Pegged Blockchain : Stablecoin

Index

- 1. Introduction
- 2. Stablecoin
 - Tether
 - KRWb
 - DAI
- 3. Benefits
- 4. Issues
- 5. Conclusion

Introduction

• 페깅(pegged blockchain)

: 암호화폐의 가격을 마치 못을 박아 놓은 듯이 <mark>특정 가치에 고정</mark>시키는 것

• 스테이블코인(stablecoin)

: 페깅을 통해서 코인의 가격을 변동없이 안정된 암호화폐

페깅 담보 종류

1. 법정화폐 담보(fiat-collateraliteralized) Ex. Tether (1USDt = 1\$), KRWb (1KRWb = 1₩)

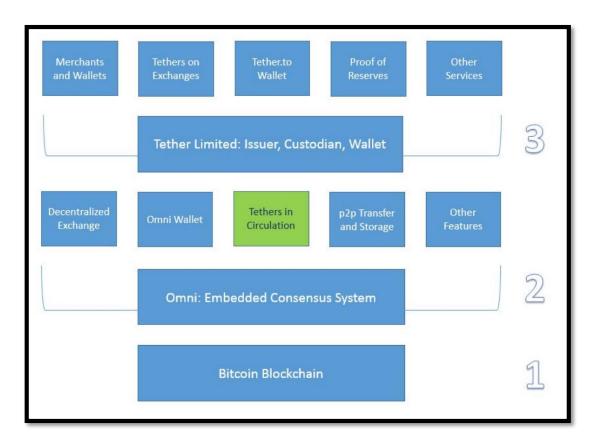
2. 암호화폐 담보(crypto-collateraliteralized) Ex. DAI (1DAI = 1\$)

Tether - Summary

- 테더(Tether) 🕞
 - : 법정화폐(USD)를 디지털 방식으로 쉽게 사용할 수 있도록 설계된 블록체인 플랫폼. 법정화폐(USD)와 일대일 비율로 예치 현재 두 개의 서로 다른 전송 프로토콜을 사용(Bitcoin, Ethereum). Omni => ERC-20 전환 추세
- Bitcoin Blockchain: Omni Protocol
 => 비트코인 네트워크 사용으로 인한 안정성 및 보안성
- Ethereum Blockchain: ERC-20 => Smart Contract와 dApp 내 테더 사용 가능. 즉, 테더는 ERC-20 토큰이므로 모든 Ethereum 주소로 보낼 수 있음.
- 총 발행량: 약 46억 USDt(Omni: 1,555,000.000 USDT, ETH: 2,298,568,033 USDT) (2020년 1월 29일 기준)[1] 시가 총액: 4,655,275,827 USD (2020년 1월 29일 기준)[2]

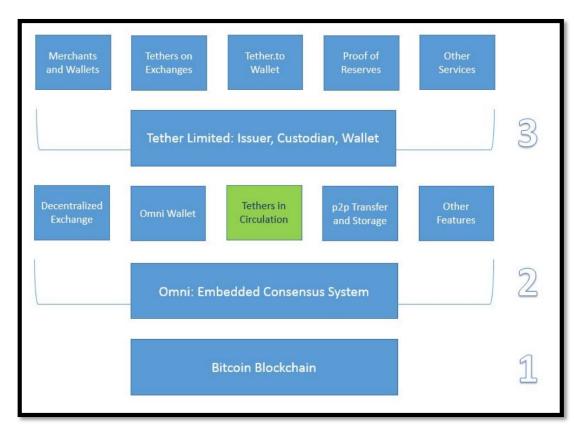
^[1] 총 발행량: Omni: https://omniexplorer.info/asset/31 ETH: https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7 [2] 시가 총액: https://coinmarketsum.com/ko/currencies/tether/

- - 1. Bitcoin Blockchain
 - 1) 비트코인 블록체인 위에서 발급
 - 2) Transactional ledger는 블록체인 메타 데이터로 저장
 - 2. Omni Layer Protocol
 - 1) 테더 발급 및 소거
 - 2) 테더 순환 기록 추적 및 보고[3]
 - 3) 사용자의 테더 및 기타 자산 처리 및 저장
 - p2p, cryptographically secure environment
 - Omni Wallet; open-source, encrypted web-wallet
 - multi-signature & offline cold storage-supporting system



