THE PPP(Purchase & Payment Plus) COIN
WHITE PAPER

Initial Version 2.1.0.0

PnPP coin, 안전하고 편리한 암호화폐의 표준 플랫폼

피피피 코인(PPP Coin)은 크립토노트(Crypto Note) 블록체인을 기반으로 개발된 토큰으로써 캐쉬(CHASH) 로 거래가 가능하도록 하여 실생활에 접목하고자 준비하였다. 피피피 코인(PPP Coin)의 전용 dApp을 사용함으로써 상품의 구매와 거래의 편의성 그리고 통일성을 확보하도록 하여 안전하고 용이하게 생활의 화폐로 사용하게 된다.

따라서, 피피피 코인(PPP COIN)은 지속적으로 일반인에게 생산 및 판매를 할 뿐만 아니라, VASA카드나 MASTER카드와 같은 방식으로의 다양한 사용처를 확대하고 가맹토록 유지하여 거래를 실시함으로써 지속적인 가치 상승의 계기를 마련하게 되는 토큰으로 자리할 것이다. 특히, 실생활에 필요한 생활코인으로써 가맹점이나 사용처를 통해 거래가 발생하는 경우 거래채굴이라는 이벤트를 발생하도록 하여 채굴의 기회를 통한 자산의 유지와 자산의 확대를 꾀할 수 있도록 하였을 뿐만 아니라 수수료가 없는 거래를 꾀하였다.

피피피 코인(PPP COIN)은 기본적으로 상품 거래를 위한 수단으로 사용하는 것을 전제로 하기 때문에 가상화폐 거래소에 상장하되 투기의 대상이 되는 것을 원칙적으로 원하지 않으며, 그러나 코인 시장의 투자대비 안정적인 수익을 얻게 함은 물론 상거래의 윤리를 어지럽히지 않는 범위 내에서 탄력적인 운영을 통해 회사와 함께 동반 성장을 가질 수 있는 수단으로써 거래의 보편화와 일반화를 함께 추진한다. 이에 구매에 있어 위의 내용을 숙지하여 구매 할 것을 권고한다.

피피피 코인(PPP COIN)을 목적과 달리 구매자가 거래의 본질을 흐리는 거래를 통해 불공정한 거래 차익 등을 위한 투자의 목적으로 구매하여 손실이 발생할 경우, 이에 대한 모든 책임은 구매자 개인에게 있다.

피피피 코인(PPP COIN)을 개발하고 유통하는데 있어 시장에 흐름에 역행하지 않고 안정적 안전자산으로 자리하고자 다양한 채굴방식을 기획하고 준비하여 기축의 자산으로 자리매김하고자 노력할 것이다.

1.가상화폐(CRYPTOCURRENCY) 개 요

1) 배 경

블록체인은 2008년 Satoshi Nakamoto의 논문 “Bitcoin: A Peer-to-Peer Electronic Cash System”에서 처음 개념화되었으며 다음 해에 Bitcoin의 핵심 기술로 구현되었다[1]. Bitcoin은 개인들이 화폐 전송 정보를 공개적으로 기록하는 금융 거래 원장으로써 블록체인 기술을 사용한다. Bitcoin은 이중 지불 문제를 해결하기 위해 블록체인을 사용한 최초의 사례다. 중앙집권적인 관리자가 없음에도 불구하고 Bitcoin은 1억8천만건의 P2P(peer-to-peer) 거래를 성공적으로 지원했으며, 이제 10억 달러 이상의 시가총액을 달성하고 있다.

Bitcoin의 성공에 뒤를 이어 블록체인 기술을 활용한 수많은 시스템이 나타났다. 수백 개의 암호화폐들이 현재 경쟁 중이며, IBM의 최근 보고서에 따르면 이제는 90% 이상의 은행들이 블록체인 기술에 투자하고 있다[2]. 화폐 거래가 블록체인 기술의 가장 보편적인 응용 프로그램이지만, 이 외에도 금융 상품 및 서비스, 물류 정보, 재산 소유권, 신원 정보 등과 같은 다른 디지털 자산을 블록체인 기술을 사용하여 관리하려는 시도 또한 다양한 그룹에서 나타나고 있다.

---

1) Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

2) *Leading the Pack in Blockchain Banking: Trailblazers Set the Pace*, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN&

2016년, 암호화폐 Ethereum은 많은 관심을 받았다. 이더리움은 “임의의 상태변환 함수 구현에 사용될 수 있는 ’계약’을 생성하는데 사용될 수 있는 본격적인 튜링-완전 프로그래밍 언어가 내장된 블록체인.“[3]이며 블록체인에 결재 시스템을 제공하는 것을 목표로 한다.

목표는 사용자가 모든 종류의 프로그램 (또는 계약)을 블록체인에 쓸 수 있게 하는 것이다. Bitcoin과 마찬가지로, Ethereum은 블록체인과 합의 메커니즘을 사용하여 악의적인 노드가 계약 내용을 위조하려고 시도하면 위조 계약이 결국 블록체인에서 제거되도록 한다. Bitcoin은 계정 사이에서 전송되는 Bitcoin의 양을 완전하게 보장한다. 이와 비슷하게 Ethereum도 실행되는 계약의 무결성을 보장해야 한다.

2) 필 요 성

모든 산업에서 가장 기본적인 인프라가 되는 것이, 바로 결제 시스템이다. 과거의 물물교환이 화폐의 등장으로, 화폐를 이용한 거래로 발전해오면서, 전자적 결제 방식을 이용하여 신용거래 시스템으로 발전해왔다.

이 과정에서 화폐의 디지털화를 위한 노력이 강조되면서, 디지털 화폐와 암호화 화폐 등이 등장하고, 블록체인 기술을 통해서 탈중앙화 방식의 암호화 화폐들을 통해서, 자유로운 개개인들의 거래를 지원하며, 상거래를 효과적으로 발전시킬 수 있다는 미래를 전망하고 있다.

