테더

백서 번역본

Tether

https://tether.to

본 번역본은 가상자산 투자자들을 위한 참고용입니다. 본 번역본은 투자 권유를 목적으로 만들어지지 않았으며 원문을 단순히 번역한 것으로, 내용의 정확성은 원문 작성 주체에 달려 있으며 크립토닷컴 코리아는 투자 결과에 대하여 어떠한 책임도 지지 않습니다. 본 번역본의 내용에 대한 자세한 문의는 백서 원문을 참고하시길 바랍니다.

개요

디지털 통화는 법정 통화로 지원되며, 개인과 조직에게 익숙한 회계 단위를 사용하면서 가치 교환을 위한 강력하고 분산된 방법을 제공합니다. 블록체인의 혁신은 감사 가능하고 암호화된 보안 글로벌 원장입니다. 자산 기반 토큰 발행자와 기타 시장 참가자들은 블록체인 기술과 내장된 합의 시스템을 활용하여 익숙하고 변동성이 적은 통화와 자산으로 거래할 수 있습니다. 책임성을 유지하고 거래 가격의 안정성을 보장하기 위해, 우리는 암호화폐 토큰(테더라고 불리는)과 그것에 연계된 현실 세계의 자산(법정 통화) 간에 1:1 비율을 유지하는 방법을 제안합니다. 이 방법은 비트코인 블록체인, 자산 보유 증명(Proof of Reserves) 및 기타 감사 방법을 사용하여 발행된 토큰이 항상 완전히 지원되고 예치되어 있음을 증명합니다.

서론

세계에는 사람들이 가치 저장, 거래 매체, 또는 투자 수단으로 자유롭게 선택하는 다양한 자산들이 존재합니다. 우리는 비트코인 블록체인이 이러한 자산을 거래하고 저장하며 회계 처리하는 데 더 나은 기술이라고 믿습니다. 대부분의 추정에 따르면, 전 세계의 자산 가치는 약 250조 달러로 측정되며, 그 중 많은 부분이 은행이나 유사한 금융 기관에 보관되어 있습니다. 이러한 자산들이 비트코인 블록체인으로 이동하는 것은 비례적으로 큰 기회를 의미합니다.

비트코인은 “신뢰가 아닌 암호학적 증거를 기반으로 한 전자 결제 시스템으로, 신뢰할 수 있는 제3자의 개입 없이 두 당사자가 직접 거래할 수 있게 하는 것”으로 만들어졌습니다. 비트코인은 새로운 종류의 디지털 통화, 즉 분산형 디지털 통화 또는 암호화폐를 창조했습니다.

암호화폐의 주요 장점 중 일부는 낮은 거래 비용, 국제적인 국경 없는 전송 및 변환성, 신뢰 없는 소유 및 교환, 의사 익명성, 실시간 투명성, 그리고 기존 은행 시스템 문제로부터의 면역입니다. 현재 암호화폐의 주류 사용이 제한적인 이유로는 변동성이 큰 가격, 기술에 대한 대중의 이해 부족, 그리고 비전문 사용자에게 불편한 사용 용이성 등이 있습니다.

자산 기반 암호화폐에 대한 아이디어는 2012년 1월 J.R. Willett이 작성한 Mastercoin 백서에 의해 비트코인 커뮤니티에서 처음으로 대중화되었습니다 [4]. 오늘날, 우리는 BitAssets, Ripple, Omni, Nxt, NuShares/Bits 등과 같은 프로젝트를 통해 이러한 아이디어가 실현되는 것을 보기 시작했습니다. 모든 비트코인 거래소와 지갑(예: Coinbase, Bitfinex, Coinapult)에서는 사용자가 특정 암호화폐의 변동성(또는 다른 특성)을 피하기 위해 법정 통화, 금 또는 다른 자산으로 판매할 수 있는 유사한 서비스를 이미 제공하고 있습니다. 또한, 법정 가치(또는 다른 자산)를 보유할 수 있는 거의 모든 기존 금융 기관 및 결제 제공업체도 유사한 서비스를 제공합니다. 이 백서에서는 법정 가치가 오픈 소스 소프트웨어, 암호화로 보안된 소프트웨어, 그리고 분산 원장 기술을 사용하는 소프트웨어로 저장되고 전송되는 응용 프로그램에 중점을 둡니다. 즉, 진정한 암호화폐를 다룹니다.

어떤 성공적인 암호화폐의 목표는 신뢰의 필요성을 완전히 제거하는 것이지만, 앞서 언급한 각 구현 방식은 신뢰할 수 있는 제3자에게 의존하거나 기술적, 시장 기반, 또는 프로세스 기반의 단점과 한계가 있습니다.

우리의 솔루션에서, 법정 통화에 연동된 암호화폐를 “테더(Tether)”라고 부릅니다. 모든 테더는 처음에 비트코인 블록체인 위에서 Omni Layer 프로토콜을 통해 발행되며, 따라서 암호화폐 토큰으로 존재합니다. 발행된 각 테더 단위는 홍콩에 본사를 둔 Tether Limited가 예치한 해당 법정 통화 단위에 대해 1:1 비율(즉, 하나의 Tether USDT는 하나의 미 달러)로 지원됩니다. 테더는 Tether Limited의 서비스 약관에 따라 기본 법정 통화로 교환/환전할 수 있으며, 보유자가 원할 경우 비트코인으로 동등한 현물 가치를 교환할 수도 있습니다. 테더가 발행되면,

비트코인이나 다른 암호화폐와 마찬가지로 전송, 저장, 지출 등이 가능합니다. 예치된 법정 통화는 암호화폐의 특성을 가지게 되며, 그 가격은 법정 통화의 가격에 영구적으로 연동됩니다.

