

상부표제: eBTC: 이더리움 토큰화 형태의 비트코인

1

eBTC: 스마트 계약, 낮은 거래 수수료와 빠른 거래속도를 갖춘 이더리움 토큰화 형태의

비트코인

eBTC 커뮤니티 재단

eBTC: 이더리움 토큰화 형태의 비트코인

2

요약

eBTC, e 비트코인 또는 이더리움의 비트코인은 이더리움 블록체인에 존재하는 ERC20 토큰화 형태의 비트코인이다. 효율성과 확장성을 극대화할 수 있는 내재적인 이더리움의 장점을 가져와 비트코인이 가지고 있는 송금 속도, 비용, 확장성 그리고 스마트 계약을 적용 못 하는 근본적인 문제를 해결하기 위해 고안되었다. 다양하고 역동적이며 헌신적인 글로벌 커뮤니티에 의해 지원되고 있으며, 더욱 유연하며 빠른 피어 투 피어 (P2P) 전자지불 시스템을 목표로 하고 있다. 비트코인이 가지고 있는 핵심의 이상을 유지하면서 이더리움 생태계에 통합 시키려고 한다. 2017 년, 비트코인의 다중적인 하드포크들이 출현하며 낮은 거래 속도, 높은 거래 비용 및 중앙 집중화된 채굴 문제를 해결하려고 하였다. 그러나 현재 포크들에는 모든 근본적인 문제를 효과적으로 해결할 능력이 없다. 하지만 eBTC 는 명백하고 단순한 기반을 갖추었으므로 이런 단점을 효율적으로 처리하는 동시에 비트코인의 핵심에 스마트 계약을 적용할 수 있다. 가상화폐 이하 암호화폐의 수용과 인식이 증가함에 따라, eBTC 는 이더리움 계층의 모든

미래 개발을 통합하며 빠르고 비용면에서 효율적인 완벽한 메커니즘을 계속해서 설계해 나갈 것이다. 이미 선두를 확고히 다지고 있는 이더리움 생태계를 사용하여 비트코인이 필요한 현대화를 가져오고 세계적으로 구현되고 있는 모든 이용 사례들을 연동하게 하면서 전자지불 방식에 대한 의미와 가치 보존에 대한 의미를 결합하며 대표하는 시스템을 목표로 한다.

eBTC: 이더리움 토큰화 형태의 비트코인

3

목차

배경: 블록체인 진화 과정과 eBTC 의 탄생

배경.....	Error! Bookmark not defined.
우려 사항 및 문제점	6
해결방안 등	9
eBTC: 토큰 솔리디티 오류와 스왑	12
eBTC:역동적인 글로벌 커뮤니티의 근본.....	13

eBTC: 기술적 특성.....	12
eBTC vs. 이더.....	14
총 발행량, 발행과 채굴	12
디플레이션 eBTC 와 인플레이션 이더	13
eBTC 의 스마트 계약 확장성과 이더리움의 미래 지향적 개발 14	
결론.....	17
참고문헌.....	19
eBTC: 이더리움 토큰화 형태의 비트코인	

4

eBTC: 스마트 계약, 낮은 거래 수수료와 빠른 거래속도를 갖춘 이더리움 토큰화 형태의

비트코인

배경: 블록체인 진화 과정과 eBTC 의 탄생 배경

비트코인은 ‘비트코인: 피어 투 피어 전자 현금 시스템 (나가모토, 2008)’이라는 논문을 통해 혁신적인 디지털 통화 자산 시스템을 만들어 냈다. 기발하게도 이중 결제

저항 능력을 갖춘 이 기술은 두 가지 중요한 요점을 우리에게 보여준다. 디지털 통화 자산과 탈중앙화 분산 합의 메커니즘.

가상화폐의 발전은 블록체인 기반 신기술을 통해 세계로 크게 확장되어 나갔다. 이중 가장 확고한 주목을 받는 기술은 이더리움의 확장 가능하고 표준화된 상호 운용이 가능한 추상 기초 계층(abstract foundational layer)의 개발 환경이다. 비탈릭 부테린이 발표한 논문 ‘차세대 스마트 계약 & 탈중앙화 애플리케이션 플랫폼 (2013)’으로 인해 비트코인과 가상화폐 세계의 진화 과정을 보여주었다. 효율성과 속도 그리고 유연성이 향상하며 개선됨에 따라 혁신적이며 탈중앙화된 해결방안을 광범위한 분야에 활용할 수 있었다. 이더리움의 추상적인 기초 계층(abstract foundational layer)과 솔리디티(환경 언어)는 스마트 계약과 탈중앙화된 애플리케이션(디앱/DApps) 그리고 탈중앙화된 자율조직(DAOs)의 탄생 배경이 되었다. 역동적인 이더리움의 근간이 되는 강점은:

“확장성,

eBTC: 이더리움 토큰화 형태의 비트코인

표준화, 기능-완전성, 개발 및 상호 운용성의 용이성”(부테린, 2013 p.13)이 되며 핵심 요소로 보여진다. 스마트계약은 이더리움 생태계의 모든 품질 특성을 향유한다.