하지만, 이 과정에서 화폐의 발전보다 더욱 중요한 것이, 상품을 거래할 때 사용되는 PPP COIN ‘가치’를 지켜내고 모든 거래의 안정적인 질서를 유지 보완하는 것이 각 개인의 재산을 보호하는 방법이라고 믿고, 우리는 블록체인(Blockchain)기술 및 보안솔루션(SECURITY SOLUTION)을 모든 결제 가능한 ‘시스템’에 적용할 것을 제안하고자 한다.

---

3) Vitalik Buterin, *Ethereum Whitepaper*, https://github.com/ethereum/wiki/wiki/White-Paper

2. CryptoNote 란

2.1 소개

“비트코인은 p2p 전자 화폐를 성공적으로 현실화한 사례이다. 전문가들과 대중들은 public transaction과 proof-of-work 방식을 신뢰할 수 있는 모델로 평가했다. 현재 사용자 기반의 전자 화폐는 꾸준히 성장하고 있다. 일반 소비자들은 전자화폐의 낮은 수수료와 익명성에 이끌리고 있으며, 상인들은 예견이 가능하고 분산화된 화폐 발행을 긍정적으로 생각한다. 비트코인은 전자화폐가 지폐처럼 단순하고 신용카드처럼 편리하다는 사실을 효과적으로 입증했다.

하지만, 비트코인에는 몇 가지 단점이 존재하는데, 예를 들어 시스템의 분배는 경직되어 있으며, 모든 네트워크 이용자들이 클라이언트를 업데이트 해야만 새로운 기능이 도입될 수 있다. 단점을 빨리 개선할 수 없다는 점은 비트코인의 확산을 막고 있다. 이러한 경우에는 기존의 것을 개선하는 것보다 아예 새로운 프로젝트를 만드는 것이 효율적이다.

이 문서에서, 비트코인의 주된 단점에 대한 해결책을 제시하고자 한다. 이러한 해결책을 통하여 전자 화폐 시스템은 건전한 경쟁을 할 수 있을 것이다. “CryptoNote”라는 우리의 전자화폐를 통해서, 전자화폐는 혁신될 수 있을 것이다.

2.2 비트코인의 단점들과 가능한 해결책들

2.2.1 트랜젝션의 추적 가능성

전자화폐에서 프라이버시와 익명성은 가장 중요한 측면들이다. 개인 간 거래는 제3자로부터 숨겨질 것이며, 이는 전통적인 은행의 거래 방식과 대조된다. 특히 T. Okamoto와 K. Ohta는 이상적인 전자화폐의 6가지 특성을 서술하였는데, 그 중 하나는 “프라이버시로, 사용자 간의 관계와 구매 내역은 어느 누구도 볼 수 없어야 한다.” Okamoto와 Ohta의 완전히 익명적인 전자

화폐 개념을 충족하기 위해서 2가지 특성을 이끌어 내었다.

비추적성 : 각각의 수신 트랜젝션에서 누가 보냈는지 알 수 없다.

비연결성 : 임의의 2개의 발송되는 트랜젝션에 대해서, 같은 사람에게 전송되었다는 것을 입증할 수 없다.

안타깝게도 비트코인은 비추적성에서 벗어난다. 네트워크의 참가자들의 트랜젝션이 모두 공개되기 때문에, 발송자와 최종 수신자가 모두 공개될 수 있다. 만약 간접적으로 거래를 하더라도, 경로 추적 기술을 이용하면 발송자와 수신자를 확인할 수 있다.
비트코인이 2번째 속성도 충족하지 않는 것처럼 보인다. 일부 연구자들에 의한 블록체인에 대해 자세히 분석하면, 비트코인 네트워크의 이용자들과 트랜젝션 사이의 관계를 알게 될 가능성이 존재한다. 많은 방법들이 부정되었지만, 공개된 데이터베이스로부터 숨겨진 개인정보가 알려질 가능성이 크다.

비트코인은 위에 서술된 2가지 속성을 충족하지 못하며, 따라서 익명성을 가장한 전자 화폐 시스템이라는 것이다. 사용자들은 이러한 단점을 빠르게 극복하고자 한다. 두 가지의 직접적인 해결방법은 “화폐세탁 서비스”와 공개된 트랜젝션과 중간 주소를 이용하는 것으로서, 제3자가 필요하다는 단점이 있다.

최근에, I.Miers는 새로운 계획을 제시하였다. “Zerocoin”은 단방향의 암호 축적 방식을 이용하며, 사용자들로 하여금 비트코인을 제로코인으로 바꾸게 하고, 디지털 서명 및 공개 키 대신에, 익명 소유권 증명으로 전송된다. 그러나, 이러한 증명 방식은 상당히 많은 용량이 필요하며, 현재의 피트코인이 30kb인 것을 고려하면 실용적이지 않다. I.Miers는 이러한 방식이 대다수 비트코인 유저로부터 외면받을 것이라고 예상했다.

2.2.2 proof-of-work 의 작동 방식

비트코인 제작자인 Satoshi Nakamoto는, proof-of-work에 대한 의사결정 방식을 “1cpu당 1표”로 설명하였고, CPU에서 시작되는 가격 결정 방식(double SHA-256)을 주장하였다. 이용자들은 트랜젝션 기록을 바탕으로 투표를 하게 된다. 이 과정이 제대로 되어야 전체 시스템이 잘 작동할 수 있다.

이러한 모델의 보안은 두 가지 단점을 지니고 있다. 첫째로는 정직한 유저의 통제 하에 두려면 51퍼센트의 네트워크 마이닝 파워가 필요하다. 두 번째로, 해당 시스템의 발전 과정(버그 수정, 보안 수정 등)을 하려면 대다수의 사용자가 변화에 지지하고 동의해야만 한다. (사용자들이 지갑 소프트웨어를 업데이트 해야 하기 때문이다. 동일한 투표 방식은 또한 일부 기능의 도입에 대한 설문조사에서 활용된다.

이러한 모델을 통해 proof-of-work 가격 방식의 속성을 이해할 수 있다. 이러한 방식은 네트워크 내의 특정 참가자가 지나치게 강한 힘을 갖는 것을 방지해야 한다. 일반적인 하드웨어와 고비용의 커스텀 장치가 서로 동등해야 한다. 최근 비트코인에서 사용되는 SHA-256 방식의 경우 고성능 CPU보다 뛰어난 고성능 GPU와 ASIC의 등장으로 인해 이러한 동등성은 상실되었다.