우리의 구현은 다른 법정 통화 연동 암호화폐에 비해 다음과 같은 장점을 가지고 있습니다:

- 테더는 덜 개발되거나 테스트되지 않은 “알트코인” 블록체인이나 중앙 집중식 개인 데이터베이스에서 실행되는 폐쇄 소스 소프트웨어가 아닌 비트코인 블록체인에서 존재합니다.
- 테더는 비트코인과 마찬가지로 P2P, 의사 익명, 분산형, 암호화 보안 환경에서 사용할 수 있습니다.
- 테더는 비트코인이나 다른 암호화폐가 통합되는 것과 동일하게 상인, 거래소, 지갑과 통합될 수 있습니다.
- 테더는 Omni Layer 프로토콜의 특성을 상속받습니다. 이 특성에는 분산형 거래소, 브라우저 기반의 오픈 소스 지갑 암호화, 비트코인 기반의 투명성, 책임성, 다자간 보안 및 보고 기능이 포함됩니다.
- Tether Limited는 Proof of Reserves를 수행하기 위해 간단하면서도 효과적인 접근 방식을 사용하여, 예치 자산의 관리자로서의 상대방 리스크를 크게 줄입니다.
- 테더 발행이나 환전은 가격이나 유동성 제약을 받지 않습니다. 사용자는 원하는 만큼 빠르고 매우 낮은 수수료로 테더를 사고팔 수 있습니다.
- 테더는 시장의 블랙 스완 사건, 유동성 부족 등과 같은 시장 리스크를 겪지 않습니다. 예비 자산이 1:1 비율로 유지되기 때문에 시장의 힘에 의존하지 않습니다.
- 테더의 1:1 지원 구현은 담보 기술이나 파생 전략에 비해 비전문 사용자들이 이해하기 더 쉽습니다.

항상 예치된 법정 통화의 잔액은 유통 중인 테더의 수량과 같거나 그보다 많습니다. 이 간단한 구성은 유통 중인 테더와 예치된 법정 통화 간의 가격 일치를 유지하는 데 근본적인 Proof of Reserves 프로세스를 가장 쉽게 지원합니다. 이 문서에서는 거래소와 지갑 감사(현재 상태에서)는 매우 신뢰할 수 없으며(즉, Proof of Solvency 방법의 결함) 대신 거래소와 지갑이 사용자 자금의 보관을 테더를 통해 우리에게 아웃소싱할 것을 제안합니다.

사용자는 Tether.to(우리의 웹 지갑) 또는 Bitfinex와 같은 지원되는 거래소에서 테더를 구매할 수 있습니다. Bitfinex는 테더를 입출금 방법으로 지원합니다. 사용자는 Ambisafe, Holy Transaction 또는 Omni Wallet과 같은 Omni Layer가 활성화된 지갑을 통해 테더를 거래하고 저장할 수

있습니다. 다른 거래소, 지갑, 상인들도 전통적인 법정 지불 방법을 대체할 수 있는 테더 통합에 대해 우리에게 연락할 것을 권장합니다.

우리의 구현이 완벽하게 분산되어 있지 않다는 점을 인정합니다. Tether Limited는 중앙 집중식으로 예치 자산을 관리해야 하기 때문입니다(비록 유통 중인 테더는 분산형 디지털 통화로 존재하지만). 그러나 우리는 이 구현이 이러한 약점을 제거하고, 새로운 제품과 서비스에 대한 강력한 플랫폼을 구축하며, 비트코인 블록체인의 장기적인 성장과 유용성을 지원하는 미래 혁신의 기반을 마련한다고 믿습니다. 이러한 혁신에는 다음이 포함됩니다:

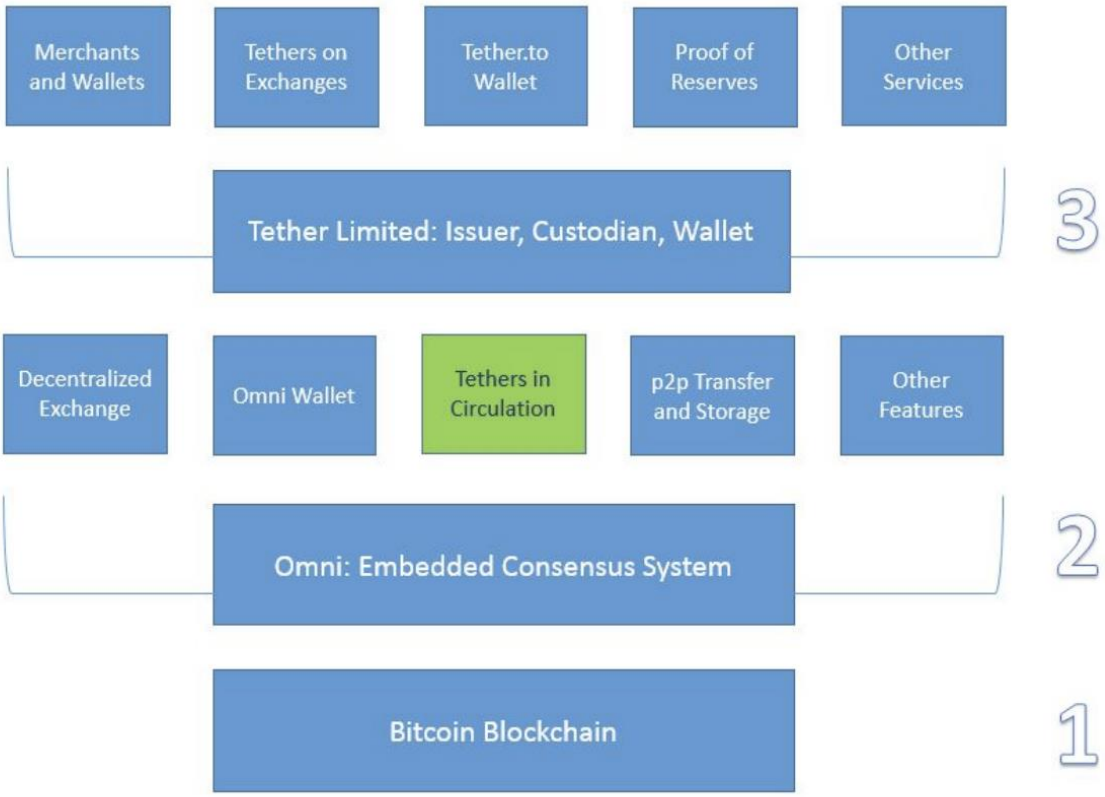
- 사용자와 다른 당사자(다른 사용자 및 상인 포함) 간의 모바일 결제 지원
- 분산된 당사자(예: 여러 거래소) 간의 즉시 또는 거의 즉시 법정 가치 전송
- 일반 보안 프로세스, Proof of Reserves을 더욱 개선하고 새로운 기능을 가능하게 하는 스마트 계약 및 다중 서명 기능 도입

