐를 발행할 때와 가상화폐가 더 이상 발행되지 않는 두 가지 상황을 가정하여 시스템 안정성과 보안을 중심으로 시스템에 대한 테스트를 진행하였다. 네덜란드 중앙은행은 아직까지 디지털화폐에는 많은 한계가 있고 다수 금융기관의 공감대가 형성되는 데도 시간이 걸리겠지만, 블록체인이 지속적으로 발생하고 있는 금융사고 등을 예방할 수 있는 플랫폼으로서 하나의 대안이 될 수 있다고 판단하고 있으며 중앙은행 발행 디지털 화폐에 대한 연구를 계속 진행할 것임을 밝혔다.[144] 캐나다 중앙은행도 블록체인을 기반으로 중앙은행이 직접 발행하는 가상화폐인 CAD Coin에 대한 아이디어를 연구 중이라고 발표했다. 역시 실제 도입을 전제로 한 연구라기보다는 기술에 대한 이해와 활용 가능성을 점검하기 위한 개념적인 테스트 단계이지만, 블록체인 기술을 통해 은행 간 지급 및 결제에서 디지털화폐를 활용할 수 있을 것이라고 보고 이를 위한 연구를 진행 중이다.[145] 정부 발행 디지털 화폐에 대한 보다 자세한 내용은 4장에서 기술한다.

또한 블록체인 기술은 모든 거래내역이 공개되고 추적될 수 있는 투명성을 바탕으로 공공기금의 운영과 소유권 증명 및 이전 분야에서도 활용 방안을 연구 중이다. 정부가 관리하는 기록 및 자료가 이미 대체로 디지털 정보로 보관되고 있어 각국 정부는 정보를 효율적이고 안전하게 관리할 수 있는 시스템을 찾고 있다. 중앙의 통제기관 없이 자유롭게 거래가 가능한 비트코인과 그 근간이 되는 블록체인 기술은 정부에서 적절한 활용 방안만 찾는다면 소수의 서버에 집중된 데이터 처리의 비효율성과 보안에 대한 불안함을 극복할 수 있는 좋은 대안으로 평가받고 있다.

144) http://www.coindesk.com/dutch-central-bank-preparing-boldest-blockchain-experiment-yet/
145) http://www.coindesk.com/bank-of-canada-pursues-hands-on-distributed-ledger-research/

영국 정부의 경우, 공공분야에서 블록체인을 활용할 수 있는 방안에 대해 많은 관심을 가지고 적극적인 연구를 진행중이다. 지난 1월 영국 과학부에서 발표한 보고서에서는 블록체인이 보안, 프라이버시, 신뢰 등의 문제를 극복한다면 공공 분야에서 다양하게 활용 가능할 것이라고 밝히며, 다양한 측면에서 블록체인 개발 연구를 진행할 것이라고 발표했다.[146] 또한 지난 7월 영국 노동연금부(Department for Work and Pensions)에서는 바클레이스 은행 및 다수의 핀테크 스타트업과 연계해 블록체인 네트워크를 통한 연금 수령 및 사용 내역 기록에 관한 연구를 진행한다고 발표했다.[147]

에스토니아 정부는 블록체인을 전면적으로 도입하고자 하는 정부 중 하나이다. 에스토니아 정부는 에스토니아 주민의 기록을 디지털화하여 관리하는 e-residency 시스템을 준비 중인데 이의 기반이 되는 플랫폼으로서 블록체인 도입을 준비하고 있음을 밝혔다.[148] 에스토니아 정부는 나스닥과 함께 동 인프라를 바탕으로 전자투표 플랫폼을 개발하는 등 e-residency 플랫폼을 통해 주민들이 빠르고 편리하게 공공 서비스를 이용할 수 있는 통합 플랫폼 구축에 적극적인 자세를 보이고 있다.

싱가포르 정부의 경우 기업과의 협업을 통한 블록체인 활용방안을 연구 중이다. 지난 7월 싱가포르 정부와 IBM이 협력 관계를 맺고, 블록체인 혁신 센터를 조성하고 IBM 연구진과 싱가포르의 개발자들이 협업하여 국가 내 여러 지역과 산업 분야에서 활용할 수 있는 블록체인 기술을 개발할 것이라고 발표했다. 싱가포르의 경제개발청(Economic Development Board)과 통화청(Monetary Authority of Singapore)은 IBM의 블록체인 기술을 바탕으로 다자간 거래 플랫폼을, 항만청(Port Authority of Singapore)은 공급사슬 개선 방안을 도출해 3년 이내에 금융과 무역 산업에서 활용할 수 있는 블록체인 기반 파일럿 프로그램들을 발표할 예정이라고 밝혔다.[149]

분산 네트워크를 가진 블록체인은 공공 문서를 등록하고 보관하는 플랫폼으로서도 공공기관의 적극적인 연구 대상이 되고 있다. 많은 정부에서 문서 보관 비용을 절감하고 증명서를 간편하게 발급할 수 있으며 다른 서비스로의 확장 또한 용이한 블록체인 기반 문서 서비스를 도입하고자 하는 움직임

146) Distributed Ledger Technology: beyond block chain, UK Government office of Science, 2016
147) https://www.cryptocoinsnews.com/uk-trials-blockchain-based-social-welfare-payments/
148) http://www.bbc.com/news/technology-36276673
149) http://www.coinspeaker.com/2016/07/12/ibm-opens-blockchain-innovation-centre-in-singapore/

이 시작되고 있다. 러시아 정부의 경우 비트코인 자체에 대해서는 회의적인 태도를 취하고 있지만, 블록체인에 대해서는 개방적인 태도를 보이며 이를 적극적으로 도입하기 위한 노력이 진행중이다. 러시아 연방 반독점청(Federal Anti-monopoly Service, 이하 FAS)은 하이퍼레저에 가입한 러시아 최대 금융기관 Sberbank와 함께 블록체인 기반 문서관리 시스템을 테스트하고 있다고 발표했다.[150]

스웨덴에서는 블록체인을 활용하여 토지의 소유권과 이전 내역을 기록하는 스마트 계약 플랫폼을 만드는 방안을 연구 중에 있다. 스웨덴 국립 토지연구소(Swedish National Land Survey)는 블록체인 스타트업, 컨설팅 기업, 통신회사와 협약을 맺고 블록체인 시스템을 활용하여 기존에 수작업으로 이루어지던 토지 조사를 보다 효율적이고 안전하게 바꾸기 위한 방안을 연구 중이며, 블록체인을 활용한 스마트 계약 플랫폼을 통해 활용한 토지 등록 시스템을 개발할 계획이라고 밝혔다.[151]

중동 또한 블록체인 도입에 매우 적극적으로 움직이는 지역이다. 아랍에미리트는 현재까지 과도하게 이어지고 있는 석유 자원에 대한 경제적 의존 구조를 탈피하기 위해 신사업에 대한 투자를 확대하는 전략의 일환으로 블록체인을 새로운 산업을 육성할 수 있는 기술로 평가하고 이에 대한 개발을 적극적으로 진행하고 있다. 금년 10월 두바이 정부는 2020년까지 전면적 도입 목표 하에 정부의 모든 문서 시스템에 블록체인을 도입하는 프로젝트를 진행한다고 발표했다. 두바이 도시 정부는 이 프로젝트를 통해 정부의 업무 효율성을 높이고 블록체인 기반 신사업을 육성한다는 입장이다.[152]

5. IT기업들의 블록체인 활용 현황

블록체인 기반 서비스를 제공하는 가장 대표적인 IT기업은 마이크로소프트와 IBM이다. 해당 IT 기업들은 다른 기업들이 활용할 수 있는 오픈소스 블록체인 플랫폼을 개발하여 다른 기업들이 블록체인 기반 서비스를 테스트하고 활용할 수 있는 서비스를 제공하고 있으며, 이를 통해 소프트웨어 기업으로서 시장의 주도권을 찾고 고객을 확보하고자 하고 있다.

150) http://www.coindesk.com/the-russian-government-is-testing-blockchain-for-document-storage/
151) http://www.coindesk.com/sweden-blockchain-smart-contracts-land-registry/
152) http://www.coindesk.com/dubai-government-documents-blockchain-strategy-2020/

가. IBM

IBM은 리눅스 재단(Linux Foundation)의 하이퍼레저 프로젝트를 주도하는 IT기업으로서 블록체인을 차세대 산업기술로 판단하고 다른 산업군과 기업들이 활용할 수 있는 블록체인 플랫폼을 소프트웨어 서비스로 제공하는 것을 목표로 개발을 추진중이다. 지난 7월 IBM은 높은 보안성을 갖는 리눅스원(LinuxONE)을 기반으로 고객들이 자유롭게 블록체인 시스템 안에서 프로그램을 테스트하고 운영할 수 있는 플랫폼을 개발했다고 발표했다. 기존의 블록체인 플랫폼을 통해 고가의 제품 데이터를 다루어 온 에버레저(Everledger) 등 블록체인 스타트업들이 새로운 플랫폼을 테스트해 보겠다는 의사를 밝혔으며, IBM은 보다 안전하고 신뢰성이 높은 새로운 블록체인 플랫폼을 보다 많은 기업들이 실험장으로 활용할 것을 기대하고 있다.[153] IBM은 최근 구글, 아마존 등의 기업의 부상으로 인해 상대적으로 좁아진 소프트웨어 기업으로서의 입지를 되찾고 새로운 먹거리를 확보하기 위한 방안으로 블록체인 플랫폼의 개발을 통해 다른 기업들과의 연계를 강화하고 고객을 확보하겠다는 구상을 가지고 있으며, 세계 각지의 컨퍼런스에서 적극적으로 IBM의 아이디어를 발표하는 등 대외적으로도 활발하게 블록체인에 대한 전략을 홍보하고 있다.

나. 마이크로소프트

마이크로소프트 또한 블록체인 기반 오픈소스 플랫폼을 개발하여 다른 기업들이 사용할 수 있는 서비스를 제공하고 있으며 다른 블록체인 기업들과의 협업을 통해 블록체인으로 응용할 수 있는 여러 플랫폼들을 구상 및 발표하고 있다.

또한 블록체인 스타트업과 협업을 통해 블록체인 기반 신분인증 시스템을 구축하겠다고 밝혔다. UN은 2030년까지 세계 모든 사람들이 법적 신분을 가지는 것을 목표로 한다고 밝혔고, 마이크로소프트는 위변조가 불가능하고 내역이 명확하게 공개되며 높은 확장성을 가진 블록체인 네트워크를 통해 개인 신분인증 플랫폼을 구축할 계획이라고 밝혔다.[154]

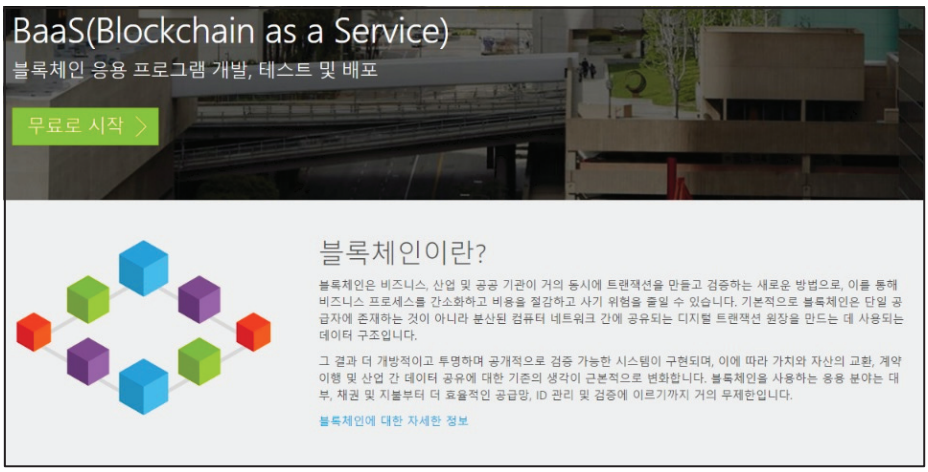
또한 마이크로소프트는 이더리움 블록체인 벤처기업 Consensys와 함께 동사의 클라우드 서비스 플랫폼인 애져(Azure) 위에 이더리움을 기반으로 한

153) https://www-03.ibm.com/press/us/en/pressrelease/50169.wss

154) https://bitcoinmagazine.com/articles/microsoft-building-open-blockchain-based-identity-system-with-blockstack-consensys-1464968713

BaaS(Blockchain as a Service)를 구축했다.[155] 마이크로소프트는 이더리움 기반 서비스를 제공함으로써 블록체인을 활용하고 싶었지만 접근성이 떨어져 활용이 어려웠던 고객들에게 블록체인 기반 어플리케이션, 프로그램 등을 테스트 할 수 있는 플랫폼을 제공하고 이를 통해 고객들을 확보하겠다는 계획이다.

<그림 1-7> 마이크로소프트의 블록체인 서비스 BaaS



6. 기타 블록체인 활용 현황

가. 정품 인증 및 소유권 이전

최근 기업 및 산업계에서는 분산화된 네트워크를 통해 위변조가 불가능하고 거래내역이 공개되는 투명성을 가진 블록체인 기술을 활용하여 안정적인 정품인증 서비스와 상품의 소유권 이전 시스템을 도입하고자 하는 데 관심을 보이고 있다. 특히 모조품 피해 발생 사례가 많고 소비자들이 이전 소유자나 제작자, 원산지 등을 알기를 바라는 고가의 제품군에서 블록체인 적용 방안을 적극적으로 모색하고 있다.

영국 기반 블록체인 스타트업인 에버렛져(Everledger)는 다이아몬드의 정보를 등록하고 소유권 내역을 확인하는 서비스를 제공하고 있다. 에버렛져는 약 98만개의 다이아몬드 정보를 블록체인에 등록하고 레이저코드를 입력해

155) https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/

해당 다이아몬드의 거래내역과 진품 여부를 확인할 수 있는 서비스를 제공 중이다. 올해 초부터는 인증 대상 범위를 미술 작품으로 확대하여 전시 작품 및 전시회 데이터베이스를 블록체인에 구축하여 위변조 여부를 확인할 수 있는 시스템을 개발 중이다.[156] 금년 7월에는 러시아의 시계 브랜드인 Raketa가 블록체인 기업과의 협업을 통해 블록체인 네트워크에 상품 정보를 등록하고 정품 인증을 제공하는 서비스를 개발 중이라고 발표했다.[157]

나. 자본시장 거래 플랫폼

비트코인 블록체인은 분산된 네트워크를 통해 거래되는 비트코인이라는 가상화폐를 실시간으로 추적할 수 있다는 장점을 가지고 있다. 이러한 기술적 장점을 바탕으로 블록체인은 단순히 돈 뿐만 아니라 주식, 채권 등 가치를 지닌 증권을 거래할 수 있는 플랫폼으로서 주목받고 있으며, 특히 자본시장에서 증권을 거래할 수 있는 플랫폼으로 개발되고 있다. 우선 블록체인을 활용하여 장외 주식 거래를 효율적으로 처리할 수 있는 시스템을 개발하는 데 많은 관심이 집중되고 있다. 장외 주식 거래는 일반적으로 거래를 담당하는 거래소 등의 중개를 거치지 않고 개인 간의 합의로 이루어지는 비상장주식의 거래를 의미한다. 일반적인 주식 거래와는 달리 공식적인 플랫폼이 없고, 플랫폼이 있더라도 직접 거래를 중개하기보다는 거래 정보를 게시할 수 있는 게시판 정도의 수준이기 때문에, 거래 대상을 찾고 이를 완결시키기까지의 과정이 매우 복잡하다. 또한 공식적인 플랫폼이 존재하지 않기 때문에 여전히 전화, 이메일 등으로 거래 주문 및 확인이 이루어지는 등 효율성이 떨어지고 거래처리 시간도 오래 소요되며 거래과정에서 사기 위험에도 종종 노출되는 문제점이 있다. 국내에는 한국금융투자협회가 개설한 K-OTC라는 장외주식 거래 시장이 있지만, 비상장회사 중 공개회사만 등록이 가능해 다른 회사들은 개인적인 연락을 통해 계약을 맺거나 사설업체에 의존하고 있는 상황이다. 이와 같이 장외주식 거래 플랫폼의 부재와 복잡한 절차로 인해 많은 사건·사고들이 일어나는 등 불편함이 지속되고 있어 장외 주식 거래 활성화에 큰 어려움이 있다.

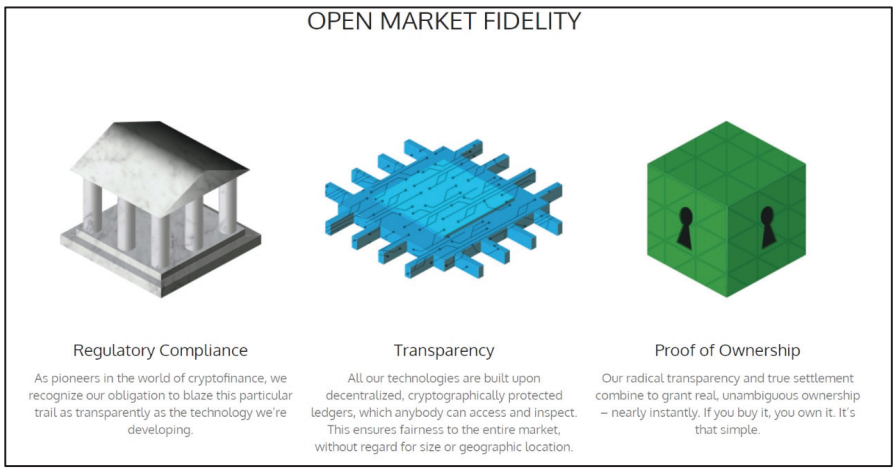
몇몇 자본시장 관련 기관들은 비활성화된 장외 주식 거래에 블록체인 기술이 대안이 될 것이라고 판단하고 블록체인 기반 장외 주식 플랫폼의 개발

156) http://www.coindesk.com/everledger-announces-partnership-vastari-combat-art-fraud/
157) https://bitcoinmagazine.com/articles/raketa-watches-trials-blockchain-technology-to-fight-counterfeiting-1467905237

및 상용화를 준비하고 있다. 거래내역이 투명하게 공개되는 블록체인은 장외 주식 거래에 신뢰를 확보할 수 있는 기반이 될 수 있고, 이미 중개인 없이 직접 거래되는 장외 주식 거래 시스템은 중개자 없이 운영되는 블록체인 플랫폼에 특히 잘 적용될 수 있을 것으로 보이기 때문이다. 현재까지 개발된 블록체인 기반 장외 주식 거래 플랫폼 중 가장 널리 알려진 것은 NASDAQ에서 10월 공개한 linq라는 플랫폼이다. 지금까지 외부에서 거래되던 장외 주식을 NASDAQ의 linq 플랫폼을 통해 거래하는 경우 거래의 투명성이 높아지고 신속한 서비스를 제공할 수 있을 것으로 기대된다.[158] 한편 NASDAQ은 linq에 적용된 블록체인 기술을 바탕으로 에스토니아 소재 거래소에 등록된 주주들을 대상으로 블록체인 기반 전자투표 시스템도 개발하여 상용화할 계획이다.[159]

한편 온라인 상거래 업체 Overstock은 블록체인 기반 주식 및 채권 거래 플랫폼인 t0를 개발했다. 여기서 t0는 기존의 거래가 청산 및 결제되는 데 통상 T+3일이 걸렸던 것과 달리 거래 즉시 청산과 결제가 이루어진다는 것을 의미한다. 동 t0플랫폼에서는 주주들이 자유롭고 신속하게 주식 거래를 할 수 있으며 이미 Overstock의 주식이 등록되었다고 발표하였다.[160]

<그림 1-8> Overstock의 주식 거래 플랫폼 t0



자료: t0.com

158) http://www.forbes.com/sites/laurashin/2015/10/27/nasdaq-unveils-blockchain-enabled-platform-linq-announces-6-inaugural-clients/#13707bbb30a3
159) http://www.coindesk.com/nasdaq-shareholder-voting-estonia-blockchain/
160) https://bitcoinmagazine.com/articles/sec-approves-overstock-com-s-filing-to-issue-shares-using-bitcoin-blockchain-1449539558

다. 전자 투표

블록체인은 분산된 네트워크를 통한 보안성을 확보할 수 있다는 장점과 거래 내역이 투명하게 공개되며 즉시 처리가 가능하다는 장점을 가지고 있어 이를 전자 투표 플랫폼으로 활용하기 위한 방안도 활발하게 연구되고 있다. 올해 8월 발표된 세계경제포럼의 블록체인 보고서에서는 일반적인 투표와 주주총회 등에서 이루어지는 위임 투표(proxy voting)를 블록체인의 대표적인 활용 분야 가운데 하나로 소개했다.[161] 특히 위임 투표의 경우 제3자의 개입이 많고 절차가 복잡해 투표율도 저조하고 오류가 생기는 경우도 많은데, 블록체인의 분산화된 네트워크를 통해 이를 극복할 수 있을 것으로 예상된다.

나스닥의 경우 에스토니아 주식시장을 담당하는 Nasdaq OMX Tallinn Stock Exchange 대상으로 블록체인 기반 전자 투표를 연구 중이라고 발표했다.[162] 나스닥은 현재 에스토니아의 주주 투표율이 낮은 상황이고 이미 에스토니아에 블록체인 기반 개인정보 플랫폼이 구축되어 있어 주식 투표 플랫폼 도입시 편익이 클 것으로 기대하고 있다.[163]

러시아의 경우 예탁결제원(National Settlement Depository)에서 블록체인 기반 전자 위임 투표(e-proxy voting) 플랫폼을 개발해 테스트에 성공했다고 발표했으며,[164] 러시아 정부도 블록체인 기술을 현재 개발 중인 전자정부 프로그램에 도입하여 지방정부의 의사결정에 시민들의 의견을 반영할 수 있는 투표 플랫폼을 개발 중이라고 밝혔다.[165] 하지만 블록체인 기반 투표 플랫폼의 경우 아직까지 확장성 문제와 투표에서 필요한 익명성의 문제를 어떻게 기술적으로 구현할 수 있을 것인가가 관건으로 남아있다.

라. 헬스케어 기록 관리 플랫폼

블록체인 활용 분야로서 최근 큰 주목을 받기 시작한 분야가 헬스케어 시장이다. 헬스케어 분야에서 개선사항이 필요하다고 평가받는 것은 환자의 건강기록 데이터를 각 병원, 업체마다 따로 보관하고 있다는 점이다. 환자의

161) The future of financial infrastructure, WEF, 102pg, 2016
162) http://ir.nasdaq.com/releasedetail.cfm?releaseid=954654
163) http://www.coindesk.com/nasdaq-shareholder-voting-estonia-blockchain/
164) https://www.cryptocoinsnews.com/russias-nds-uses-blockchain-for-e-proxy-voting/
165) http://www.coindesk.com/moscow-russia-government-blockchain-voting/

기록이 병원이나 업체들 간에 공유되지 않기 때문에 환자의 건강 상태를 모든 병원이 확인하는 데 많은 비용이 소요될 뿐만 아니라 환자 입장에서도 연속성 있는 치료를 받을 수 없다는 문제가 있다. 그렇다고 하나의 일원화된 통합 관리 시스템을 만들어서 모든 진료 기록을 등록 및 보관하기에는 관리하는 주체를 선정하기 어렵고 데이터가 안전하게 보관될 것이라는 보장을 하기 어려운 문제가 있었다. 헬스케어 시장에서는 데이터가 분산된 네트워크를 통해 등록 및 관리되고 지속적으로 동기화되는 블록체인을 활용하는 경우 환자의 기록을 관리 및 추적하기가 용이해짐으로써 효과적인 치료법을 제시하는 데 기여할 수 있을 것으로 기대하고 있다.

우선 지난 5월 미국 보건복지부(US Department of Health and Human Services)는 헬스케어 데이터의 상호 운용을 중심으로 블록체인을 헬스케어 분야에서 활용할 수 있는 방안에 대한 논문 경연대회를 개최했다.[166] 경연대회를 통해 70여개 이상의 아이디어가 제안되었고, 이 경연대회에 제출된 제안들을 바탕으로 하이퍼레저의 참가자인 IBM, 엑센추어 및 일부 스타트업이 헬스케어 분야에서 블록체인을 활용하기 위한 방안을 연구하는 조직을 만들어서 연구를 진행중이다.[167]

국가적으로 블록체인 기반 건강기록 시스템을 도입하고자 하는 사례도 있다. 블록체인을 기반으로 하는 디지털 신원 시스템을 보유 중인 에스토니아 정부의 경우 블록체인 기반 시스템을 국가의 헬스케어 시스템에도 도입하기 위해 준비 중이다. 현재 에스토니아 전자정부 시스템에 포함되어 있는 개인 건강기록부를 블록체인을 활용하여 실시간으로 업데이트해서 확인할 수 있으며, 이를 통해 건강 정보를 외부의 공격과 기록 위변조로부터 안전하게 지킬 수 있을 것으로 기대하고 있다.[168]

166) http://www.coindesk.com/health-human-service-department-seeks-blockchain-papers/
167) http://www.coindesk.com/hyperledger-launches-blockchain-working-group-for-healthcare/
168) http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/

Ⅱ. 개방형 / 폐쇄형 블록체인

본 장에서는 블록체인의 두 가지 유형인 개방형 블록체인과 폐쇄형 블록체인의 특징을 설명하고 각 블록체인이 가진 장점과 과제 그리고 활용 방안에 대해 서술한다.

1. 개방형 블록체인

가. 개방형 블록체인의 특징 및 장점

블록체인은 운영 방식에 따라 개방형 블록체인(Public Blockchain)과 폐쇄형 블록체인(Private Blockchain)으로 나눌 수 있다. 개방형 블록체인과 폐쇄형 블록체인은 분산된 네트워크를 통해 정보를 관리한다는 기본적인 개념은 동일하지만, 참여 기관의 제한 여부, 운영 체제의 차이를 갖는다. 아래는 개방형 블록체인과 폐쇄형 블록체인의 특징을 구분해 놓은 표이다.