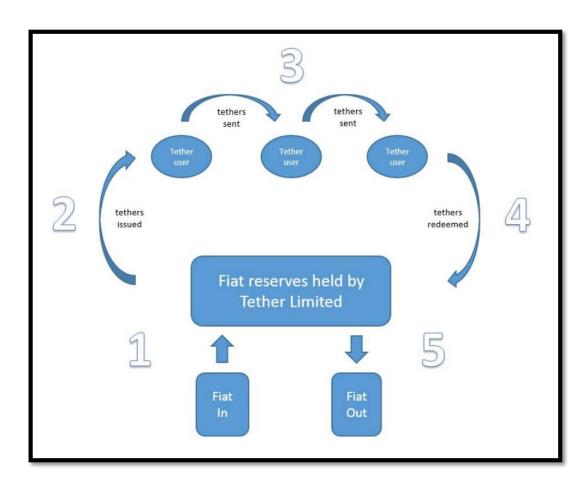
[그림 1] Tether Technology Stack

- - 3. Tether Limited
 - 1) 예치금 수령 후, 이에 상응하는 테더 발행 Grant
 - 2) 법정화폐 인출 시, 이에 상응하는 테더 소각 Revoke
 - 3) 유통 중인 모든 테더의 환전 예치금 보관 Custody
 - 4) Proof of Reserves(PoR)과 감사 결과 보고 Report
 - 5) 기존 블록체인/비트코인 지갑, 거래소, Manage 블록체인 기업과의 통합 시작 및 관리
 - 6) 테더 전송, 수신, 저장, 변환 가능한 Web Wallet 제공



[그림 1] Tether Technology Stack

- Flow of Funds Process
 - 1. Tether Limited 은행 계좌로 법정화폐(USD) 예금
 - 2. 테더 계정 생성 이후, 예금된 양과 동일한 테더 발급
 - 3. Bitcoin 기반 플랫폼을 통해 테더 거래, 전송, 교환, 저장
 - 4. Tether Limited를 통해 테더를 법정화폐로 환급요청
 - 5. 환급된 테더는 소각 이후, 은행 계좌로 법정화폐 보냄



[그림 2] Tether flow of funds process

• Proof of Reserves(PoR)

Proof of Solvency, Real-Time Transparency...

- 테더의 전체 통화량 = Tether Limited 은행에 예치된 달러 총액 (1USDt = 1USD, 일대일 대응)

- 은행 잔고를 알리고 정기적인 감사실시를 통해은행 내 예치 금액 증명
- TUSD: 현재 순환 중인 총 테더 수

TUSDissue: Omniexplorer.info 내 테더 ID에 따라 발급된 총 테더 수

TUSDredeem: Omniexplorer.info 내 테더 ID에 따라 상환된 총 테더 수

TUSD = TUSDissue - TUSDredeem

- DUSD: Tether Limited 은행 계좌의 달러 잔액

DUSDdepo: Tether Limited 은행 계좌에 입금된 총 금액

DUSDwithd: Tether Limited 은행 계좌에서 인출된 총 금액

DUSD = DUSDdepo - DUSDwithd

TUSD = "Total Property
Tokens" for asset ID #31 at
Omnichest.info

DUSD = Daily Bank Account
Balance

TUSD <= DUSD
All Tethers Are Fully
Reserved

[그림 3] Tether Transparency Page

The Solvency Equation for Tether System
TUSD ≤ DUSD

KRWb - Summary

• KRWb(Korean Won on the Blockchain) w

: 법정화폐(KRW)인 원화 증거금 기반으로 발행된 전자증표(토큰). 원화 법정통화와 일대일 비율로 예치. 이더리움 전송 프로토콜 사용

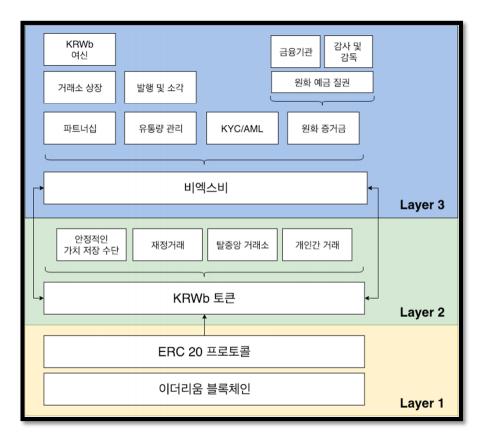
Ethereum Blockchain: ERC-20
 Smart Contract와 dApp 내 테더 사용 가능. 즉, 테더는 ERC-20 토큰이므로 모든 Ethereum 주소로 보낼 수 있음.