기술 스택 및 프로세스

유통되는 각 테더는 홍콩에 본사를 둔 Tether Limited가 예치한 해당 법정 통화와 1:1 비율로 지원됩니다. 우리가 자산의 관리자로서 신뢰받는 제3자로서 그 자산에 대한 책임을 지고 있습니다. 이러한 리스크는 법정 통화와 암호화폐 감사의 복잡성을 집합적으로 줄이는 간단한 구현을 통해 완화되며, 이러한 감사의 보안성, 증명 가능성, 투명성을 높입니다.

테더 기술 스택

스택은 3개의 레이어와 많은 기능으로 구성되어 있으며, 다이어그램을 통해 가장 잘 이해할 수 있습니다.



각 레이어에 대한 검토는 다음과 같습니다:

1. 첫 번째 레이어는 비트코인 블록체인입니다. 테더 거래 원장은 임베디드 합의 시스템인 Omni를 통해 비트코인 블록체인에 메타데이터로 포함됩니다.

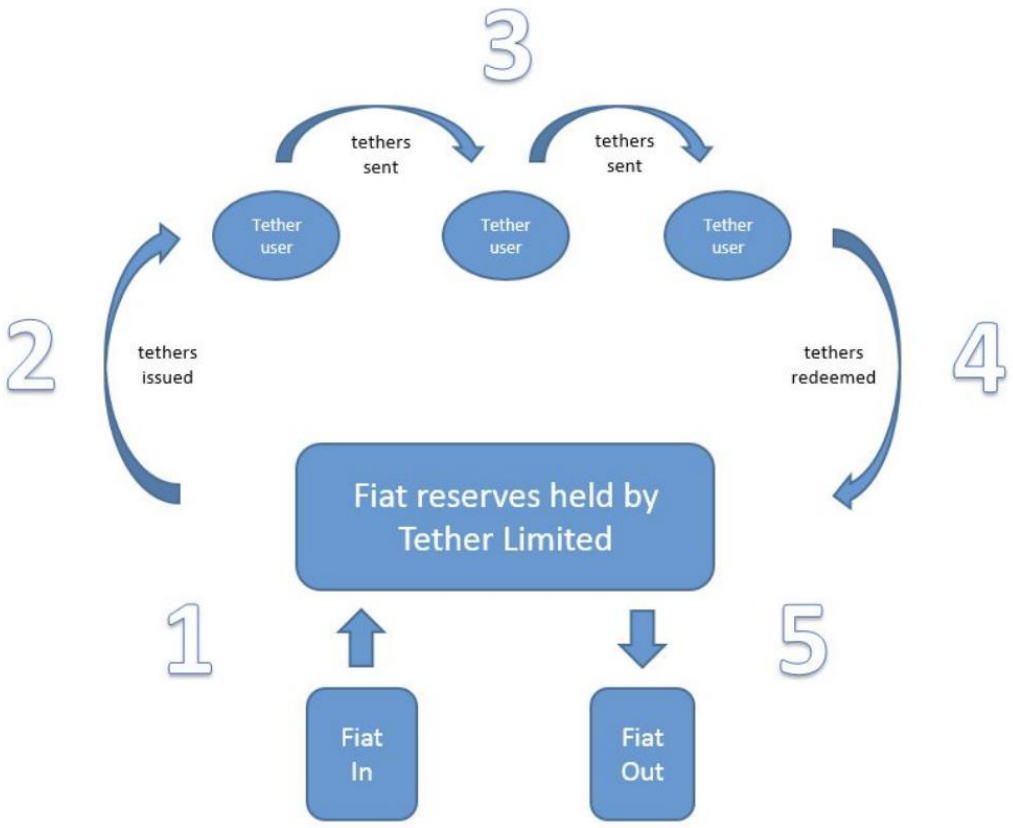
2. 두 번째 레이어는 Omni Layer 프로토콜입니다. Omni는 다음과 같은 기본 기술을 제공합니다:
   a) 비트코인 블록체인에 메타데이터로 표현된 디지털 토큰을 생성(발급)하고 폐기(소멸)할 수 있습니다. 이 경우, 법정 통화에 연동된 디지털 토큰, 즉 테더입니다.
   b) Omnichest.info(예를 들어, Omni 자산 ID #31은 TetherUSD를 나타냄)와 Omnicore API를 통해 테더의 유통을 추적하고 보고할 수 있습니다.
   c) 사용자가 테더 및 기타 자산/토큰을 거래하고 저장할 수 있도록 지원합니다: i) P2P, 의사 익명, 암호화 보안 환경에서. ii) 오픈 소스, 브라우저 기반의 암호화된 웹 지갑: Omni Wallet. iii) 다중 서명 및 오프라인 콜드 스토리지 지원 시스템.

3. 세 번째 레이어는 테더 리미티드(Tether Limited)로, 주로 다음을 담당합니다:
   a) 법정 통화를 수락하고 이에 상응하는 테더를 발급합니다.

b) 법정 통화를 송금하고 이에 상응하는 테더를 회수합니다.
c) 유통 중인 모든 테더를 지원하는 법정 통화의 보관.
d) Proof of Reserves 및 기타 감사 결과를 공개적으로 보고합니다.
e) 기존 비트코인/블록체인 지갑, 거래소, 상인과의 통합을 시작하고 관리합니다.
f) 사용자가 테더를 편리하게 송금, 수신, 저장 및 변환할 수 있는 웹 지갑인 Tether.to를 운영합니다.

자금 흐름 프로세스

테더의 생애 주기에는 다섯 단계가 있으며, 다이어그램을 통해 가장 잘 이해할 수 있습니다



단계 1 – 사용자가 법정 통화를 Tether Limited의 은행 계좌에 입금합니다.