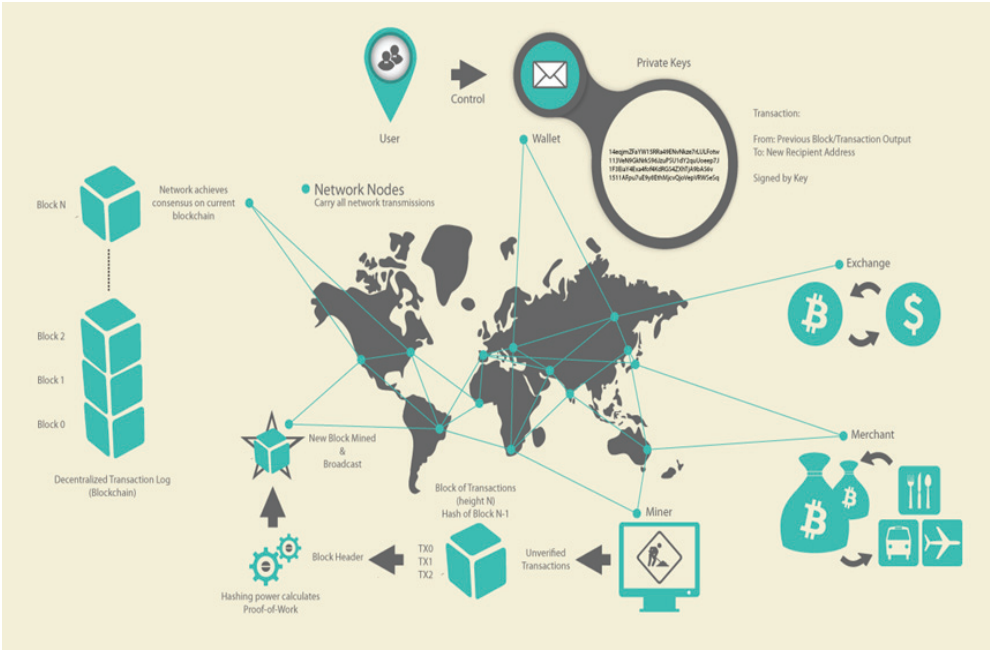
<표 2-1> 개방형, 폐쇄형 블록체인 비교

	개방형 블록체인	폐쇄형 블록체인
거래 기록의 열람	누구나 익명으로 잔고와 거래내역 열람 가능	통제기관과 거래당사자만 거래 기록 열람 가능
거래 참여	큰 인증 과정 없이 누구나 쉽게 계좌를 개설하고 거래에 참여	승인된 기관만이 거래에 참여 가능
거래의 검증/승인	누구나 에너지를 투입하여 검증/승인 과정 참여 가능	승인된 기관과 통제기관만이 거래의 검증/승인 과정 참여
거래의 보관	누구나 거래 내역을 보관할 수 있음	승인된 기관(e.g. 거래당사자)나 통제기관이 거래를 보관
합의의 도출	작업 증명 (Proof-of-Work), 지분 증명 (Proof-of-Stake) 등의 알고리즘으로 합의 도출	BFT(Byzantine Fault Tolerance) 계열 알고리즘을 통해 합의 도출
자체 암호화폐 필요 여부	필요함	꼭 필요하지는 않음
결제의 완결성 보장	네트워크 분기 (Fork) 등의 문제로 결제가 왜곡될 가능성이 존재	시스템적으로 결제의 완결성 보장
충분한 확장 가능성	제한적 확장	활용 방안에 따라 적합한 확장 가능
예시	비트코인, 이더리움	R3 CEV, DAH, Fidoledger

자료: 피넥터

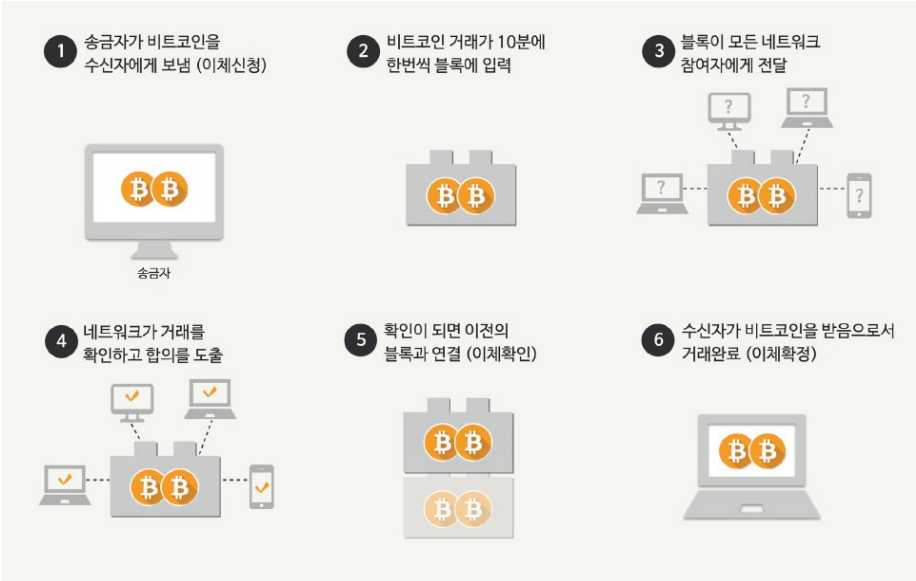
개방형 블록체인(Public Blockchain)은 참여 인원 혹은 기관의 제한이 없이 누구나 참여할 수 있는 블록체인 시스템을 의미한다. 개방형 블록체인은 대부분의 사람들이 생각하는 일반적인 블록체인의 개념으로, 누구나 제약 없이 블록체인에 참여할 수 있으며 특정한 기능을 구현하는 하나의 고정된 형태로 존재하는 플랫폼이다. 잘 알려져 있는 비트코인의 시스템이 개방형 블록체인의 대표적인 예시라고 할 수 있다. 이후 개방형 블록체인에 대한 내용은 비트코인 블록체인을 중심으로 서술한다.

<그림 2-1> 개방형 블록체인



비트코인 블록체인은 비트코인이라는 가상화폐를 거래하는 개방형 블록체인 플랫폼으로써 비트코인을 구매하고 소유한 사람은 물론 비트코인이 없지만 비트코인 주소를 가지고 있는 사람도 비트코인 프로토콜에 참여할 수 있고, 누구나 블록체인의 거래 내역들을 조회할 수 있다. 비트코인 블록체인의 운영 시스템은 다음과 같다.

<그림 2-2> 비트코인의 거래 절차



자료: 피넥터

한 사람이 다른 사람에게 비트코인을 전송하겠다는 거래 내역을 전송하면, 그 거래 내역은 거래 당사자의 주변 네트워크 참여자(이하 노드)에게 전파된다. 거래 내역을 받은 노드들은 거래가 문제없이 유효하다고 판단하면 다른 주변 노드들에게 전파를 하고 이 과정을 거쳐 모든 노드들은 거래 내역을 보유하게 된다. 이 거래의 전파는 몇 십초 정도의 매우 짧은 시간 안에 진행되며 결국 모두가 거래 장부를 확인하고 보유하게 하는 프로세스이다. 즉, 두 사람 간의 거래가 진행되는 동시에 비트코인 블록체인에 참여하는 다른 노드들에게 거래 내역이 전파된다.

한편, 노드들에게 전파된 거래는 검증과 승인을 위해 추가적인 절차가 필요하다. 그리고 전파된 거래가 검증되고 승인이 되기 위해서는 비트코인 블록체인 내의 핵심적인 시스템 유지 방식인 작업 증명(Proof-of-Work)과 채굴(mining)이 이뤄진다. 비트코인 블록체인에서는 일정한 연산을 계속해야 풀 수 있는 문제가 10분마다 만들어진다. 채굴자(miner)들은 이 문제를 풀기 위해 본인들의 컴퓨팅 파워를 투입한다. 암호화 해시 알고리즘을 기반으로 하는 이 연산에 대한 풀이를 작업 증명이라 부르고, 이 소모적으로 보이는 컴퓨팅 파워의 투입은 비트코인을 발행하고 내·외부의 공격으로부터 블록체인을 보호하는 보안의 기반이 된다. 작업 증명을 위해서는 각 문제에 설정된

솔루션이 나올 때까지 각 채굴자들은 SHA-256^2이라는 암호화 알고리즘을 통해 전체 비트코인 네트워크에 걸쳐 반복적으로 초당 수천 건의 암호화 작업을 진행해야 한다. SHA-256^2는 데이터를 암호화하는 기법 중 하나로 주어진 데이터를 특정 암호 알고리즘을 통해 데이터의 크기에 상관없이 32바이트, 즉 64자리의 결과값으로 치환하는 암호기법이다. 해당 암호기법은 언제나 같은 데이터를 동일한 해시값으로 전환하고, 데이터의 작은 변화에도 완전히 다른 해시값이 만들어지기 때문에 해당 거래의 암호값을 통해 위·변조의 여부와 진위여부를 파악할 수 있는 틀이 되며, 특정 자료의 진본 여부를 인증하는 서비스로 확장될 수 있다.

<그림 2-3> SHA-256 암호기법

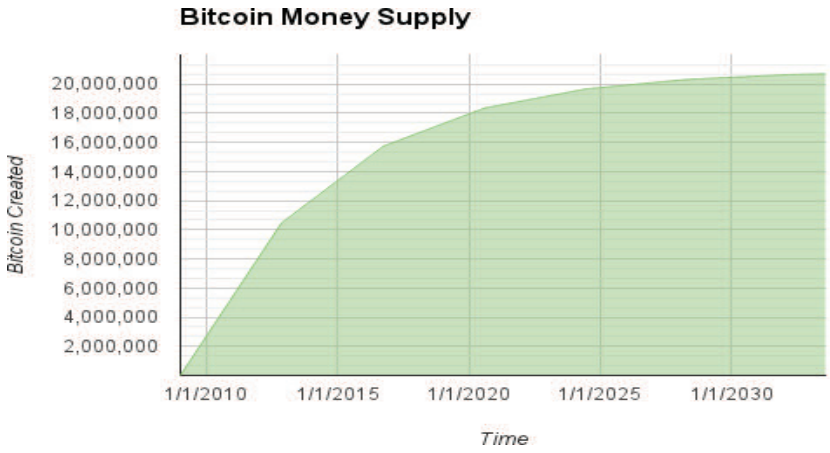
자료: 피넥터

채굴자의 컴퓨터를 일명 풀 노드(Full Node)라고 부른다. 풀 노드는 비트코인 블록체인 안에서 비트코인의 거래 정보를 저장하고 거래를 승인하는 등 비트코인 블록체인의 모든 과정에 참여하는 노드들을 의미하며 채굴 또한 이 과정에 포함된다. 현재는 전 세계적으로 약 7,000개의 풀 노드가 있으며 이들 각각이 저장하는 블록체인의 크기는 약 80GB이다. 노드에 대한 설명은 4장에서 더 상세히 서술한다.

문제의 난이도는 채굴자들이 함께 문제를 풀었을 때 10분 안에 풀 수 있는 수준으로 자동으로 조정된다. 정확히는 매 2,016개의 블록이 만들어질 때마다 난이도가 조정되는데, 새 블록이 약 10분마다 형성된다고 했을 때 약 2주간의 시간을 의미한다. 2,016개의 블록이 만들어지는 평균시간이 블록당 10분보다 짧으면 2,016개의 블록이 생성된 이후 난이도를 상향 조정해 블록 생성시간을 늘리고, 반대로 평균시간이 10분보다 길게 형성되면 이후에는 난이도를 하향 조정하여 블록 생성 시간을 줄이는 시스템이다.

이렇듯 컴퓨팅 파워를 투입하여 지난 10여분간의 거래 내역이 기록된 블록을 최초로 형성한 채굴자(혹은 집단)에게 승인한 거래 내역의 모음인 블록을 기존 블록체인(장부)에 등록할 수 있는 권한을 주고, 블록 생성을 통해 새롭게 발행된 비트코인을 보상으로 지급한다. 투입하는 에너지가 많을수록 채굴 경쟁에서 이겨 신규 발행 비트코인을 받을 확률이 높아지기 때문에 채굴만을 위해 엄청난 양의 컴퓨팅 파워를 투입하여 전문적으로 채굴을 하는 사례 또한 증가하고 있다. 최근까지 한 번의 채굴로 발행된 비트코인은 한 블록당 25BTC였으나 올해 7월 반감(halving)이 발생하여 채굴 비트코인 양이 이전의 절반인 12.5BTC로 줄어들었다. 한편 블록 형성에 성공한 채굴자는 신규 발행 비트코인과 함께 거래 과정에서 지급된 소액의 수수료 또한 추가 보상으로 받게 된다. 비트코인 프로토콜은 일정 기간(약 4년)마다 반감이 발생하여 최종적으로 2140년에 약 2,100만개의 비트코인이 발행된 이후에는 추가적인 채굴 없이 거래 수수료만으로 운영되게끔 설계되어 있다. 구조적으로 한정된 양의 금액을 발행하고 그 발행량도 시간이 지나면서 지수적으로 줄어들기 때문에 화폐 발행량 증가로 인한 인플레이션이 발생하지 않는 구조를 가지고 있다.

<그림 2-4> 비트코인 통화 공급량

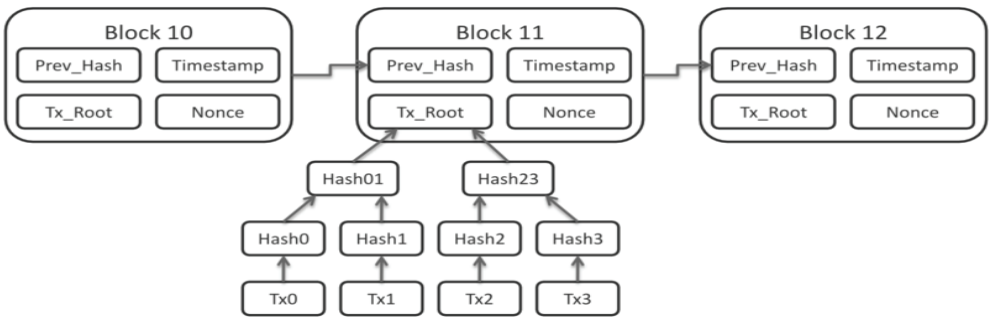


자료: Mastering Bitcoin

이러한 과정으로 만들어진 비트코인의 블록에는 거래 내역 및 정보가 저장되어 있다. 블록 내 핵심적인 주요 데이터를 담고 있는 앞부분을 블록 헤더(Header)라 부르고 이 블록 헤더에는 거래의 주요 정보들이 담겨 있다. 우선 블록 헤더에는 해당 블록의 직전 블록인 부모 블록의 암호(Hash) 값이 있다.

각 블록의 앞부분에 이전 블록의 정보가 연결되어 있는 구조이기 때문에 마치 블록이 연결되어 있는 것 같다는 의미의 블록체인이라는 이름이 지어졌다. 이러한 구조에서 과거에 생성된 특정 블록을 위변조하기 위해서는 다음 블록체인이 연결될 약 10분의 시간동안 그 블록 이후에 연결되어 있는 모든 블록을 새롭게 생성해 내야 하기 때문에 이런 구조적 특성이 블록체인의 위·변조를 사실상 불가능하게 만들며 블록체인을 비가역적 데이터라고 부르는 요인이 된다. 그 외에도 블록 헤더 부분에는 해당 블록 채굴 당시의 난이도, 블록 생성 시간을 보여주는 타임스탬프, 논스(Nonce)값이 표시되며, 모든 거래 내역의 요약본이라고 할 수 있는 머클 트리 루트가 표시된다. 머클 트리는 블록에 들어가는 수많은 거래 데이터를 요약하고 검증할 수 있도록 만드는 데이터 구조를 의미하며, 각 거래 내역을 암호화한 노드가 쌍으로 구성되어 하나의 노드로 합쳐져 다시 암호화되는 과정이 반복된다. 머클 트리의 과정을 거쳐 모든 암호화된 거래 내역이 요약되어 있는, 가장 상위에 있는 하나의 값을 머클 트리 루트라고 부른다. 아무리 많은 건수의 거래 내역이 요약되어 있다 하더라도 머클 트리 루트의 크기는 32바이트로 동일하다. 머클 트리 구조는 수많은 거래값을 요약해 헤더에 보관한다는 장점뿐 아니라, 요약된 거래 내용이 루트에서 출발하여 아래로 연결되어 갈라지는 모습을 하고 있기 때문에 루트와 거래를 연결하는 인증 경로를 통해 해당 거래의 유효성을 입증할 수 있고 잘못된 거래 내역이 발생할 시 짧은 시간에 신속하게 파악이 가능하다는 장점이 있다. 머클 트리에 대한 추가적인 내용은 3장에서 서술한다.

<그림 2-5> 블록 헤더의 구성도



자료: Matthaus Wander

비트코인 블록체인으로 대표되는 개방형 블록체인은 일반적으로 하나의 단일한 목적을 가지고 운영되며 익명의 사람들이 참여할 수 있고 악의를 가진

참여자들의 공격을 막기 위해 채굴 등의 내부 시스템을 통해 구조적으로 신뢰를 구축한다. 우선, 개방형 블록체인의 장점은 중앙기관이 없어도 거래 플랫폼을 유지할 수 있다는 안정성에 있다. 이전에도 분산된 서버를 통한 P2P 네트워크를 활용한 사례는 있었지만 분산원장을 통한 가상화폐 플랫폼을 개발한 경우는 비트코인 블록체인이 처음이다. 가장 견고한 보안 체계가 필요한 화폐 시스템을 블록체인 네트워크로 구현하여 지금까지 중앙 기관 없이 운영되고 있는 비트코인은 개방형 블록체인이 가지고 있는 견고함과 안전성을 보여준다. 비록 마운트곡스나 홍콩 비트코인 거래소 해킹 등 거래소에서 비트코인이 유실된 사건들이 있었지만, 은행에 강도가 들었다고 해서 화폐 시스템에 대한 문제로 볼 수 없듯이 이는 비트코인을 담당하는 거래소에 국한된 사례로 볼 수 있다. 비트코인 블록체인 자체는 악의적 공격을 미연에 방지하고 대응할 수 있는 보안성을 가지고 있고 이는 개방형 블록체인 위에서 움직이는 비트코인이 여전히 화폐적 가치를 지니고 있는 기반이 된다.

또한 개방형 블록체인은 높은 개방성과 투명성의 장점을 가지고 있다. 일반적으로 금융거래를 하기 위해서는 개인정보 등록이나 계좌 생성 등 긴 절차를 가지고 있다. 금융에 있어서 정보와 보안은 가장 중요한 이슈이기 때문이다. 하지만 운영 주체가 없이 시스템만으로 운영되는 개방형 블록체인은 높은 진입장벽을 가지고 있는 기존 서비스들과 달리 시간의 제약없이 쉽게 주소를 만들어서 네트워크에 참여할 수 있고 일정한 컴퓨팅 파워만 있으면 원하는 역할을 모두 수행할 수 있다. 필요에 따라서는 채굴에만 참여할 수도 있고 전자화폐를 이용만 할 수도 있으며 블록체인 네트워크에 필요한 모든 역할을 수행할 수도 있다. 역할의 선택과 변화에 제약이 없다. 개방형 블록체인인 이더리움의 경우에도 누구나 모든 거래 내역을 확인할 수 있다. 비트코인에 등록된 모든 거래 내역, 수/발신 주소, 잔액 등의 기록을 다 확인할 수 있으며 이는 개방형 블록체인 내의 거래 시스템이 위·변조를 막고 위·변조 시도가 있을 시 실시간으로 검증할 수 있게끔 투명하게 운영되게 하는 기능을 한다.

나. 개방형 블록체인의 과제 및 대안

개방형 블록체인은 이름 그대로 모두에게 개방되어 있고 불특정한 익명의 참가자들이 참여할 수 있다. 그렇기 때문에 시스템 상으로 서로간의 신뢰를 가지고 거래를 하고 악의적인 내·외부의 공격을 방지하기 위해 높은 안정성

을 가진 시스템 구축이 필요하며 실제로 많은 장치들을 개방형 블록체인 내에서 구축하고 있다. 일반적인 화폐 시스템에서는 중앙은행 등 특정 기관이 유통 및 관리를 책임지고 그 기관에 대한 신뢰를 바탕으로 화폐 시스템에 대한 신뢰가 형성된다. 하지만 이와 달리 비트코인 블록체인의 경우 거래와 시스템을 전적으로 통제할 중앙기관이 아예 없기 때문에 익명의 참여자들 간의 신뢰를 형성하고 안전을 확보할 수 있는 많은 장치들이 개방형 블록체인을 안정적으로 운영할 수 있는 기반이 된다.

하지만 개방형 블록체인이 외부의 공격으로부터 완벽하게 자유로운 시스템이라고 부르는 데에는 한계가 있으며, 위에서 언급한 장점들이 오히려 단점이 되어 개방형 블록체인을 다른 분야로 응용하는 데 한계로 작용하기도 한다.

우선 비트코인 블록체인의 경우 분산원장 시스템을 기반으로 모든 거래 내역이 공개되는 투명성이 금융기관이 개방형 블록체인을 활용하는 데 제약이 된다. 개방형 블록체인에서는 모든 참여자가 모든 거래 내역을 조회할 수 있으며 각 계좌에 대한 정보도 찾아볼 수 있다. 개방형 블록체인의 투명성은 비트코인 시스템에 신뢰를 부여하고 높은 안정성을 가지는 데 결정적인 역할을 하지만 이 투명성은 블록체인을 다른 분야로 응용하는 데 제약이 되며 특히 금융기관에서 응용하기에 어려운 점으로 작용한다. 금융기관 간의 거래는 기본적으로 개인정보의 보안을 유지할 필요성이 크기 때문에 개인정보의 무제한적인 개방은 부적절하며, 금융기관 내에서도 공개하면 안 되는 기밀 자료들이 존재한다. 이렇듯 금융기관을 이용하는 고객과 금융기관들은 거래 내역이 자신의 거래와 관계없는 기관 및 단체에게도 공개된다는 사실을 받아들이기 쉽지 않을 것이다.

그리고 개방형 블록체인의 익명성 또한 활용성을 제약하는 요인으로 작용한다. 비트코인 같은 개방형 블록체인은 기본적으로 어떠한 참여의 제한이 없이 익명으로 거래가 이루어지는 플랫폼이다. 하지만 정반대로 금융기관이나 일반 기업에서는 고객의 정보를 아는 것이 매우 중요한 과제이다. 전 세계적으로 자금세탁 방지(Anti Money Laundring), 고객 알기 제도(Know Your Customer) 등과 같이 탈세, 마약 밀매, 테러자금 조달 등을 방지하기 위한 규제가 주요 이슈이며, 우리나라에서도 원칙적으로 본인 명의가 아닌 다른 사람의 이름으로 계좌를 만들거나 거래하는 것이 금지되어 있다. 따라

서 금융기관이 광범위하게 블록체인을 사용하기 위해서는 고객들이 실명으로 거래하는 시스템이 필요하며, 익명을 유지하며 사용할 수 있는 금융서비스는 매우 협소하거나 사실상 없다고 볼 수 있다. 이는 개방형 블록체인의 기본 전제인 익명성과는 사실상 정반대의 상황이기 때문에 금융기관과 일반 기업들이 개방형 블록체인을 그대로 사용하는 것은 매우 까다로운 일이다.

또한 개방형 블록체인은 효율성에 있어서도 한계점이 명확한데, 개방형 블록체인을 유지하는 데 필요한 과도한 시간, 비용 그리고 작은 용량 등이 지적된다. 우선 개방형 블록체인을 유지하는 데 많은 비용이 든다. 비트코인 화폐 시스템에서 화폐를 발행하기 위한 방법인 채굴은 비트코인 네트워크에서 신뢰성을 확보하기 위한 가장 중요한 장치이다. 위에서 언급했듯이 채굴이란 비트코인 네트워크의 참여자가 본인의 컴퓨팅 파워를 이용해 직접 거래를 승인하고 블록체인에 거래 내역을 등록한 후, 발행된 비트코인이 거래의 승인과 등록에 기여한 컴퓨터 중 하나에 보상으로 주어지는 과정을 말한다. 채굴은 익명의 참여자가 비트코인 블록체인을 공격할 수 없게끔 신뢰를 형성하고 비트코인 화폐 시스템을 운영하게 만드는 핵심적인 방안이지만 많은 시간과 많은 전력 소모량을 필요로 한다는 단점이 있다. 작업 증명과 채굴의 과정을 통해 시스템을 보호하는 컴퓨팅 파워를 가지게 되지만 거래 자체만을 놓고 봤을 때는 굳이 그렇게 많은 에너지를 소모할 필요가 없다.

또한 개방형 블록체인의 긴 승인 시간은 특히 금융기관에서 활용하기에는 시간적 비효율성이 있다. 일반적으로 비트코인 거래의 최종 승인은 6 Confirmation이라고 부르는데, 거래를 완료한 이후 6개의 블록이 만들어지면 거래 위·변조의 가능성이 사실상 없기 때문이다. 평균적으로 1개의 블록이 만들어지는 데 10분이 걸리기 때문에 통상 1시간 정도가 지나야 해당 거래가 완전히 안전하다고 판단할 수 있다. 일반적인 거래에서 승인까지 1시간이 걸린다면 그 화폐는 실질적인 활용도를 가진다고 보기 어려울 것이다. 가게에서 물품을 사고 결제를 하는데 최종 승인이 날 때까지 1시간이 걸린다면 이용에 큰 불편함이 초래되기 때문이다.

비트코인의 작은 거래 용량과 블록의 크기도 활용을 어렵게 만든다. 비트코인은 현재 1초에 약 7건의 거래를 처리하는데 이는 세계적 지급카드 네트워크인 비자(Visa)의 처리량인 초당 약 2,000건보다 한참 못 미치는 수준이다. 이는 거래가 기록되는 블록의 용량이 최대 1MB에 불과하고 거기에서도 활

용할 수 있는 공간은 제한적이기 때문인데, 따라서 일반적인 금융기관들이 요구하는 다양하고 많은 용량의 정보들을 처리하는 데는 큰 한계를 보일 수 밖에 없다.

또한 개방형 블록체인이 가진 비가역성은 금융기관이 활용하는 데 어려움으로 작용한다. 비트코인 블록체인의 경우 화폐를 발행하고 거래를 중개하는 중앙기관이 없는 혁신적인 모델이지만 화폐 시스템을 책임지는 중앙기관이 없기 때문에 거래시 사고 등이 발생하는 경우 모든 책임이 거래 당사자에게 귀속된다는 문제가 있다. 비트코인 주소나 거래금액을 잘못 기입해서 전송하는 경우에도 이에 대해 정정을 요청할 수 있는 중앙기관이 없으며, 비트코인 주소를 제외하면 송금을 받는 상대방에 대한 정보를 알 수 없기 때문에 서로 아는 사이가 아닌 한 잘못된 송금을 받은 사람을 찾는 것은 매우 어렵다. 또한 따로 비트코인 계정을 보관해서 관리하는 주체도 없기 때문에 비트코인 주소를 분실한 경우 다시 돈을 돌려받거나 계정을 찾을 수 있는 방법은 사실상 없다. 중개기관을 없앤 가상화폐 플랫폼이라는 비트코인 블록체인의 시스템은 금융기관의 관심을 가지게 할 만한 흥미로운 모델이지만 중앙기관이 관리하는 정보가 없는 분산화된 네트워크의 속성은 오히려 소비자 정보를 관리하고 중개함으로써 신뢰를 얻는 금융기관이 활용하기에 어려움으로 작용한다.

이렇듯 일반적인 개방형 블록체인은 익명의 다수가 참여할 수 있도록 견고한 시스템을 갖추고 있으나, 다른 분야로의 활용에 있어서는 여러 한계점을 가지고 있다. 하지만 이미 다수가 참여하고 목적과 기능이 제한되어 있는 기존 개방형 블록체인을 일방적으로 변형하거나 수정할 수 없기 때문에 개방형 블록체인의 장점을 유지하면서 새로운 기능들을 더하여 특정 기능을 강화하거나 활용도를 높인 개방형 블록체인들이 새롭게 개발되어 등장하고 있다.

