프라이빗 블록체인 기반 기부금 관리

Donation Management System using Private Blockchain

김 세 환(SYNCO)

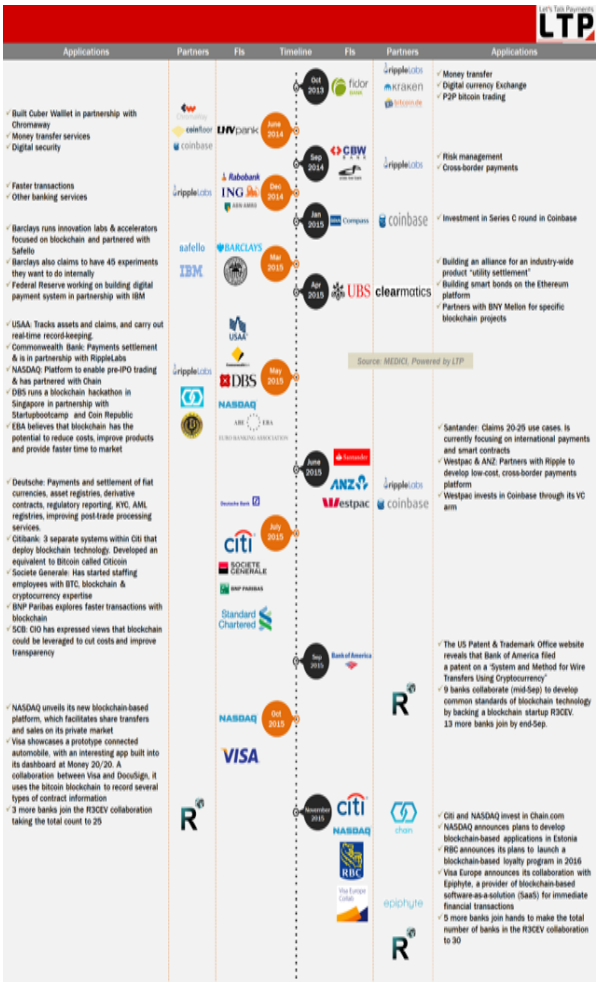
차 례

■ Keyword : Private Blockchain | Multichain | Donation

1. 서론

탈중앙화 구조 하에서도 신뢰 기반이 없는 당사자간 직접 가치 이전을 가능하게 해주는 블록체인 관련 기술들은 금융권 제도권내에서도 활성화시키겠다는 의지들이 공개적으로 확인되고 있다[1]. 은행의 경우를 보면, 그동안 고객들은 신뢰할 수 있는 은행 시스템을 통해 각종 금융 서비스를 수행해왔다. 즉, 은행 시스템이 중앙화된 형태로 고객 간의 자금이체 업무 등을 대행해주는 구조로 다양한 금융 서비스를 제공해온 것이다. 하지만, 블록체인 기술은 이러한 중간 레이어에 은행과 같은 신뢰할 수 있는 시스템 혹은 매개체가 없더라도 당사자 간 직접 자금을 이체할 수 있는 기능들을 제공한다. 근본적으로 중간 유통 구조의 필요성을 없앰으로써 서비스 이용자들은 기존 구조에서 지불해왔던 비용 등을 절감할 수 있고 한발 더 나아가 해당 기술 제공자들은 새로운 사용자 생태계를 제시하면서 사용자들에게 참여에 대한 직접적인 보상을 제공하는 서비스들이 출현하고 있다[2]. 또한, 이러한 현상은 비단 금융뿐만 아니라 전 산업 영역으로 확장 적용되고 있다. 4차 산업혁명의 핵심기술이라고 언급하는 데 이러한 배경이 있으며 기존의 구조와 완전히 다른 구조로 각 영역별로 새로운 유즈케이스들이 활발하게 개발되고 있다[3]. 특히, 블록체인 네트워크를 통해 가치를 이전할 수 있는 점은 금융 영역에 있어 더욱더 기존 금융 서비스 구조를 파괴할 수 있는 가능성이 크다. 따라서, 선진 금융사들의 경우 기존 비즈니스를 방어하려는 모습보다는 적극적으로 블록체인 기술을 도입하여 새로운 구조 하에서 다양한 실험들을 진행하고 있다[4].