비트코인의 경우 CPU소유자보다 GPU 및 ASIC 채굴자들이 더 많은 투표력을 갖기 때문에, 실제 투표력과 차이가 발생한다. “1CPU 1투표” 원칙을 어기기 때문이다.

일부에서는 적지 않은 참가자들이 의사결정을 행사하기 때문에, 해당 문제가 보안과 관련된 사항은 아니며, 대신에 의사결정 참가자들의 정직성이 중요하다고 주장한다. 이러한 주장에 대한 반론이 존재하는데, 값이 저렴하며 채굴에 특화된 하드웨어가 존재할 가능성 때문이다. 예를 들어, 만약 악의적인 채굴업자가 값싼 하드웨어로 채굴을 하게 된다고 가정해보자. 그리고 전세계의 해쉬레이트가 감소했다고 가정해보자. 잠깐일지라도 그는 chain fork 및

double-spend가 가능해진다. 이러한 상황의 가능성이 충분하다는 것을 이 글에서 설명할 것이다.

2.2.3 불규칙적인 생성

비트코인의 생성속도는 기존에 정해져 있다. 각 블록을 채굴하면 고정된 액수의 코인을 얻을 수 있다. 약 4년마다 이러한 보상은 반으로 줄어든다. 원래의 의도는 완만하게 지수함수형 붕괴(exponential decay) 하도록 하는 것이었으나 현실은 구분적선형(piecewise linear) 의 형태로 중단점(breakpoint)에서 비트코인 인프라에 대한 문제점이 발생할 수 있었다.

문제점이 발생하면, 기존의 보상에 비해서 절반의 가치만을 얻게 된다. 12.5와 6.25 BTC의 차이(2020년에 예상)는 그래도 괜찮아 보인다. 그러나, 50과 25BTC의 차이는 2012.11.28.에 발생하였으며, 채굴 업계에서 상당히 부적절한 일로 비춰졌다. 그림에서는 11월 말 네트워크 해쉬레이트가 급격히 감소했다는 상황을 나타내며, 보상이 절반으로 감소한 직후 일어난 일이었다. 악의적인 개인이 double spending attack을 일으킬 완벽한 순간이다.

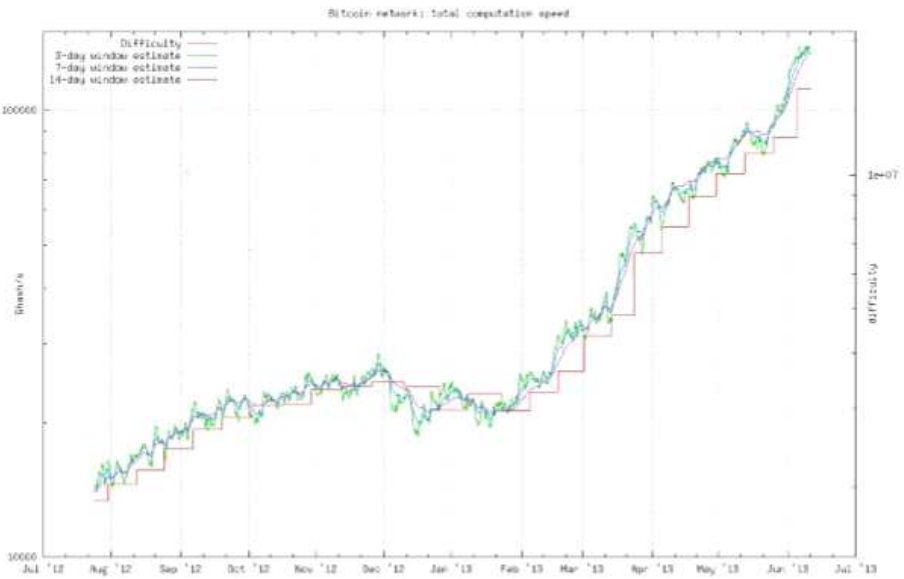

Fig. 1. Bitcoin hashrate chart
(source: http://bitcoin.sipa.be/ick_name% on 2018-11-01

2.2.4 수정이 어려움(Hardcoded Constants)

비트코인은 수정이 어렵다는 단점이 존재하고, 원래의 디자인(block frequency, 최대 통화 공급량, 확인의 개수 등)에 문제가 있다. 특히 가장 큰 문제는 단점을 빠르게 개선하지 못한다는 점이다. 적시에 수정하지 못할 경우 끔찍한 결과가 발생할지도 모른다.

수정이 어려운(hardcoded) 문제점 중 하나는 블록 사이즈 리미트가 250kb라는 것이다. 약 10,000건의 일반 거래를 감당하기에는 충분하다. 2013 초기에 거래량이 이 정도에 도달하였으며, 리미트를 올리고자 합의하였다. 지갑 버전 0.8에서 도입되었으며, 결과적으로 24-block chain split과 double-spend attack이 발생하게 되었다. 비트코인 프로토콜 자체에는 버그가 없었으나, 데이터베이스 엔진에 문제가 있었으며, 만약에 인위적인 블록 사이즈 제한이 없었다면 스트레스 테스트를 통해서 미리 알 수 있었을 것이다.

Constant는 또한 중앙화로 유도하기도 한다. 비트코인은 p2p 방식이지만, 대다수의 node가 특정 그룹에서 만들어낸 공식 클라이언트를 활용하고 있다. 이 특정 그룹은 프로토콜을 변화시키려 하며, 대다수의 사람들은 “정확성”과 관계없이 이러한 변화를 받아들이나. 일부 결정과정에서 토론은 과열되었으며 보이콧되기도 하였다. 커뮤니티와 개발자들이 특정한 부분을 반대할지도 모른다는 점을 나타낸 것이다. 따라서 이용자가 조장할 수 있는 변수를 가진 프로토콜을 사용하는 것이 논리적인 해결책으로 보여졌다.