우선 비트코인의 대체 암호 화폐(Alternative Cryptocurrency)인 알트코인이 있다. 알트코인은 비트코인 블록체인의 화폐적 기능의 개선을 위해 만들어진 대체 암호화폐들을 통칭하며 비트코인이 화폐로서 가지고 있는 확장성, 거래속도 등의 문제점들을 극복하고 더 활용도가 높은 암호화폐를 만들기 위한 시도들이다. 현재 거래되고 알트코인의 종류는 약 700개로 추산된다.[169] 대부

169) www.coinmarketcap.com

분의 알트코인은 비트코인과 유사한 시스템과 기능을 가지고 있기 때문에 비트코인과 기본적인 시스템은 동일하며, 많은 디지털화폐 거래소에서 다양한 알트코인들이 실제로 거래되고 있다. 하지만 비트코인이 암호 화폐 시장에서 차지하는 점유율이 약 90%에 달할 정도로 압도적이고 비트코인 블록체인에 투입된 자원과 인력이 많기 때문에 알트코인이 실질적으로 비트코인이 가진 화폐의 역할을 대신하기는 어려울 것이다. 하지만, 통화 발행의 속도와 발행량 조절, 합의 알고리즘을 변경하거나 새로운 기능을 추가하는 등의 변형을 통해 암호화폐의 기능적 확장과 활용에 있어서의 새로운 가능성을 모색하려는 시도가 이어지고 있다.

대표적인 예시로는 라이트코인(Litecoin)을 들 수 있다. 라이트코인은 가장 먼저 만들어진 알트코인 중 하나로 현재 비트코인, 이더리움, 리플에 이어 암호화폐 시가총액 기준 4위의 암호화폐이다. 주요 특징은 블록의 생성 시간을 10분에서 2분 30초로 단축하고 기존 비트코인에서 사용하던 SHA-256 암호화 방식 대신 Scrypt 방식을 사용하며, 총 화폐 발행량도 비트코인의 약 2,100만 코인보다 4배가 많은 8,400만 코인으로 늘어나는 등 기존 비트코인 시스템보다 빠르고 유연하고 확장성 있는 시스템으로 운영되고 있다.

이외에도 비트코인보다 더 강력한 익명성을 구현하기 위해 만들어진 모네로(Monero), 작업증명 채굴 방식 대신 순수한 지분 증명(Proof-of-Stake) 방식으로 구현하고 블록생성 시간을 1분으로 줄인 넥스트(NXT), 라이트코인으로부터 분기되어 나와서 2015년까지 1,000억 코인을 발행할 정도로 발행 규모를 높인 도기코인(Dogecoin) 등 기존 비트코인 블록체인의 시스템을 개선하여 더 확장성이 있고 활용이 쉬운 알트코인 개발이 이어지고 있다.

<그림 2-6> 암호 화폐의 자본 규모 순위 (10월 기준)

All Currencies

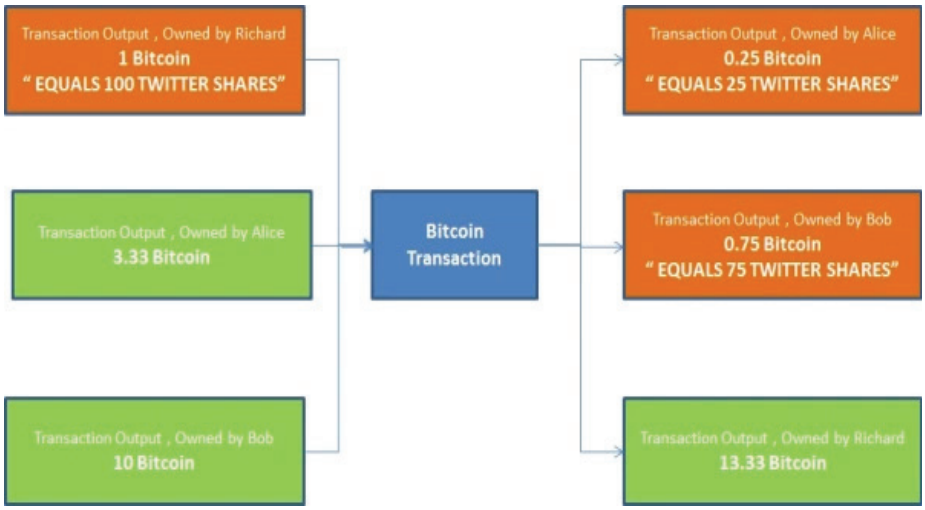
All ▾ Currencies ▾ Assets ▾ USD ▾ ← Back to Top 100

#	Name	Symbol	Market Cap	Price	Available Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$9,490,080,851	$597.49	15,883,140	$60,872,600	0.03%	0.04%	-1.80%
2	Ethereum	ETH	$1,121,526,200	$13.31	84,248,631	$23,603,100	0.66%	1.24%	11.37%
3	Ripple	XRP	$243,871,892	$0.006878	35,458,607,580 *	$1,506,640	0.04%	-0.38%	-11.96%
4	Litecoin	LTC	$179,891,543	$3.77	47,681,429	$1,071,260	0.20%	-2.06%	-1.00%
5	Monero	XMR	$133,190,360	$10.28	12,959,791	$3,189,580	-0.93%	-0.12%	6.23%
6	Ethereum Cla...	ETC	$107,031,359	$1.27	84,203,066	$5,405,380	-0.16%	8.17%	-0.80%
7	Dash	DASH	$78,331,006	$11.59	6,757,566	$414,224	0.17%	1.34%	-4.57%
8	Steem	STEEM	$71,868,313	$0.472179	152,205,654	$514,707	1.22%	13.28%	-5.31%
9	NEM	XEM	$46,750,500	$0.005195	8,999,999,999 *	$49,733	-0.17%	-4.46%	-6.90%
10	MaidSafeCoin	MAID	$38,454,238	$0.084972	452,552,412 *	$103,734	1.20%	-0.13%	-12.73%
11	DigixDAO	DGD	$30,063,000	$15.03	2,000,000 *	$112,260	6.50%	-5.70%	0.18%
12	Factom	FCT	$26,304,736	$3.01	8,753,219 *	$1,426,300	3.09%	-1.52%	-12.12%
13	Lisk	LSK	$24,408,300	$0.244083	100,000,000 *	$328,924	-0.20%	-1.39%	-4.29%
14	Dogecoin	DOGE	$24,079,742	$0.000227	106,153,917,124	$96,647	0.46%	-1.59%	-3.80%
15	Waves	WAVES	$18,922,000	$0.189220	100,000,000 *	$41,369	-1.25%	-1.34%	14.89%
16	Nxt	NXT	$15,640,044	$0.015656	998,999,994 *	$162,471	-0.20%	0.04%	-21.11%
17	Emercoin	EMC	$14,888,289	$0.385861	38,584,592	$38,105	-0.48%	-0.57%	-4.03%
18	Counterparty	XCP	$14,106,966	$5.38	2,623,195 *	$236,096	0.61%	8.77%	25.72%

자료: coinmarketcap

개방형 블록체인의 활용도를 높이기 위한 또 다른 방법으로는 컬러드 코인(Colored Coin)이 있다. 여기서 컬러드(Colored)라는 단어는 비트코인에 특정한 가치를 입힌다는 뜻으로 해석할 수 있다. 따라서 새롭게 블록체인을 만든 알트코인과는 달리 컬러드 코인은 기존의 비트코인 블록체인을 이용하는 방법으로, 비트코인 블록체인의 기록에 다른 자산 기록들의 정보를 '입히는' 방식으로 이용한다. 컬러드 코인을 사용하고자 하는 기관은 비트코인의 정보가 저장되는 공간에 유통하고자 하는 디지털 자산의 정보를 입히고 자산의 정보가 입혀진 코인은 해당 기관에 의해 관리된다. 컬러드 코인을 기반으로 자체적인 플랫폼을 만들어 해당 기관의 고객들이 하나의 가치를 가진 자산으로써 활용하되, 해당 기관이 컬러드 코인의 개인키를 가지고 있기 때문에 고객이 비트코인의 용도로 사용을 제한하고 컬러드 코인으로써만 사용하게 하는 환경을 조성할 수 있다. 연관성을 제거하여 컬러드 코인의 컬러를 뺄 수도 있고 그냥 비트코인으로 거래를 하여도 문제는 없다. 다만, 현재 성공적으로 발행 및 유통되고 있는 비트코인에 또 다른 가치를 입혀서 비트코인을 다른 방향으로 활용할 수 있는 방법 중에 하나로 볼 수 있다.

<그림 2-7> 컬러드 코인의 전개



자료: Richard Gendal Brown

컬러드 코인 기술은 법적으로 공식적인 효력을 갖지 않을 수도 있지만 이미 많은 참여자들과 컴퓨팅 파워가 투입되어 사실상 조작하는 것이 불가능할 정도로 견고한 비트코인 블록체인 구조를 바탕으로 특정 시점에서 자신의 소유권과 상태를 확인할 수 있는 수학적 근거로 제시될 수 있다. 다만, 컬러드 코인에 비트코인보다 훨씬 높은 가치의 자산이 입혀졌을 경우 비트코인 블록체인 시스템에 대한 공격의 유인이 될 수 있기 때문에 각 금융기관이나 단체가 당장 도입을 하기에는 한계가 있다. 현재 비트코인 블록체인에 투입되는 전력의 양은 연간 약 5천억원 규모로 추산하는데 이 금액을 넘어서는 자산이 컬러드 코인으로 거래가 된다면 외부에서 그 비용을 감수하고 비트코인 블록체인을 공격하는 유인이 생기게 되며 이는 블록체인 시스템 자체에도 큰 위협이 된다. 또한 서로 다른 기관이 만든 컬러드 코인끼리 거래할 수 있는 방식이 비트코인 거래로 제한된다는 점도 컬러드 코인의 활용을 어렵게 만든다. 결제의 동시성이 중시되는 금융거래에서 약 1시간 동안 승인을 기다려야 하는 개방형 블록체인 거래 메커니즘은 활용의 범위를 제약한다. 활용 확장성에 있어서의 한계점으로 인해 금융기관에서 컬러드 코인의 활용도는 떨어지지만, 최근에는 컬러드 코인의 메커니즘을 차용한 폐쇄형 블록체인 플랫폼들이 등장하고 있다. 대표적인 사례는 Colu라는 미국의 스타트업이다. Colu는 상품권, 티켓 등의 정보를 블록체인의 코인 형태로 등록하거나 새로운 코인을 만들어서 자유롭게 거래할 수 있도록 만든 블록체인 플랫폼으로 폐쇄형 블록체인을 활용했지만 블록체인의 코인에 특정 자산의 가

치를 입혀 거래를 용이하게 하는 컬러드 코인의 플랫폼을 차용한 사업 모델이다.

알트코인과는 다르게 화폐 플랫폼으로써 블록체인이 아닌 다른 기능에 주목하여 새롭게 만든 블록체인 프로토콜 또한 개방형 블록체인의 한계점을 극복하기 위한 방안으로 제시되고 있다. 앞에서 설명했던 이더리움과 리플 등이 그 예시가 될 수 있다. 최근 DAO를 통해 각광을 받은 이더리움의 경우는 기존 블록체인보다 스마트 계약(Smart Contract)의 기능을 강화하고 처리 속도를 높인 개방형 블록체인이며, 송금 및 결제 기능을 강화한 리플이나 스텔라(Stellar) 등의 개방형 블록체인 등도 등장하여 활용 방안을 찾고 있다. 하지만 아직까지 이러한 대안적 개방형 블록체인들도 한계점을 가지고 있다. 이더리움의 경우 최대 처리 속도를 12초로 대폭 단축하며 활용 가능성을 높였지만, 여전히 개발 초기 단계에 있고 프로토콜의 용량이나 보안의 문제에 있어서는 여전히 개선이 필요하다는 의견이 있다. 최근 발생한 DAO 해킹 사건의 경우에도 이더리움 블록체인 자체의 문제에서 비롯된 사고는 아니었지만 블록체인의 활용법에 있어서 문제점이 나타나는 경우 블록체인의 안전성에 상관없이 많은 사람들이 피해에 노출될 수 있음을 시사한다.

또 다른 개방형 블록체인에 대한 대안은 폐쇄형 블록체인(Private Blockchain)이다. 폐쇄형 블록체인은 블록체인에 참여하는 기관의 수를 제한함으로써 정보 공개 범위를 제한할 수 있으며 참여 기관이 공개하기를 원치 않는 회사 혹은 고객의 정보를 밖으로 드러내지 않을 수 있다는 장점을 가지고 있다. 폐쇄형 블록체인에 대한 상세한 설명은 다음 장에서 서술한다.

다. 개방형 블록체인의 활용 방식

개방형 블록체인의 경우 모두가 참여할 수 있는 플랫폼이지만 특정한 목적을 가지고 만들어진 블록체인 플랫폼인 만큼 활용에 제약이 많고 플랫폼 자체를 변형하거나 조작하는 것이 불가능에 가까워 이를 응용하여 다른 분야로 활용하기가 매우 까다로운 편이다. 하지만 개방형 블록체인의 경우 누구나 자유롭게 참여해 활용할 수 있는 공유지와 같은 플랫폼인 만큼 뒤에 언급할 폐쇄형 블록체인보다 일반적인 접근성이 뛰어나기 때문에 활용성의 제약에도 불구하고 쉽게 이용할 수 있다는 특징이 있다. 특히 과도한 중개자의 개입 필요성으로 인해 비효율성이 초래되는 분야에서 개방형 블록체인의 응

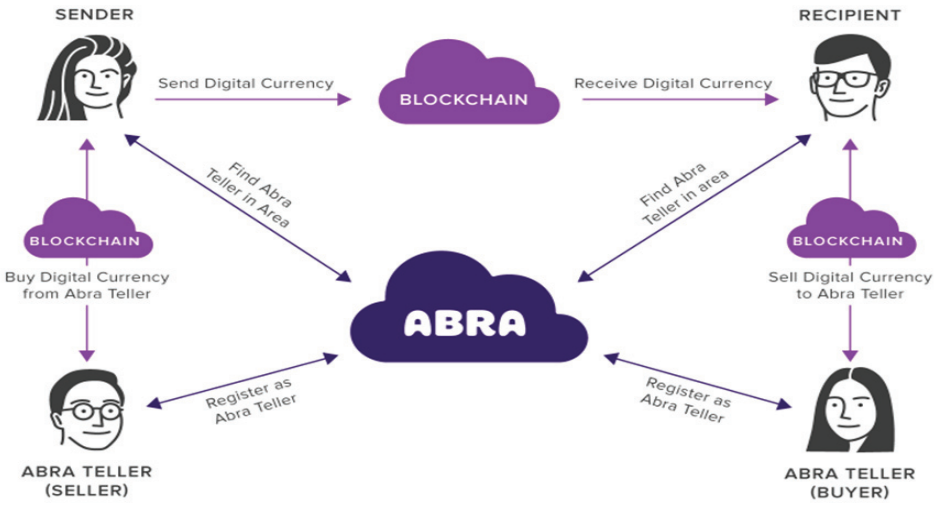
용이 적절히 활용될 수 있다.

(1) 해외 송금

가장 대표적인 분야는 송금, 그 중에서도 해외송금이다. 현재 해외송금의 경우 SWIFT 등의 전산망과 중개은행을 거치면서 많은 수수료가 부과되고 이는 특히 해외로 소액 송금을 하는 사용자에게 높은 수수료 부담으로 전가된다. 하지만 누구나 사용할 수 있으면서도 위·변조의 위험이 적고 화폐와 국경의 경계에 구애 받지 않는 비트코인 블록체인은 낮은 수수료로 돈을 전송할 수 있는 플랫폼으로 활용될 수 있으며 실제로 많은 스타트업이 이를 해외송금 플랫폼으로 활용하고 있다. 대부분의 경우 송금하게 될 금액을 해당 국가 화폐로 환전하기 전에 먼저 비트코인으로 전환하고, 전환된 비트코인을 해당 수신 국가의 화폐로 다시 전환하는 시스템을 적용한다.

대표적인 사례는 필리핀 기반 해외 송금 업체인 Abra다. Abra를 통해 필리핀에 거주하는 사람이 미국에 사는 사람에게 송금하려고 할 때, 송금 송신자는 우선 본인과 가장 가까이 있는 Abra 텔러를 찾아 송금할 돈을 건네준다. 금액을 받은 Abra 텔러는 해당 금액을 비트코인 블록체인 시스템에 전환하여 넣는다. 이후 송금 수신자는 본인과 가장 가까운 Abra 텔러를 찾아 송금한 금액을 요청하고, 수신자와 가까이 있는 텔러는 블록체인 내의 금액을 인출하여 수신자에게 지급하는 시스템이다. Abra는 비트코인 블록체인이 가진 개방성을 송금 서비스에 적용하여 성공한 사례이다. 리플의 경우 Abra 등 송금 업체가 활용하는 비트코인 블록체인과는 다르게 송금 및 결제에 특화된 자체 개방형 블록체인 프로토콜을 개발하고 여기에 금융기관들이 참여하고 있는 케이스다. 리플은 분산화된 네트워크를 통해 은행 간 혹은 국가 간 송금을 복잡한 절차 없이 빠르게 진행할 수 있다. 이와 같이 누구나 쉽게 활용할 수 있고 중개자와 국경의 경계 없이 활용할 수 있다는 비트코인 블록체인의 장점을 기반으로 송금 플랫폼을 만들어 수수료를 대폭 절감하고 송금 시간을 단축을 도모하는 사례들이 다수 생겨나고 있다.

<그림 2-8> 아브라의 개방형 블록체인 활용 구조도



자료: Abra

(2) 크라우드 펀딩

불특정 다수가 참여하여 금액을 모으고 투자하는 크라우드 펀딩도 개방형 블록체인을 적용할 수 있는 또 다른 분야이다. 특히 비트코인보다는 이더리움 등 타 개방형 블록체인을 통해 지속적으로 연구되고 있다. 계속 언급되는 DAO의 경우 이더리움이라는 개방형 블록체인 프로토콜 위에 얹어진 일종의 어플리케이션으로 누구나 참여할 수 있다는 개방형 블록체인의 장점을 이용해 이더리움 블록체인을 크라우드 펀딩에 적용한 사례라고 할 수 있다. 비록 이후 해킹 사고와 이후 처리 과정에서 논란이 발생하기도 했지만, 역대 모금액 1위의 이더리움 기반 크라우드 펀딩 플랫폼이었던 분산형 자치 조직 DAO가 개방형 블록체인을 활용한 크라우드 펀딩의 성공적인 예시라고 할 수 있다.

(3) 앵커링(Anchoring)

또한 개방형 블록체인은 기능적으로 폐쇄형 블록체인(Private Blockchain)을 보조하는 역할을 할 수도 있다. 뒤에서 언급할 폐쇄형 블록체인은 참여 기관의 수를 제한하는 블록체인 네트워크로서 참여기관의 현황 파악이 쉬우며 거래 내역을 추적하기에 용이하다. 하지만 참여기관이 소수이기 때문에 개방

형 블록체인에 비해 내부자에 의한 데이터 공격에 취약점을 노출할 수 있으며, 외부 기관이 폐쇄형 블록체인의 데이터가 위·변조 및 조작되지 않았고, 100% 신뢰할 만한 블록체인 시스템이라는 수학적 근거를 제시하기가 어려울 수도 있다. 개방형 블록체인은 앵커링(Anchoring)이라는 방식으로 이러한 폐쇄형 블록체인의 취약성과 신뢰의 문제를 해소하는 데 도움을 줄 수 있다. 앵커링은 폐쇄형 블록체인의 데이터를 암호화하여 개방형 블록체인의 블록 안에 저장하는 기술을 말한다.

비트코인 블록체인의 경우 전 세계적으로 네트워크가 구축되고 이미 많은 블록이 형성되고 컴퓨팅 파워가 투입된 블록체인 네트워크이기 때문에 위·변조에 대한 문제가 사실상 없다고 할 수 있다. 비트코인 블록체인에 폐쇄형 블록체인 데이터의 해시값을 등록함으로써 기존 데이터에 대한 신뢰도를 확보하고 거래 위·변조 여부에 대한 증거로 응용될 수 있다.

<그림 2-9> 앵커링 구조도

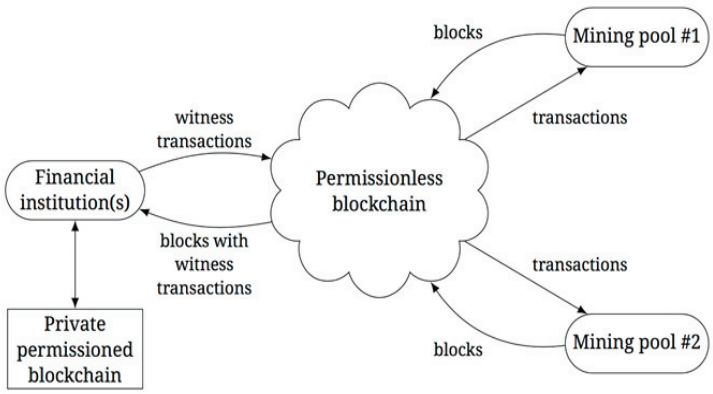


Figure 5: Anchoring a private permissioned blockchain with the supporting public blockchain (e.g., Bitcoin). Unlike merged mining, anchoring requires no or limited cooperation with mining pools

자료: Bitfury WhitePaper 2015

2. 폐쇄형 블록체인

가. 폐쇄형 블록체인의 특징 및 장점

위에서 언급한 바와 같이, 개방형 블록체인이 가진 여러 한계점들을 보완하

고 활용도를 높이기 위해 등장한 것이 폐쇄형 블록체인(Private Blockchain)이다. 금융기관과 기업들은 비트코인과 같은 개방형 블록체인을 통해 블록체인이 기존의 중앙화된 금융 및 산업 시스템의 비효율성과 문제점을 해결해 줄 분산화된 네트워크로써 대안이 될 수 있음을 알게 되었다. 하지만 위에서 언급한 한계점들로 인해 활용상에 많은 제약들이 있었고 이를 극복하기 위한 방안으로 개방형 블록체인의 기본적인 틀을 유지하면서 확장성을 높이는 폐쇄형 블록체인이 등장하게 되었다.

폐쇄형 블록체인의 기본적인 운영 원리는 개방형 블록체인과 크게 다르지 않다. 폐쇄형 블록체인 시스템도 기본적으로 특정 중앙서버가 없이 여러 노드들이 분산형 네트워크를 구성하고, 구성된 노드들의 승인 과정을 통해 데이터 모음이 완성되는 방식으로 이루어져 있으며, 이는 개방형과 폐쇄형 두 블록체인 시스템이 동일하다. 하지만 현재 개방형 블록체인이 가지는 확장성, 익명성, 활용성 측면에서의 한계가 명확하기 때문에 블록체인이 가지고 있는 비용, 보안, 속도 등의 강점만을 활용하기 위한 블록체인으로 개발된 것이 폐쇄형 블록체인이다. 위에서 언급한 R3 CEV, 하이퍼레저 등의 컨소시엄과 기업들의 블록체인 연구 사례들이 폐쇄형 블록체인을 만들고자 하는 대표적인 시도들이다.

즉, 폐쇄형 블록체인은 개방형 블록체인과 활용상 제약을 극복하고 각 분야에 맞게 개량해서 만들어진 블록체인을 통칭한다. 그렇기 때문에 따로 표준화된 기준이나 모델은 없지만 하나로 묶이는 가장 큰 폐쇄형 블록체인의 특징은 블록체인을 사용하는 기업 혹은 기관의 용도와 목적에 맞게 참여자의 수를 제한하고 블록체인의 기능을 변형하였다는 점이다.

우선, 폐쇄형 블록체인은 목적과 상황에 맞게 승인된 기관만이 거래에 참여할 수 있고 거래 기관의 종류와 수도 제한할 수 있다는 특징이 있다. 하나의 블록체인을 만든 후 참여 기관을 제한하여 받아들이는 방법도 있고, 아예 다수의 기관들이 같이 모여서 컨소시엄 형태로 서로 합의 하에 새로운 폐쇄형 블록체인을 함께 구성할 수도 있다. 기관들의 참여에 제한을 두기 때문에 개방형 블록체인과 달리 참여 기관이 어디인지 알 수 있는 기명 블록체인 네트워크를 구성할 수 있고, 그렇기 때문에 참여 기관의 신뢰성 확보가 쉽다는 장점을 가진다. 기관의 수와 종류에 제한을 둘 수 있을 뿐만 아니라 권한도 차등적으로 설정할 수 있다. 개방형 블록체인에서도 역할의 구분은 존재하지

만 각 참여자가 임의로 역할을 설정하거나 변경할 수 있으며, 구조적으로 개별 참여자를 통제할 수 있는 방법은 없다. 하지만 폐쇄형 블록체인은 참여하는 블록체인의 합의, 거래, 검증 등의 역할을 미리 정하여 구성할 수 있기 때문에 블록체인의 기능을 더 효율적으로 수행할 수 있다.

또한 폐쇄형 블록체인은 참여 기관의 수가 제한적이고 기관의 현황 또한 알기 쉽기 때문에 어떤 기관이 언제 거래를 했는지에 대한 내역도 보다 구체적으로 파악할 수 있다. 개방형 블록체인의 경우 거래 내역이 모두에게 투명하게 공개가 되지만 거래에 참여하는 사람들은 익명의 다수이기 때문에 거래에 문제가 생겼더라도 누가 문제를 일으켰는지 알아내기가 어렵다. 하지만 폐쇄형 블록체인에서는 해당 네트워크의 허가를 받은 제한된 참여자들만으로 구성되기 때문에 거래 당사자가 누구이며 거래 내역은 어떤지 파악하기가 용이하다. 이는 기존 개방형 블록체인이 익명의 다수에 대한 보안을 위해 조성한 작업 증명 등의 에너지 소모적인 방법 대신 더 낮은 비용으로 효율적인 보안 시스템을 구성할 수 있다는 장점으로도 이어진다.

그리고 특정 사안에 있어서 논의를 하고 합의를 이끌어내는 데 있어 개방형 블록체인보다 구성원의 의견을 모으는 데 용이하다. 이에 더하여 참여자의 현황과 거래 내역을 쉽게 파악할 수 있다는 특성은 개방형 블록체인에서 다수의 익명의 참여자들 간의 신뢰를 구축하기 위한 시스템을 운영하기 위해 만들었던 채굴 등의 장치들을 다른 효율적인 방법으로 대체할 수 있다는 장점이 있다.

그리고 폐쇄형 블록체인은 참여 기관들이 모든 정보를 공유할 필요가 없다는 장점도 있다. 개방형 블록체인은 기본적으로 블록체인 네트워크에 참여하는 노드들이 거래를 검증하고 전파하여 모든 노드들이 장부를 보유하는 시스템이기 때문에 모든 참여자들이 다른 참여자들의 거래 내역을 확인하고 공유할 수 있으며, 이는 장부 조작을 막을 수 있는 수단 중 하나가 되었다. 하지만 이러한 구조는 정보에 대한 보호가 필수적인 금융기관들이 활용하기에는 많은 리스크를 가지고 있다는 문제가 있었다. 하지만 폐쇄형 블록체인은 각 참여자들이 어떤 자료를 공개하고 하지 않을 것인지, 공개한다면 어떤 범위까지 공개를 할 것인지 범위를 설정할 수 있다. 이는 블록체인의 투명성, 효율성 등 기존에 가지고 있던 장점을 유지하며 활용도를 높일 수 있는 근간이 된다.