본고에서는 프라이빗 블록체인 기술에 대한 기본적인 이해를 돕기 위한 내용들을 소개하고 프라이빗 블록체인



▶▶ 그림 1. 금융권 블록체인 적용 히스토리, 출처: LTP, 2016

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	– Generic blockchain platform	– Modular blockchain platform	– Specialized distrib-uted ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private[4]	– Permissioned, private	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understand-ing of consensus that allows multiple approaches – Transaction level	– Specific understand-ing of consensus (i.e., notary nodes) – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) – Smart legal contract (legal prose)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode	– None

▶▶ 그림 2. 이더리움 vs Fabric vs R3 Corda, 출처 [8]

기술이 왜 도입되었으며, 대표적인 프라이빗 블록체인들의 기술적인 관점에서 비교해보고, 해당 기술을 기부금 관리 시스템에 적용한 예제를 소개함으로써 블록체인 기술 적용의 장·단점 등을 분석한 내용을 제공하고자 한다. 이를 통해 프라이빗 블록체인 기술을 활용한 서비스를 구축하거나 분석하는데 도움을 줄 것으로 기대한다.

본고의 구성은 다음과 같다. 1장에서 블록체인 기술의 기본 개념 및 적용현황 등에 대하여 살펴보았다. 2장에서 프라이빗 블록체인의 종류와 기술적 특징들에 대해 소개한다. 이어 3장에서 Multichain이라고 하는 오픈소스 프라이빗 블록체인에 대해 소개한다. 4장에서 프라이빗 블록체인 기술을 적용하여 구축한 기부금 관리 시스템 구축내용에 대해 소개하고, 5장에서 결론을 맺는다.

2. 프라이빗 블록체인

본고에서는 대표적인 프라이빗 블록체인인 R3 CEV[5] 콘소시엄의 Corda와 Hyperledger 프로젝트의 Fabric[6]에 대해 살펴보겠다. 2014년 글로벌 금융기관들과 R3 블록체인 스타트업에 의해 설립된 R3 CEV 콘소시엄은 2016년 12월 Corda라는 블록체인 솔루션을 오픈소스로 릴리즈하였다[7]. Corda의 경우 초기부터 금융권에 최적화된 블록체인 개발을 목표로 설정하여 공개 블록체인의 데이터 프라이버시 이슈, 스마트 컨트랙 증명 강화 기능들을 초기부터 탑재하여 개발하였고 글로벌 금융기관들 사이의 공유 원장을 토대로 한 기존 업무의 자동화 및 중복 원장 제거 등을 목표로 몇 가지 PoC 프로젝트들을 진행하고 그 결과들을 회원사 중심으로 공유하는 형태로 진행하여왔다. 2015년 12월 리눅스 재단에 의해 설립된 Hyperledger 프로젝트는 Corda와는 달리 범산업적으로 적용 가능한 프라이빗 블록체인 솔루션 개발을 목표로 시작되었다. v0.6까지는 전체 원장이 공유되는 모델이었으나 v1.0부터는 channel 개념을 도입하여 프라이버시 이슈를 해결하였다. 그림2에서 대표적인 퍼블릭 블록체인인 이더리움과 Fabric, Corda의 기술적 유사성 및 차이점을 정리하였다[8]. 공통적으로 스마트 컨트랙을 지원한다는 점 이외에 유사한 점은 찾기 힘들다는 걸 알수 있다.