이 두 가지 블록체인의 점진적인 진화과정에서 자연스럽게 eBTC는 직접적인 결과를 보여줄 해결방안으로 고안되었다. 본질에서 이더리움의 ERC20 토큰화에 기간을 두지만 이상적으로는 비트코인 형태를 보여주면서 이더리움 플랫폼의 방대한 기능을 보유한 잠재적 가치를 갖게 개발되었다.

우려 사항 및 문제점

비트코인의 구현에서 가장 중요한 측면 중 하나는 제 3자 신뢰의 필요성을 제거하고 그러한 중개 계약과 관련된 불가피한 거래 비용을 제거하는 것이다. 나가모토의 논문에 따르면 중개자가 있는 거래 방식은 소규모 또는 격식 없는 거래의 제한을 가져온다고 말한 바 있다. P2P의 근본을 언급하며 비트코인은 중개자의 필요성을 상쇄시키고 소규모의 거래방식을 진행되게 만들 해결방안으로 고안되었다고 언급했다. 하지만 아이러니하게도 급격히 상승하는 시장 규모와 잦은 변동으로 인해

사용자들은 시간이 갈수록 소규모의 거래를 할 수밖에 없어지며 시장 규모와 비례하며 거래의 수수료 또한 증가하고 있다.

eBTC: 이더리움 토큰화 형태의 비트코인

6

증가하고 있는 비트코인의 거래수수료는 기존에 존재하던 자산거래 수단의 거래수수료를 따라잡고 있다. 현재 비트코인의 평균 거래 수수료는 약 2 ~ 5 북미달러이며 이는 30,000 사토시 정도가 된다. 비트코인의 거래 속도 또한 큰 문제점으로 떠오르고 있다. 평균 블록 생성 시간은 현재 10 분이며 총 6 번의 승인이 필요하기 때문에 한 번의 거래로 60 분가량 소모된다고 말할 수 있다. 이 두 가지 요소는 비트코인이 본래 제안한 비트코인 생태계의 독창성을 손상하며 디지털 거래의 지속 가능한 매체로서의 비트코인 채택을 제한하게 된다. 비트코인으로 일상적인 사용을 위한 효율적인 전자 화폐 시스템으로 사용하는 것이 점점 어려워진다. 2 북미달러 이하의 물품을 거래하는 경우에서 이러한 문제점을 확고히 볼 수 있다.

전통적인 은행 업무의 대안으로 탄생한 대조적인 비트코인의 철학은 지속적인 거래 수수료의 상승과, 느린 블록 생성주기 그리고 끝이 없는 포킹(forking) 논쟁으로 인하여 그 의미가 서서히 희미해져 가고 있다. 최근 주목을 받으며 비트코인에서 포킹(forking)된 가상화폐들은 이런 여러 문제점을 보완하기 위해 고안되었다는 것을 볼 수 있었다. 하지만 그중 비트코인 생태계를 뒤덮는 근본적인 문제를 모두 일괄적이며 효율적으로 해결할 능력이 없다. 따라서 이러한 근본적인 문제점들을 해결하며 뚜렷한 비전을 실현하려면 더욱 근간이 되는 방안을 보이며 비트코인을 현대화 시켜야 한다.

eBTC: 이더리움 토큰화 형태의 비트코인

7

현시점에서 비트코인 캐시와 비트코인 골드가 비트코인에서 포킹(forking)된 가상화폐 중 가장 많이 알려져 있으며 세그윗 2X 또한 이번에 포킹(forking)을 마친 상태다. 하지만 모든 포킹(forking)된 비트코인들은 블록생성 주기의 문제점을 확고히 해결하지 못하였다. 다음은 느린 블록생성주기를 비교 분석하기 위한 표이다

비교 BTC/BTG/BCH/B2X	비트코인 BTC	비트코인 캐시 BCH	비트코인 골드 BTG	세그윗 2X B2X
발행량	21 Million	21 Million	21 Million	21 Million

블록생성주기	10 Minutes	10 Minutes	10 Minutes	10 Minutes
블록 사이즈	1M (2-4M)	8M (8M)	1M (2-4M)	2M (4-8M)