또한 폐쇄형 블록체인을 통해 기존의 개방형 블록체인보다 비용 절감에서도 이점이 있다. 분산형 네트워크인 블록체인은 중앙 서버를 관리하고 유지하는 비용을 절감할 수 있다는 장점이 있었지만, 개방형 블록체인의 경우는 외부의 공격과 블록에 대한 조작 등 보안상의 문제를 해결하기 위해 작업증명과 채굴이라는 과정을 통해 실제 거래에 필요한 양보다 훨씬 많은 에너지와 전기를 사용하여 시스템을 보호하도록 설계되었다. 하지만 참여 기관을 제한하도록 설계된 폐쇄형 블록체인은 이같은 소모적 보안 시스템 없이도 네트워크를 구성할 수 있게 되었으며, 데이터베이스의 분산을 통해 비용을 절감할 수 있는 효과를 누릴 수 있다. 그리고 익명의 다수의 안전한 거래를 위해 필요한 10분간의 거래 검증 시간도 다른 보안의 방법으로 대체할 수 있게 되기 때문에 거래 검증의 시간을 대폭 단축하고 초당 거래 건수도 확장할 수 있는 등 활용상의 유연성을 확보할 수 있게 된다.

나. 폐쇄형 블록체인의 과제 및 대안

모든 폐쇄형 블록체인에는 자료와 거래 내역의 공개 범위 제한을 기술적으로 어떻게 구현할 것인가의 과제가 있다. 가령 중앙은행이 주관하고 금융 기관들이 참여하는 블록체인을 구성했을 때, 각 금융기관들은 중앙은행에는 공개할 수 있지만 타 금융기관에는 공개하고 싶지 않은 정보들이 있다. A은행이 B은행에 송금을 한다고 가정했을 때, A은행과 B은행은 이 거래 내역은 거래를 한 당사자와 중앙은행에는 공개하겠지만 타 은행에는 공개하기를 원치 않을 것이며 공개할 필요도 없을 것이다. 하지만 개방형 블록체인의 작업증명 방식을 그대로 폐쇄형 블록체인에 적용한다면 민감한 정보를 노출하기 원하지 않는 금융기관들은 해당 블록체인 네트워크에 참여를 꺼리게 될 것이다. 따라서 폐쇄형 블록체인을 구성할 때 각 금융기관의 정보를 어디에게 어느 정도까지 공유할 것이며, 그 공유 범위를 기술적으로 어떻게 설정할 것인가가 폐쇄형 블록체인 활용에서 가장 중요한 요소 중 하나라고 할 수 있다. 이에 대한 기술적으로 블록체인 내의 공개키(Public key)와 개인키(Private Key)의 Control을 통해서 구현할 수 있다. 접근 권한에 대한 기술적 통제 방안은 제 3장의 블록체인 기반 지급결제시스템에서 상세히 서술한다.

또한 폐쇄형 블록체인에서 중요한 점은 어떻게 하나의 합의된 시스템을 구축할 것인가에 있다. 비트코인 블록체인 등의 개방형 블록체인의 경우, 모두가 접근하여 블록체인을 사용할 수 있는 구조이다. 한편으로 모두가 접근할

수 있다는 의미는 비트코인을 사용하고 비트코인 블록체인의 일원이 된다는 것이고 이는 비트코인 블록체인이 가지고 있는 시스템에 합의를 한다는 뜻이자 비트코인이 가진 채굴 등의 시스템과 블록체인에 담기는 정보, 거래 절차 등에 규칙을 따르겠다는 의미를 내포하고 있다. 반면, 폐쇄형 블록체인은 특정 기관들만이 참여하는 블록체인이기 때문에 접근성에 있어 제한을 둘 수 있지만, 기관들이 활용하기 위해 만들어지는 블록체인이기 때문에 블록체인을 개발하는 모든 부분에 있어서 합의를 도출해야 한다.

시스템에 대한 합의 내용은 기술적 측면도 있지만 각 참여 기관의 내역을 통합해야 한다는 정책적 측면도 존재한다. 예를 들어 금융기관들이 스마트 계약을 바탕으로 하나의 통합 폐쇄형 블록체인을 구축한다고 가정했을 때, 그 스마트 계약에는 어떤 내용들이 들어가야 할지, 금융 거래 유형을 어떻게 구분할지, 형식은 어떻게 갖춰야 할지, 정보의 접근 권한은 어떻게 설정해야 할지 등을 모두 고려해야 한다. 사실상 하나부터 열까지 다 합의를 통해 완전히 새로운 통합 시스템을 만드는 것이다. 각 금융기관은 기존에 유지하고 있는 시스템이 있고 그 시스템에 담긴 세부 내용 및 절차는 각자 달랐다. 이전 중앙화된 구조에서는 중개 혹은 결제를 담당하는 제3기관의 형식에 맞춰서 거래를 진행했지만, 폐쇄형 블록체인을 구성하게 되면 블록체인에 기록할 모든 사항에 대한 합의가 필요하기 때문에 많은 시간이 소요될 수밖에 없다. 지금까지는 합의와 조율을 담당하는 제3기관(예를 들면 외환 거래의 SWIFT망)이 그 역할을 수행했고, 제3기관으로 인해 초래되는 시간적, 비용적 비효율성을 블록체인이 해결해 줄 것으로 기대하고 있지만, 그 이전에 각 폐쇄형 블록체인이 합의안을 어떻게 구성할 것인가의 문제를 해결해야 할 것이다. 게다가 하이퍼레저처럼 업무상의 공통분모가 적은 금융기관과 비금융기관이 함께 사용하는 폐쇄형 블록체인을 만드는 복합적인 컨소시엄의 경우라면 특정한 합의점을 찾아내는 것이 더 어려운 일이다. 합의된 시스템을 구성하는 문제는 기술적인 영역도 존재하지만 블록체인 플랫폼에 채워질 내용의 문제로서 각 블록체인 컨소시엄 혹은 업체들이 블록체인의 활용에 있어서 시스템과 구성 요소에 대한 충분한 논의와 합의가 필요한 사항이다. 이를 해결하기 위한 1차적인 방안으로는 한 기업이 우선 주도적으로 블록체인 플랫폼을 개발하여 참여자들을 모으거나(R3 CEV가 이와 유사하다) 기업들이 모여 여러 플랫폼들을 개발하고 테스트하고 피드백을 받으면서 개선을 하는 방안이 있다(하이퍼레저가 이와 유사하다).

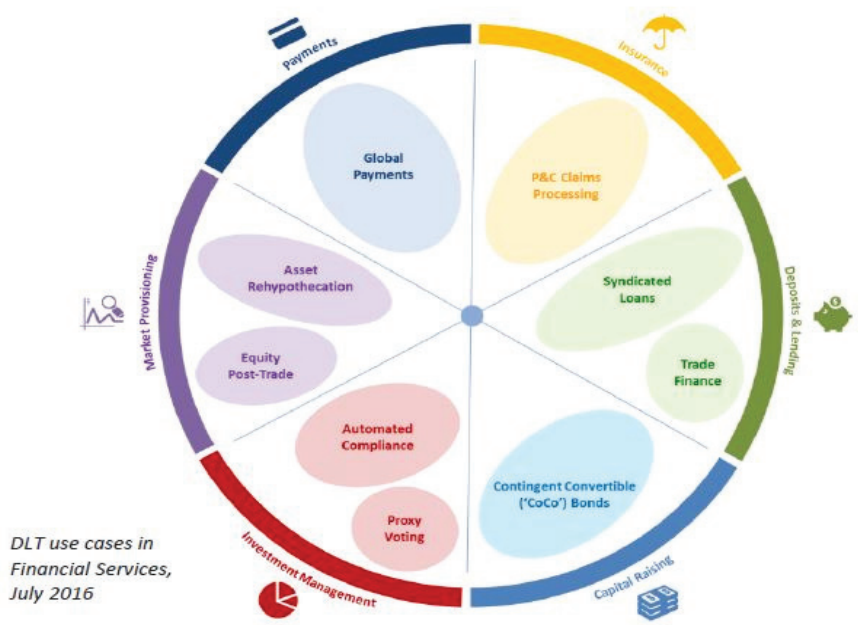
또한 폐쇄형 블록체인의 과제중 하나는 개방형 블록체인이 가지고 있던 보안 장치들을 대체하는 방법을 찾는 것이다. 개방형 블록체인이 높은 보안성을 가질 수 있는 이유 중 하나는 컴퓨팅 파워 측면에서 웬만한 수준으로는 공격할 수가 없는 시스템을 가지고 있기 때문이다. 비트코인 블록체인의 경우 수많은 컴퓨터가 자발적으로 블록체인 네트워크에 참여하고, 작업 증명과 채굴의 과정을 위해 수많은 전기 에너지가 비트코인 블록체인에 투입이 된다. 비트코인의 거래 내역을 조작 혹은 위·변조 하기 위해서는 해당 컴퓨팅 파워의 절반 이상을 보유해야 하는데, 이는 전세계 슈퍼컴퓨터 중 성능을 기준으로 상위 1위에서 500위까지의 용량을 합친 것보다 크다. 결국 구조적으로 공격하기가 거의 불가능에 가까울 뿐만 아니라, 공격이 가능할 정도의 에너지를 가지고 공격에 성공하더라도 비트코인 블록체인에 대한 경제적 이익을 볼 수 없고 오히려 손해를 보게 된다. 하지만 폐쇄형 블록체인은 참여기관의 수가 제한되어 있기 때문에 아무리 큰 기업들이 블록체인 네트워크에 참여하더라도 최대 용량에는 한계가 있으며 개방형 블록체인에 비해 쉽게 공격에 노출될 수도 있다. 또한 소수의 기관이 참여하는 만큼 내부 참여 기관의 악의적 공격에 대해서는 더 취약하기 때문에 내부 공격에 대비할 수 있는 합의 알고리즘 시스템과 관련 규정, 사용자 관리 방안 등에 대한 철저한 구성이 필요하다. 금융기관의 경우 블록체인의 활용은 돈과 이에 관련된 정보에 직결되는 문제이고 중앙은행의 경우 한 번의 보안상의 문제도 국가 경제에 큰 손실을 일으킬 수 있는 만큼 어떻게 폐쇄형 블록체인이 내·외부적 문제에 대해 안심할 수 있을 정도의 보안 체계를 구축하는가는 폐쇄형 블록체인의 운영에 있어서 중요한 문제이다.

내부적 보안 문제를 보완할 수 있는 대안 중 하나로 개방형 블록체인의 활용 사례로 언급한 앵커링을 들 수 있다. 앵커링은 내부 자료가 위·변조가 되지 않았다는 수학적, 구조적 신뢰도를 얻기 위한 방법으로 폐쇄형 블록체인의 정보를 암호화하여 비트코인 블록체인의 블록 내에 연결하여 해당 거래가 위변조가 되지 않았다는 신뢰를 확보할 수 있는 방안이다. 하지만 이는 보안에 대한 근본적인 대책이라기 보다는 파일들이 위·변조되지 않았음을 증명하는 방법에 그친다는 한계가 존재한다.

다. 폐쇄형 블록체인의 활용 가능 분야

폐쇄형 블록체인은 개방형 블록체인이 갖는 활용상의 한계를 극복하기 위해 참여 기관을 제한하는 모든 블록체인을 통칭하는 표현이고, 활용하고 싶은 블록체인의 특징들을 선택하여 만드는 블록체인이다. 블록체인으로 구현하고자 했던 모든 분야에서 활용할 수 있기 때문에 활용 방안은 다양하다. 앞선 사례들에서 언급한 기업, 정부, 금융 기관 등이 활용하고자 하는 블록체인은 대부분 기업이 자체적으로 개발하거나 블록체인 기업과 협업하여 만드는 폐쇄형 블록체인이며 이를 가상화폐, 개인 문서 및 정품 인증, 유통, 결제 및 청산 시스템 등 다양한 분야에서 활용하여 시스템의 효율성을 제고하고자 하고 있다. 실제로 올해 8월에 세계경제포럼(WEF)에서 발표한 분산원장 보고서에 따르면 블록체인은 금융 시장의 결제, 협조 융자, 보험, 무역금융 등 약 9개의 분야에서 활용할 수 있을 것이라고 발표했는데,[170] 이는 기존의 개방형 블록체인의 확장성의 한계를 넘어서 기술적으로 발전한 폐쇄형 블록체인이 등장하기 시작했기 때문에 가능한 결과이다.

<그림 2-10> 금융 기관의 분산 원장 활용 케이스



자료: WEF

170) The future of financial infrastructure, World Economic Forum, 2016

(1) 결제 시스템

폐쇄형 블록체인은 개방형 블록체인이 가진 분산형 네트워크를 유지하기 때문에 데이터의 분산화와 실시간 검증이 가능하다는 장점을 가진다. 거기에 더하여 폐쇄형 블록체인은 기존의 개방형 블록체인이 가진 처리속도상 한계를 극복(비트코인의 경우 1초당 평균 7건의 거래를 처리하기 때문에 초당 수천 건의 거래를 처리하는 금융 기관의 거래량을 감당하기 어려움)하고 더 많은 거래량과 신속한 합의 체계를 구현할 수 있어 금융기관의 결제 시스템에서 많이 활용될 수 있다.

기존 분산형 네트워크의 장점을 유지하여 정보를 실시간으로 처리하며 검증할 수 있는 블록체인은 해외 송금이나 문서, 자산을 전송하는 업무에 용이하게 적용될 수 있다. 중개기관이나 검증 절차 필요 없이 실시간으로 정보를 동기화하여 공유할 수 있기 때문에 결제 리스크를 줄일 수 있다. 다만, 불특정 다수가 참여하는 개방형 블록체인의 경우 정보의 보안을 중시하는 금융기관에서는 활용이 어렵기 때문에 자체적인 폐쇄형 블록체인 개발을 통해 결제 시스템을 구현하고자 하는 사례들이 있다. 앞에서 언급한 디지털 에셋 홀딩스가 대표적인 사례가 될 수 있다.

(2) 자체 운영 디지털 화폐

중앙은행과 은행이 주로 연구하는 금융기관 운영 가상화폐에 있어서도 폐쇄형 블록체인이 중심이 되고 있다. 비트코인으로 대표되는 개방형 블록체인은 통제하는 중앙기관 없이 통화를 발행, 유통 및 관리할 수 있는 혁신적인 사례이다. 비트코인 블록체인의 시스템은 금융기관에게는 디지털 화폐를 운영할 수 있는 기술적 가능성을 보여줬지만, 개방형 블록체인을 그대로 활용하기에는 확장성, 익명성, 높은 투명성 등이 문제가 되었다. 그로 인해 블록체인의 장점을 유지하면서도 금융기관에 맞는 디지털 화폐에 대한 필요성이 제기되었고 이 틀에 맞는 금융권들의 폐쇄형 블록체인 개발이 진행 중이다. 민간 금융기관 중에서는 1장에서 언급한 MUFG 코인이나 Utility Settlement Coin 등을 대표적인 사례로 들 수 있으며, 영란은행의 RSCoin도 이 경우에 해당한다.

(3) 인증

블록체인이 가진 무결성과 보안성을 바탕으로 인증 서비스에 활용하는 방안이 활발히 개발되고 있다. 블록체인 자체에 문서를 올린다기보다는 문서가 가지고 있는 고유의 암호값을 만들어 이를 블록체인에 등록하고 블록체인에 등록된 암호값을 통해 디지털 정보가 진본인지 아닌지를 확인할 수 있는 플랫폼으로 활용하고 있다. 많은 고객의 기밀 정보를 보관하는 금융기관이나 다양한 국민들의 정보를 관리해야 하는 공공 기관에서 블록체인을 활용한 인증 서비스를 구축하고 있다. 개방형 블록체인의 경우 확장성의 문제와 활용의 제약 등으로 넓은 범위의 활용이 쉽지 않기 때문에 폐쇄형 블록체인으로 개발하여 문서의 처리량과 속도를 높이고 안전성을 담보하고자 하는 시도들이 진행중이다. 국내에서는 KB국민카드가 블록체인 기업인 코인플러그와 함께 블록체인 기반 개인인증 서비스를 개발하여 11월 국내 최초 서비스 상용화를 준비하고 있으며,[171] IBM과 마이크로소프트도 인증 플랫폼을 개발중이다.[172][173]

(4) 무역 금융(Trade Finance)

현재 무역금융 시스템은 국제송금 시스템과 유사하게 복잡한 절차에 따른 시간적, 비용적 비효율성을 가지고 있다. 다수의 중개기관을 통해 문서와 금액이 보내지기 때문에 중개기관을 통해 이동하는 시간 동안 결제 리스크에 노출되며 중개기관에 지불해야 하는 비용도 높다. 또한 많은 문서들을 확인하고 전송하는 작업이 상당 부분 여전히 수작업으로 진행되기 때문에 이 과정에서도 시간의 지연과 실수가 발생하고 결제 리스크가 발생한다.

세계 주요 금융기업들은 무역금융 블록체인 플랫폼을 연구하거나 출시했다. UBS는 IBM과 함께 하이퍼레저를 기반으로 무역의 전 과정을 관리할 수 있는 블록체인 플랫폼을 개발 중이라고 발표했고[174] JP Morgan, 바클레이스나 뱅크 오브 아메리카 등의 금융기관들도 일제히 스마트 계약 등을 통해 무역금융의 프로세스를 자동화, 일원화 할 수 있는 무역금융 플랫폼을 개발하고 있다.

---

171) http://news.mk.co.kr/newsRead.php?no=739530&year=2016
172) http://www.coindesk.com/microsoft-identity-platform-multiple-blockchains/
173) http://www.coindesk.com/ibm-completes-blockchain-trial-french-bank-credit-mutuel/
174) http://www.coindesk.com/ubs-blockchain-prototype-trade/

(5) 스마트 계약(Smart Contract) 관련 플랫폼

스마트 계약은 자기 강제적 언어(self-enforcing language)로 특정 조건을 프로그램화하여 조건이 충족되면 자동으로 실행이 되는 컴퓨터 코드이다. 예를 들어 채권을 스마트 계약에 등록을 한다고 가정했을 때, 만기, 이자율, 지급 지시 등의 내용을 코드로 블록체인에 입력하면 이에 따라서 자동으로 시행되는 방식이다.

사실 스마트 계약 자체는 폐쇄형 블록체인에만 해당하는 내용은 아니다. 비트코인의 경우에도 작업증명 및 채굴의 과정이 일종의 스마트 계약을 기반으로 하는 프로그램이라 볼 수 있으며, 이더리움의 경우에는 스마트 계약에 특화되어 여러 프로그램들을 실행할 수 있는 프로토콜로 발전하고 있다. 블록체인을 도입하는 금융기관 혹은 단체가 폐쇄형 블록체인을 기반으로 하는 자체적인 블록체인 플랫폼을 구축하고자 하는 경우 이더리움을 기반으로 자체적인 블록체인을 만드는 프라이빗 이더리움(Private Ethereum) 플랫폼을 활용하거나 자체적으로 스마트 계약을 입힌 폐쇄형 블록체인을 도입할 수 있다.

전자투표, P2P 펀딩 등 현재 복잡한 절차를 가지고 있거나 많은 부분 수작업으로 이뤄지고 있어서 보안 및 결제 리스크에 노출되는 금융 서비스들을 위주로 스마트 계약을 이용한 서비스 플랫폼 개발이 활발하다. 아직까지 스마트 계약 프로그램은 많은 측면에서 추가적인 개발이 필요한 부분이 있지만 많은 폐쇄형 블록체인 기업들이 이를 블록체인의 활용도를 높일 수 있는 핵심적인 기술로 인식하고 연구개발을 적극 추진중이다.

결국 현재 폐쇄형 블록체인은 중앙화된 시스템이나 과도한 중개기관의 개입 혹은 수동으로 진행되는 절차 등으로 효율성이 떨어진다고 판단되는 분야를 중심으로 논의 또는 적용되고 있다. 이 경우 블록체인을 통한 비용의 절감, 절차의 간소화, 거래 시간의 단축 등 많은 부분에서 개선을 이끌어낼 수 있기 때문이다.

Ⅲ. 중앙은행의 블록체인 활용 방안

본 장은 신한은금융망에 대한 설명과 블록체인기술을 신한은금융망에 적용하는 방안에 대해 기술한다. 해당 장에서 설명하고 블록체인 기술을 적용하는 신한은금융망은 한국은행과 금융기관 간의 거래를 담당하는 거액결제시스템, 그 중에서도 혼합결제시스템으로 범위를 좁혀서 기술한다.

1. 한국은행의 지급결제시스템의 구성

가. 신한은금융망의 혼합형 결제 시스템

한국은행은 기존의 한은금융망을 개선한 신한은금융망(BOK-Wire+)를 개발하여 2009년부터 운영하고 있다. 신한은금융망을 운영하기 이전 기존 한은금융망은 금융기관들이 유동성 리스크에 잘 대처할 수 있도록 특정 시간에 모든 거래 내역을 확인하여 상계 처리하는 실시간 총액결제 방식으로 운영하고 있었다. 하지만 거래 유형이 다양해지고 거래량 또한 증가하면서 이에 걸맞는 새로운 금융망 시스템이 필요하게 됨에 따라 한국은행은 한은금융망에서 동시처리를 더 쉽게 하기 위해 혼합형결제시스템을 추가한 신한은금융망 시스템을 개발하여 운영하고 있다. 신한은금융망은 기존의 전용 단말기에 거래 내역을 입력하는 단일 방식에서 벗어나, 한국은행의 금융망과 금융기관의 서버를 연결하는 서버 간 직접접속 방식을 병행하여 사용함으로써 업무처리의 편의성과 신속성을 강화했으며, 양자간 거래 및 다자간 거래를 위한 실시간 거래 동시처리가 용이한 혼합결제시스템을 추가로 운영하여 신용리스크와 시스템리스크를 감소시킬 수 있게 되었다.

주요 지급결제 업무는 주로 혼합결제시스템에서 처리되는데, 혼합결제시스템에서 관리하는 업무는 크게 세 가지로 나뉜다. 수취인 지정 자금 이체를 포함하는 금융기관 간 일반 자금이체 업무와 콜거래 자금결제 업무, 그리고 증권대금 동시결제(DvP)가 혼합결제시스템의 업무이다.

현재 신한은금융망에 참여하고 있는 금융기관들은 약 130여개이다. 각 금융기관들은 한은금융망에 연결되어 있는 전용 단말기를 통해 한은금융망에서 거래를 진행한다. 이후 신한은금융망이 등장하면서 국내 대형 은행과 일부

증권사, 콜거래 기관은 서버 직접 접속 방식을 통해 바로 신한은금융망을 사용하거나 단말기와 서버 접속 방식을 병행하여 사용할 수 있고, 나머지 기관들은 전용 단말기를 통해 신한은금융망을 이용하고 있다.

나. 일반자금 이체 업무

혼합형 결제 시스템에서의 일반자금 이체 업무는 금융기관 간의 동시 처리 필요성이 높은 이체 업무를 처리한다. 우선 일반자금 이체 업무는 결제 처리의 신속성에 따라 신속지급지시와 보통지급지시로 나뉜다. 신속지급지시는 빠른 시간에 지급지시를 이행하기 위한 시스템으로 A가 B에게 지급지시를 보낼 경우, A의 계좌에 잔고가 있고 한도가 충분하다면, 금액을 지급받게 되는 B의 상황에 상관없이 바로 금액이 보내지는 지급지시이다. A의 계좌에 잔고가 충분하지 않거나 한도를 초과한 경우에는 결제되지 않고 대기파일로 이동한다.

보통지급지시는 계좌에 잔액과 한도가 충분하더라도 바로 결제되지 않고 대기하는 지급지시 시스템으로 A가 B에게 보통지급지시를 신청한 경우, B의 대기 파일에 A에게 보내야 할 지급지시가 있을 때 묶어서 양자간 상계처리를 하는 지급지시 시스템이다. 신속지급지시가 잔액 부족이나 지급 한도 초과일 경우에는 대기파일로 이동하게 되고, 보통지급지시는 상계 처리할 상대의 지급지시가 없으면 바로 대기 파일로 이동하는 구조이다. 신한은금융망의 시스템 마감 시간이 임박한 17시 이후에는 신속지급지시만 입력되며 대기파일에 남아있던 지급지시들도 모두 신속지급지시로 전환된다. 기본적으로 신속지급지시는 보통지급지시에 비해 우선적으로 처리되지만 잔액과 지급한도, 유동성 등의 상황에 따라 유연하게 조정할 수 있다.

일반자금 이체 업무의 처리 방식에 따라서는 양자간 동시처리와 다자간 동시처리로 나눌 수 있다. 양자간 처리는 일반적으로 보통지급지시를 이행하는 방식으로 지급지시 입력 기관(A)이 신규 보통지급지시를 입력하면 거래 상대 기관(B)의 대기 파일을 검색하고 A기관에게 보낼 지급지시 파일이 있다면 동시처리를 시도하는 방식이다. 일반적으로 신속지급지시가 보통지급지시보다 먼저 처리되지만 동시처리 결과 유동성이 유입되는 기관의 경우는 보통지급지시를 우선적으로 처리할 수 있다.

다자간 동시처리는 30분마다 한 번씩 수행되는데 각 금융기관별로 대기중인 지급지시를 확인하여 기관별 예상 유출입액을 계산한 후 잔액과 한도 안에서 결제가 가능한 경우 해당 기관들의 지급지시를 동시에 수행하는 시스템이다. 한 번의 결제에 참여할 수 있는 기관의 수에는 제한이 없고 모든 금융망에 참여하는 금융기관의 거래 내역을 최대한 한 번에 처리하기 때문에 거래 내용이 복잡해질 수 있다.

다. 콜거래 업무

콜거래 업무는 혼합결제시스템에 참여하는 금융기관들을 통해 이루어지는 기업 간의 콜거래를 결제하는 업무를 뜻한다. 콜 중개를 담당하는 회사도 혼합결제시스템에 참여하고 있지만 금융기관 간의 직접 거래도 가능하다. 신한은금융망은 콜자금의 공급과 상환에 관련한 자금들을 결제하는 플랫폼을 제공하고 있으며 하루 이상의 상환 기한이 있는 기일물과 하루 내에 공급 및 상환이 이뤄지는 반일물거래 모두 이용이 가능하다. 콜거래 시스템은 다른 혼합결제와 달리 거래 시간이 정해져 있고 거래 금액 상환도 특정 시간에 일괄적으로 내역을 처리한다. 오전 반일물 거래는 신한은금융망 업무 개시 시점부터 10시50분까지 공급한 후 오후 2시5분에서 일괄적으로 상환되며, 오후 반일물 거래는 11시10분부터 13시50분까지 공급하여 오후 5시5분 상환, 하루를 넘어가는 1일물 이상의 콜거래는 거래 시간에 공급되고 매일 오전 11시5분에 금액을 상환하는 시스템을 가지고 있다. 콜자금이 콜거래 시스템을 거치지 않고 일반 원화자금 이체 시스템으로 전달이 된 경우 콜자금 상환 영수증을 어음교환에 회부하거나 아예 일반 원화자금 이체를 통해 자금을 이체할 수 있다. 신한은금융망에서는 콜거래의 유형, 기관, 금리, 금액 등을 파악할 수 있기 때문에 단기금융시장의 자금흐름을 쉽게 파악할 수 있으며, 여기서 파악한 자료들을 통해 단기적으로 금리를 조정하거나 금융기관에 필요한 정보를 제공할 수 있다.