- 거래 내역 및 발행 총량은 공개 분산 장부상에서 검증 가능
- 총 발행량: 16,860,432.45 KRWb (2020년 1월 20일 기준)[4] 원화 증거금 잔액: 16,860,433 KRW (2020년 1월 20일 기준)[4]

^[4] KRWb attestation reports(Jan 20th, 2020): https://krwb.io/static/20200120-Attestation-Report.pdf

KRWb - Features

- Technology Stack
 - 1. Ethereum Blockchain Smart Contract
 - 1) 이더리움 블록체인 위에서 발급
 - 2) ERC-20 기반 스마트 컨트랙트
 - 2. KRWb token **Applications**
 - 1) 스마트 컨트랙트를 통해 보관
 - 2) 지갑 보유중인 당사자들 교환 가능
 - 3) 재정거래(arbitrage) 활용 가능
 - 3. BxB Services
 - 1) KRWb 발행 및 소각
 - 2) 거래소 상장
 - 3) 원화 증거금 관리



[그림 4] KRWb Architecture

KRWb - Features

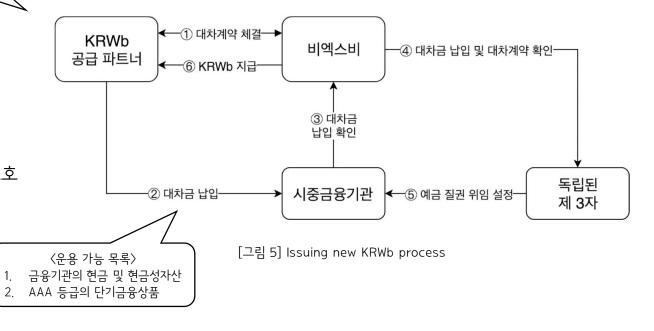
- Process KRWb 신규 발행
 - ① 0% 금리의 대차계약 체결
 - ② BxB 지정 국내 금융기관에 대차금 입금
 - ③ 대차계약에 명시된 원화 대여금 입금 확인
 - ④ 대차계약관련 정보를 제 3자에게 알림
 - ⑤ 제 3자는 공급 파트너의 질권 권한 위임 받아 자산 보호

BxB와 특수 관계가 없는 자.

공급 파트너 수: 99인 미만 (사모 채권 발행 규정)

⑥ 일대일 비율로 KRWb 토큰 지급

- ❖ ICO^[5]를 통해서 자금을 공모하지 않고, 오직 <mark>공급 파트너와 대차계약</mark>을 통해 신규 발행 공급 파트너가 암호화 화폐 거래소, OTC^[6] 등을 통해 시장에 유통
- ❖ 질권이 해지되지 않는 한, 해당 예금이 BxB에 의하여 이동되거나 사용될 수 없으며, 지정된 외부 감사가 해당 계좌의 잔액이 대차계약으로 결정된 금액과 일치여부를 확인함

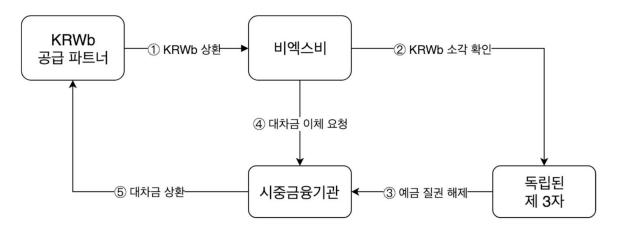


^[5] ICO(Initial Coin Offering): 신규 코인 발행. 프로젝트 자금 유치를 위해 토큰이 출시되지 않은 상태에서 선판매 [6] OTC(Over-The-Counter): 장외거래. 거래소를 거치지 않고 당사자 간 직접 거래

KRWb - Features

- Process KRWb 원화 교환
 - ① 대차계약 동일 금액의 KRWb 상환
 - ② 반환 받은 KRWb 소각 후, 대차계약내용 제 3자에게 알림 제 3자는 블록체인 상에 KRWb의 반환 및 소각을 확인
 - ③ 제 3자의 대차금액에 대한 예치금 질권 설정 해제
 - ④ 대차금 반환 사유로 원화 예금에 대한 출금/이체 요청
 - ⑤ 반환된 KRWb에 해당한 원화를 상환

- ❖ KRWb의 단순 소유는 원화 반환 요청에 대한 권리를 가지지 않음
- ❖ 계약 금액보다 많은 양을 상환할 경우, 타 파트너의 대차계약 양도 후 상환 진행 가능
- ❖ KRWb를 교환하는데 있어 ERC-20 스마트 컨트랙트를 사용 => 가스(gas) 발생



[그림 6] Redeeming fiat KRW with KRWb process

DAI - Summary

• DAI(or Daicoin) 🔷



: 암호화폐인 Ethereum을 기반으로 발행된 스테이블코인. USD와 일대일 비율로 예치 Maker 사용(MakerDAO의의 Smart Contract)

Maker platform

=> 부채 담보부 포지션(CDP) 등을 통한 DAI 가치를 안정시키는 이더리움 상의 스마트 컨트랙트 플랫폼

- 총 발행량: 56,200,391 DAI (2020년 1월 29일 기준)[8]

시가 총액: 103,233,404 USD (2020년 1월 29일 기준)[8]

^[7] DAO, Decentralized Autonomous Organization: 분산 자치 조직

^[8] 총 발행량 및 시가 총액: https://etherscan.io/token/0x6b175474e89094c44da98b954eedeac495271d0f