2.2.5 방대한 스크립트

비트코인의 스트립트 시스템은 방대하고 복잡한 기능이다. 잠재적으로 한 객체는 복잡한 트랜젝션을 만들어낼 수 있으며, 일부 기능은 보안상의 이유로 제한되었고, 일부는 전혀 이용된 적이 없다. (송신자와 수신자 부분을 포함하여) 비트코인의 대다수의 트랜젝션은 다음과 같이 사용된다.

<sig> <pubKey> OP DUP OP HASH160 <pubKeyHash> OP EQUALVERIFY OP CHECKSIG.

이 스크립트는 164 바이트의 길이이지만, 유일한 목적은 수신자가 그의 서명을 확인하기 위한 암호 키를 가지고 있는지를 체크하는 것이다.

2.3 크립토노트 기술

2.3.1 추적 불가능한 트랜젝션

우리는 비추적성, 비연결성 조건을 모두 충족하는 완전히 익명의 트랜젝션 방식을 제안한다. 여기서 핵심적인 부분은 자주성이다. 송신자는 트랜젝션을 위해 다른 사용자 또는 신뢰할 수 있는 제3자와 협력할 필요가 없으며, 따라서 각각의 참가자들은 독립적으로 거래를 한다.

2.3.2 타원곡선 파라미터(Elliptic curve parameters)

우리는 EdDSA를 이용하려고 하며, 이 내용은 D.J. Bernstein에 의하여 개발되었다. 비트코인의 ECDSA와 유사하게 타원곡선 로그 문제(elliptic curve logarithm problem)에 근거하고 있으며, 우리의 방식은 미래에 비트코인에도 적용될 수 있을 것이다.

일반적인 파라미터는 아래와 같다.

q: a prime number; $q = 2^{255} - 19$;

d: an element of $\mathbb{F}_q$; $d = -121665/121666$;

E: an elliptic curve equation; $-x^2 + y^2 = 1 + dx^2y^2$;

G: a base point; $G = (x, -4/5)$;

l: a prime order of the base point; $l = 2^{252} + 27742317777372353535851937790883648493$;

$\mathcal{H}_s$: a cryptographic hash function $\{0,1\}^* \to \mathbb{F}_q$;

$\mathcal{H}_p$: a deterministic hash function $E(\mathbb{F}_q) \to E(\mathbb{F}_q)$.

2.3.3 용어

private ec-key is a standard elliptic curve private key: a number $a \in [1, l-1]$;

public ec-key is a standard elliptic curve public key: a point $A = aG$;

one-time keypair is a pair of private and public ec-keys;

private user key is a pair (a, b) of two different private ec-keys;

tracking key is a pair (a, B) of private and public ec-key (where $B = bG$ and $a \neq b$);

public user key is a pair (A, B) of two public ec-keys derived from (a, b);

standard address is a representation of a public user key given into human friendly string with error correction;

truncated address is a representation of the second half (point B) of a public user key given into human friendly string with error correction.

트랜젝션 구조는 비트코인의 구조와 유사하다. 트랜젝션 아웃풋이 가능하며, 대응하는 개인 키로 서명하여 다른 주소로 보낼 수 있다.

비트코인과의 차이점은, 한 유져가 독특한 개인 키와 공개 키를 가지고 있을 경우에, 송신자는 수신자의 주소와 랜덤 데이터에 근거해서 1회용 공개키를 만들어낸다. 이러한 방식으로, 동일한 수신자에 대한 트랜젝션은 1회용 공개 키를 통해 이루어진다. 특정 주소로 바로 전송되지는 않으며, 정당한 수신자만이 개인 키 부분을 복원하여 자금을 수신할 수 있다. 수신자는 ring signature을 이용하여 자금을 소비할 수 있으며, 소유권을 유지하면서 익명성을 유지할 수 있다. 프로토콜의 자세한 부분은 다음 항목에서 설명된다.

2.3.4 비연결성 지불

전통적인 비트코인 주소는, 일단 발행된 후에, 돈을 지불할 수 있는추상적인 identifier가 되며, 둘을 서로 묶게 되며, 수신자의 가명(pseudonyms)으로 연결(tie)된다. 만약 누군가 연결되지 않은(untied) 트랜젝션을 수신하려면, 그의 주소를 송신자에게 사적인 채널을 통해서 전송해야 한다. 만약 어떤 사람이, 같은 사람인지 증명되지 않은 다양한 트랜젝션을 수신하려 하면, 모든 다양한 주소를 생산해야 하며, 그 자신의 가명(pseudonym)으로 공개해서는 안된다.

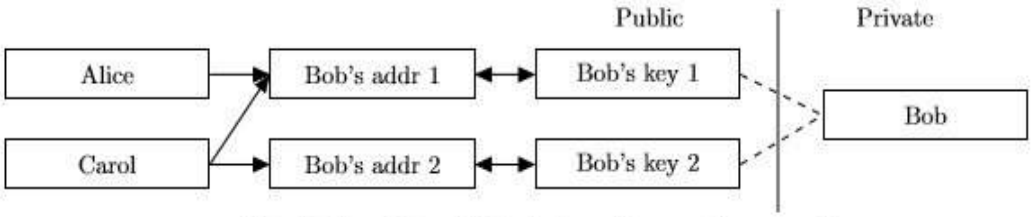

Fig. 2. Traditional Bitcoin keys/transactions model.

사용자가 단일 주소를 공개할 수 있으며, 무조건적으로 비연결성의 지불을 받을 수 있는 단일 주소를 발행할 수 있는 방식을 제안한다. 각각의 크립토노트 output은 기본적으로 공개 키 방식이며, 수신자의 주소와 송신자의 랜덤 데이터로부터 발생한다. 비트코인과의 주된 차이점은 모든 destination key가 기본적으로 독특하다는 것이다. (동일한 송신인이 동일한 데이터를 동일한 수신인에게 보내는 경우를 제외). 따라서, 이러한 방식에서 "주소 재사용"에 대한 문제는 없으며, 제3자가 특정 주소에 대한 전송을 확인할 수는 없다.