3. Multichain

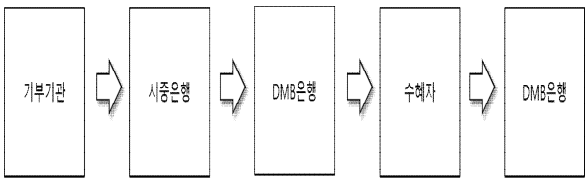
Coin Science Ltd.사에서 오픈소스로 제공하는 multichain[9]은 bitcoin이 가진 기술적 제약사항으로 인해 기관내 혹은 기관간 적용하기 어려운 점을 극복하기 위해 제안된 프라이빗 블록체인 플랫폼이다.

PoW[10]방식의 mining 대신 miner를 지정하고, mining diversity 파라미터 조정을 통해 세부적으로 block producing을 제어할 수 있다. 따라서, 거래는 전

송 즉시 완결되며 하드포크가 발생하지 않는다. 또한, 네트워크에 대한 접속 및 거래 전송 등도 권한 부여를 통해서만 가능하도록 설계되었다. 임의의 key, value를 네트워크상에 저장/조회가 가능하여 account 기반의 처리도 가능하다.

CoinSpark에서 제안하는 tokenization 프로토콜[11]을 기반으로하여 별도의 디지털 자산을 발행 및 전송할 수 있는 기능을 내재하여 기부금 관리 및 기타 다른 목적으로 신규 가상 에셋을 관리하기 용이한 측면이 있고, 이렇게 발행된 커스텀 자산 간의 atomic swap을 지원하는 점은 눈여겨 볼 부분이다. 그 외, command-line이나 API 등의 인터페이스는 bitcoin core와 호환성을 유지하고 있으며, bitcoin protocol 및 트랜잭션 포맷 및 블록체인 구조는 기본적으로 bitcoin 기반으로 한다.

하지만, 네트워크 접속 제한을 통한 프라이버시 해법 외 Fabric이나 Corda처럼 권한있는 접속자간에도 데이터 프라이버시를 해결할 수 있는 방법을 제공하고 있진 않다[12,13].



▶▶ 그림 3. 기금 관리 플로우

4. Multichain 기반 기부금 관리

본고에서는 국내 모 은행에서 개인 혹은 각 단체들로부터 수령한 기부금을 신용대출 등이 어려운 자영업자 혹은 단체에게 제공하는 사업을 수행하는 데 있어 앞서 언급한 multichain 플랫폼을 적용한 내용을 기술한다. 기대효과 측면에서 보면, 블록체인 기술 적용을 통해 기부금 관리 내역에 대한 투명성/위·변조 방지를 보장할 수 있고, 기부금 관리에 기부자, 기부사업자, 수혜자의 직접 참여가 가능하고 기부 사업자 입장에서도 효율적인 기부금 관리 업무가 가능하다라는 장점이 기획되었다.

4.1 기부금 관리 플로우

기부금을 수령하여 이를 필요로 하는 개인/단체를 대상으로 운용하는 은행을 편의상 DMB(Donation Management Bank)라 칭하겠다. 전체 구조를 이해하기 위해 우선 기부금 관리 업무 플로우를 이해할 필요가 있는데 개략적으로 기술하면 다음과 같다.

- 기금 수령: 기관 혹은 개인들로부터 기부금을 수령한다. 현재 오프라인 기반으로 진행되고 있으며 본 시스템에서는 온라인으로 시중 은행과 연계하여 은행으로부터 기금 생성 내역을 전송받아 처리하는 방안으로 설계하였다.
- 기금 실행: 신용 등급 등이 낮아 일반 대출이 어려운 영세 사업자 혹은 단체 등에 자금 집행을 통해 지원하되 전액 무상으로 제공하는 것이 아니라 수혜대상이 일정 기간 자금 사용 이후 일정 비율의 자금 사용에 대한 이자 및 원금 등을 단계적으로 상환하는 구조로 집행한다. 다만, 수혜 대상에게 이자/원금 상환에 대한 법적 책임을 묻진 않는다. 이 프로세스는 기부금 관리 업무에서만 독립적으로 진행되진 않고 별도의 대출 관련 처리 업무 Legacy 시스템과 연계하여 처리된다. 그림3과 같은 단계를 거쳐 기금을 관리한다.