단계 2 – Tether Limited는 사용자의 테더 계좌에 테더를 생성하고 입금합니다. 테더가 유통에 들어갑니다. 사용자가 입금한 법정 통화의 금액 = 사용자에게 발급된 테더의 금액(예: 10,000 USD 입금 = 10,000 테더USD 발급).

단계 3 – 사용자는 테더를 거래합니다. 사용자는 P2P 오픈 소스, 의사 익명, 비트코인 기반 플랫폼을 통해 테더를 전송, 교환 및 저장할 수 있습니다.

단계 4 – 사용자가 테더를 Tether Limited에 예치하여 법정 통화로 환전합니다.

단계 5 – Tether Limited는 테더를 소멸시키고 법정 통화를 사용자의 은행 계좌로 송금합니다.

사용자는 위의 과정 외에도 거래소나 다른 개인을 통해 테더를 얻을 수 있습니다. 테더가 유통에 들어가면 어떤 사업체나 개인 간에 자유롭게 거래할 수 있습니다. 예를 들어, 사용자는 Bitfinex에서 테더를 구매할 수 있으며, 곧 더 많은 거래소가 추가될 예정입니다.

자금 흐름 다이어그램에서 전달하고자 하는 주요 개념은 Tether Limited가 유일하게 테더를 유통에 발행할 수 있고(생성할 수 있으며), 유통에서 제거할 수 있는(소멸시킬 수 있는) 당사자라는 것입니다. 이것이 시스템의 지급 능력이 유지되는 주요 프로세스입니다.

Proof of Reserves 프로세스

지급 능력 증명(Proof of Solvency), 자산 보유 증명(Proof of Reserves), 실시간 투명성(Real-Time Transparency) 및 유사한 용어들은 암호화폐 산업에서 점점 더 주목받고 있습니다.

현재 형태의 거래소 및 지갑 감사는 매우 신뢰할 수 없습니다. 비트코인 생태계에서는 해킹, 관리 부실, 또는 명백한 사기 등으로 인해 여러 차례 지급 불능 사태가 발생했습니다. 사용자들은 거래소를 신중히 선택하고 거래소 사용에 주의해야 합니다. 그럼에도 불구하고, 정통한 사용자라도 위험을 완전히 제거할 수는 없습니다. 게다가, 트레이더와 기업과 같이 거래소에 항상 상당한 법정 통화를 보유해야 하는 사용자들도 있습니다. 금융 용어로 이는 제3자에게 가치를 저장하는 "상대방 위험(counterparty risk)"으로 알려져 있습니다.

현재 형태의 거래소 및 지갑 감사는 신뢰할 수 없다고 결론 내리는 것이 안전하다고 생각합니다. 이러한 프로세스는 관리인이나 거래소가 지급 능력이 있는지 사용자에게 보장하지 않습니다. Merkle 트리 접근 방식[6]과 같은 거래소 감사 프로세스를 개선하기 위한 많은 기여가 있었지만, 여전히 주요 결함이 남아 있습니다.

테더의 Proof of Reserves 구성은 유통 중인 테더의 총 수량(부채)이 항상 예치된 법정 통화의 동일한 양(자산)에 의해 완전히 지원되고 있음을 증명하는 과정을 단순화하기 때문에 독창적입니다. 우리의 구성에서는 유통 중인 각 테더USD가 우리 보유 자산의 1달러를 나타내며(즉, 1:1 비율), 이는 모든 테더의 총합이(어떤 시점에서든) 우리의 USD 보유 잔액과 정확히 일치할 때 시스템이 완전히 예약되었음을 의미합니다. 테더가 비트코인 블록체인에 존재하므로, 어떤 시점에서든 테더의 증명 가능성과 회계 처리는 사소한 일입니다. 반대로, 우리의 예치 자산으로 보유된 총 USD 금액은 은행 잔액을 공개하고 전문가에 의해 주기적인 감사 과정을 거쳐 입증됩니다. 이 구현에 대한 자세한 내용은 아래에서 확인할 수 있습니다:

- 테더 리미티드는 모든 테더를 Omni Layer 프로토콜을 통해 발행합니다. Omni는 비트코인 블록체인 위에서 작동하며, 따라서 발행, 환급 및 존재하는 모든 테더는 거래 내역을 포함하여 Omnichest.info에서 제공하는 도구를 통해 공개적으로 감사할 수 있습니다.
  - 테더USD의 Omnichest.info 자산 ID는 #31입니다.
    - 링크: http://omnichest.info/lookupsp.aspx?sp=31 ○ 이 자산 ID로 발행된 총 테더 수를 TUSDissue로 표기합니다.
  - 이 자산 ID로 환급된 총 테더 수를 TUSDredeem으로 표기합니다.
  - 어느 시점에서든 유통 중인 총 테더 수를 TUSD로 표기합니다. ■ TUSD = TUSDissue - TUSDredeem ■ TUSD = “Total Property Tokens” @ http://omnichest.info/lookupsp.aspx?sp=31
- 테더 리미티드는 테더를 직접 구매/환급하는 사용자에게 법정 통화를 송금받고 송금하는 은행 계좌를 보유하고 있습니다.
  - 이 계좌에 입금된 총 금액을 DUSDdepo로 표기합니다.
  - 이 계좌에서 인출된 총 금액을 DUSDwithd로 표기합니다.
  - 이 은행 계좌의 달러 잔액을 DUSD로 표기합니다.
    - DUSD = DUSDdepo - DUSDwithd
- 발행된 각 테더는 동일한 양의 통화 단위(하나의 테더USD는 하나의 달러)로 지원됩니다. 위의 암호화폐 및 법정 통화 회계 프로세스를 결합하여 테더 시스템의 "지급 능력 방정식(Solvency Equation)"을 도출합니다. ○ 지급 능력 방정식은 단순히 TUSD = DUSD입니다.
  - 발행되거나 환급된 모든 테더는 비트코인 블록체인에 공개적으로 기록되며, 이는 은행 계좌에서의 자금 입금 또는 출금에 해당합니다.
  - TUSD의 증명 가능성은 앞서 논의된 바와 같이 비트코인 블록체인에 의존합니다.
  - DUSD의 증명 가능성은 여러 프로세스에 의존합니다:

■ 우리는 웹사이트의 투명성 페이지에서 은행 계좌 잔액을 공개합니다.