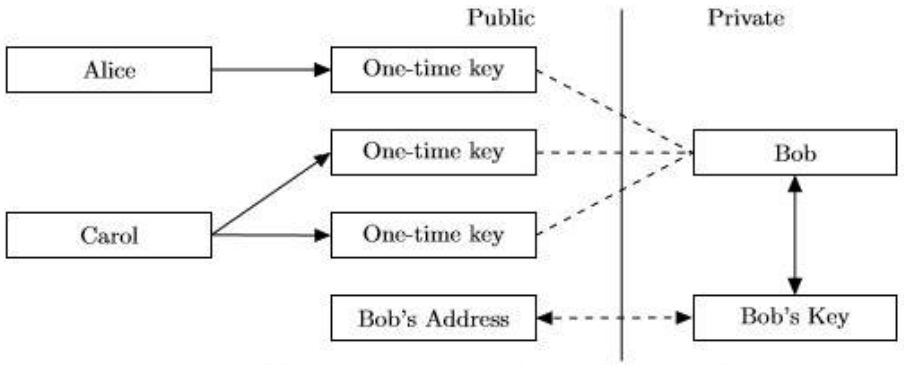

Fig. 3. CryptoNote keys/transactions model.

첫째로, 송신자는 Diffie-Hellman 교환을 이용하여 그의 데이터의 비밀을 공유하며, 수신자의 주소의 절반을 얻게 된다. 그리고 나서 공유된 비밀과 주소의 나머지 절반을 이용하여 1회용 destination key를 계산한다. 이러한 2단계의 과정에서 수신인은 2개의 서로 다른 ed-key를 준비해야 하며, 따라서 일반적인 크립토노트 주소는 비트코인 지갑 주소보다 거의 2배 정도 길다. 수신자는 또한 Diffie-Hellman 교환을 수행하여 상응하는 비밀 키를 해독해

야 한다.

일반적인 거래 과정은 다음과 같다.

1. Bob은 표준 주소를 공개하였으며, Alice가 Bob에게 전자화폐를 보내고자 한다. Alice는 주소를 분석하고 Bob의 공개키를 얻는다. (A,B)
2. Alice는 랜덤의 r(1,-2 중 하나)을 만들어내고, 1회용 공개키를 계산해낸다. 공개키 P = Hs(rA)G + B.
3. Alice는 output에 대해서 P를 destination key로 사용하고, R 값을 해석한다. R=rG(Diffie-Hellman 교환의 일부) 또 다른 공개 키를 활용하여 다른 output을 만들어낼 수도 있다. (수신인의 키가 다르면(Ai, Bi), 동일한 r에 대해서도 서로 다른 Pi가 도출된다.)

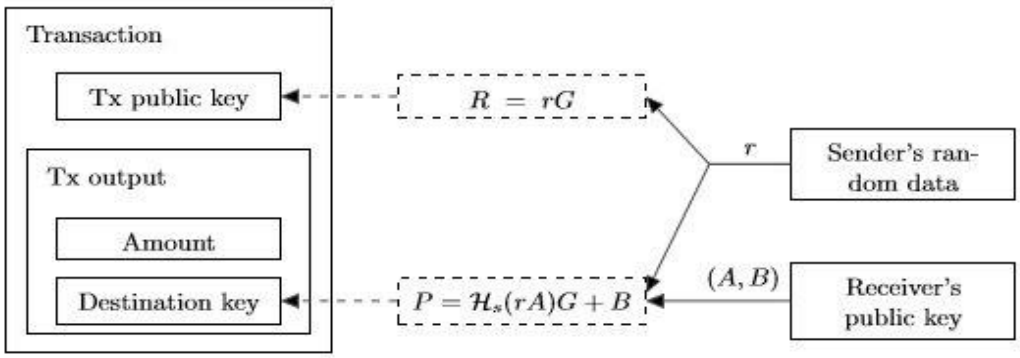

Fig. 4. Standard transaction structure.

4. Alice는 트렌젝션을 전송한다.
5. Bob은 개인키(a,b)를 이용하여 트랜젝션을 체크하며, P0 = Hs(aR)G + B라는 내용을 계산한다. 만약 Alice와 Bob의 트렌젝션이라면 aR = arG = rA and P' = P.
6. Bob은 상응하는 1회용 개인 키를 얻을 수 있다. x = Hs(aR) + b. 따라서 P = xG가 되며, x로 서명함으로써 원할 때에 output을 전송할 수 있게 된다.

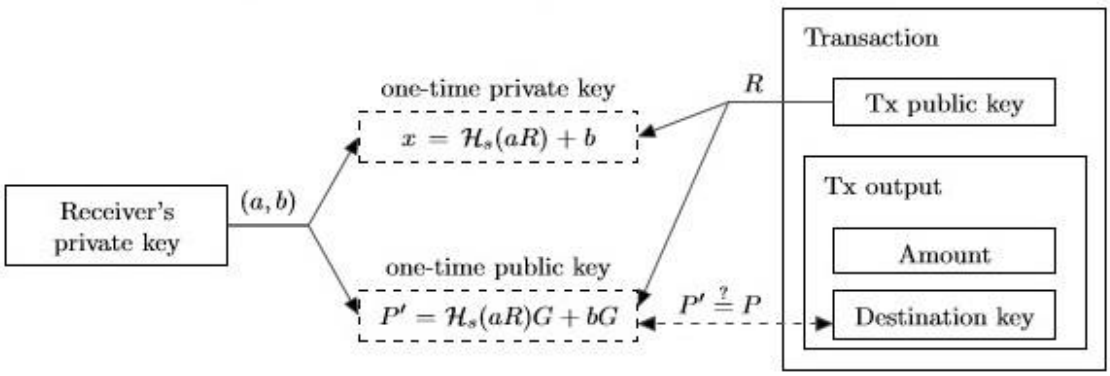

Fig. 5. Incoming transaction check.