4.2 시스템 구성

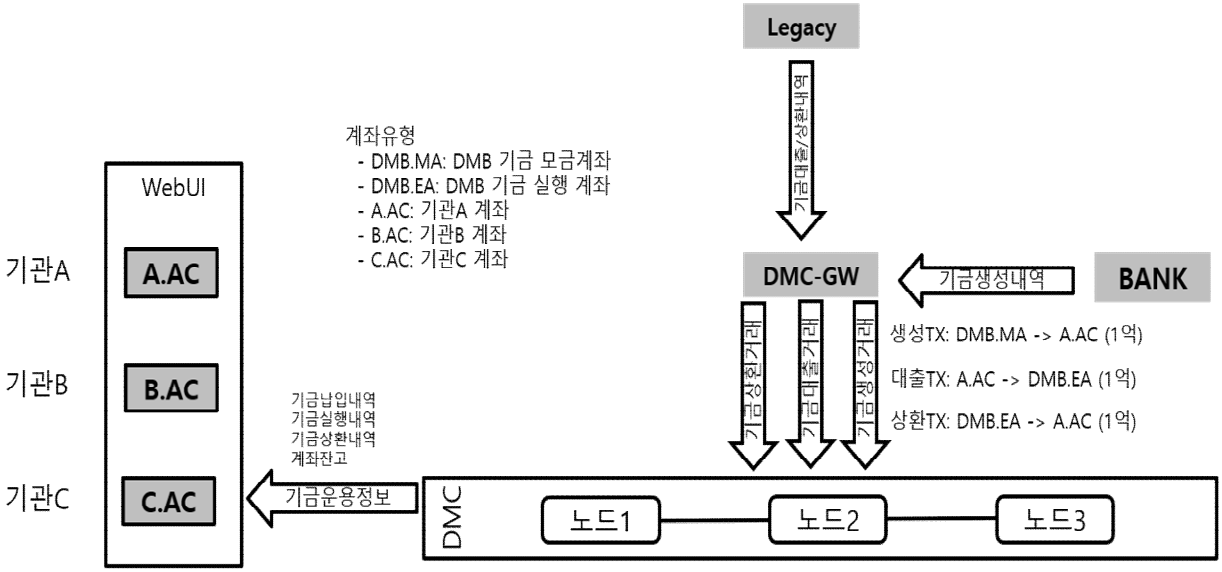
상기의 기부금 관리 업무를 수행하기 위해 그림4와 같이 본 시스템을 크게 3개의 모듈로 나눠 구성하였다.

1) Web UI (기관 등 기부자 인터페이스)

기부금을 전달한 기관 및 개인은 Web UI를 통해 기금 납입 내역, 실행 내역, 상환 내역 등을 조회할 수 있다. 본 프로젝트에서는 Web UI를 통한 직접적인 기금 납입은 불가하도록 1차 설계되었지만, 암호 화폐를 기반으로 한 직접 납입 및 납입된 암호 화폐의 법정 화폐 교환 기능 등을 내장하는 것을 전제로 추후에 Web UI를 통한 직접 납입도 가능하리라 본다.