■ 전문 감사인이 정기적으로 우리의 은행 잔액과 금융 이체 명세서를 검증하고 서명하여

발표합니다.

사용자는 이 정보를 우리의 투명성 페이지에서 확인할 수 있으며, 페이지는 다음과 같이 보일 것입니다:

명확성을 위해, 테더 시스템과 Tether.to 웹 지갑의 Proof of Reserves(자산 보유 증명)가 다르다는 점을 인정하고자 합니다. 이 문서에서는 주로 테더 시스템의 Proof of Reserves에 집중합니다. 즉, 어떤 시점에서든 유통 중인 모든 테더를 포함합니다. 반면, Tether.to 지갑은 클로즈드 소스 코드와 중앙 집중식 서버에서 운영되는 소비자용 웹 지갑입니다. 이 지갑에 대한 Proof of Reserves를 수행하는 것은 테더 시스템에 대해 설명한 것과 근본적으로 다릅니다.

우리는 Tether.to 지갑을 위한 PoR(자산 보유 증명) 기반 투명성 솔루션의 배포를 계획하고 있습니다. 우리는 이것이 현재 존재하는 가장 진보된 PoR 시스템이 될 것이라고 믿습니다. 이 시스템은 이 주제에 대한 부록에서 설명된 거의 모든 도전 과제를 극복합니다. 참고로, 사용자는 언제든지 개인 키를 직접 관리하거나 Omni Wallet을 통해 테더를 안전하게 보호할 수 있습니다.

구현 약점

우리는 우리의 구현이 즉시 완전히 신뢰 없는 암호화폐 시스템을 만드는 것은 아니라는 점을 이해하고 있습니다. 주로 사용자들이 테더 리미티드와 우리의 기존 은행 기관을 자산의 보관자로 신뢰해야 하기 때문입니다. 그러나 거의 모든 거래소와 지갑(USD/법정 통화를 보유한다고 가정할 때)도 동일한 약점에 노출되어 있습니다. 이러한 서비스의 사용자들은 이미 이러한 위험에 직면해 있습니다. 다음은 우리의 접근 방식에서의 약점 요약입니다:

- 우리가 파산할 수 있습니다.
- 우리의 은행이 지급 불능 상태가 될 수 있습니다.
- 우리의 은행이 자금을 동결하거나 압수할 수 있습니다.
- 우리가 예치 자금을 착복할 수 있습니다.
- 위험이 단일 실패 지점으로 다시 집중될 수 있습니다.

거의 모든 디지털 통화 거래소와 지갑(USD/법정 통화를 보유한다고 가정할 때)이 이미 이러한 도전에 직면해 있다는 점을 주목할 필요가 있습니다. 따라서 이러한 서비스의 사용자들은 이미 이러한 위험에 노출되어 있습니다. 아래에서는 이러한 우려가 어떻게 해결되고 있는지 설명합니다.

우리가 파산할 수 있음 - 이 경우, 사업체인 테더 리미티드가 파산하더라도 고객 자금은 안전하며, 모든 테더는 여전히 환급 가능합니다. 비트코인 관련 보안 침해 사건 대부분은 은행 계좌보다 암호화폐를 목표로 했습니다. 모든 테더가 비트코인 블록체인에 존재하므로, 개인들이 자신의 개인 키를 안전하게 보관함으로써 직접 저장할 수 있습니다.

우리 은행이 지급 불능 상태가 될 수 있음 - 이는 기존 금융 시스템의 모든 사용자와 모든 거래소 운영자들이 직면하는 위험입니다. 테더 리미티드는 현재 대만의 Cathay United Bank와 Hwatai Bank에 계좌를 보유하고 있으며, 두 은행 모두 테더의 비즈니스 모델이 적절하다고 인식하고 있습니다. 추가적인 은행 파트너가 다른 관할권에서도 설립되어 이 우려를 더 줄일 수 있습니다.

우리 은행이 자금을 동결하거나 압수할 수 있음 - 우리의 은행들은 비트코인의 본질을 이해하고 있으며 비트코인 사업을 받아들이고 있습니다. 그들은 또한 세계적으로 일부 주요 비트코인 거래소에 은행 서비스를 제공합니다. 우리가 따르는 KYC/AML 프로세스는 현재 은행 서비스 제공 중인 다른 디지털 통화 거래소에서 사용되는 것과 동일합니다. 그들은 우리가 완전히 준수하고 있다고 보장했습니다.

우리가 예치 자금을 착복할 수 있음 - 회사 정관은 공개되어 있으며, 사업 소유자의 이름, 위치, 평판도 공개되어 있습니다. 계좌 소유권은 법적으로 회사 정관에 구속됩니다. 은행 계좌로의 모든 입출금은 관련 기록을 남기며 엄격한 내부 정책에 따라 처리됩니다.

위험의 단일 실패 지점으로의 재집중 - 이 문제를 극복할 방법에 대한 아이디어가 있으며, 향후 블로그와 제품 업데이트에서 이를 공유할 예정입니다. 이 문제를 해결할 수 있는 방법은 여러 가지가 있습니다. 현재 이 초기 구현은 이러한 혁신을 다음 버전에서 실현하기 위한 올바른 방향으로 나아가고 있습니다. 우리가 선택한 플랫폼을 활용함으로써, 우리는 중앙 집중화 위험을

토큰의 생성과 환급이라는 하나의 책임으로 줄였습니다. 시스템의 다른 모든 측면은 분산되어 있습니다.

주요 애플리케이션

이 섹션에서는 비트코인/블록체인 생태계와 전 세계 다른 소비자들에 대한 테더의 주요 애플리케이션을 요약하고 논의합니다. 우리는 수혜자를 세 가지 사용자 그룹으로 나눕니다: 거래소, 개인, 그리고 상인들입니다.