표 1: 현재 존재하는 비트코인들의 블록 생성주기와 사이즈 비교 (비트코인 골드, 2017)

해결방안 등

블록체인 기술이 비트코인에서 이더리움으로 진화함에 따라 이더리움 인프라에서 개발자들이 더욱 혁신적이고 분산화된 애플리케이션을 추상 기본 계층(abstract foundation layer)에 얹어 개발할 수 있게 되었다. 계층을 통해 진정한 분권화되고 신뢰가 필요 없는 가상화폐를 만들 수 있다. 이 기능으로 인해 P2P 전자거래 지불 시스템의 eBTC 가 고안되었다. 비트코인의 핵심 이상을 토큰화된 버전으로 개발하여 높은 트랜잭션 속도를 제공하고 가상화폐 사용자 등의 세계 시장과 함께 작업 할 수 있는 능력을 통해 위에서

eBTC: 이더리움 토큰화 형태의 비트코인

8

언급한 문제를 해결한다. eBTC 는 가상화폐 및 지불 시스템으로서 이더리움

블록체인에서 비트코인의 핵심 속성을 지속해서 대표할 뿐만 아니라 스마트 계약을

지원한다. 이더리움의 스마트 계약 기능을 통해 eBTC 는 세계 시장의 디지털 트랜잭션 시스템이 될 것이다.

eBTC 이 이더리움의 추상 기본 계층(abstract foundation layer)에 존재하기

때문에 이더리움의 전송 속도, 거래 수수료, 스마트 계약 등의 기능을 따라간다. 그러므로

인해 eBTC 의 거래 수수료는 0.15 에서 0.5 달러의 비용이 되며 비트코인과 비트코인

포킹(forking)으로 인해 생긴 가상화폐들보다 10 배가량 빠른 블록생성 주기를 보여준다.

아래의 차트에서 비트코인과 비트코인에서 포킹(forking)된 가상화폐들의 수치를

비교해볼 수 있다.

“비트코인들”	BTC (Bitcoin)	BCH (Bitcoin Cash)	BTG (Bitcoin Gold)	B2X (SegWit2X)	eBTC (eBitcoin)
총 발행량	21 Million	21 Million	21 Million	21 Million	21 Million
플랫폼	Original Bitcoin “1MB”	Bitcoin Fork “8 MB”	Bitcoin Fork “Equihash”	Bitcoin Fork “2MB”	ERC20 Token on Ethereum
채굴	Yes (ASIC & Cent.)	Yes (ASIC)	Yes (GPU)	Yes (ASIC)	No (T. in Circulation)
출시일	2009-Jan.	2017-Aug.	2017-Oct.	2017-Nov.	2017-Oct.
블록생성시간	~ 10 Minutes	~ 10 Minutes	~ 10 Minutes	~ 10 Minutes	~ 15 Seconds
거래승인	6 Confirmations (~ 60 min.)	6 Confirmations (~ 60 min.)	NA	NA	12 Confirmations (~ 3 min.)

거래 수수료	~ (\$2 – \$5)	~ (\$0.06 – \$0.3)	NA	NA	~ (\$0.15 – \$0.5)
방식	PoW	PoW	PoW	PoW	PoW (soon PoS)
스케일링	Lightening Network (not launched)	Larger Block Size No layer on top	Lightening Network (not launched)	Lightening Network (not launched)	Lightening + Sharding + Plasma
보안	Dandelion (not live)	NA	NA	NA	zkSNARKs (on testnet)
스마트 계약	No	No	No	No	Yes
가능성	Payments (Rootstock soon)	Payments	Payments	Payments	Payments + Smart contracts
지불방식 상용화	High	Medium	Minimal (In Progress)	NA	Minimal (In Progress)
깃허브 평가	18,707	239	296	326	97
시가 총액	~ \$120 Billion	~ \$10 Billion	~ \$3 Billion	NA	~ \$2 Million

표 2: 포킹(forking)된 비트코인들과 비트코인 그리고 eBTC 의 비교 (as adopted from Larsson, 2017)

eBTC: 이더리움 토큰화 형태의 비트코인

9

eBTC 는 비트코인 생태계에 계속해서 일어나는 포킹(forking) 문제를 효과적으로 해결할 것이다. 이더리움의 지속 가능하고 장래가 밝은 미래 개발을 유입하면서, 다양하고 확장성이 뛰어난 혁신적인 플랫폼을 만들며, 비트코인의 핵심이 되었던 글로벌