2) DMC (Donation Management Chain)

기금 생성 내역, 기금 실행 내역, 기금 상환 내역 등이 모두 기록되는 multichain mainet이다. 3개의 노드로 구성하였으며 3개 노드가 모두 마이닝 권한을 가지며 Round-robin 형태로 마이닝하도록 파라미터를 설정하였다. 기금 관리를 위한 별도의 계정 등을 key-value store로 활용할 수 있도록 multichain에서 제공하는 stream 기능을 이용하여 구현하였는데, 기금 모금 계좌



▶▶ 그림 4. 기부금 관리 시스템 구성

와 실행 계좌 그리고 각 기부 단체별 별도의 계좌를 정의하였다. 기금 생성 거래가 DMC 네트워크에 전달된 경우, 기금 모금 계좌에서 기금 토큰을 기관 계좌에 이체하는 형태로 mainnet에서 처리하였다. 기금이 실행된 경우엔 기관 계좌에서 실행된 자금이 DMB 실행 계좌에 자금을 전송하는 거래로 처리하였고, 상환의 경우 DMB 실행계좌에서 기관 계좌로 상환 금액을 이체하는 형태로 처리하였다. 즉, 상환의 경우엔 DMB가 상환 대행을 하는 구조로 기금 관리가 설계된 것을 알 수 있다. 이 부분도, Web UI를 통해 추후 기금 수혜자가 직접 상환을 하도록 설계 변경이 가능하다고 보고 있으나 자금 사정이 어려운 입장에서 DMB측에서 대행해주는 기존의 업무 프로세스를 유지하고자 하여 반영하지 않고 대행하는 구조로 시스템을 설계하였다.

3) DMC-GW

앞서 언급한 바와 같이 기금의 생성, 대출, 상환 거래 등은 모두 실제 법정화폐 기반으로 진행되며 본 시스템과 연결된 시중은행의 계좌에 실제로 자금이 이체된 경우 이 내역을 반영하는 형태로 진행된다. 따라서, DMC-GW 모듈에서 각각의 자금 이체 내역을 등록된 시중은행 계좌와의 연계를 통해 실제 자금 이체 내역과 DMC 메인넷 거래 내역을 동기화시켜줄 필요가 있다. 또한, 기금이 무상으로 제공되지 않고 대출/상환의 전통적인 대출 업무의 형태로 기금 관리가 운용되어야 한다는 업무 요건으로 인해 해당 처리 내역을 기존의 Legacy 시스템과 연동하는 기능을 DMC-GW 모듈에서 담당하도록 설계하였다. Legacy 연동 내역은 API 연동하도록 구성하였으며 증빙 자료 등은 블록체인 상에 보관가능하나 파일의 크기 제한이 있다[14]. 이 부분도 multichain의 초기 파라미터 설정 시 고려하여 반영하였으며 이 부분은 genesis block 생성시점에 반영되고 변경될 수 없다. 또한, 전체 블록크기와도 관련성이 있어 면밀하게 검토하여 제약사항 등을 사전에 설정하고 진행할 필요가 있다.

5. 결론

본고에서는 multichain 프라이빗 블록체인을 활용하여 기부자, 기부 관리 대행 기관, 수혜자 사이의 기부금 관련 모금, 집행, 상환 등의 관리 업무에 적용함으로써 투명하고, 보안성이 높으며, 직접 참가를 기반으로 한 효율적인 기부금 관리 기능을 제공하고자 진행한 프로젝트의 결과를 요약하였다.

구축결과 시사점은 다음과 같이 정리해보겠다.

- 블록체인 적용 타당성: 블록체인 기술을 적용하여 기존의 central 방식으로 구축한 경우 대비 그 기대효과가 명확하지 않은 경우는 기존 구축방식을 적용하는 것이 좋다는 점을 고려해볼 필요가 있다[15].
- 기존 시스템 연동: 블록체인을 적용하여 구축한 업

무가 독립적으로 수행되는 경우는 드물며 원장 수준에서의 공유가 어려운 관계로 API 연동 및 데이터 연계 방안에 대한 설계 고려가 필요하다.