모든 그룹에 적용 가능한 주요 이점:

- 비트코인의 특성을 다른 자산 클래스에 부여
- 덜 변동성이 크고, 친숙한 회계 단위
- 세계 자산이 비트코인 블록체인으로 이동

거래소를 위한 애플리케이션

거래소 운영자들은 기존 금융 시스템을 통해 법정 통화를 입출금하는 것이 복잡하고, 위험하며, 느리고, 비용이 많이 든다는 것을 이해하고 있습니다. 이러한 문제에는 다음과 같은 것들이 포함됩니다:

- 거래소에 적합한 결제 제공자 식별
    - 되돌릴 수 없는 거래, 사기 방지, 최저 수수료 등
- API가 없는 은행과 플랫폼 통합
- 이러한 은행과의 협력하여 규정 준수, 보안, 신뢰 구축
- 소액 송금에 대한 부담스러운 비용
- 국제 송금이 처리되는 데 3~7일 소요
- 불리한 환율 수수료

테더를 제공함으로써 거래소는 위의 복잡성을 덜어내고 추가적인 이점을 얻을 수 있습니다. 예를 들어:

- 기존 은행이나 결제 제공자를 사용하는 대신, 암호화폐 법정 통화를 입출금/저장 방법으로 수용
    - 사용자가 거래소 내에서 법정 통화를 더 자유롭고 빠르며 저렴하게 이동할 수 있게 함
- 법정 통화 보관 위험을 테더 리미티드에 아웃소싱하고 암호화폐만 관리

- 플랫폼에 다른 테더 법정 통화 쌍을 쉽게 추가
- 고객 자산을 순수한 암호화폐 프로세스를 통해 안전하게 보호
    - 다중 서명 보안, 콜드 및 핫 월렛, HD 월렛 등
    - 순수 암호화폐 환경에서 더 쉽게 및 안전하게 감사 수행
- 거래소에서 비트코인으로 할 수 있는 모든 것을 테더로도 수행 가능

거래소 사용자들은 거래소에서 법정 통화를 보유하는 것이 얼마나 위험할 수 있는지 알고 있습니다. 지급 불능 사건의 증가로 인해 위험할 수 있습니다. 앞서 언급했듯이, 우리는 테더를 사용하면 거래소 사용자가 거래소에서 계속 법정 통화를 보유하는 것보다 상대적으로 낮은 상대방 위험에 노출된다고 믿습니다. 또한, 테더를 보유하는 데는 다른 이점들도 있으며, 이는 다음 섹션에서 설명됩니다.

개인을 위한 애플리케이션

오늘날 전 세계에는 다양한 종류의 비트코인 사용자가 있습니다. 매일 수익을 얻으려는 트레이더부터, 비트코인을 안전하게 보관하려는 장기 투자자, 신용 카드 수수료를 피하거나 개인 정보를 보호하려는 기술에 정통한 쇼핑객, 세상을 변화시키려는 철학적인 사용자, 글로벌 송금을 더 효과적으로 하려는 사람들, 재정 서비스에 처음으로 접근하려는 개발도상국의 사용자, 새로운 기술을 개발하려는 개발자들까지, 비트코인에는 다양한 용도가 있습니다. 이러한 개인들 각각에게, 우리는 테더가 다음과 같은 유용한 방법으로 사용될 수 있다고 믿습니다:

중개자 없이 USD/법정 통화 가치로 거래를 수행하고, 의사 익명성을 유지하며 거래

자신의 개인 키를 안전하게 보관하여 USD/법정 통화 가치를 콜드 스토리지

거래소에서 법정 통화를 보관하는 위험을 피하고, 암호화폐 법정 통화를 거래소 간에 쉽게 이동

법정 통화 가치를 저장하기 위해 법정 통화 은행 계좌를 개설할 필요 없음

비트코인과 함께 작동하는 애플리케이션을 쉽게 테더를 지원하도록 향상

개인으로서 비트코인으로 할 수 있는 모든 것을 테더로도 수행 가능

상인을 위한 애플리케이션

상인들은 비즈니스에 집중하고 싶어하지, 결제 문제에 신경 쓰고 싶어하지 않습니다. 전 세계의 상인들은 여전히 글로벌하고 저렴하며 보편적인 결제 솔루션의 부족으로 어려움을 겪고 있습니다. 상인들은 더 나은 서비스를 받을 자격이 있습니다. 테더가 이들에게 도움이 될 수 있는 몇 가지 방법은 다음과 같습니다:

비트코인 대신 USD/법정 통화 가치로 상품 가격 책정 (변동 환율/구매 창이 없음)

비트코인에서 USD/법정 통화로의 전환과 관련 수수료 및 과정 피하기

차지백 방지, 수수료 감소 및 더 큰 프라이버시 확보

법정 통화와 암호화폐의 특징을 통해 새로운 서비스 제공

마이크로 팁, 기프트 카드 등

상인으로서 비트코인으로 할 수 있는 모든 것을 테더로도 수행 가능

미래의 혁신

다중 서명 및 스마트 계약

지급 능력 증명의 혁신

결론

테더는 오늘날 존재하는 최초의 비트코인 기반 법정 통화 연동 암호화폐입니다. 테더는 가장 안전하고 잘 테스트된 블록체인 및 공공 원장인 비트코인 블록체인 위에 기반하고 있습니다. 테더는 시장의 힘, 가격, 유동성 제약과 완전히 독립적인 1:1 비율로 완전히 예약되어 있습니다. 테더는 간단하고 신뢰할 수 있는 증명 구현을 가지고 있으며 정기적인 전문 감사를 받습니다. 우리의 기본 은행 관계, 규정 준수, 및 법적 구조는 우리가 예약 자산의 관리자가 되고 테더를 발행할 수 있는 안전한 기반을 제공합니다. 우리 팀은 비트코인 생태계 및 그 너머에서 경험이 풍부하고 존경받는 기업가들로 구성되어 있습니다.

우리는 암호화폐 분야의 기존 비즈니스와 통합을 주도하고 있습니다. 거래소, 지갑, 상인 등 다양한 비즈니스와 통합되어 있으며, Bitfinex, HolyTransaction, Omni Wallet, Poloniex, C-CEX 등과 이미 통합되어 있습니다. 더 자세한 정보를 원하시면 저희에게 연락해 주시기 바랍니다.