커뮤니티의 힘과 융합될 것이다. 또한, eBTC는 이더리움의 생태계에서 가치 보유의 대표적인 자산이

eBTC: 이더리움 토큰화 형태의 비트코인

10

있다는 것을 보여줄 수 있고 이로 인해 이더리움의 생태계도 전략적인 새로운 가치를 갖게 된다.

eBTC: 토큰 솔리디티 오류와 스왑

eBTC의 기존 ERC20 솔리디티 코드에는 오류가 있었다, 이로 인해 2천 1백만 개의 총량을 지녀야 했던 eBTC의 수량에 추가로 발행할 수 있는 여지가 생겼다. 하지만 이러한 의도하지 않은 오류를 지닌 토큰은 공개되지 않았기에, 이러한 오류로 프로젝트의 신뢰도에 문제가 생길 수도 있었지만 eBTC 재단에서 모든 오류가 있던 토큰을 1:1 비율로 새로운 오류가 없는 토큰으로 스와프가 이뤄졌다. eBTC 재단은 성공적으로 새로운 ERC20 스마트 계약이 가능한 토큰으로 교체했다. 현재 코드는 누구나 검토할 수 있게 GitHub에 소스 코드가 공개되어있다.

eBTC 재단의 공식적인 발표에도 불구하고 개인키가 있는 지갑에 보유하지 않은 탈중앙화된 거래소의 수량으로 인해 약 2 백 1 십만 개의 토큰이 인간이 제어 할 수 없는 스마트 계약의 범주에 있었기 때문에, 이와 같은 수량의 토큰은 새로운 토큰의 총량에 추가 되지 않을 것이다. 새로운 토큰의 전체 및 순환 공급량은 약 1 천 8 백 9 십만 개에서 2 천 1 백만 개이다.

eBTC: 이더리움 토큰화 형태의 비트코인

11

eBTC: 역동적인 글로벌 커뮤니티의 근본

eBTC 는 커뮤니티로 지원/운영되는 ERC20 토큰화된 비트코인이며 비트코인에서 볼 수 있는 커뮤니티 운영방식과 이더리움의 기술을 융합한 시스템이다. 이더리움 토큰화 형태의 비트코인이기 때문에 두 환경을 모두 접할 수 있다. 비트코인이 가지고 있는 자산 가치의 저장소로서의 행태를 빠르고 발전 가능성이 높은 이더리움의 블록체인에 올림으로써 혁신적인 현대화 비트코인으로 발전할 것이다.

이더리움 블록체인에서 비트코인을 대표하는 ERC20 토큰을 만든다는 것이 어찌 보면 “너무 간단해” 보일 수도 있지만, 이더리움의 블록체인이 가져오는 빠른 트랜잭션 속도와 낮은 수수료 비용 그리고 비트코인의 이상을 결합하는 것은 더 이상의 포킹(forking) 논란과 중앙 집중화된 채굴을 상쇄할 혁신적인 진화일 것이다. eBTC는 강력하고 역동적인 가상화폐(암호화폐) 기반 매니아 커뮤니티가 전체 생태계의 지속 가능한 진화에 결정적인 역할을 할 것으로 믿는다. eBTC 커뮤니티 재단은 eBTC의 단일 목적을 파괴하는 원인을 발전시키는 데 전념하고 영감을 주며 다양하고 역동적인 글로벌 조직으로 구성될 것이다. 또한, 중앙 집중화되는 권력과 지휘를 무너트리며 새로운 온라인 금융거래의 가장 강력한 원동력이 되는 것이 커뮤니티의 큰 목적이라고 할 수 있다.

eBTC: 이더리움 토큰화 형태의 비트코인

12

eBTC: 기술적 특징

eBTC vs. 이더

eBTC 는 이더리움을 지원하는 현금 및 전자 지불 시스템이며 이더는, “이더리움 네트워크를 위한 암호화 연료”이다. (“이더란 무엇인가”, 2017), 이더는 이더리움 블록체인을 통해 eBTC 트랜잭션을 검증하는 역할을 한다. 생태계에 연료의 역할을 하는 이더는 전반적인 이더리움의 생태계를 지원한다.

명확히 말하자면 이더는 이더리움의 통화 자산이 되기 위해 나타난 시스템이 아니다. 대신 이더리움의 분산 응용 프로그램 플랫폼에서 연료의 역할을 하기 위해 존재한다. (“이더란 무엇인가”, 2017). “이것은 고객이 요청한 작업을 실행하는 기계에 지불하는 방식입니다” (“이더란 무엇인가”, 2017). 반면 eBTC 는 가장 순수한 의미에서 매일 사용할 수 있는 디지털 통화 및 최적화된 지불 시스템, 즉 더 빠르고 저렴한 교환 및 가치 저장 매체이다.