라. 증권대금 동시결제(Delivery Versus Payment: DvP)

증권대금 동시결제 업무의 경우, 기존의 증권을 구매할 때 대금을 결제하는 시기와 증권을 수취하는 시기 사이의 결제리스크를 극복하기 위한 방안으로 만들어진 시스템으로 한국은행, 한국예탁결제원, 금융기관이 연결된 3자간 거래 시스템이다. 기관 간에 증권매매거래가 체결되면 한국예탁결제원에서는

매도자의 계좌에서 매수자의 계좌로 증권을 이체하는 동시에 대금결제의 내역을 금액, 종류별로 구분하여 한국은행으로 전송한다. 이후 거래를 체결한 금융기관이 신한은금융망을 통해 거래 내역을 확인하고 매수자가 결제를 신청하면 결제전용예금계좌를 통해 매수자의 계좌에서 매도자의 계좌로 거래금액을 송금하는 방식이다. 증권대금 동시결제는 유형상 신속지급지시로 구분이 되어, 양자간 및 다자간 동시처리 없이 건별로 바로 결제되는 방식으로만 처리된다.

마. 혼합결제시스템 지급지시 유형 요약

신한은금융망의 혼합결제시스템은 역할에 따라 크게 일반자금 이체, 콜거래, 증권대금동시결제로 나뉜다. 일반자금 이체는 보통 금융기관이 지급지시를 통해 자금을 보내는 방법이며 콜거래는 단기간에 자금을 빌리고 받는 초단기 대출을 의미한다. 증권대금동시결제는 한국예탁결제원과 연동한 시스템으로 예탁결제원에서 증권의 거래가 체결되면 신한은금융망의 계좌와 연동하여 거래에 참여한 금융기관의 자금을 송금하는 시스템을 의미한다.

각 유형의 거래 방식은 세부적인 절차에서 차이가 있지만 크게는 신속지급지시와 보통지급지시로 나눌 수 있다. 신속지급지시는 상대방의 상태에 상관없이 지급지시 신청 기관의 잔액과 한도를 초과하지 않으면 바로 지급지시를 이행할 수 있는 지급지시 유형이며, 보통지급지시는 상대방이 지급지시 신청 기관에 보내야 할 금액이 있으면 그 둘을 상계 처리하는 방식을 말한다. 일반자금 이체와 콜거래는 신속지급지시와 보통지급지시 중 하나를 선택하여 이행할 수 있으며 증권대금동시결제는 신속지급지시로만 진행할 수 있다.

해당 두 지급지시를 뒷받침하는 시스템은 대기파일이다. 신속지급지시의 경우 잔액이나 한도 부족 등의 이유로 전송할 수 없는 경우, 보통지급지시의 경우 상계처리할 수 있는 상대방의 지급지시내역이 없는 경우에 대기파일로 이동하게 된다. 두 파일은 이후 상대방의 지급지시에 따라서 상계 처리가 되며 일반적으로는 신속지급지시가 보통지급지시보다 우선적으로 처리되지만 지급지시의 유형이나 순서 등의 변경을 통해 각 지급지시의 우선순위를 조정할 수 있다.

대기파일에 있는 지급지시는 양자간 혹은 다자간 동시처리를 통해 해소된다. 양자간 처리는 일반적인 보통지급지시 시스템을 의미하는 것으로 상대방이 보내야 할 지급지시가 있으면 그 둘을 상계하여 처리하는 방식이다. 다자간 동시처리는 30분마다 한번씩 모든 금융기관의 대기파일의 거래 내역을 상계처리하여 대기파일에 있는 지급지시를 최대한 한번에 처리하는 방법으로 두 방식 모두 금융기관의 유동성을 확보하기 위한 시스템이다.

신속지급지시의 경우는 양자간 혹은 다자간 동시처리를 통해 해소가 가능할 뿐만 아니라 계좌의 잔액 혹은 한도의 증가나 대기 순서 조정과 같은 변동사항이 있을 경우 바로 총액결제로 처리될 수 있다.

2. 지급결제시스템에서 블록체인의 활용 방안

가. 분산원장의 핵심 기술

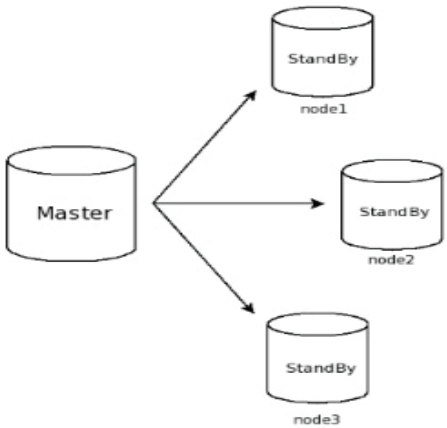
혼합결제시스템에서의 블록체인의 활용 방안을 설명하기에 앞서 지급결제시스템에 적용할 수 있는 블록체인, 즉 분산원장 기술(Distributed Ledger Technology:DLT)의 핵심 기술에 대한 정리가 필요하다고 판단하여 주요 기능을 중심으로 기술에 대한 설명을 덧붙이고자 한다. 분산원장 기술은 분산 데이터베이스, 암호화 해시함수, 공개키 암호화 기술, P2P 네트워크 프로토콜, 합의 알고리즘 등 다음의 5가지 주요 핵심 기능을 가지고 있다. 따라서 분산원장 기술을 적용한 시스템을 설계하기 위해서는 위에서 언급한 5가지 기능을 우선적으로 고려하여야 한다.

(1) 분산 데이터베이스

우선 블록체인의 기본적 구조인 분산 데이터베이스(distributed database)를 설명한다. 분산 데이터베이스란 네트워크상에서 다수의 저장 공간에 데이터를 분산 저장하는 데이터베이스를 의미한다. 이에 바탕이 되는 시스템은 통합 분산 데이터베이스 관리 시스템(distributed database management system, 이하 DDBMS)인데, DDBMS는 사용자로 하여금 모든 데이터가 한곳에 저장된 것처럼 보일 수 있도록 데이터를 관리한다. 즉, DDBMS는 특정 데이터베이스에서 데이터가 저장, 변경, 삭제될 때, 자동으로 혹은 주기적으로 모든 데이터베이스의 데이터를 동기화하는 시스템을 의미한다.

아래의 그림은 분산데이터베이스의 예를 보여준다. 분산데이터베이스의 목적은 데이터 처리의 지역화, 데이터 운영 및 관리의 지역화, 데이터 처리부하의 분산 및 병렬 데이터 처리 및 데이터의 가용도와 신뢰성 향상이다. 분산 데이터베이스 기술은 네트워크의 성능 향상에 따라 빅데이터 처리에 주로 사용되고 Master/Standby 형태를 가진다.

<그림 3-1> 분산데이터베이스의 예시 (Master/Standby 형태)



하지만 본 연구에서 제안하는 한국은행 지급결제시스템에서 사용되는 분산데이터베이스는 통합관리시스템이 존재하지 않는다. 즉, 분산 데이터베이스를 가지고 있는 사용자가 데이터에 대한 저장 요청을 받게 되면 정해진 규칙에 따라 데이터의 정합성을 스스로 판단하고 기록하는 역할을 수행한다. 또한, 분산원장의 분산 데이터베이스는 저장은 가능하지만 변경, 삭제가 원천적으로 불가능한 비가역성(irreversibility)을 주요 특징으로 한다. 아래의 그림과 같이 모든 데이터베이스는 모두 Read/Write를 지원하는 동등한 레벨로 유지된다.

<그림 3-2> 동등한 레벨의 데이터베이스 유형

(2) 암호화 해시 함수

암호화 해시 함수(cryptographic hash function)는 해시 함수의 일종으로, 만들어진 해시 값으로부터 원래의 입력 값과의 관계를 찾기 어려운 성질을 가지는 경우를 의미한다. 암호화 해시 함수가 가져야 하는 성질은 다음과 같다.

첫 번째는 역상 저항성(preimage resistance)이다. 역상 저항성은 만들어진 해시값을 가지고 그 해시값을 생성하는 입력값을 찾는 것이 계산상 불가능함을 의미한다. 입력값을 통해 해시값을 생성하지만 해시값을 통해서는 입력값을 찾는 것이 불가능한 일방향함수의 특성을 가지고 있다.

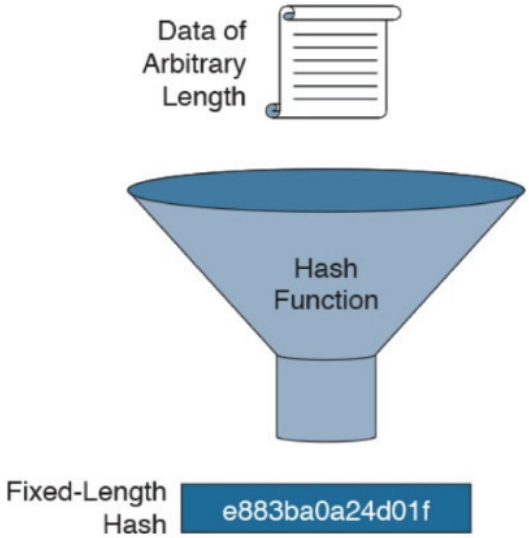
두 번째는 제2역상 저항성(second preimage resistance)이다. 제2역상 저항성은 해시값을 생성하는 입력값에 대해서, 그 입력의 해시값을 바꾸지 않은 상태로 입력값을 변경하는 것이 계산상 불가능함을 의미한다.

세 번째는 충돌 저항성(collision resistance)이다. 충돌 저항성은 같은 해시값을 생성하는 다른 두 개의 입력값을 찾기가 계산상 불가능함을 의미한다.

즉, 암호화 해시 함수는 수학적으로 해시값을 변경하지 않은 상태로 입력값을 수정하는 공격이 불가능하기 때문에 안전하며, 결국 이러한 성질을 가지는 해시값은 원래 입력값이 의도적으로 손상되지 않았는지에 대한 검증 장치로 사용할 수 있다. 해시함수는 가상화폐 시스템에서 폭넓게 사용되고 있

다. 검증노드(validator)는 거래내역과 해시함수에 의해 생성된 축약값(digest)을 비교하여 자신이 저장하고 있는 데이터와 다른 저장소에 있는 값들이 정확하게 일치하는지를 빠른 속도로 확인할 수 있다. 아래 그림은 해시 함수의 동작 예를 나타낸 것으로 임의의 크기의 데이터가 입력으로 사용되고, 출력으로는 선택한 해시 함수의 종류에 따라 동일한 크기의 값이 나오게 된다.

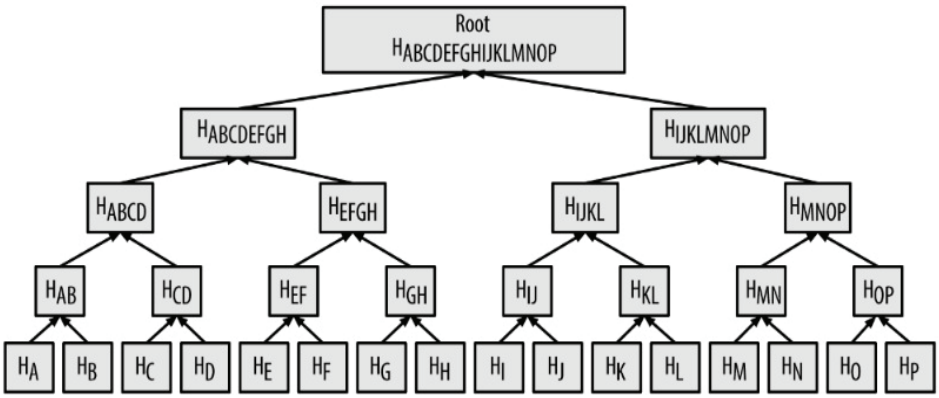
<그림 3-3> 해시함수 동작 원리도



제안하는 지급결제시스템에서는 원래의 데이터를 하나하나 비교하지 않고도 데이터의 무결성을 빠른 시간에 확인할 수 있도록 머클 트리(Merkle Tree) 방식을 사용한다. 2장에서도 간략하게 설명한 머클 트리는 이진 해시 트리(binary hash tree)라고도 하는데, 규모가 큰 데이터 집합의 완전성을 효율적으로 요약하고 검증하는 데 사용되는 데이터 구조로서, 암호 해시를 담고 있는 이진 트리다. 머클 트리는 블록 내에 있는 모든 거래를 요약하기 위해 사용되며, 거래의 집합 전체에 대한 디지털 지문을 만들어내고, 특정 거래가 블록 내부에 포함되는지 여부를 검증하는 데 매우 효율적인 프로세스를 제공한다. 루트 혹은 머클 루트(Merkle Root)라고 부르는 해시 하나가 남을 때까지 노드 쌍을 반복적으로 암호화해서 머클 트리를 만든다. 이렇게 생성된 머클 트리는 비트코인이나 이더리움 같은 개방형 블록체인에 기록되며, 허가된 요청에 따라 거래 내역의 묶음이 해당하는 시간에 해당 금액만큼 거래가 이루어졌다는 사실을 확인할 수 있으며, 지급결제시스템에 저장된 데이터의 무결성을 검증하는데 사용된다.

아래의 그림은 머클 트리의 16개의 입력 값으로부터 머클 루트를 생성하는 과정을 나타낸다. 그림에서 H는 해시 함수를 뜻하고, A~P는 해시 함수의 입력으로 사용된 값을 나타낸다.

<그림 3-4> 머클 트리의 구조도



자료: Mastering Bitcoin

(3) 공개키 암호화 방식

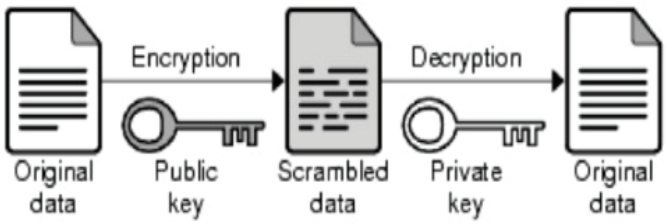
공개키 암호 방식은 암호 방식의 한 종류로, 사전에 비밀키를 나눠가지지 않은 사용자들이 안전하게 통신할 수 있도록 하는 기술이다. 공개키 암호 방식에서는 공개키(Public Key)와 비밀키(Private Key)가 존재하며, 공개키는 누구나 알 수 있지만 그에 대응하는 비밀키는 해당 키의 소유자만이 알 수 있어야 한다. 공개키는 은행의 계좌번호에, 비밀키는 비밀 PIN번호에 대입해서 생각하면 유사한 개념이다. 공개키 암호를 구성하는 알고리즘은 비대칭 암호라고 부르기도 한다. 공개키 암호 기술은 크게 두 가지 종류로 나눌 수 있다.

첫 번째는 공개키 암호이다. 공개키 암호는 특정한 비밀키를 가지고 있는 사용자만 암호화된 내용을 복호화하고 원래 메시지를 읽어볼 수 있음을 의미한다.

두 번째는 공개키 서명이다. 공개키 서명은 해당 데이터가 특정한 비밀키로 만들었다는 것을 해당 공개키를 이용하면 누구나 확인할 수 있음을 의미한다.

아래의 그림은 공개키 암호화의 과정을 설명하는 도식이다. 최초의 데이터에 PKI의 공개키를 적용하여 암호화(encryption)하고 이렇게 생성된 암호화된 데이터(scrambled or encrypted data)는 해당 공개키에 상응하는 개인키로 복호화(decryption)하면 원본 데이터를 얻을 수 있게 된다.

<그림 3-5> 공개키 암호화의 과정



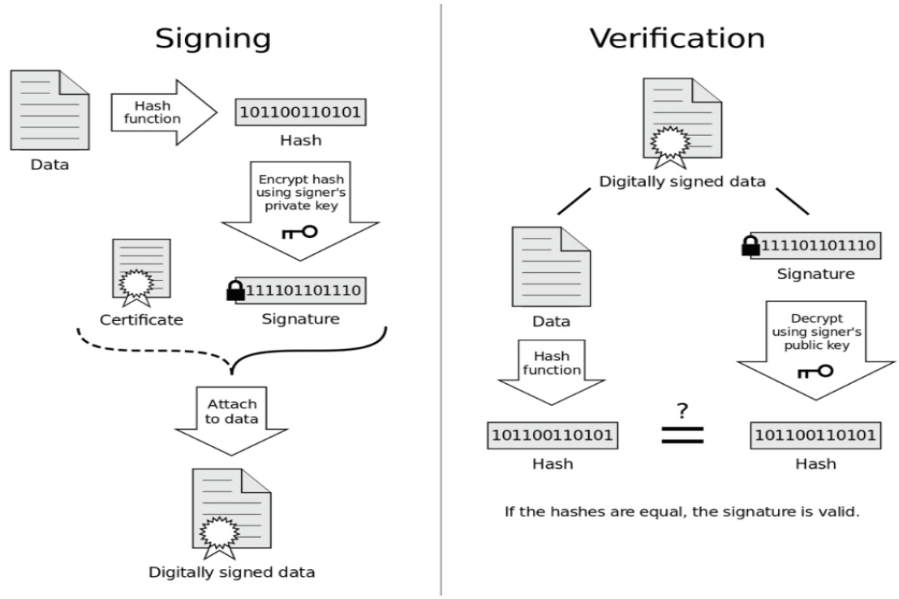
일반적으로 공개키 암호 방식은 비밀키 암호(혹은 대칭 암호)보다 계산이 복잡한 단점이 있기 때문에, 효율을 위해 비밀키 암호와 함께 사용된다. 메시지를 임의로 만들어진 비밀키를 이용해 암호화한 다음 이 비밀키를 다시 수신자의 공개키로 암호화하여 메시지와 함께 전송하는 것이다. 이렇게 하면 공개키 암호 기술로는 짧은 비밀키만을 암호화하고 보다 효율적인 비밀키 암호 기술로 전체 메시지를 암호화하므로 양쪽의 장점을 취할 수 있다.

제안하게 될 분산원장 기술 기반 지급결제시스템에서는 효율적인 공개키 암호 기술과 공개키 서명 기술을 모두 사용한다. 우선, 공개키 암호기술은 사용자의 거래를 기록할 때, 거래내역을 암호화하여 저장함으로써 거래에 참여한 사용자와 관리자만이 해당 내역을 읽어볼 수 있도록 한다. 공개키 서명 기술의 경우, 거래를 생성한 주체가 본인이 생성한 데이터가 변경되지 않았음을 증명하는데 사용되며 해당 거래를 생성할 권리(즉, 개인키의 보유여부)가 있음을 나타낸다. 아래의 그림은 전자서명의 과정을 나타내고 있다.

왼쪽의 서명(Signing) 과정을 살펴보면 다음과 같다. 우선 원본 데이터로부터 암호화 해시함수를 통하여 해시 값을 생성한다. 이후에 해시함수를 통해 생성된 해시 값을 서명인의 개인키를 이용하여 암호화(encryption)한다. 이렇게 암호화를 통해 만들어진 서명 값, 서명인의 공개키를 가지고 있는 인증서, 그리고 원본 데이터를 모두 포함하는 서명된 데이터(Digitally signed data)를 생성한다.

오른쪽은 서명된 데이터(Digitally signed data)를 통신채널로 전달받아 검증(Verification)하는 과정을 나타내고 있으며, 과정은 다음과 같다. 우선 서명된 데이터(Digitally signed data)로부터 서명 값, 인증서 및 원본데이터를 분리한다. 분리된 데이터들 중 원본 데이터로부터 해시 값을 생성하고, 인증서는 유효성을 확인한 이후 서명인의 공개키를 추출한다. 이후에 추출된 공개키를 이용하여 서명 값을 복호화(Decryption)하고, 복호화된 서명 값과 원본데이터의 해시 값을 비교하고, 두 값이 일치하면 검증이 완료된다.

<그림 3-6> 공개키 기술 전자서명의 과정



(4) P2P 네트워크 프로토콜

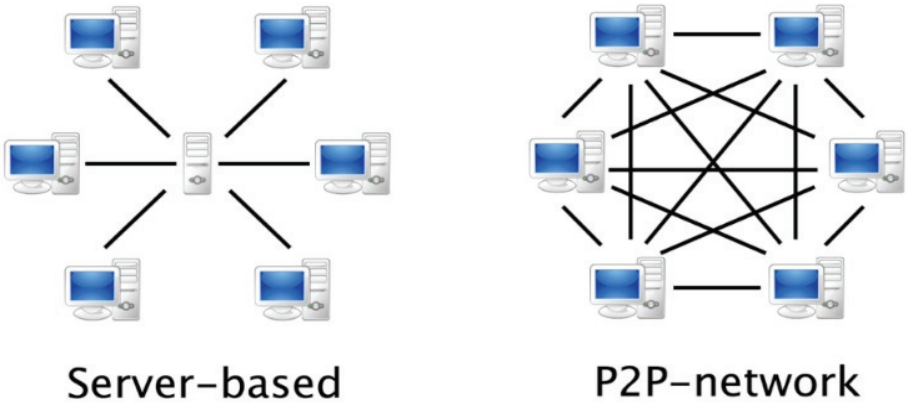
거의 모든 개방형 블록체인은 인터넷상에서 피어 투 피어(peer-to-peer) 네트워크 아키텍처 구조를 이루고 있다. 피어 투 피어, 즉 P2P라는 용어는 네트워크에 참여하는 개인은 서로에게 동료이며 모두 동등한 지위를 가지고 있고 '특별한' 노드는 존재하지 않으며 모든 노드가 네트워크 서비스를 공급하는 역할을 분담하는 것을 의미한다. 네트워크상의 여러 노드는 서로 '동등한' 토폴로지를 가지면서 그물망 네트워크에서 서로 연결되어 있으며, 네트워크 내에는 어떠한 서버나 중앙화된 서비스, 위계질서도 존재하지 않는다. P2P 네트워크의 노드는 서비스를 제공하고 동시에 서비스를 이용하는 공급

자이자 동시에 소비자의 역할을 한다. P2P 네트워크는 본질적으로 회복력이 있고 분산화되어 있으며 개방 체제다. P2P 네트워크 아키텍처의 좋은 예는 IP 네트워크상의 노드들이 모두 동등했던 초기 인터넷에서 찾아볼 수 있다. 오늘날의 인터넷 아키텍처는 초기보다는 계층적이지만 인터넷 프로토콜은 여전히 동등한 토폴로지를 유지한다. 비트코인을 제외하고 P2P 기술을 가장 광범위하게 성공시킨 사례는 파일 공유의 선구자이자 비트토렌트(BitTorrent)의 전신인 냅스터(Napster)다.

아래의 그림은 클라이언트-서버 구조의 네트워크와 P2P 네트워크를 비교한 그림이다. 웹 시스템도 확장된 '클라이언트 서버 시스템'으로 분류되나, 일반적으로는 클라이언트-서버 시스템이라고 하면, 사용자 PC에는 클라이언트가 설치되어 화면을 처리하고 서버에서는 자료를 처리하는 시스템을 일컫는다. 서버(Server)란 서비스를 제공하는 컴퓨터이며, 다수의 클라이언트를 위해 존재하기 때문에 일반적으로 매우 큰 용량과 성능을 가지고 있었다. 가장 대표적인 예로 월드와이드웹(www)를 들 수 있다.

반면에 P2P 네트워크는 망 구성에 참여하는 기계들의 계산과 대역폭(bandwidth) 성능에 의존하여 구성되는 통신망을 뜻한다. P2P 네트워크는 오디오나 비디오, 데이터 등 임의의 디지털 형식 파일의 공유에 사용되는 것이 매우 보편적이다. 또한, 인터넷 전화(VoIP)같은 실시간 데이터 등도 P2P 기술을 통해 서로 전달될 수 있다.

<그림 3-7> 클라이언트-서버 구조와 P2P 구조의 비교



한편, 블록체인의 P2P 네트워크 아키텍처는 토폴로지의 선택 그 이상을 의미한다. 블록체인 설계의 주요 원리는 분산화된 통제이며, 이는 동등하고 분산화된 P2P 합의 네트워크 상에서만 시행 및 유지될 수 있다. '블록체인 네트워크'라는 용어는 P2P 프로토콜을 실행하는 노드의 집합을 말한다.

본 연구에서 제안하는 지급결제시스템에서는 다수의 거래장부가 존재하며 이를 관리하는 관리자 모듈이 존재한다. 이 관리자 모듈은 거래장부와의 모든 상호작용을 관리 총괄하며 다른 관리자 모듈과의 P2P 통신을 지원하는 역할을 수행한다.

(5) 합의 알고리즘

분산 데이터베이스에 동일한 내용을 기록하기 위해서는 합의 알고리즘이 사용되어야 한다. 합의 알고리즘과 접근 제어는 분산원장의 목적에 따라 다양한 방법들이 사용될 수 있다. 개방형 블록체인 네트워크의 접근제어가 불가능하기 때문에 악의적인 참여자를 배제할 수 없다. 그러므로 데이터 조작에 대한 안전하고 강력한 방어책이 필요하며 작업증명(Proof-of-Work)이나 유사한 방법들을 합의 알고리즘으로 사용하는 방법이 합리적이다. 폐쇄형 블록체인의 경우에는 장부의 접근 권한을 오직 신뢰할 수 있는 사용자에게만 부여하기 때문에, 다량의 정보를 PBFT(Practical Byzantine Fault Tolerance) 같은 효율적인 합의 알고리즘을 이용하여 안전하게 저장 관리하는 것이 가능하다.

PBFT에서 사용되는 노드는 다음의 세 가지다. 첫 번째는 리더노드이다. 리더노드는 비트코인 블록체인의 채굴자와 같은 역할을 하는 노드로 새로운 블록을 만들고 네트워크에 전파하는 기능을 수행한다. 리더노드의 선정은 round robin이나 contention-based의 다양한 방식을 사용할 수 있다.

두 번째는 검증노드이다. 검증노드는 개방형 블록체인의 풀노드(Full Node)에 해당하며 모든 블록체인에 저장된 데이터를 로컬에서 검증하는 것이 가능하며 리더노드로부터 전달받은 블록의 유효성을 판단하여 리더노드에게 응답하는 기능을 수행한다.