- 최소 업무 요건 만족 플랫폼 선정: 블록체인 플랫폼의 종류는 매우 다양하며 업무 요건을 만족하는데 충분한 수준인지에 대한 사전 검토가 진행될 필요가 있다.
- 플랫폼 파라미터 최적화: 프라이빗 블록체인의 경우 접속 권한 설정, 마이닝 권한 설정 등 퍼블릭 블록체인 대비 별도의 구성 관리가 필요하고, 또한 성능 측면에서 사전에 설계된 업무 요건 등을 감안하여 별도의 플랫폼 Sizing이 필요하며 이는 기존 시스템의 물리적인 성능 Sizing과는 완전히 별개의 플랫폼 엔지니어링을 바탕으로 진행되어야 하며 만족할만한 성능을 내기 위한 구성은 많은 성능 테스트를 요구한다.
- 사용자 인터페이스: 기부자, 기관 등 기금 관리 시스템에 대한 각 사용자별 인터페이스는 기존 웹 방식 인터페이스로 유지함으로써 백엔드에 블록체인 네트워크가 존재하는지 여부를 숨기는 것은 사용자 입장에서 익숙한 UI를 통한 친숙한 접근성을 제공할 필요가 있다.

- 히스토리 내역 실시간 조회 제약사항: 블록체인 네트워크를 통해 반영된 거래의 경우 실시간 대응이 미흡한 측면은 사용자에게 다소 불만족스러운 성능 경험치를 제공할 수도 있다. 이는 multichain이 bitcoin의 UTXO[16] 모델을 기반으로 각각의 거래가 논리적으로 연결된 구조이기 때문이다. 따라서, 이러한 부분을 보완하기 위해 본 프로젝트에서의 히스토리 조회에 대한 부분은 Web 서버단에서 별도의 히스토리 내역 조회 기능을 기존 RDB에 구축하여 보여주고, 이 내역에 대한 동기화는 별도로 블록체인 네트워크와 진행하는 형태로 시스템을 구축하였으며 이는 히스토리성 데이터의 실시간 조회요건이 필요한 업무의 경우 재고해봐야하는 측면이라고 생각한다.

상기와 같은 시사점을 통하여 프라이빗 블록체인을 적용하여 특정 업무를 구현하는 경우 시스템 설계시 혹은 관리, 성능 측면에서 고려사항들을 정리해보게 되었고, 향후 유사한 서비스를 구축할 경우 도움이 될 수 있기를 기대한다.

참고문헌

[1] http://blockchainnews.co.kr/news/view.php?idx=1145&mcode=m78v9sh
[2] STEEM, https://steemit.com/
[3] https://www.weforum.org/communities/the-future-of-blockchain
[4] https://gomedici.com/an-overview-of-blockchain-technology/
[5] R3 CEV, https://www.r3.com/
[6] Hyperleder, https://www.hyperledger.org/
[7] R3 Corda, https://github.com/corda/corda
[8] https://www.experfy.com/blog/comparison-of-ethereum-hyperledger-fabric-and-corda
[9] MULTICHAIN, https://www.multichain.com/
[10] Proof of Work, https://en.bitcoin.it/wiki/Proof_of_work
[11] Colored Coins, https://en.bitcoin.it/wiki/Colored_Coins
[12] Fabric Channels, http://hyperledger-fabric.readthedocs.io/en/release-1.0/channels.html
[13] R3 Corda Security Model, https://docs.corda.net/releases/release-M8.2/key-concepts-security-model.html
[14] multichain documentation, https://www.multichain.com/developers/
[15] https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/
[16] UTXO, https://en.wikipedia.org/wiki/Unspent_transaction_output

저 자 소 개

● 김 세 환(Se Hwan Kim)

- 1997년 8월 : KAIST 전산학과 학사
- 2004년 2월 : 서울대학교 컴퓨터공학과 석사
- 2003년 4월 ~ 2014년 3월 : ㈜ TmaxSoft/Core, S-Core, 실장
- 2014년 4월 ~ 2018년 2월 : ㈜ WebCashInnovalue, BankwareGlobal, 상무이사
- 2018년 3월 ~ 현재 : ㈜ SYNCO, CTO

<관심분야> : 블록체인, DB암호화, 운영체제, 모바일 플랫폼, 코어뱅킹시스템