총 발행량, 발행 및 채굴

eBTC 의 전체 및 최대 공급량은 2100 만 개이며 소수점 이하 8 자리로 나눌 수 있다. 모든 eBTC 보유자들은 처음 발행 되었을때 투명하게 ICO 가 없는 방식으로 다양하고 헌신적인 전 세계의 가상화폐 매니아 커뮤니티에게 제공됨으로 공정하게 분배되었다.

eBTC: 이더리움 토큰화 형태의 비트코인

13

태초부터 채굴의 시스템이 없었으며 가상화폐 매니아 커뮤니티와 eBTC 커뮤니티 재단에 97.92 : 2.08 의 비율로 발행되었다.

디플레이션 eBTC 와 인플레이션 이더

eBTC 의 총 공급량이 2100 만으로 제한되어 있기 때문에, 비트코인의 디플레이션 속성을 보다 유연하고 스마트한 이더리움 블록체인에 반영한다. 이로써 eBTC 의 가치는 지속해서 성장함과 함께, 비트코인의 모습을 보이며 디플레이션 속성을 가진 이더리움 생태계의 비트코인이 될 것이다. 디플레이션 속성은 이더리움 환경에서 지속할 수 있고 적절한 가치 보유 메커니즘으로 적용할 수 있다.

아이러니하게도 현재 이더의 총 발행량에 제한이 없다. 이것은 eBTC 이 디플레이션 속성을 가진 가상화폐가 되면서 인플레이션 속성을 가지며 생태계의 연료 역할을 하는 이더의 흥미로운 현상을 만들어낼 것이다. 이더의 가치 상승률과

상대적으로 안정화된 가치로 볼 때, eBTC는 계속해서 낮은 거래 수수료를 보존하는 이더리움 네트워크의 장점을 갖고 갈 것이다.

eBTC: 이더리움 토큰화 형태의 비트코인

14

이더리움 토큰화 형태로 비트코인이 만들어지고 사용된다면 eBTC는 다양한 이더리움 스마트 계약, 디앱 및 DAO와 같은 혁신적인 이점을 가져갈 수 있다. eBTC는 글로벌하고 접근성이 좋은 전자 현금 및 지불 시스템으로 진화하는데 도움이 되기 위해 이미 이더리움 환경을 적용하고 발전해오고 있는 생태계에 모두 적용하면서 혁신을 이뤄갈 것이다. eBTC의 채택 및 점진적인 발전으로 이더리움 환경 생태계의 전략적 자산이 될 수 있다.

결론

우리는 효율적이고 견고하며 유연한 피어-투-피어(P2P) 전자 현금 및 지불 시스템의 기본 설계, 개념 및 구현 기능에 대해 논의했다. 우리는 비트코인의 신뢰가 없는

합의 메커니즘의 진화와 이더리움의 더욱 유연하고 다양하며 상호 운용이 가능한 추상 기반 계층(abstract foundational layer)에서의 진화된 현대화 비트코인으로 진전하기 위해 시작했다. 우리는 eBTC 가 어떻게 이더리움의 블록체인에서 비트코인의 역할을 할 것인지에 대해 논의했다. 현재 비트코인에서 가장 근본적인 문제점들인 블록생성 주기, 높은 수수료, 중앙집중화된 채굴방식 그리고 계속되고 있는 비트코인의 포킹(forking)을 가장 효율적이며

eBTC: 이더리움 토큰화 형태의 비트코인

15

혁신적으로 해결하는 방법을 이더리움 토큰화 형태의 비트코인으로 만드는 것이라고 결론을 지었다. 우리는 또한 eBTC 의 기본 사항, 기술적인 측면, 커밋 방법 및 글로벌 커뮤니티가 eBTC 의 전반적인 인식 및 주류 채택에 중요하다는 것을 알고 있다. 우리는 eBTC 을 채택과

인식을 통해 글로벌 공동체가 새로운 비트코인을 다시 한번 경험할 것으로 생각한다.

우리는 더욱 유연하고 효율적인 블록체인을 보유하고 있다.

참고문헌

비트코인 골드. (2017). 비트코인 골드와 비트코인들 : <https://btcgpu.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf>

비탈릭 부테린의 이더리움 백서 : http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Larsson, A. (2017). 비트코인의 상태. *allcoinwiki.com*. Retrieved from <https://allcoinwiki.com/bitcoin/>

나가모토 사토시 비트코인 백서 <https://bitcoin.org/bitcoin.pdf>

나가모토 사토시 비트코인 P2P 금융 시스템

<http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>

‘이더란 무엇인가’ 이더리움 재단 <https://ethereum.org/ether>