결과적으로 Bob은 전자화폐를 지불받게 되며, 제3자는 연결 불가능한 1회용 공개 키가 활용된다. 추가적으로,

* Bob이 스스로의 Transaction을 "인지" 하면(step 5) 실질적으로 그의 개인 정보의 절반만을 이용한다. (a, B). 이 한 쌍은 또 tracking key로 알려져 있으며, 제3자 (Carol) 에게 전달될 수 있다. Bob은 새로운 트랜젝션에 대한 진행을 Carol에게 위임할 수 있다. 특히 대역폭이 낮거나 성능이 떨어지는 경우(스마트폰, 하드웨어 지갑 등) 유용하게 사용이 가능하며, Bob의 개인 키가 없다면 1회용 비밀 키를 알 수 없으므로, Carol을 완전히 신뢰하지 않아도 된다.

* 만약 Alice가 Bob의 주소로 보낸 트랜젝션을 확인하려면, r을 공개하거나, zero-knowledge protocol을 사용하여 그녀가 r을 안다는 것을 입증하면 된다. (예를 들어 트랜젝션을 r로 서명할 수 있다.)

* 만약 Bob이 연결 가능하고, 조사 가능한 주소를 원한다면 tracking key를 공개하거나, 생략된 주소를 사용하면 된다. 이 주소는 단지 하나의 공개 ec-key만을 의미하며, 프로토콜이 요구하는 나머지 부분은 다음과 같이 도출된다. a = Hs(B) 그리고 A = Hs(B)G. 두가지의 경우 모두에서 모두들 Bob이 트랜젝션을 수신했다는 것을 알 수 있다. 그러나 물론 비밀 키 b를 알지 못하면 어느 누구도 해당 자금을 소비할 수 없다.

2.3.5 일회용 ring signature

1회용 ring signature에 기반하면, 이용자들은 무조건적인 비연결성을 갖게 된다. 안타깝게도 일반적인 암호화폐의 암호화된 서명을 통해 개별적인 송신인과 수신인들에게 추적할 권한을 얻을 수 있다. 기존 전자화폐와 차별화된 서명 방식을 사용한다는 것이 해결책이다.

우선 전자화폐와는 별도로 ring signature 알고리즘을 설명하겠다.

1회용 ring signature은 4개의 알고리즘을 포함한다. (GEN, SIG, VER, LNK):

GEN: takes public parameters and outputs an ec-pair (P, x) and a public key I.

SIG: takes a message m, a set $\mathcal{S}'$ of public keys $\{P_i\}_{i \neq s}$, a pair (P_s, x_s) and outputs a signature σ and a set $\mathcal{S} = S' \cup \{P_s\}$.

VER: takes a message m, a set $\mathcal{S}$, a signature σ and outputs "true" or "false".

LNK: takes a set $\mathcal{I} = \{I_i\}$, a signature σ and outputs "linked" or "indep".

프로토콜 이면의 아이디어는 상당히 단순하다. 한 사용자가 1개의 특정한 공개키가 아니라 여러개의 공개키 세트로 체크될 수 있는 서명을 한 사용자가 생성한다. 소유주가 동일한 열쇠 짝을 이용하여 두 번째 서명을 발행하지 않는 한, 서명자의 아이덴티티는 공개 키의 동일한 세트 중에서 구별할 수가 없다.

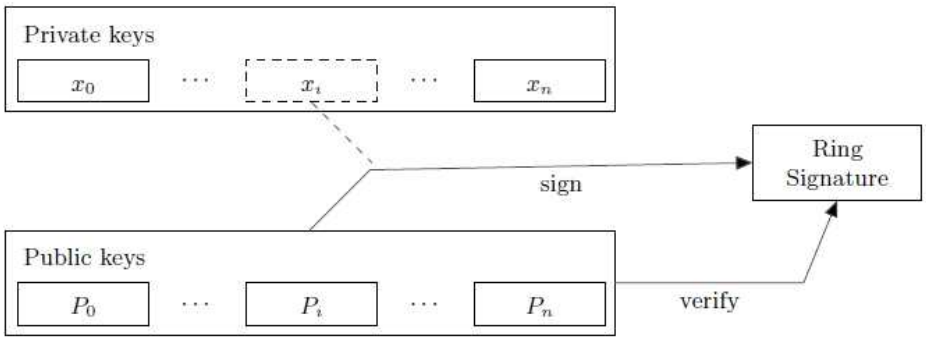

Fig. 6. Ring signature anonymity.

GEN : 서명인은 랜덤한 비밀키 x ∈ [1,l−1]를 선택하며, 상응하는 공개키 P = xG를 계산한다. 추가적으로 또 다른 공개키 I = xHp(P)를 계산해야 하며, 이러한 것을 “키 이미지”라고 부른다.

SIG : 서명인은 기술을 활용하여 1회용 ring signature를 비상호작용적인 zero-knowledge proof와 함께 생성한다. 서명인은 다른 이용자들의 공개 키 Pi, 자신만의 keypari (x,P), Key image I로부터 랜덤한 하위집합 S0를 선택한다. S(그의 공개키는 Ps)에서의 서명인의 비밀 인덱스를 0 ≤ s ≤ n 라고 하자.

서명인은 랜덤의 {qi ¦ i = 0...n}를 선택하며 (1...l)로부터 {wi ¦ i = 0...n,i 6= s}를 선택하며, 다음의 변환에 적용된다.

$$L_i = \begin{cases} q_i G, & \text{if } i = s \\ q_i G + w_i P_i, & \text{if } i \neq s \end{cases}$$

$$R_i = \begin{cases} q_i \mathcal{H}_p(P_i), & \text{if } i = s \\ q_i \mathcal{H}_p(P_i) + w_i I, & \text{if } i \neq s \end{cases}$$

The next step is getting the non-interactive *challenge*:

$$c = \mathcal{H}_s(m, L_1, \ldots, L_n, R_1, \ldots, R_n)$$

Finally the signer computes the *response*:

$$c_i = \begin{cases} w_i, & \text{if } i \neq s \\ c - \sum_{i=0}^{n} c_i \mod l, & \text{if } i = s \end{cases}$$

$$r_i = \begin{cases} q_i, & \text{if } i \neq s \\ q_s - c_s x \mod l, & \text{if } i = s \end{cases}$$

The resulting signature is $\sigma = (I, c_1, \ldots, c_n, r_1, \ldots, r_n)$.