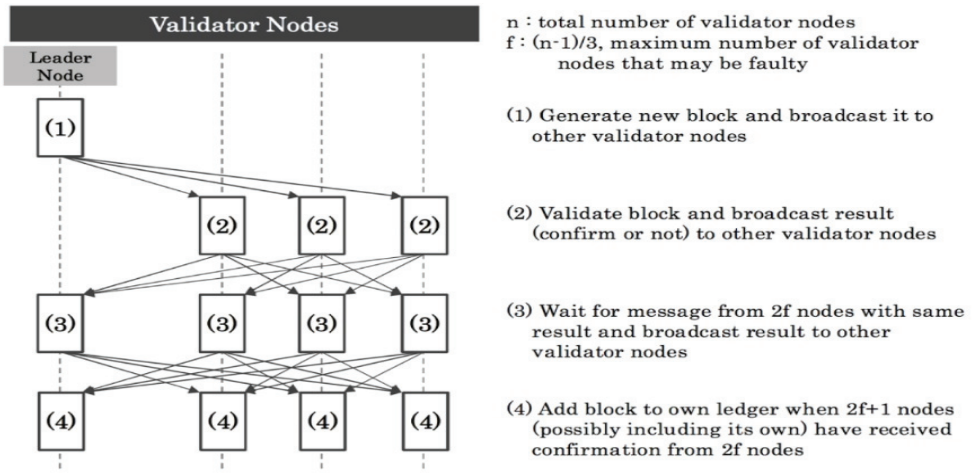
세 번째는 비검증노드이다. 비검증노드는 개방형 블록체인의 SPV(Simple Payment Verification) 노드에 해당하며, 전체 블록체인을 저장하고 있지는 않지만 하나의 거래를 생성하는 것이 가능하며 검증노드의 도움을 받으면 각각의 거래를 검증하는 것도 가능하다.

PBFT 기반 알고리즘은 약 참여노드의 2/3이상이 거래 내역들을 검증하게 되면 합의에 이르게 된다. 이는 안전하며 안정된 즉각적인 합의를 가능하게 하기 때문에, 블록체인의 분기를 막는 것이 가능하다. PBFT기반 알고리즘에서 검증노드는 장부에 거래 내역을 기록하고 합의과정에 참여하는 기능을 하고 있다. 반면에 검증 기능이 없는 노드는 거래를 만드는 데는 참여하지만 합의과정에는 참여할 권한을 가지지 못한다.

아래의 그림은 PBFT의 합의과정을 나타내고 있다. 비잔티움 장애 허용(Byzantine Fault Tolerance)은 두 장군 문제(Two Generals Problem)를 일반화한 문제인 비잔티움 장군 문제(Byzantine Generals Problem, 이하 BGP)로부터 파생된 장애 허용 분야 연구의 한 갈래다. BGP는 레슬리 램포트와 쇼스탁, 피스가 공저한 1982년 논문에서 처음 언급됐다. 이 논문에서 저자들은 적군의 도시를 공격하려는 비잔티움 제국군의 여러 부대가 지리적으로 떨어진 상태에서 각 부대의 지휘관들이 전령을 통해 교신하면서 공격 계획을 함께 세우는 상황을 가정하고 있다. 이 부대의 지휘관 중 일부에는 배신자가 섞여있을 가능성이 있고, 배신자는 규칙을 충실히 따르는 충직한 지휘관들과 달리 규칙에 얽매이지 않고 마음대로 행동할 수 있다. 이 때 배신자의 존재에도 불구하고 충직한 지휘관들이 동일한 공격 계획을 세우기 위해서는 충직한 지휘관들의 수가 얼마나 있어야 하며, 이 지휘관들이 어떤 규칙을 따라

교신해야 하는지에 대한 문제가 BGP이다.

<그림 3-8> PBFT 기반 합의 알고리즘

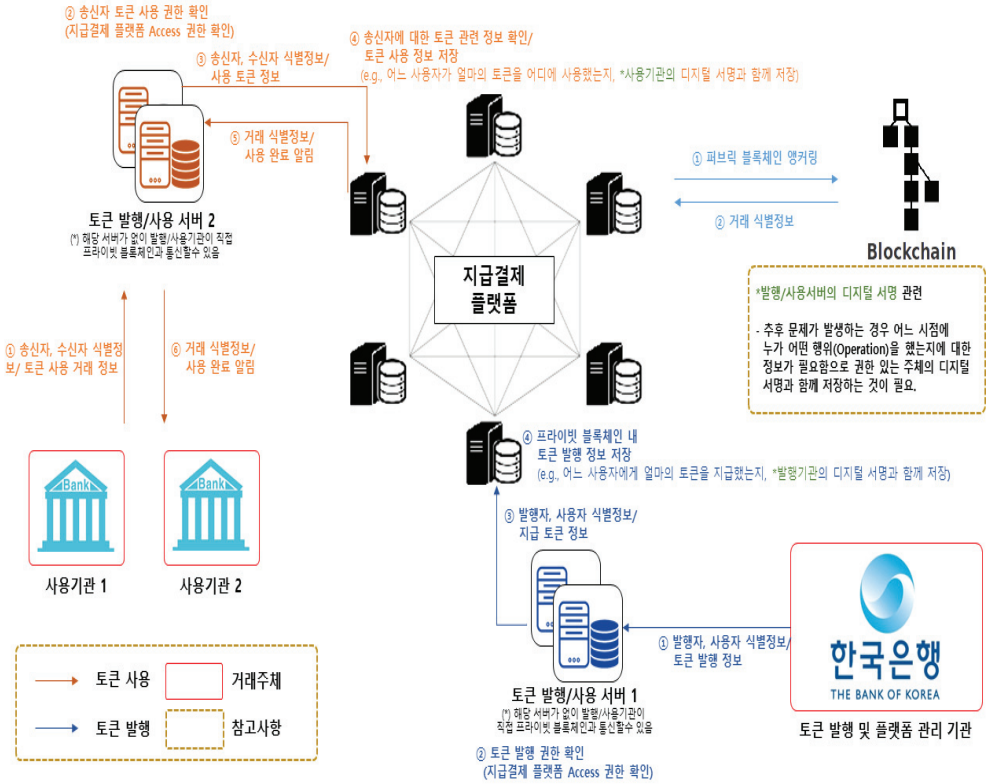


자료: JPX working paper

제안하는 지급결제시스템에서는 모든 금융기관이 검증노드가 될 필요는 없으며, 한국은행을 제외한 대부분의 금융기관은 검증기능을 보유하지 않는 노드이다. 검증노드의 숫자는 합의 알고리즘을 위한 메시지 트래픽 때문에 네트워크 대역폭에 영향을 준다. 그러므로 특정 금융기관만이 검증노드의 역할을 수행하게 된다. 합의과정에는 블록을 생성하는 리더노드가 존재해야하며, 리더노드가 메시지를 전파하면 이를 전송받은 검증노드는 정해진 규칙에 따라 메시지를 검증하고 유효하면 각각의 원장을 독립적으로 업데이트 하게 된다.

나. 블록체인의 적용 방법

<그림 3-9> 토큰 기반 블록체인 지급결제시스템 흐름도



자료: 코인플러그

위 그림은 혼합결제시스템을 블록체인 플랫폼을 이용하여 구성한 시스템의 기본적인 흐름도이다. 기본적으로 블록체인을 기반으로 하여 지급결제시스템 내에서 유통될 Digital 토큰(이하 토큰)을 발행하고 유통하는 형태로 지급결제시스템이 구성된다. 기본적인 흐름은 다음과 같다. 지급결제 플랫폼 내에서 사용하는 토큰을 권한 있는 발행자가 생성(토큰 생성 시에는 토큰 발행자의 전자서명을 포함)하고 인가받은 참여자들이 토큰의 거래(거래 시에는 참여자의 전자서명을 포함)를 폐쇄형 블록체인에 기록하고 거래 내역을 영구히 보존하는 방식이다.

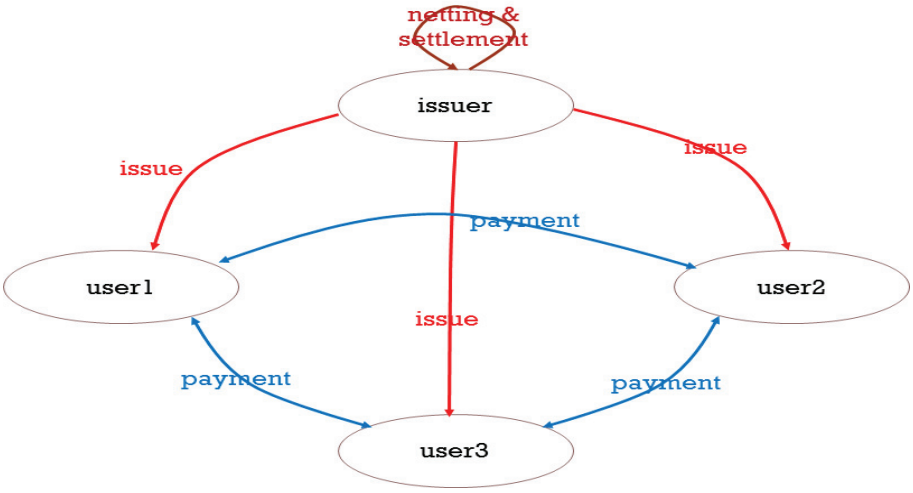
(1) 사용의 전제 조건

본 시스템을 사용하기 위한 전제조건은 다음과 같다. 첫째로는 토큰의 사용자들(금융기관)은 본인이 사용할 공개키(public key)를 사전에 지급결제시스템 블록체인 관리자(대부분의 경우 토큰 발행기관이 관리자의 역할을 함께 수행)에 등록하여야 한다. 이는 토큰 발행을 담당하게 될 발행기관, 즉 한국은행이 금융망에 참여하는 금융기관들의 모든 공개키를 관리하는 역할을 함께 수행하고 모든 거래 내역을 승인, 관리, 점검하는 역할을 수행하게 된다는 것을 의미한다.

둘째, 한국은행의 지급결제 플랫폼에 참여하는 모든 사용자들은 암호학적으로 유효한 공개키를 사용하여야 한다. 대표적인 방법으로는 RSA와 ECC 등의 기법이 있다

세 번째로는 지급결제시스템 플랫폼에서 생성되는 모든 거래는 유효한 서명(Signature)을 적어도 하나이상 포함하고 있어야 한다. 여러 참여자의 공개키들로부터 가공된 값을 사용하면 다중서명 방식을 적용할 수도 있다. 다중서명 방식은 n개의 공개키가 보관이 되어 있고, 하나의 거래를 만들기 위해서는 적어도 m개 이상의 개인키가 서명을 제공해야 한다는 조건을 설정하는 것이다. m-of-n 제도라고도 알려져 있는데, 예를 들어 2-of-3 다중서명이면 공개키 3개가 잠정적 서명자로 등록이 되어 있고 유효한 거래를 만들기 위해서는 적어도 2개의 개인키를 사용해야 하는 경우라고 설명할 수 있다. 다자간 거래 등에서 다중서명 방식이 적합하다고 판단될 경우 해당 기술의 적용 방안을 모색해 사용할 수 있을 것이다.

<그림 3-10> 토큰의 발행자와 사용자간의 블록체인의 구성도



자료: 코인플러그

위 그림은 지급결제시스템에 참여하는 토큰의 발행자와 사용자간에 발생할 수 있는 모든 이동을 간략하게 나타낸 구성도이다. 이는 토큰의 생성, 거래, 정산 등의 모든 과정을 포함한다. 지급결제시스템은 다음과 같은 특성을 가진다.

첫 번째로 모든 거래는 암호화되어 분산원장에 기록되어야 하며, 관리자의 역할을 하는 한국은행과 거래에 참여한 기관만 거래 내역을 읽어볼 수 있도록 구성한다.

두 번째로 결제의 유형은 현재 혼합결제시스템과 마찬가지로 신속결제와 보통결제로 구분된다. 신속결제는 사용자가 충분한 양과 한도의 토큰이 있을 경우 실시간으로 처리하며, 보통거래의 경우는 사용가능한 잔액에 상관없이 거래 요청을 각 금융기관의 대기 파일의 역할을 하는 임시 데이터베이스에 저장하고 상계처리가 가능할 때 혹은 정해진 시간에 처리한다.

세 번째로 모든 거래는 관리자 혹은 사용자의 유효한 전자서명을 포함하고 있기 때문에, 권한이 있는 제3의 감사자가 감사에 사용할 수 있는 근거 자료가 될 수 있다.

네 번째로는 사용자의 잔고는 결제가 완료된 후 항상 positive 값을 유지하

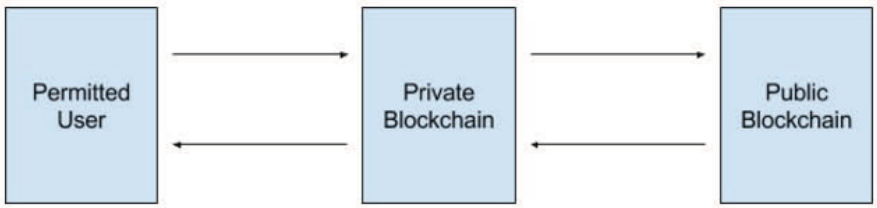
여야 한다. 거래가 완료된 이후에는 잔고가 마이너스로 표시될 수 없으며 각 사용자의 토큰 잔고는 항상 0 이상으로 유지되어야 한다.

(2) 금액의 예치

우선 블록체인 기반 혼합결제시스템의 사용자, 즉 참여 금융기관이 블록체인 기반의 지급결제시스템을 이용하기 위해서는 결제시스템에서 사용할 만큼의 금액을 예치해야 한다. 사용자가 시스템의 관리자, 즉 한국은행에 사용할 만큼의 금액을 예치하면 관리자는 예치한 금액에 따라 사용할 수 있는 토큰을 발행한다. 토큰의 발행은 오로지 시스템의 관리자인 한국은행만이 할 수 있으며, 토큰의 발행량은 예치 금액과 1:1 비율 혹은 다른 방법으로 시스템의 운영 방식과 활용 방안에 맞게끔 조정할 수 있다.

(3) 사용자 인가 및 등록 절차

<그림 3-11> 사용자 인가 및 등록 절차



모든 지급결제시스템 참여자(한국은행 금융망 참여 금융기관)는 블록체인 기반 지급결제시스템을 사용하기에 앞서, 본인을 인증하고 해당 시스템에서 사용할 공개키를 선 등록하여야 한다. 절차는 다음과 같다.

(가) 처음 참여하는 시스템 참여자 A(이하 User A)는 사용할 공개키 A와 개인키 A를 안전하게 로컬에서 생성한다.

(나) 공개키 A를 지급결제 블록체인 관리자(이하 Private BCM)에게 전송한다. 지급결제시스템에서는 한국은행이 Private BCM을 담당한다.

(다) 한국은행(Private BCM)은 User A가 유효하다고 판단되면 임의의 번호(Random Number, 이하 RN)를 생성하여 User A에게 전달한다. 이 때,

해당 User A의 유효성을 판단하는 방법은 여러 방법이 있는데 공인 인증서나 블록체인 인증서 등 PKI 기반 인증서를 사용할 수 있으며, 기타 참여자가 유효함을 증명하는 온오프라인의 어떠한 방법을 사용해도 무방하다.

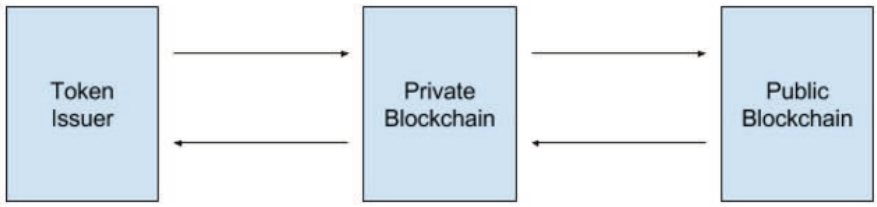
(라) User A는 발급받은 임의의 번호(RN)를 개인키 A로 전자서명을 하고 전자서명을 한 개인키의 결과값인 전자서명 A를 블록체인 관리자인 한국은행에 전달한다.

(마) 한국은행은 서명이 정상적으로 되었는지를 검증하고, 검증이 완료되면 해당 전자 서명값, RN, 공개키 A를 지급결제 블록체인 데이터베이스에 저장한다. 이후 한국은행은 해당 값들을 검색할 수 있는 거래 ID(이하 Txid A)를 User A에게 전달한다.

(바) 위의 절차가 완료되면 User A는 지급결제시스템의 사용자로의 등록이 완료된다.

(4) 토큰 발행 절차

<그림 3-12> 토큰 발행 절차



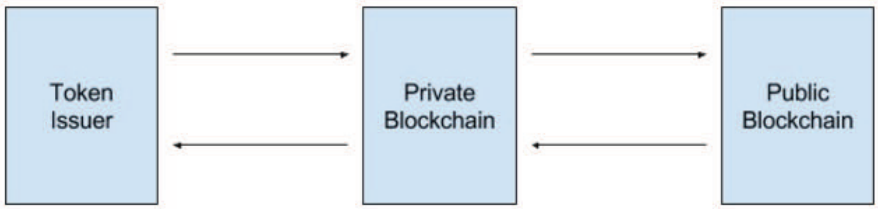
사용자의 등록이 정상적으로 완료되면, 해당 사용자는 지급 및 입금 채널을 통하여 예치금을 입금하고 이에 해당하는 토큰을 발급받게 된다. 토큰의 발급은 발급기관이 담당하게 되는데 지급결제시스템의 관리자(한국은행)가 전적으로 이를 담당한다. 우선 아래의 절차를 통하여 토큰이 발행된다.

(가) 토큰 발행기관인 한국은행은 토큰을 발행하기 위하여 토큰 발행 거래(Issuance Transaction)를 생성하고 지급결제 블록체인 관리자에 전송한다.

(나) 한국은행 내 블록체인 관리자(Private BCM)는 토큰 발행기관의 공개키를 이용하여 발행거래의 유효성을 검증한다. 발행거래가 유효하면 지급결제 블록체인 데이터베이스에 등록하고 블록체인 거래 ID를 토큰 발행기관과 사용자에게 전달한다. 만약 발행거래가 유효하지 않으면(e.g., 전자서명 검증 실패), Error message를 발행기관에 전달한다.

(5) 토큰 사용 절차

<그림 3-13> 토큰 사용 절차



정상적으로 토큰을 발급받은 사용자인 금융기관들은 서로의 전자서명을 사용하여 거래를 생성하고 토큰을 상호간에 전달할 수 있다.

(가) 우선 토큰 사용자들은 구매한 토큰을 사용하기 위하여, 지급 지시를 생성하고 지급결제 블록체인 관리자에게 전송한다.

(나) 지급결제 블록체인 관리자는 가지고 있는 사용자의 공개키를 통해 지급지시의 유효성(전자서명)을 검증한다.

(다) 지급지시가 유효하고 지급지시의 유형이 '신속'이고 토큰 잔액이나 한도가 충분하면, 블록체인 데이터베이스에 거래내역을 등록하고 PrivTxid를 거래에 참여한 모든 사용자에게 전달한다.

(라) 지급지시가 유효하고 지급지시 유형이 '보통'이거나 혹은 '신속'인데 잔액이나 한도가 충분하지 않다면 해당 거래를 대기 폴더의 역할을 하는 Netting DataBase(이하 NDB)에 등록하고 이후 상응하는 거래가 들어왔을 때 상계 처리 및 결제를 시도한다. 결제가 성공하면 관련 거래 내역들을 PrivBCDB에 등록하고 블록체인 거래 ID들을 거래에 참여한 사용자들에게 전달하고, NDB에 있던 거래항목들은 삭제한다.

(마) 지급지시가 서명 등의 문제로 유효하지 않으면, Error message를 거래를 생성한 사용자에게 전달한다.

3. 블록체인 도입의 조건 및 고려사항

가. 프라이버시 문제

가장 널리 사용되고 있는 개방형 블록체인인 비트코인의 경우, 익명성을 가진 ID들로 이루어진 모든 거래내역이 저장되어 있고 누구나 원하면 내용을 접근하여 읽어보는 것이 가능하다. 따라서 특정 ID에 얼마나 많은 비트코인이 할당되어 있는지 알아내는 것이 가능하다. 이렇듯 높은 투명성과 변조가 불가능한 장부의 기능은 개인의 소유권을 증명할 수 있는 비트코인의 분산 특성의 기본이 되고 있다. 하지만, 금융데이터를 직접 저장해야하는 지급결제시스템에서 거래금액과 참여금융기관들의 ID를 암호화하지 않고 저장하게 될 경우, 참여금융기관의 모든 거래내역이 블록체인에 접근할 수 있는 모든 노드에게 유출될 수 있다. 일반적인 금융거래에서 거래내역(거래 규모, 가격 등)은 관계된 금융기관이 아닌 상대에게 공개되지 않기 때문에, 개방형 블록체인 형태를 그대로 사용하는 것은 부적절하다.

하지만 모든 거래내역을 암호화할 경우, 관리자 노드(즉, 특수권한이 주어져 거래를 승인하는 등의 역할을 하는 노드, 지급결제시스템 블록체인에서는 한국은행이 그 역할을 한다) 또한 암호화된 데이터를 읽어볼 수 없게 된다는 문제점이 있다. 결국 상황과 필요에 따라 선택적인 거래 내역의 공개가 필요하다. 이에 대한 해결방안들이 몇 가지가 존재하는데 대표적인 방법은 다음의 두 가지 경우들이다.

(1) PKI based Key Exchange(e.g., Diffie-Hellman)

Diffie‐Hellman key exchange는 암호키를 교환하는 하나의 방법으로, 두 사람이 암호화되지 않은 통신망을 통해 공통의 비밀키를 공유할 수 있도록 한다. 휫필드 디피와 마틴 헬만이 1976년에 발표하였다. Diffie‐Hellman key exchange 방법은 암호키를 교환하는 하나의 방법으로, 두 사람이 암호화되지 않은 통신망을 통해 공통의 비밀키를 공유할 수 있도록 하는 기술이다. 이 방법을 사용하게 되면 거래에 관여하는 두 기관이 서로의 공개키만을 이용

하여 비밀키를 생성하는 것이 가능하다. 이후 두 거래자는 모든 거래 내역을 비밀키를 이용하여 암호화한 후에 전송하게 된다. 현재 제안하는 지급결제시스템에서는 토큰 발행자(한국은행)라는 Super Node가 존재하므로 두 거래자는 거래를 생성하기 전에 토큰 발행자의 공개키를 이용하여 두 당사자 간의 거래에 사용할 비밀키를 암호화하여 전송하면 토큰 발행자는 모든 거래당사자들의 비밀키를 획득하게 되고 이를 이용하여 거래내역을 살펴볼 수 있다.

송신자와 수신자가 공개된 통신망에서 Diffie - Hellman Key Exchange를 하기 위해서는 다음과 같은 절차를 거친다.

(가) n,g : 크기가 큰 정수들로서 메시지의 송수신에 참여하는 모든 사람들에게 공개되어 있다. 그리고 특히 g값은 n보다는 작고 1보다는 크다.

(나) 송신자는 비교적 크기가 큰 난수 x를 발생시키고 이 값을 보관한다.

(다) 수신자 역시 비교적 크기가 큰 난수 y를 발생시키고 이 값을 보관한다.

(라) 송신자는 다음의 계산을 하여 그 결과를 수신자에게 보낸다.

$$X = gx \bmod n$$

(마) 수신자는 다음의 계산을 하여 그 결과를 송신자에게 보낸다.

$$Y = gy \bmod n$$

(바) 송신자는 Y를 받아서 다음의 계산을 한 후 비밀키 Ks를 얻는다.

$$Ks = (Y)x \bmod n = gyx \bmod n$$

(사) 수신자는 X를 받아서 다음의 계산을 한 후 비밀키 Kr을 얻는다.

$$Kr = (X)y \bmod n = gxy \bmod n$$

위의 (바)와 (사)에서 계산된 결과인 Ks와 Kr이 같은 값을 갖는다는 것을 알 수 있다. 따라서 송신자와 수신자는 이 값을 비밀키로 하여 메시지를 암호화/복호화할 수 있게 된다.

(2) Confidential Transactions(e.g., hyperledger)

Confidential Transaction(이하 CT)은 Blockstream의 Sidechain에서 최초 적용한 방식으로 현재는 하이퍼레저의 기본 거래방식이다. CT를 사용하게 되면 거래 당사자들만이 거래량을 확인할 수 있으며, 개방형 블록체인의 UTXO(Unspent Transaction Output)과 같이 이중지불을 막을 수 있는 것이 가능하다. CT에서는 비밀 주소의 개념을 사용할 수도 있어서 거래당사자의 신원도 보호하는 것이 가능하다.

나. 권한 분리와 접근 제어

개방형 블록체인 네트워크는 모두에게 읽고 쓰기의 접근권한을 부여하고 있다. 하지만, 본 연구에서 제안하는 블록체인 기반 혼합결제시스템의 폐쇄형 블록체인은 인가된 사용자에게만 제한적으로 네트워크의 접근권한을 부여하게 된다. 본 보고서에서는 지급결제시스템의 사용 노드 권한을 다음의 두 가지로 구분한다.

(1) 토큰 발행자 (토큰 Issuer)

제안하는 블록체인 시스템에서 사용되는 모든 토큰 및 참여기관의 등록/파기를 관리하는 슈퍼 노드(Super Node)로서 사용자들에게 읽고 쓰는 권한을 부여할 수 있으며, 등록된 토큰 사용자에게 새로운 토큰을 발행할 수 있다(한국은행 담당). 토큰 발행자는 모든 거래내역을 읽을 수 있는 권한을 가지고 있으나, 블록체인의 특성상 거래가 승인되어 블록체인에 기록된 거래내역을 변경하는 것은 원천적으로 불가능하다. 또한, 제안하는 블록체인의 주요 서비스 중 하나로 장부에 기록되어 있는 거래내역이 생성 후에 변경되지 않았음을 확인 가능하게 해주는 감사기능이 제공되는데 이를 통해 필요한 감사정보를 인가된 제3자에게 제공할 수 있다.

(2) 토큰 사용자(토큰 User)

토큰 사용자(토큰 User)는 토큰 발행자로부터 발급받은 토큰을 타 사용자에게 이동하기 위해서, 발행자에게 사전에 등록한 공개키와 연동되어 있는 개인키로 전자서명을 하여 거래를 생성할 수 있는 권한이 있으며, 거래장부에

서 본인의 거래와 관련된 내역은 항시 읽어볼 수 있는 권한이 있다. 한국은행을 제외한 혼합결제시스템에 참여하는 대부분의 금융기관은 토큰 사용자 노드들이라고 할 수 있다.

다. 개방형 블록체인과의 연결(앵커링)

앞에서 언급했듯이 폐쇄형 블록체인에는 채굴이라는 개념이 존재하지 않는다. 이는 빠르게 합의에 이를 수 있는 좋은 방안이기도 하지만 악의적인 블록체인 관리자가 존재한다면 분산장부의 무결성을 증명하는 것이 불가능하다. 이러한 이유로 보고서에서 제안하는 지급결제시스템은 개방형 블록체인과의 연결을 주기적으로 실시하는 구조를 선택적으로 가질 수 있다. 즉, 한국은행 블록체인의 분산장부에 기록되는 내용을 가공하여(즉, 프라이빗 분산원장의 내용을 전혀 노출시키지 않는 방법으로) 머클트리를 블록별로 생성하고 머클트리의 최종값인 머클루트를 개방형 블록체인에 기록한다. 이를 통해 개방형 블록체인을 최소한으로 이용하면서도 개방형 블록체인의 채굴파워를 이용하여 한국은행의 폐쇄형 블록체인의 무결성을 유지할 수 있게 된다. 개방형 블록체인을 이용하여 폐쇄형 블록체인의 데이터를 가공하여 기록하는 방법인 앵커링을 통해 폐쇄형 블록체인의 무결성을 증명하고 신뢰를 제고할 수 있다.