별첨

감사 결함: 거래소와 지갑

다음은 기술 기반 거래소 및 지갑 감사에서 발견된 현재의 결함 요약입니다.

Merkle 트리[6] 접근법에서는 사용자가 자신의 잔액(사용자 노드)이 거래소의 부채 선언에 올바르게 반영되었음을 수동으로 보고해야 합니다(거래소의 사용자 잔액 데이터베이스의 Merkle 해시). 이 제안된 솔루션은 충분한 사용자가 자신의 계정이 트리에 포함되었음을 확인하면 작동합니다. 만약 자신의 계정이 포함되지 않은 경우, 이 사례는 보고됩니다. 잠재적인 위험 중 하나는 거래소 데이터베이스 소유자가 데이터베이스의 진정한 표현이 아닌 해시를 생성할 수 있다는 것입니다. 즉, 불완전한 데이터베이스를 해시하여 고객에 대한 부채를 줄이고 검증 당사자에게 지급 능력이 있는 것처럼 보이게 할 수 있습니다. 다음은 사기 거래소가 계정을 제외할 수 있는 시나리오입니다:

- “Bitdust” 계정: 비활성 또는 낮은 활동 계정은 관심이 없는 사용자가 불일치를 확인하거나 보고할 가능성을 줄입니다. 이러한 긴 꼬리 계정은 거래소의 부채에서 중요한 비율을 차지할 수 있습니다.

- “공모하는 큰손” 공격: 대형 비트코인 거래자들이 다양한 거래소에서 운영하며 시장을 크게 움직이고 있다는 증거가 있습니다. 이러한 거래자들은 대형 거래소에 자본 준비금을 두어 신속하게 주문을 실행할 필요가 있습니다. 종종 거래자들은 “신뢰하는” 거래소를 선택합니다. 이 방식으로 해킹이나 유동성 문제가 발생할 경우 우선적으로 돈을 인출할 수 있습니다. 이 경우

거래소와 거래자는 해시되기 전에 큰손의 계정 잔액을 데이터베이스에서 제거하기 위해 공모할 수 있습니다.

- 키 임대 공격: 악의적인 거래소는 자신이 소유하지 않는 비트코인의 개인 키를 임대하여 감사를 통과할 수 있습니다. 이는 자산을 증가시켜 지급 능력이 있는 것처럼 보이게 하지만 이러한 자금이 대출된 것임을 인정하지 않습니다. 마찬가지로, 그들은 같은 방식으로 법정 화폐를 “빌릴” 수 있습니다.

- 더 많은 공격이 논의되지 않았습니다.

통계적 유의성 도달(보고의 완전성): 이러한 세 가지 공격 벡터 외에도, 조작된 데이터베이스는 충분한 수의 사용자가 잔액을 검증하지 않으면 감지되지 않을 수 있습니다. 사용자 전체의 100%가 잔액을 검증할 확률은 제로에 가까울 것이며, 사용자가 잔액을 검증하도록 유인 구조를 제대로 갖추어도 마찬가지입니다. 따라서 감사자는 샘플링 빈도, 크기 및 기타 특성을 기반으로 거래소 데이터베이스의 유효성에 대한 진술을 할 수 있는 통계 도구가 필요합니다.

현재 사용자는 거래소에 문제가 생길 경우 법적으로 보상을 받을 방법이 없습니다. 예를 들어, Mt.Gox가 운영을 종료했을 때, 많은 사용자가 자신의 계좌 잔액을 독립적으로 기록하지 않았을 수 있습니다(스크린샷, 자신에게 서명된 메시지 등). 이러한 사용자들은 거래소가 해당 해시 트리 또는 원본 데이터베이스 기록을 게시할 수 있는지에 의존하게 됩니다.

이 감사를 수행할 구조는 여전히 미세하지만 중요한 결함을 포함하고 있습니다. 특히 기관의 웹사이트에서 데이터 보고(해시 트리)는 사용자에게 아무런 보장을 제공하지 않습니다. 악의적인 거래소는 다른 사용자 그룹에 다른 상태/잔액을 게시하거나 상태를 사후에 변경할 수 있습니다. 따라서 이 데이터를 안전한 방송 채널을 통해 게시하는 것이 필수적입니다. 예를 들어, 비트코인 블록체인입니다.

프라이버시는 자동화된/공개 감사 시스템의 채택에 장애물이 됩니다. 더 나은 프라이버시를 위한 진행이 있었지만, 완벽한 해결책은 아직 없습니다. 또한, 정확한 사용자 검증 부채 공간을 구축하기 위해 사용자들은 거래소와 비트코인 주소와 함께 계좌 잔액을 보고해야 합니다. 일부 사용자는 유인에 관계없이 이 정보를 보고하지 않을 가능성이 있으므로, 보고 목표를 달성하면서 암호학적으로 안전한 프라이버시를 제공하는 것이 매우 중요합니다.

시계열: Merkle 트리 해시는 단일 시점에서 데이터베이스의 단일 스냅샷입니다. 데이터베이스의 어느 정도 연속적인 시계열이 없으면 중요한 공격 벡터가 열립니다. 또한, 사용자가 보고한 정보의 시계열이 필요하며, 이는 보고된 사기 사건의 역사를 맞추는 데 필요합니다.

신뢰할 수 있는 제삼자: 현재 모든 거래소 감사는 어떤 “평판이 좋은” 신뢰할 수 있는 제삼자에게 일부 검증을 의존해왔습니다. Coinbase 감사[7]에서는 Andreas Antonopoulos가, Kraken 감사[8]에서는 Stefan Thomas가 있었습니다. 반드시 신뢰할 수 있는 제삼자에 의존해야 한다면, 감사 기준 및 절차가 이러한 약점을 보강해야 합니다.

기존의 법정 화폐 연동 시스템의 한계

여기 기존 법정 화폐 연동 시스템의 몇 가지 일반적인 단점과 한계가 있습니다:

- 시스템은 폐쇄 소스 소프트웨어를 기반으로 하며, 개인 중앙 집중식 데이터베이스에서 실행됩니다. 본질적으로 Paypal 또는 다른 기존 대량 시장 소매/기관 자산 거래/이전/저장 시스템과 다를 바 없습니다.