VER : 역변환을 이용하여, 확인자는 서명을 체크할 수 있다.

$$\begin{cases} L'_i = r_i G + c_i P_i \\ R'_i = r_i \mathcal{H}_p(P_i) + c_i I \end{cases}$$

결과적으로, 확인자는 위 그림을 찾게 되며,

만약 등식이 성립한다면, 알고리즘 LNK를 작동하게 된다. 그렇지 않다면 확인자는 서명을 거부한다.

LNK : 확인자는 I가 이전의 서명에서 사용되었는지를 조사한다. 다중의 사용들에서 두 개의 서명들이 같은 비밀 키에서 만들어졌다는 것을 시사하게 된다.

프로토콜의 의미 : L 변환을 적용함으로써 서명자는 그러한 x가 적어도 Pi=xG라는 사실을 입증하게 된다. proof를 반복 불가능하게 하기 위해서 키 이미지를 I=xHp(P)로 설정한다. 서명인은 같은 계수(ri,ci)를 활용하여 거의 동일한 명제인 “그러한 x가 적어도 Hp(Pi)=I・xˆ-1이라는 사실을 안다.”는 것을 증명한다.

만약 x에서 I로의 대응이 injection mapping이라면
1어느 누구도 키이미지로부터 공개키를 복원할 수 없으며, 서명인을 알 수 없다.
2서로 다른 I들과 동일한 x를 가지고 두 개의 서명을 만들어낼 수 없다.

2.3.6 표준 크립토노트 트랜젝션

비연결적 공개키와 비추적성의 ring signature이라는 2가지 방법을 결합하면, Bob은 원래의 Bitcoin 방식과 비교하여 발전된 수준의 프라이버시를 갖게 된다. Bob은 개인키 하나 (a,b)만 가지고 있으면 충분하며, (A, B)를 공개하여 익명의 트랜젝션을 송수신 할 수 있게 된다.

각 트랜젝션을 유효화하기 위해서, Bob은 추가적으로 단지 2개의 타원곡선(elliptic curve)을 다중 발행하고, Bob 소유의 트랜젝션인지를 확인하기 위하

여 output 당 1개를 추가하게 된다. Bob은 각각의 output에 대하여 1회용 keypair (pi, Pi)를 복원하며, 지갑에 저장하게 된다. 단일한 트랜젝션인 경우에만 동일 소유주의 input으로 확인될 수가 있다.

ring signature에 대해서 Bob의 input은 효과적으로 익명성이 유지될 수 있다. 트랜젝션이 누구의 것인지에 대한 추론이 어려우며, 이전의 th유주인 Alice 또한 다른 제3의 관찰자와 같이 정보가 없다.

만약 Bob이 n개의 외부로의 output을 같은 금액으로 전송하고, 섞어 버린다고 가정하자. Bob 스스로는 (어느 누구라도) 이러한 지불 중 어느 것이 전송되었는지 알 수가 없다. output은 수천개의 서명에서 추상적인 요소(ambiguity factor)로 활용될 수 있으며, 숨김의 대상이 될 수는 없다. 이미 사용된 키 이미지 집합으로부터 체크함으로써, LNK 단계에서 double spend 검사가 발생된다.

Bob은 추상 정도(ambiguity degree)를 스스로 설정할 수 있다. n=1이라는 의미는 그가 output을 전송했을 확률이 50퍼센트라는 의미이다. n=99일 때는 1퍼센트의 확률을 나타낸다. 결과적인 서명은 선형적으로 O(n+1)로 증가된다. 따라서 Bob의 익명성 비용이 향상되면 트랜젝션 수수료가 높아진다. 또 Bob은 n=0이라고 설정할 수 있으며, 스스로의 ring signature를 단지 하나의 구성요소로도 만들 수 있다. 하지만 이러한 경우 그는 익명성을 전혀 보장받을 수 없다.

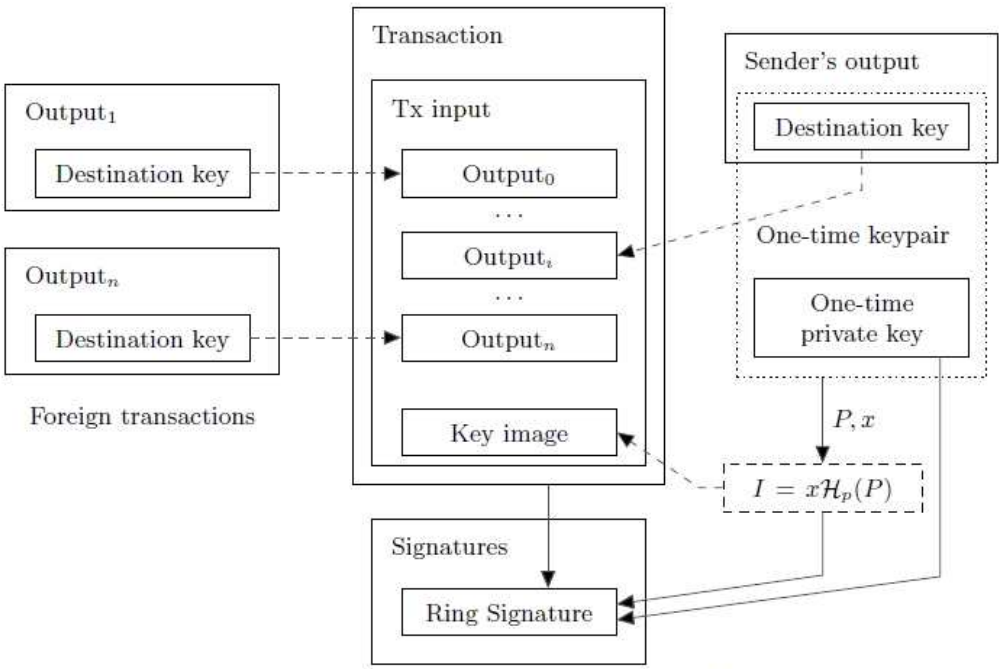

Fig. 7. Ring signature generation in a standard transaction.