라. 기술 관련 리스크

(1) 블록체인의 확장성

우선 블록체인의 처리 가능한 거래량이 현재 신한은금융망 등에서 금융기관의 실제 거래 규모를 처리할 수 있을 만큼 충분한지 고려해야 한다. 현재 코인플러그가 출시한 폐쇄형 블록체인인 FIDO Ledger를 예를 들어 보면, FIDO Ledger는 3000TPS(Transactions per second)의 데이터 처리량을 가지고 있기 때문에, 현재 신한은금융망의 거래 규모를 고려했을 때 FIDO Ledger를 포함한 다른 폐쇄형 블록체인을 적용하는 것 자체에는 큰 문제는 없을 것으로 보인다. 하지만 현재까지 지급결제시스템에 블록체인 기술을 상용화한 사례가 많지 않고, 시간별 거래 건수의 편차나 참여하는 기관이 다양해지고 결제의 종류도 다양해지는 등 추가적인 변수가 다수 존재한다는 점을 고려할 필요가 있다. 그렇기 때문에 폐쇄형 블록체인의 확장성에 대한 지

속적인 연구와 개발이 필요할 것으로 보이며, 중앙은행과 금융기관들도 계속적인 테스트를 통해서 어느 정도의 폐쇄형 블록체인의 개발이 필요한지 확인할 필요가 있을 것이다.

(2) 데이터의 감시 및 통제 방법

한국은행 블록체인에 참여하는 모든 토큰 사용자 노드들(토큰 User)은 토큰 발행자 노드(토큰 Issuer, 한국은행)로부터 읽고 쓰는 권한에 대해서 엄격하게 접근통제를 받게 되어 있다(Ⅲ-3-나. 권한 분리와 접근 제어 참조). 또한 토큰 Issuer는 개방형 블록체인과의 연결을 통하여 데이터의 감사요청이 발생할 때, 데이터가 생성시점부터 변조되지 않았음을 증명할 수 있다.

(3) 보안상의 리스크

폐쇄형 블록체인에 사용하는 PBFT 합의 알고리즘은 2/3이상이 합의할 경우에만 데이터의 기록이 가능하다. 그러므로 악의적인 검증노드가 1/3이상이 존재한다면 유효한 데이터를 기록하는 것이 불가능하다. 이는 개방형 블록체인의 51% 공격과 유사하지만, 폐쇄형 블록체인은 허가받지 않은 노드들의 참여가 원천적으로 불가능하기 때문에 1/3이상의 검증노드가 악의적으로 동작할 가능성은 매우 낮다. 하지만 이같은 한계를 고려하여 접근제어의 명확한 룰과 적용이 필수적이며, 토큰 발행자의 책임 하에 운영되어야 한다.

한편, 폐쇄형 블록체인에는 채굴이라는 방식이 존재하지 않기 때문에 장부의 데이터를 변경시키는 공격에 대비하여 다량의 연산자원을 투입하지 않아도 블록체인을 운영할 수 있다. 하지만 이에 따라 폐쇄형 블록체인은 보안상의 공격에 대하여 근본적인 한계를 가지며 이를 극복하기 위해서는 개방형 블록체인과의 앵커링을 주기적으로 실시하고 제3자가 항시 감사에 참여하는 방안을 이용할 수 있다.

마. 민간 분산원장 시스템과의 권한 구분

현재 블록체인의 개발 진행은 구체적인 활용법을 찾기 위한 초기 단계로서, 대부분의 경우 블록체인 기술을 가지고 있는 다양한 민간 기관들이 블록체인을 연구하며 활용 방안을 찾고 기업들 간의 협업을 통해 블록체인 활용에

대한 테스트를 진행하고 있다. 앞에서 언급했던 블록체인 기반 컨소시엄인 R3CEV나 하이퍼레저 프로젝트 등은 기업들 간의 공동 연구를 통해 개발 및 운영되고 있는 민간 분산원장 컨소시엄이며 리플 등의 블록체인 프로토콜도 금융기관에서 송금 및 결제 플랫폼으로 관심을 보이며 여러 협업들을 진행하고 있다. 또한 IBM과 마이크로소프트 등의 IT 기업들도 각자의 블록체인을 개발하며 활용 방안에 대한 연구를 진행하고 있다. 국내에서는 블록체인 기업인 코인플러그(Coinplug)가 기업용 폐쇄형 블록체인인 FIDO Ledger를 개발하여 금융기관들의 관심을 받고 있다.

현재 단계에서 중앙은행 혹은 공공 기관이 자체적으로 블록체인 기술을 개발하는 데는 많은 어려움이 있다. 자본의 투입과 기술적 노하우가 필요한 블록체인 개발에는 많은 시간과 비용의 투입이 불가피하고, 더욱이 아직까지 어느 중앙은행 혹은 공공 기관이 블록체인 상용화를 한 사례는 많지 않다. 그렇기 때문에 우선 블록체인 기술을 연구 및 도입하고자 하는 공공 기관은 어떤 식으로든 민간 기관의 도움이 불가피하며 블록체인 기술을 보유하고 있는 민간 기관과의 협업을 통해 블록체인의 활용 가능 분야 및 구체적 활용 방안에 대해 연구를 하고, 그와 동시에 이후 블록체인 개발 및 활용을 어떻게 할지, 민간기관의 도움을 받거나 민간 기관이 운영하는 블록체인을 활용한다면 권한 설정을 어떻게 할 것인가 등의 논의도 이루어져야 할 것이다. 영란은행의 디지털 화폐 연구도 대학 교수들과 함께 진행하고 있으며 싱가포르의 공공기관의 경우 IBM과 함께 여러 분야에서 함께 블록체인의 활용 방안을 연구 중이다.

이렇듯 현재 블록체인 도입 과정에서 자체적인 블록체인 개발이 어려운 상황임을 고려할 때 민간 혹은 타 기관의 분산원장 시스템 도입이 불가피하며, 그렇기 때문에 분산원장을 도입할 때 블록체인 기관과 중앙은행의 역할 분담을 어떻게 할지, 어떻게 단계를 설정해서 분산원장을 도입할지 등을 검토할 필요가 있다. 단기적으로는 시스템에 대한 운영은 한국은행이 맡아서 하되, 시스템에 대한 관리나 개발은 블록체인을 개발하는 기관이 담당하고 장기적으로는 한국은행이 모든 시스템을 전담해서 관리할지, 계속해서 민간 기관이 개입할지, 개입을 한다면 어느 분야까지 개입을 할지에 대한 논의가 필요할 것으로 보인다.

4. 블록체인 도입의 기대효과

현재까지 지급결제 분야에서 블록체인 도입에 대한 구체적 사례가 많지 않기 때문에 비용 등의 측면에 있어서 직접적인 비교는 어려운 점이 있다. 하지만, 현재까지 블록체인이 가지고 있는 보안성, 실시간 결제, 확장성 있는 플랫폼 등의 장점은 여러 연구를 통해 이미 검증이 되었으며 현재의 지급결제시스템을 개선할 수 있는 가능성이 있는 데이터베이스 플랫폼이라는 것은 분명한 사실이다. 많은 금융기관과 중앙은행이 블록체인 기반의 지급결제시스템의 연구에 착수하고 있고 높은 활용도를 가지고 있다는 것이 분명하다면 중앙은행 시스템에 대한 테스트 환경을 마련하여 선제적으로 실험을 해보고 활용방안을 찾을 필요가 있을 것으로 보인다.

가. 보안적으로 갖추어진 데이터베이스 플랫폼

블록체인은 중앙화된 시스템의 보안 이슈를 보완할 수 있는 데이터베이스 플랫폼으로 기능할 수 있다. 우선 블록체인은 단일 공격점이 없기 때문에 외부의 공격으로부터 더 안전하다는 장점을 가지고 있다. 외부의 공격을 통해 하나의 노드가 손상을 입더라도 블록체인의 동기화 과정을 통해 다른 노드들이 쉽게 문제를 파악할 수 있고, 다른 노드들에는 원 데이터가 남아있기 때문에 빠르고 쉽게 자료를 복구할 수 있다. 이는 내부의 공격에 있어서도 적용된다. 내부에서 거래 내역의 위변조를 시도하게 되면 블록체인의 분산화된 네트워크를 통해 데이터를 실시간으로 검증할 수 있다. 또한 모든 거래 내역은 블록의 형태로 연결이 되어 있고 블록은 해시값을 부여받게 되는데 해당 해시값은 이전 블록과 현재 블록을 근거로 만들어진다. 결국 하나의 거래 내역을 조작하기 위해서는 이와 연결되어 있는 모든 거래 내역들을 위변조 해야 하기 때문에 위변조를 성공하기 어려우며 공격 시도도 바로 확인하여 검증할 수 있는 구조를 가지고 있다.

또한 블록체인은 거래 과정에서도 암호화 서명을 통해 위변조의 위험을 방지한다. 블록체인 내에서는 거래의 당사자의 서명이 있어야만 거래가 공식적으로 승인되는 구조를 가지고 있다. 혼합결제시스템에 적용될 블록체인의 경우 거래를 하는 두 당사자의 서명과 한국은행의 사인이 거래에 포함되어야 정식적으로 거래를 인정받고 블록에 등록될 수 있기 때문에, 거래와 상관없는 주체가 거래를 방해하는 경우를 방지할 수 있다.

나. 타 시스템으로의 확장성 있는 플랫폼

블록체인 플랫폼이 새로운 시스템으로 각광을 받고 있는 데에는 거래 내역의 투명성, 거래의 안전성, 분산 네트워크를 통한 신속성 등 기능적으로 가지고 있는 여러 장점들이 있지만 특히 블록체인이라는 하나의 플랫폼을 통해 여러 서비스를 만들어 낼 수 있다는 서비스 상의 확장성이 주된 장점으로 알려져 있다. 1장에서 나온 여러 연구 사례들에서 알 수 있듯이, 많은 분야에서 블록체인이 갓 도입을 시작했거나 실험과 연구, 테스트 위주의 초기 단계임에 불과하지만, 인증, 기록, 결제 및 청산, 송금, 스마트 계약, 투표, 가상화폐 등 다양한 분야에서 이를 응용하기 위한 연구가 진행중이다. 블록체인으로 무엇이든 할 수 있다고 말할 수는 없겠지만, 기존에 전체적인 사업의 프로세스가 여러 절차 혹은 여러 기업 등으로 쪼개져 있고 이로 인해 시간적, 비용적 비효율성이 심각한 사업 분야의 경우, 분산화된 네트워크를 통해 프로세스를 간소화하고 시간적, 비용적 절감을 구현할 수 있다. 이를 바탕으로 여러 서비스를 붙여 해당 분야의 서비스를 통합해서 제공할 수 있는 플랫폼으로 활용될 가능성도 있다.

또 하나의 장점은 단순히 여러 분야에서 사용할 수 있고 여러 서비스를 만들 수 있는 것 뿐 아니라, 만들어진 서비스들을 하나의 블록체인 기술을 기반으로 서로 연동할 수 있다는 점이다. 블록체인은 기본적으로 분산형 네트워크로 구성되어 있고 각 금융망들이 하나의 큰 노드 역할을 수행하여 서로 다른 분야의 시스템이 연동할 수 있는 블록체인 네트워크를 만들 수 있다. 현재 한국은행에는 이번에 보고서에서 적용한 혼합결제시스템뿐만 아니라 총액결제, 소액결제, 증권결제 등 다른 지급결제시스템이 운영되고 있고 외환전산망, 국고전산망 등 한국은행 내에서 다른 기능을 담당하는 전산망들도 존재한다. 현재에도 각 금융망들이 서로 연동될 수는 있으나 근본적으로 각각의 목적으로 만들어진 분리된 망이기 때문에 시스템 연동에 있어서 개선이 필요하며 보안, 관리 등에도 각각의 비용이 소요된다. 반면, 블록체인 플랫폼은 하나의 플랫폼으로 실시간으로 다수의 서비스를 동기화할 수 있어 서비스의 이용과 보안상의 비용 절감을 할 수 있다는 장점을 가진다.

다. 결론

블록체인을 기반으로 하는 지급결제시스템은 실시간 데이터의 동기화를 통해 실시간 결제 및 청산이 가능하며 분산 네트워크와 암호 알고리즘을 통해 보안적으로 안전한 네트워크를 구성할 수 있다. 또한 하나의 플랫폼으로 여러 서비스를 연동하여 사용할 수 있다는 플랫폼 확장성을 가지고 있기 때문에 세계 각국의 금융기관과 은행에서 블록체인 기반 결제 시스템 플랫폼을 개발하며 도입을 준비 중에 있다. 하지만, 현재까지는 시스템의 전환 비용이나 신기술에 대한 적용 방안 문제 등 활용시 고려해야 할 사항들이 존재하기 때문에 중앙은행의 지급결제시스템 및 금융망의 블록체인 적용 방안에 대한 지속적이고 적극적인 연구 및 개발과 함께 적용을 위한 단계적인 접근이 필요할 것으로 보인다.

Ⅳ. 블록체인 기반 디지털 통화의 가능성

1. 블록체인 기반 디지털 통화 개발 현황

가. 현금 없는 사회의 도입

현재 세계적으로 '현금 없는 사회'에 대한 논의가 증가하고 있다. 2030년까지 현금 없는 사회를 목표로 했으나 오히려 속도를 늦춰야 할 필요성을 느낀다는 스웨덴의 경우나 상점에서 현금을 합법적으로 거부할 수 있는 덴마크 등의 북유럽의 예시는 이미 많이 알려진 사례이다. 대한민국 또한 '현금 없는 사회'에 대한 논의를 진행하고 있는데, 점진적인 연착륙을 위해 우선적으로 2020년을 목표로 '동전 없는 사회'를 준비하고 있다. 대한민국을 포함한 많은 국가들이 현금 없는 사회에 대한 논의를 본격적으로 시작하고 있는 첫 번째 이유는 현행 현금 유통 시스템의 문제점을 개선하기 위함이고 두 번째 이유는 그 문제점을 개선할 수 있을 정도의 기술적 발전이 이루어지고 있기 때문이다.

현금 없는 사회를 도입하고자 하는 첫 번째 이유는 현행 현금 시스템이 가지고 있는 발행, 관리, 유지상의 비효율성 때문이다. 현금의 경우 절도와 분실 및 손실 등 실물 화폐로서 가질 수 있는 위험으로부터 자유롭지 못하다. 노르웨이 중앙은행의 연구에 따르면, 현금 거래에 소요되는 건당 비용은 카드를 이용했을 때 보다 약 73%가 높으며, 미국의 경우 ATM 사용료, 도난, 인쇄 비용 등 현금 발행, 사용 및 관리를 위해 민간과 정부가 부담하는 비용이 미국 GDP의 1.2%에 육박할 것으로 보인다.[175]

특히 가장 큰 문제를 유발하는 것은 현금 중에서도 동전과 고액권인데, 동전은 발행과 유통의 어려움, 고액권은 지하경제로 인한 유통의 어려움이 주요 이유이다. 우선적으로 동전은 액면 대비 제조 원가가 비싸 발행 자체에도 비용 부담이 크다. 지난해 100원짜리 동전 2억5,000만개를 포함하여 동전 6억개를 제조하는 데 든 비용은 539억원에 달하지만 동전의 환수율은 10%에 불과할 정도로 제조와 발행 비용에 비해 유통이 잘 되지 않는 구조를 가지고 있다.[176] 고액권은 높은 가치의 화폐를 지폐로 유통하기 때문에 비용상

175) 현금 없는 경제: 의미와 가능성, KERI, 2016
176) http://biz.chosun.com/site/data/html_dir/2016/05/05/2016050500724.html

문제는 없지만 가치가 너무 높기 때문에 유통이 되지 않는다는 문제점이 있다. 2015년 기준 5만원권 환수율은 40.1%로 1만원권의 95.3%의 절반에도 못 미친다.[177] 이는 고액권이 유통되기보다는 가치를 보관하는 목적에 머물러 있으며 이에 따라 현금의 유통과 관리에 있어 비효율성이 발생된다.

두 번째는 이미 국내에서 현금 없는 사회를 논의하기 충분할 정도로 전자 거래의 비중이 높고 활성화가 되어 있기 때문이다. 기존의 거래 방식들의 불편함과 비효율성에도 불구하고 현재까지도 현금과 동전이 상당 부분 이용되고 있으나, 전자 거래 기술의 발달로 더 효율적인 전자 거래를 할 수 있는 기반이 구성되었고 이를 바탕으로 기존의 지폐 시스템이 가지고 있는 불편함을 개선할 수 있다는 것이다.

특히 한국의 경우 정보통신 인프라가 잘 갖춰져 있고 신용카드 결제 등 전자결제 인프라가 잘 구축되어 있는 등 전자 거래가 활성화되어 있는 국가이다. 한국은 국제정보통신연맹(ITU)에서 매년 발표하는 정보통신기술발전지수(IDI)에서 2015년 1위를 차지할 정도로 기술적인 발전이 빠른 상황이다.[178] 거래건수에서도 지급수단별 이용비중이 신용카드(39.7%)가 현금(36.0%)을 추월하면서 비현금거래가 현금거래보다 비중이 높아지는 추세이다. 이미 많은 부분에서 금융 거래의 전자화가 이뤄지고 있고, 국민들이 전자 거래에 익숙해지는 상황에서, 중앙은행 또한 디지털 화폐를 직접 발행하기 위한 기술적, 제도적 논의도 본격적으로 이뤄지고 있으며 이를 구현할 수 있는 기술로서 블록체인이 큰 가능성을 갖고 있다고 판단하여 관련 연구가 활발히 진행되고 있다.

나. 블록체인 기반 디지털 통화의 장점

이미 많은 분야에서 전자화된 금융 거래가 활성화되고 기존 전자 거래의 시스템에 대한 기술적 발전도가 높은 상황이다. 하지만 디지털 통화 발행에 있어 많은 금융기관과 중앙은행은 비교적 새로운 기술로 평가받고 있는 블록체인 기술을 중심으로 연구를 추진하고 있다.

비교적 새로운 기술이라 할 수 있는 블록체인을 기반으로 하는 디지털 화

177) http://www.newsis.com/ar_detail/view.html?ar_id=NISX20160319_0013968457&cID=10401&pID=10400
178) http://www.m-economynews.com/news/article.html?no=17662

폐에 대한 가능성이 언급이 되는 것은 특정 기업이나 고객에 국한된 전자화폐가 아닌 중앙은행이 국민들을 대상으로 발행하는 전자 화폐이기 때문이다. 중앙은행이 전자화된 화폐를 발행한다는 것은 기존에 오프라인으로 유통되던 화폐를 온라인으로 유통을 한다는 의미이며, 이는 발행, 유통, 환수 등 화폐가 만들어내는 모든 과정을 디지털화하고 이를 전적으로 중앙은행이 관리한다는 의미이다. 이를 위해서는 현금을 대체할 수 있을 정도의 보안성과 확장성이 필요하고 현 화폐 시스템의 문제를 해결할 수 있는 투명성 확보가 가능한 화폐 시스템이 필요하다는 것을 의미한다. 현재 전자거래 시스템이 화폐를 대체해 나가고 있지만 중앙은행이 이같은 시스템을 기반으로 디지털 화폐를 발행하는 경우 보안의 문제나 거래 규모의 문제를 감당할 수 있을지에 대한 의문이 있고 시스템을 관리하기 위한 비용문제 또한 존재한다.

블록체인은 비트코인의 기반기술로서 이미 시스템적으로 화폐를 발행하고 유통할 수 있다는 가능성이 확인되었다. 비록 비트코인 등의 개방형 블록체인은 그 활용에 있어서의 한계로 인해 타 기관이 직접적으로 사용할 수는 없지만, 비트코인의 기반 기술인 블록체인이 가지고 있는 가능성은 많은 곳에서 확인되었고 이를 통해 폐쇄형 블록체인의 연구개발과 컨소시엄 구성 등이 활발해졌다. 이 연구는 다시 특정 기관이 발행하는 가상화폐에 대한 연구로 이어졌고 정부가 직접 디지털 화폐를 발행하는 방안에 대한 관심으로까지 이어지게 되었다.

우선 전자화폐 플랫폼으로서 블록체인 도입을 고려하는 이유 중 하나는 블록체인을 통해 거래의 투명성을 담보할 수 있기 때문이다. 기존 화폐 시스템의 단점 중 하나는 화폐가 어떻게 사용되고 있는지 내역을 파악하기가 어렵다는 점이고, 이 어려움으로 인해 낮은 환수율과 저조한 사용도의 문제를 극복하기 어렵게 만든다. 반면, 블록체인이 가지고 있는 가장 큰 장점 중 하나는 투명성이다. 분산형 네트워크를 통해 장부를 공유하기 때문에 거래 내역을 확인하고 개별 거래들을 추적할 수 있다. 개방형 블록체인의 대표적인 사례인 비트코인은 누구나 거래 내역을 조회할 수 있고, 폐쇄형 블록체인도 구성하기에 따라서 블록체인 관리 기관이 모든 거래 정보를 확인할 수 있다는 장점이 있다. 이는 현재의 화폐 시스템의 단점인 고액, 저액 화폐의 낮은 환수율과 고액권이 지하 경제로 스며드는 문제를 극복할 수 있으며, 화폐 사용 내역들을 통해 화폐의 흐름을 분석하고 거시적인 화폐 정책을 구상하는 데도 도움이 될 수 있다는 장점을 가지고 있다.

두 번째로는 블록체인을 통해 거래내역을 추적할 수 있으면서도 익명성을 구현할 수 있는 플랫폼을 구성할 수 있기 때문이다. 다른 여러 보안적 장치와 함께 블록체인 내의 거래의 투명성은 거래의 위변조를 방지하고 실시간으로 거래를 파악할 수 있는 기반이 되었다. 하지만 다른 한편으로 일체의 거래내역이 공개되는 투명성으로 인해 거래내역과 기밀 정보의 보안을 강조하는 금융기관들이 개방형 블록체인을 직접 활용하는 데 어려움이 컸고, 이를 극복하기 위해 각 금융기관과 스타트업들은 기록들의 열람과 조회의 권한을 설정할 수 있는 폐쇄형 블록체인을 개발하기 시작했다. 기본적으로 거래 내역을 투명하게 공개하는 블록체인이지만 폐쇄형 블록체인의 경우는 접근 권한 설정에 따라 거래 당사자만이 거래를 확인할 수 있는 시스템을 구성할 수 있고 이는 개방형과 거래의 익명성을 동시에 유지할 수 있는 플랫폼으로 활용될 수 있다.

세 번째는 활용도, 특히 동전으로 대표되는 소액 현금 결제의 활용도를 높일 수 있다. 현재 동전은 환수율이 10%에 불과할 정도로 유통이 저조한데, 이는 물가상승으로 인해 동전으로 거래할 만한 물품이 많지 않은 데다 무게와 부피 때문에 많은 금액을 동전으로 들고 다니기도 힘들기 때문이다. 또한 분실도 잦아서 제대로 사용되지 못하는 경우도 많다. 디지털 통화는 지폐와 동전을 전자화함으로써 소지의 불편함 문제를 줄일 수 있고, 쉽게 사용할 수 있는 환경을 만들어준다. 또한 실물 화폐처럼 분실할 염려가 없기 때문에 활용도와 환수율을 높이고 숨어있던 화폐의 유통을 활발하게 만들 수 있는 시스템으로 활용될 수 있다.

네 번째로는 블록체인 기술이 보안상 문제를 극복할 수 있는 방안이 될 수 있다. 블록체인 기술은 중앙기관 없이 화폐를 발행 및 유통한 대표적인 케이스인 비트코인의 근간이 되는 시스템이다. 비트코인 블록체인이 기능적인 한계점들을 가지고 있지만, 보안상으로는 비트코인 블록체인에 대한 내외부 공격으로 인한 피해 없이 정상적으로 운영이 되고 있다. 블록체인 기술은 시스템에 대한 내외부 보안에 큰 비용을 지출할 필요 없이 분산화된 네트워크를 통해 시스템적으로 보안의 문제를 해결한 플랫폼이다. 전자화된 화폐를 발행할 때 이용자들이 사용하는 전자화폐가 안전하게 보관되고 분실이나 위변조를 방지할 수 있는 안정성 있는 플랫폼을 제공할 수 있어야 하며, 이를 뒷받침할 수 있는 기술로 블록체인이 활용될 수 있을 것이라고 보고 있다.

다. 블록체인 기반 디지털 통화 연구 현황

현재 블록체인 기반의 디지털 통화에 대한 연구는 초기 단계에 있다고 볼 수 있다. 디지털 화폐가 현금의 문제점과 비효율성을 극복할 수 있는 대안으로 평가받고 있지만 아직까지 현금에 대한 수요가 상당 수준을 유지하고 있고, 현금을 전자화하는 데 따른 기술적 문제, 국민들이 전자화폐를 받아들이는 데 있어 정서적 문제 등이 남아있기 때문이다. 현재는 화폐 발행 및 유통 플랫폼으로서 블록체인의 기술적 가능성과 활용 방안에 대한 검토에 착수하고 있는 단계이며 향후 본격적인 활용에 앞서 심도 있는 연구가 우선 추진되고 기술적 성숙도가 높아질 필요가 있는 것으로 판단된다.

블록체인 기반 디지털 화폐에 대해 구체적인 보고서를 작성한 중앙은행은 사실상 영란은행이 유일하다. 영란은행은 올해 4월 블록체인 기반 중앙은행 발행 디지털 화폐인 RSCoin 보고서를 발표했고, 현재까지 계속해서 관련 연구를 진행중인 것으로 알려져 있다. 네덜란드 중앙은행(DNB Coin), 캐나다 중앙은행(CAD Coin) 등도 블록체인 기반의 디지털 화폐에 대한 연구를 진행 중이라고 밝혔지만, 디지털 화폐를 연구한다는 언론 발표 이후에 보고서 등의 구체적인 결과물은 아직 공개되지 않은 상태다. 중국 정부도 올해 2월 전자화폐 발행을 위한 기술로 클라우드 컴퓨터, 전자 칩 기술 등과 함께 블록체인을 고려하며 연구를 진행 중이라고 밝혔지만,[179] 이후에 블록체인에 대한 구체적인 추가 언급은 없는 상태이다.