- 비트코인과 같은 다른 블록체인만큼 스트레스 테스트되거나 개발되거나 검토되지 않은 대체 코인 블록체인에 의존하는 분산 시스템입니다.

- 파생 메타 자산 헤징, 효율적 시장 이론 또는 기초 자산의 담보화에 의존하는 연동 프로세스입니다. 이에는 유동성, 이전 가능성, 보안 및 기타 문제가 있을 수 있습니다.

- 수탁자에 대한 투명성 부족 및 감사 부족, 암호화폐, 법정 화폐 또는 내부 장부와 관련된 (폐쇄 소스 및 중앙 집중식 데이터베이스와 동일).

- 자산의 이전 및 정산 메커니즘으로서 기존 은행 시스템 및 신뢰할 수 있는 제삼자(은행 계좌 소유자)에 의존합니다.

시장 리스크 예시

담보화 방법에서는 담보로 사용되는 자산의 가격이 연동/연계되는 자산의 가격과 반대 방향으로 움직일 수 있으므로 시장 리스크가 존재합니다. 이로 인해 담보의 총 가치가 발행된 자산의 총 가치보다 적어지며 시스템이 지급 불능 상태가 될 수 있습니다. 이 리스크는 수탁자가 이 상황이 발생하기 전에 포지션을 종료함으로써 완화됩니다. 즉, 담보 가격이 연동 자산 가격과 같아지면 담보는 (개방 시장에서) 매각되고 포지션이 종료됩니다. 이는 훌륭한 접근 방식이며, 전통적인 은행 및 금융 시장에서 많은 유동적인 시장에서 사용됩니다. 그러나 글로벌 금융 위기에서 보았듯이 이러한 사건의 가속화로 인해 “유동성 부족” 상황이 발생하여 담보가 거래 의무를 충족하기 위해 충분히 빠르게 매각되지 못하게 되는 경우가 있습니다. 암호화폐 시장은 너무 작고 변동성이 크기 때문에 이러한 유형의 사건이 발생할 가능성이 훨씬 더 큽니다. 또한, 전체 접근 방식은 연동 자산의 생성에 필요한 충분한 담보를 게시하는 사용자 공급이 필요하기 때문에 다른 유동성 및 가격 제약이 있습니다.

파생 상품 접근 방식에서는 자산의 가격이 여러 파생 상품 전략 중 하나를 통해 연동됩니다. 예를 들어 스왑 전략, 커버 및 나체 옵션 전략, 다양한 선물 및 포워드 전략이 있습니다. 각 전략은 고유한 강점과 약점을 가지고 있으며, 이에 대한 논의는 여기서 하지 않겠습니다. 요약하자면, 이러한 연동 프로세스는 앞서 언급한 담보화 방법과 유사한 “시장 리스크” 특성을 가지고

있습니다. 두 방법이 상호 배타적이지 않고, 종종 특정 거래, 헤지 또는 리스크 관리 기능에서 결합되어 사용된다는 점을 주목해야 합니다.

마지막으로, 위의 접근 방식 중 일부 조합이 자산을 보증/연동하는 안전하고 신뢰할 수 있으며 일반적으로 리스크가 없는 프로세스가 될 수 있다고 믿습니다. 그러나 현재로서는 유동성과 가격 안정을 보장하기 위해 이러한 방향이 실현 가능한지 확신할 수 없습니다. 또한, 전체 산업이 성장함에 따라 예약 기반 접근 방식이 항상 존재하고 이러한 다른 접근 방식을 보완할 것이라고 믿습니다. 기술 발전이 계속됨에 따라, 우리는 100% 상환 보장을 유지하면서 가능한 모든 이점을 평가하고 통합할 것입니다.

법률 및 준수

Tether Limited(“Tether”)는 홍콩 회사 조례에 따라 설립된 유한 회사입니다. 이 회사는 BVI Business Companies Act, 2004에 따라 설립된 BVI 사업 회사인 Tether Holdings Limited가 전액 소유하고 있습니다.

Tether는 미국 재무부의 금융범죄단속네트워크(Financial Crimes Enforcement Network, FinCEN)에 돈 서비스 사업자로 등록되어 있습니다(MSB 등록 번호 31000058542968). Tether는 미국 내 Tether 사용자들에게 더 나은 서비스를 제공하기 위해 미국의 금융 기관과 관계를 구축하고 있습니다.

Tether는 RenRenBee Limited(“RenRenBee”)와 주체–대리인 계약을 체결하고 있습니다. RenRenBee는 홍콩 세관 및 소비세 부서(Hong Kong Customs and Excise Department)로부터 돈 서비스 운영자로 라이센스를 보유하고 있습니다(라이센스 번호 13-09-01265). 계약에 따라 RenRenBee는 Tether의 대리인으로서 자금 세탁 방지 준수 작업 및 고객 실사 절차를 제공합니다.

이와 다른 조치를 통해 Tether는 미국 법률 및 홍콩의 자금 세탁 방지 및 테러 자금 조달(금융 기관) 조례에 부합하는 고객 실사, 기록 보관 및 보고 절차를 수행하고 있습니다.

Tether Limited는 현재 대만의 Cathay Bank와 Hwatai Bank에 계좌를 보유하고 있으며, 두 은행 모두 Tether의 비즈니스 모델이 수용 가능하다는 것을 인지하고 확신하고 있습니다.

이들 은행은 우리의 프로세스에 만족하고 있으며, 우리의 비즈니스가 대만의 해외 은행 규정을 준수하고 있다는 점에도 만족하고 있습니다. 모든 은행은 계좌를 개설하기 전에 자체 법무, 준수 및 본사에 확인 요청을 했으며(우리의 요청에 따라서도), 초기부터 준수하는 운영을 목표로 하여 은행 파트너들에게 최대한의 신뢰를 제공하고자 했습니다. 또한, 이들 은행은 다른 비트코인 기반 사업체와도 협력하고 있습니다.