2. 중앙은행의 디지털 통화 발행 방안

중앙은행이 발행하는 블록체인 기반 디지털 화폐는 화폐의 발행 권한을 전적으로 담당하는 중앙은행의 시스템과 발행 권한이 완전히 분산화된 비트코인 블록체인의 기술적 장점을 조합하려는 독특한 시도이다. 하지만 기존의 지폐와 동전으로 대표되는 화폐 시스템의 비효율성을 극복하기 위한 방안을 찾는 중에 분산화된 네트워크에서 화폐를 발행·유통하는 비트코인은 디지털 화폐발행을 가능하게 해주는 기술적 근거를 제공해 주었고, 비트코인으로 대표되는 개방형 블록체인의 한계를 극복할 수 있는 방안으로 폐쇄형 블록체인이 대두되고 기술적 개발이 이어지면서 각 중앙은행을 중심으로 블록체인을 기반으로 하는 디지털 화폐의 발행 논의가 올해 들어 본격적으로 시작되고 있다.

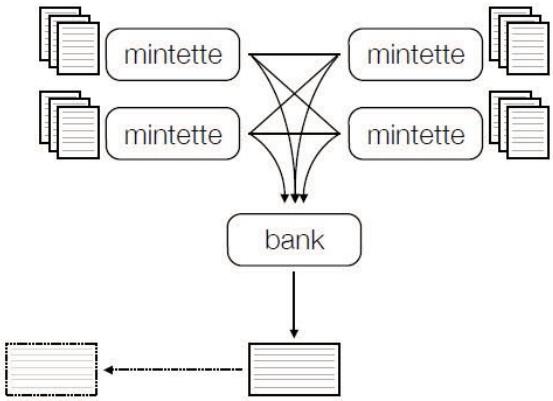
179) http://www.coindesk.com/chinas-central-bank-weighing-blockchain-as-one-option-for-digital-currency/

본 보고서에서는 영란은행이 발표한 RSCoin에서 제안된 모델을 중심으로 중앙은행 발행 디지털 화폐의 구조와 한국은행에 시사하는 점을 서술하고자 한다.

가. RSCoin의 블록체인 기반 화폐 유통

RS코인은 올해 4월 영란은행에서 발표한 중앙화된 은행 기반 암호화폐(Centrally Banked Cryptocurrencies)라는 이름의 보고서에서 처음 등장했다. 비트코인처럼 블록체인의 분산화된 네트워크를 도입하되 중앙은행이 전적으로 발행과 통제를 담당하는 구조를 가지고 있다.

<그림 4-1> RS코인의 개괄적인 구조도



자료: RSCoin Report

RS코인 모델의 가장 큰 특징은 분산원장 기술을 활용하지만 중앙은행이 모든 것을 통제하는 블록체인이라는 것이다. 블록체인의 형식을 빌려서 여러 노드들이 거래를 확인하고 승인하는 과정을 거치지만 화폐의 발행과 거래에 대한 최종 승인 등 주요 절차는 모두 중앙은행이 담당을 하고 다른 절차들은 중앙은행이 승인한 타 기관들에 위임하는 식으로 블록체인을 운영한다. 결국 블록체인이라는 형식을 따온 중앙집권화된 발행 시스템을 구현하고자 한다.

두 번째 특징은 블록체인 구조를 이원화하여 운영한다는 것이다. RS코인 구조도를 살펴보면 거래의 수집과 초기 블록들을 생성하는 하위 단계 블록

(lower-level block)과 최종 블록의 생성 및 화폐의 발행을 담당하는 상위 단계 블록(higher-level block)으로 나뉜다. 여기에서 중앙은행은 기능적으로 상위 단계 블록을 담당하고, 하위 단계 블록의 역할을 담당하지는 않지만 이를 통제하는 권한을 가진다. 이는 결국 실질적인 업무는 최소화하되 통제의 권한은 최대화한 구조로 하위 단계 블록에서 1차적으로 거래를 확인하고 블록을 생성하면 상위 단계 블록에 전송을 하고, 상위 단계 블록을 담당하는 중앙은행에게 가장 중요한 승인과 블록 등록의 역할을 맡기지만, 다른 역할들은 최소화하면서 시스템을 유지하게 한다.

단계별 블록에 대해 보다 상세히 살펴보면, 하위 단계 블록은 거래 내역을 종합하는 Mintette가 모여서 구성이 되는데 Mintette는 거래 내역을 모아서 블록을 만드는 역할을 한다. 개방형 블록체인에서의 채굴자 역할과 유사하며, 블록을 만드는 절차도 비트코인 등의 개방형 블록체인과 비슷하다. 개방형 블록체인에서의 채굴자와 차이점은 Mintette의 경우 작업 증명 등의 채굴 과정을 통해 블록을 만드는 대신 PKI 방식 등을 통해 중앙은행의 승인을 받아 블록을 생성한다. 중앙은행의 승인을 받은 Mintette들은 거래의 모음인 블록을 생성하며 다른 노드들과의 공유를 통해 1차적인 블록을 완성한다. Mintette는 중앙은행이 담당할 수도 있고 중앙은행이 신뢰할 만한 대형 상업 은행 등의 금융망 참여기관들이 담당할 수도 있는 등 다양한 방식을 선택할 수 있다.

<그림 4-2> 하위 단계 블록의 거래 승인 절차

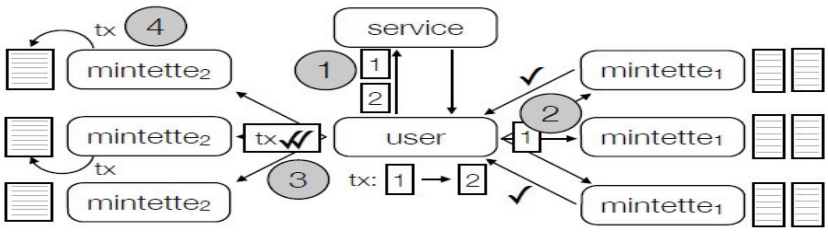


Fig. 2: The proposed protocol for validating transactions; each mintette m_i is an owner of address i. In (1), a user learns the owners of each of the addresses in its transaction. In (2), the user collects approval from a majority of the owners of the input addresses. In (3), the user sends the transaction and these approvals to the owners of the transaction identifier. In (4), some subset of these mintettes add the transaction to their blocks.

자료: RSCoin Report

상위 단계 블록에서는 하위 단계 블록에서 만든 블록들을 공식적인 블록체인에 등록하는 역할을 한다. 상위 단계 블록은 하위 단계에서 만들어진 블록의 무결성을 검증하고 확인이 되면 이를 상위 레벨의 블록체인에 등록한다. 즉, 1차적으로 정리가 된 블록을 마지막에 검증하여 2차적으로 공식적인 블록체인에 등록하는 것을 의미한다. RS코인의 사용자는 상위 단계 블록만을 확인해도 충분히 거래 내역을 체크할 수 있는 구조가 되며, 하위 단계 블록에 대한 확인을 하고 싶은 경우에도 거래 내역을 확인할 수 있도록 설계하는 것도 가능하다.

RS코인은 결국 블록체인의 형식을 빌려 분산화 네트워크를 활용하되 발행 등 주요 권한은 중앙은행이 보유하는 네트워크를 가진다. RS코인을 통해 기존의 비트코인보다 더 확장성이 있으면서도 중앙은행이 활용을 높일 수 있는 방법을 찾겠다는 것이 보고서의 주요 내용이다. 더욱이 보고서에는 하위 단계 블록의 역할을 중앙은행이 신뢰할 만한 금융기관들이 담당할 수도 있다고 설명하고 있으며, 중앙은행은 Mintette에 대해 전적인 권한을 가지고 있고 하위 단계 블록을 담당하는 Mintette에게 일정량의 수수료를 지급하는 내용도 포함되어 있다. 이는 하위 단계 블록에서 기존 개방형 블록체인의 모델을 최대한 유지하면서 화폐 유통을 담당하게끔 만들고, 중앙은행은 화폐 발행기관으로서 화폐를 발행하고, 유통된 거래에 대해 최종적으로 승인을 하고, 화폐 유통을 관리하는 하부 기관을 관리하고 보상하는 역할만을 맡겠다는 의미를 가진다.

나. 디지털 화폐 발행 방법

RS코인의 보고서 자체는 이원화된 블록체인 구조를 바탕으로 거래를 검증하고 합의를 도출하는 등 시스템을 운영하는 방법을 간략히 설명한 자료이며, 디지털 화폐에 대한 구체적인 발행의 절차, 거래 내역을 전달받는 방식 등 실제 운영을 위한 구체적인 요건 등에 대한 설명은 담겨 있지 않다. 중앙은행이 어떤 블록체인 구조를 가지고 검증을 하며 블록체인을 구성할지도 중요한 요소이지만 블록체인을 통해 발행된 화폐를 어떻게 발행하며 사람들이 사용하도록 할 수 있을지도 고려해야 할 요소일 것이다.

장기적으로 블록체인 기반의 디지털 화폐를 만들기 위해서는, 우선적으로 역할에 대한 구분이 필요하다. 이를 위해서는 비트코인 블록체인의 구조를

참조할 수 있다. 현재까지의 개방형 블록체인 중 가장 많은 사용자를 보유하고 있는 비트코인 블록체인은 익명의 다수를 대상으로 하는 개방형 블록체인 네트워크로서 각 노드들은 서로 동등한 위치에 있지만 각자 다른 역할을 가지며 유지될 수 있다. 비트코인 블록체인의 노드들은 크게 네 가지 기능을 가질 수 있으며 이 기능을 어떻게 나누어 가지고 있느냐에 따라 비트코인 네트워크에서의 역할이 달라진다.

기능적으로 봤을 때 비트코인 네트워크의 노드들은 모든 블록체인 정보의 데이터베이스가 담겨있는 풀 블록체인 데이터베이스(full blockchain database), 비트코인 채굴을 담당하는 채굴자(Miner), 거래와 블록을 전파하는 네트워크 라우팅(Network Routing), 비트코인 거래를 할 수 있는 지갑(wallet)이 있다. 이 네 가지 기능이 어떻게 조합되는지에 따라 노드의 역할이 바뀌며 참여자가 자유롭게 변경할 수 있다.

우선 모든 노드들은 네트워크 내에 라우팅 기능을 가지고 있으며, 여기에서 다른 기능들이 더해진다. 라우팅 기능을 통해 모든 노드들은 거래와 블록을 검증하고 전파하면서 노드들을 연결하고 블록체인 네트워크를 유지하는 역할을 수행한다.

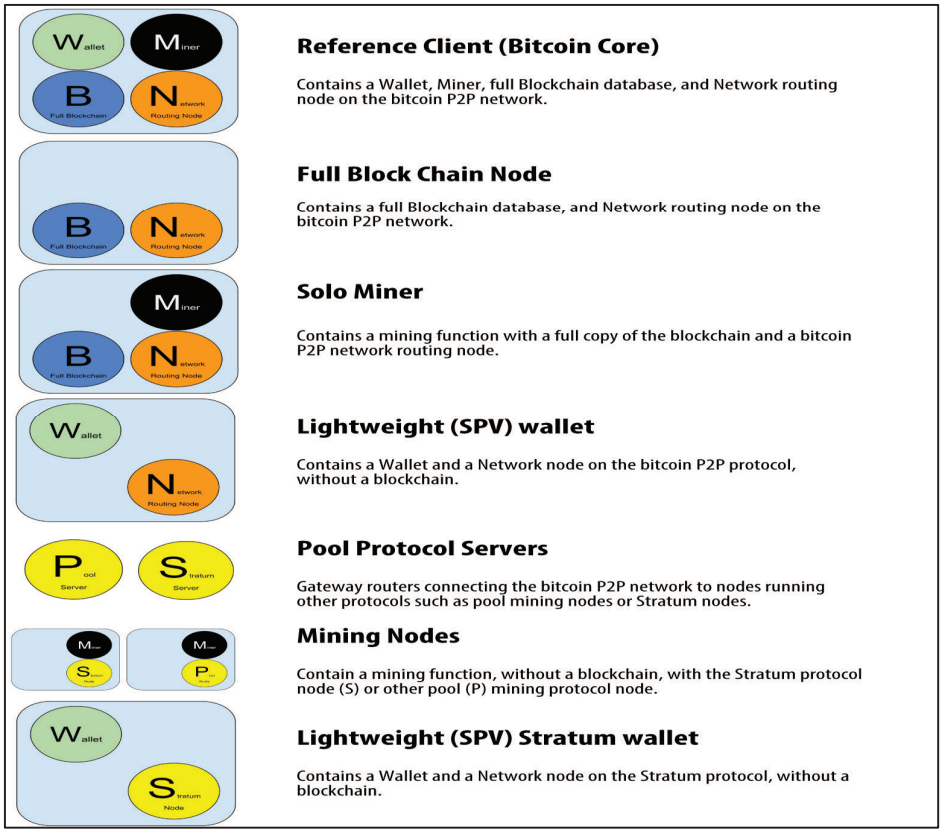
풀 노드(full node)라고 불리는 노드들은 모든 데이터베이스를 가장 최신의 상태로 가지고 있는 노드들이다. 비트코인 거래의 모든 정보를 저장하고 독자적으로 신뢰할 수 있는 방법을 통해 거래를 검증하는 사용자로서 비트코인 생태계를 유지하는 모든 기능을 직접 수행하는 사용자다.

두 번째로는 채굴 노드(Miner)가 있다. 채굴 노드는 작업증명을 푸는 전용 하드웨어를 가지고 평균 약 10분마다 나타나는 문제를 풀기 위해 경쟁하는 노드들로서 채굴을 통한 신규 화폐 발행이 그들의 동기부여가 된다. 채굴 노드는 풀 노드로서 블록체인 거래 내역 전부를 들고 있을 수도 있지만, 풀 노드 없이 서버에 의존하여 기능할 수도 있다.

다른 하나는 라이트웨이트 노드(lightweight node)가 있다. 라이트웨이트 노드는 SVP(Simple Payment Verification) 노드라고도 불리는데, 풀 노드처럼 전체 블록체인 기록을 가지고 있지는 않지만 단순지불검증이라는 방법을 이용하여 거래를 검증하고 비트코인 거래에 참여하는 노드들을 의미한다. 비트

코인 거래를 원하지만 다른 부담을 지고 싶지 않아하는 경우로 일반적인 비트코인 플랫폼 사용자들은 대부분 라이트웨이트 노드들이다. 라이트웨이트 노드는 블록 헤더만 다운로드하고 각 블록에 있는 거래들은 가지고 있지 않기 때문에 풀 노드보다 약 1,000배 가량 작은 크기를 가지고 있으며, 거래를 검증할 때는 이웃 노드들에게 의존하는 방법을 이용하여 거래를 검증한다. 풀 노드와 라이트웨이트 노드를 비교하여 검증 과정을 설명하자면, 풀 노드는 해당 지역 전체를 볼 수 있는 지도를 가지고 여행을 다니는 사람이라면, 라이트웨이트 노드들은 지도 없이 주변 사람들에게 길을 물어보며 여행을 다니는 사람에 해당한다고 볼 수 있다.

<그림 4-3> 비트코인 네트워크에서 노드들의 역할



자료: Mastering Bitcoin

비트코인 노드들의 기능과 비교해 보자면, 중앙은행은 풀 노드로서 모든 거래 내역을 보유하고 화폐를 발행하는 역할을 하게 되고 이를 이용하는 국민들은 라이트웨이트 클라이언트로서 전자화폐의 사용만을 할 수 있는 역할을 하게 될 것이다. 채굴 노드의 경우도 화폐를 발행하는 중앙은행이 이 기능을 맡게 되지만, 구체적으로는 블록체인의 구조에 따라 다른 방법으로 대체될 수 있다. 이는 개방형 블록체인에서 채굴을 위해 만들어진 작업 증명 등의 방식 대신 다른 방법으로 화폐 발행을 대체할 수 있기 때문이다. 3장에서 소개된 혼합결제시스템의 방식처럼 발행을 담당하는 중앙은행이 발행 거래를 생성하여 배포하는 방식 등을 활용할 수 있다.

3. 디지털 통화 도입의 조건 및 고려 사항

가. 보안성

정부가 발행하는 디지털 화폐는 지폐, 동전과 마찬가지로 모든 국민들이 사용하게 될 화폐이다. 그렇기 때문에 견고한 보안 시스템은 필수적이며 국민들에게 기술적으로 문제가 없다는 신뢰를 보장해야 한다.

정부가 블록체인을 기반으로 하여 화폐를 발행하게 된다면 사용자 관리와 화폐 발행은 중앙은행이 담당하게 되겠지만, 사용 대상이 대한민국에 사는 모든 사람들 혹은 한국의 화폐를 사용하고자 하는 모든 사람들이 된다면, 사실상 불특정 다수가 사용하는 개방형 블록체인의 형태에 가까울 것이다. 개방형 블록체인의 가장 대표적인 사례인 비트코인 블록체인의 경우는 거래에 참여하는 노드들이 직접 채굴 노드와 풀 노드들의 역할을 맡았고 노드들이 작업 증명 등을 통해 투입한 컴퓨팅 파워가 외부의 공격을 어렵게 하는 보안상의 근거가 되었고, 노드들은 그 대가로 비트코인을 발행받도록 설계되어 있다. 즉, 개방형 블록체인은 사용자가 발행자가 되어 보안 시스템을 자발적으로 구성하는 메커니즘으로 운영이 된다. 하지만 중앙은행이 발행하는 디지털 화폐의 경우 다수의 인원이 자유롭게 참여한다는 점에서는 개방형 블록체인의 성격을 가지고 있지만 역할과 권한의 구분이 명확하고 특정 발행기관이 정해져 있다는 점에서 기본적으로 폐쇄형 블록체인이라고 할 수 있다. 그리고 발행과 거래 내역의 기록 등의 권한은 중앙은행 고유의 권한으로서 이 역할을 다른 기관 또는 개인에게 양도할 수는 없다.

결국 개방형 블록체인처럼 운영되는 폐쇄형 블록체인인 정부 발행 디지털 화폐에서는 기존 개방형 블록체인에서 참여자가 자발적으로 수행하는 기능을 중앙은행이 어떻게 처리할 것인가의 문제가 남는다. RS코인의 방식에서와 같이 하위 단계의 블록들이 참가자들의 거래 내역을 모아 하나의 블록을 생성하고 상위 블록인 중앙은행은 거래의 유효성을 재검사하고 승인하여 공식 블록체인에 등록하는 등 많은 사용자와 거래 건수를 안전하게 처리하고 내역을 등록할 수 있는 시스템에 대한 연구가 필요하다.

나. 확장성 (처리 용량 및 속도)

블록체인 기술이 디지털 화폐를 구현할 수 있는 기술로 각광을 받고 많은 중앙은행과 금융기관이 이를 기반으로 하는 디지털 화폐에 관한 연구를 진행하고 있지만 현재까지 개발된 블록체인 기술이 한 국가의 화폐를 유통할 만큼의 처리 용량과 속도를 가지고 있는지도 고려해야 할 것이다. 3장에서 설명한 지급결제시스템의 경우에는 혼합결제시스템에 참여하는 금융 기관만이 블록체인 기반 지급결제시스템에 참여하고 거래 유형 또한 금융 기관 간의 거액 결제에 국한된다. 이렇듯 기관의 수와 거래의 유형이 제한적이기 때문에 거래의 건수 또한 상대적으로 많지 않다. 일반적으로 블록체인 내에서 거래의 규모는 거래 금액의 크기보다는 건수가 더 중요한 문제이기 때문에 거액결제시스템에서는 확장성의 문제는 큰 이슈가 아닐 것으로 보인다. 하지만 일반 개인간 거래에서 현금이 유통되는 건수도 비교할 수 없을 정도로 많고 거래에 참여하는 대상자가 전 국민이다. 현재의 블록체인의 기술적 수준이 이를 감당할 수 있을 만큼 높아지기에는 개발과 기술의 추가적인 진보가 필요할 것으로 보인다.

우선 중앙은행은 지속적으로 블록체인 활용 방안을 연구하면서 동전을 대체하는 전자지갑이나 소액 결제 등에서만 활용하는 등 규모와 역할의 제한을 두는 블록체인 기반 화폐 유통을 우선 시작하고 이후 점진적으로 블록체인 기반 디지털 화폐 도입을 확대해 나가는 것과 같은 접근법이 필요할 것으로 보인다.

또한 현금 유통의 경우 일일 거래 건수를 정확하게 파악하기가 불가능하기 때문에 다양한 테스트를 통해서 어느 정도 규모의 현금 거래를 블록체인에 적용할 수 있을지, 전면적인 도입을 가정할 때는 어느 정도의 기술적 개선이

필요한지 등에 대해 지속적으로 연구할 필요가 있다.

다. 시장, 국민의 디지털 화폐에 대한 적응

기술 자체에 대한 문제는 아니지만 화폐를 실제 사용하는 시장, 국민들의 기술에 대한 적응 문제도 중요한 이슈이다. 거래 수단이 다변화되고 전자 거래의 비중이 높아지고 있지만 여전히 많은 부분에서 현금거래가 이루어지고 있다. 한국은행의 조사에 따르면 지난해 소비자들의 지급결제 수단 중 신용/체크/직불카드의 비중이 전체의 53.8%를 차지했지만, 반면 현금결제 비중은 38.9%에서 36.0%로 줄어들었으며, 금액 기준으로 보면 29%에 불과하다. 따라서 약 60%의 거래가 신용카드 등의 전자적인 방법으로 이루어지고 있으나, 반대로 생각하면 36%에 달하는 상당수 거래가 현금으로 이루어지고 있음을 의미한다. 특히 장노년층과 재래 시장 등의 특정 부분에서는 아직 전자거래가 익숙하지 않기 때문에 이와 같은 측면에서 충격을 최소화하면서 점진적으로 도입하기 위한 방안 등에 고민도 함께 따라야 할 것이다.

또한 국민들의 디지털 화폐 사용에 대한 정서적인 문제도 고려해야 한다. 디지털 화폐를 발행하는 우선적인 목표는 화폐 발행 및 보관을 위한 비용을 절감하고 지폐 사용에 따른 번거로움을 줄임으로써 국민들의 화폐 활용 편의성을 증대하는 것과 함께 지하경제의 양성화를 통한 세율 인상 없는 넓은 세수 확보이다. 하지만 디지털 화폐가 정부에 유리하고 국민에 불리한 정책을 도입하기 위한 교두보라는 인식이 확산될 수 있는 데다, 국가가 개인의 모든 거래 내역을 상시 감시하고 자유로운 화폐의 사용을 제한할 수도 있다는 점에서 국민적 반감이 형성될 수도 있다.

또한 최근 화두로 등장한 현금 없는 사회의 추진 목적이 저금리 기조 하에서 마이너스 금리 정책을 실시하기 위한 것이 아닌가 하는 논의도 진행되고 있다. 현재 중앙은행에서 마이너스 금리를 도입하더라도 개인들이 금융자산을 현금으로 보유하는 경우에는 경기 부양 정책으로서 실질적으로 효과가 크게 줄어든다. 하지만 모든 현금을 전자화하여 정부가 직접 발행 및 관리한다면 마이너스 금리 정책을 보다 용이하게 실시할 수 있고, 결국 국민들은 피해를 보게 될 수 있다는 우려도 형성되고 있다.

결국 디지털 화폐를 이용하는 주체는 국민이기 때문에 정서적 반감의 진위

여부를 떠나서 중장기적으로 공감대를 형성하고 제도 도입을 충실하게 준비하기 위한 시간이 필요하다. 화폐 사용의 감시 문제와 관련하여 정부의 목적이 사적인 거래의 감시가 아니며 편리하고 투명한 거래를 보장하기 위함임을 적극 홍보하여 불안을 해소하는 한편, 기술적으로도 개인의 거래 내역 노출이 최소화될 수 있도록 보호장치에 대한 연구가 동반되어야 할 것이다.

라. 디지털 화폐 구축을 위한 기술적 인프라 문제

비록 현재 국내에서 전자거래의 비중이 크고 현금결제가 빠르게 전자 거래로 대체되고 있지만, 중앙은행이 발행하는 디지털 화폐를 전면적으로 도입했을 때, 전자 결제에 익숙하지 않는 기관들에게 어떻게 기술적 인프라를 공급할 수 있을 것인가의 문제 또한 고려할 필요가 있다.

현재 현금 시스템이 가지고 있는 가장 큰 장점은 어디서나 즉시 거래가 가능하다는 편의성이다. 현금을 보유하고 있으면 돈을 주는 주체나 받는 주체 모두 추가적인 장치나 절차 없이 바로 거래가 성사되는 편의성과 즉시성이 현금 거래의 가장 큰 장점이다. 현재 신용카드, 각종 페이 등으로 대표되는 전자거래는 돈 그 자체가 아니라 돈의 역할을 대신하는 지급결제 수단을 수용하는 것이기 때문에 신용카드나 다른 지급결제 서비스의 수용 여부는 개인의 선택이며 이를 강제할 수 없다. 하지만 중앙은행이 발행하는 전자화폐는 100% 화폐의 역할을 해야 하기 때문에 모든 사람들이 현금으로 거래를 하는 데에 전혀 문제가 없듯이, 지금의 현금 거래처럼 혹은 현금 거래에 준하는 편의성을 제공해야 전자화폐에 대한 활용도가 높아질 수 있을 것이다.

마. 결론

현재 블록체인 시스템은 디지털 통화 시스템을 구현할 수 있는 안정성, 투명성, 익명성 등의 장점을 가지고 있지만 거래 규모, 확장성 등의 블록체인 자체의 문제와 디지털 화폐의 도입 방안 및 인프라와 같은 외부적인 문제가 존재한다. 그러나, 블록체인은 디지털 화폐 인프라를 구현할 수 있는 가능성 있는 기술로 인정받고 있으며, 현재도 혁신성 있는 기술로서 계속 연구가 진행되고 있고 빠른 속도로 발전해나가고 있다. 디지털 화폐의 플랫폼으로서 블록체인에 대한 지속적인 연구와 함께 '동전 없는 사회'의 전자 지갑 도입 및 이를 위한 플랫폼 연구 등을 점진적으로 추진해 나감으로써 블록체인을

통해 현금 없는 사회를 정착하기 위해 노력해야 할 것이다.

제2부 참고문헌

한국은행 금융결제국, 신한은금융망(BOK-Wire+) 구조 해설, 2009

한국은행, 2015년도 지급결제보고서, 2016

Antonopoulous, M, Andreas, “비트코인, 블록체인과 금융의 혁신“ (Mastering Bitcoin), 고려대학교 출판문화원, 2015

Citibank, Digital Disruption: How fintech is forcing banking to a tipping point, 2016

Coindesk, Banks and the blockchain report, 2015

Danezis, George and Meiklejohn, Sarah, Centrally Banked Cryptocurrencies, 2016

Deloitte, Blockchain: Enigma, Paradox, Opportunity, 2016

Finector, 블록체인 발전 과정과 이해, 2016

Finector, 금융기관을 위한 블록체인의 이해, 2016

IMF, Virtual Currencies and Beyond: Initial Considerations, 2016

Japan Exchange Group, Applicability of Distributed Ledger Technology to Capital Market Infrastructure, 2016

Moodys, Robust, Cost-effective Applications Key to Unlocking Blockchain’s Potential Credit Benefits, 2016

Nomura Research Institute, Survey on Blockchain Technologies and Related Services, 2015

UK Government Chief Scientific Adviser, Distributed ledger technology: beyond block chain, 2016

World Economic Forum, The future of financial infrastructure, 2016