2.3.7 평등화된 Proof-of-work

이 부분에서 새로운 proof-of-work 알고리즘을 제안하고자 한다. CPU(다수) 마이너와 GPU/FPGA/ASIC(소수) 마이너 사이의 차이를 줄이기 위한 것이다. 일부 마이너가 우위를 선점하는 것은 적절한 일이지만, 그들의 투자는 power에 대해서 적어도 선형적으로 증가해야 한다. 일반적으로 특수 목적의 장치들(주 : ASIC 등)은 가능한 수익성이 적어야 한다.

2.3.6.1 Related works

원래 Bitcoin의 proof-of work 프로토콜에서는 CPU에 중점을 둔 가격 결정 함수 SHA-256을 사용하였다. 주로 basic logical operators로 구서되었으며, 프로세서의 계산 속도에 따라서면 바뀌기 때문에 multicore/conveyer 의 적용에 완벽히 적절하였다.

하지만 현대적인 컴퓨터의 경우 초당 operation 숫자에 의해서만 제한되는

것이 아니라, 메모리 사이즈에 의해서도 제한을 받는다. 프로세서 간의 속도 차이가 상당할 수는 있으나 메모리 사이즈는 큰 차이가 없다.

메모리를 기준으로 가격을 결정하는 함수는 Abadi에 의하여 맨 처음 소개되었으며 "주로 메모리에 접속한 시간에 의하여 계산 시간이 결정되는 함수"라고 정의되었다. 핵심적인 아이디어는 큰 블록 데이터인 스크래치패드를 상대적으로 느리게 접속될 수 있는 메모리(ram 등)에 할당하는 알고리즘을 만들고, 그 안에서 "예측 불가능한 sequance of locations의 접속을 수행"하는 것이다. 블럭이 충분히 커야만 각각의 access 마다 다시 계산하는 것보다 저장하는 것이 유리해진다. 이 알고리즘은 내부적인 병렬성(internal parallelism)을 방지해야 하며, 따라서 N의 동시적인 쓰레드는 N배 많은 메모리를 요구해야 한다.

Dwork는 이러한 접근 방식에 대해 연구 및 체계화 하였으며, 이를 통해 가격 결정 함수의 또 다른 방식인 "Mbound"가 탄생할 수 있었다. F.Coelho은 가장 효과적인 솔루션 "Hokkaido"를 제안했다.

현재 보편적으로 거대한 array 내에서 유사 난수 검색(pseudo-random searches)을 하는 방식은 "scrypt"라고 일컬어진다.(C. Percival) 이전의 함수들과 달리 핵심적인 derivation에 주목하고 있으며, proof-of-work system과 차이점이 존재한다. 이러한 사실에도 불구하고, scrypt는 우리의 목적을 충족할 수 있는데, 부분적인 해쉬 변환 문제에서 가격 결정 함수로 잘 작동한다는 것이다. 예를 들면 Bitcoin에서의 SHA-256이 있다.

현재 이미 Litecoin에 scrypt는 적용되었으며 일부 다른 Bitcoin 포크들에도 적용되었다. 그러나 이러한 적용은 사실상 메모리 기반의 접근방법이 아니다. "메모리 접속 시간 / 총 시간"은 공간이 충분하지 않은데, 단지 128KB만을 사용하기 때문이다. 이를 통해 GPU 채굴자들은 거의 10배 더 효율적으로 채굴이 가능하며, 저렴하면서도 채굴효율이 좋은 장비가 등장할 가능성이 충분하다.

게다가, 스크립트를 작성하는 것으로 인해, 스크래치패드의 모든 블록이 이전의 것으로부터 발생되기 때문에, 메모리 사이즈와 CPU 속도가 반비례적으로 움직이게 된다. 예를 들어, 모든 두 번째 블록을 저장할 수 있으며, 필수적인 경우에만 다른 모든 블록들을 느린 방식으로 재계산할 수 있다. 유사 난수 인덱스(pseudo-andom index)들은 일괄적으로 배분되는데, 따라서 추가적인 블록의 재계산은 기댓값은 1/2N이다. (N은 반복수). scratchpad를 준비하고 모든 반복에 대해서 해시하는 작업과 같은 시간 독립적(constant time) operation들로 인해서 전체적인 계산 시간은 절반보다는 덜 증가하게 된다. 2/3의 메모리 사용을 줄이려면 N의 추가적인 재계산이 필요하다. 9/10을 줄이려면 4.5의 추가적인 재계산이 요구된다. 정리하면 만약 모든 블럭의 1/s만을 저장하게 되면 (s-1)/2 만큼을 곱한 것보다 덜 증가하게 된다. 바꾸어 말하면, 현대의 CPU 보다 200배 빠른 CPU는 320 byte의 scratchpad 만을 저장할 수 있다.

2.3.6.2 새로운 알고리즘의 제안

proof-of-work 가격 설정 함수에 대해서 새로운 메모리 기반(memory-bound) 알고리즘을 제안한다. 느린 메모리에 대한 랜덤 엑세스에 의존하게 되며, 레이턴시 의존성을 강조한다. 스크립트와는 다르게, 모든 새로운 블록(64바이트 길이)은 이전의 모든 블록에 의존적이다. 결과적으로 매모리 절약기(“memory-saver”)는 계산 속도를 기하급수적으로 증가시킬 것이다.

우리의 알고리즘은 다음의 이유로, 인스턴스당 2MB 정도를 요구한다.

1. 최신 CPU의 코어당 L3캐쉬에 적당하며, 몇 년 안에 주류가 될 CPU의 사양이다.

2. 최신 ASIC 파이프라인에 대해서 1MB의 내부 메모리는 부적절하다.

3. GPU의 uddn tnqor의 인스턴스를 동시에 처리할 수 있으나, GDDR5 메모리는 CPU의 L3캐쉬보다 느리고, 대역폭은 넓지만 랜덤 엑세스 속도는 낮다.

4. scratchpad가 확장되면 필연적으로 반복적 계산이 증가하게 되며, 전체적인 시간이 증가하게 된다. 신뢰성이 낮은 p2p 네트워크에서 많은 계산량은 심각한 취약점으로 남을 수 있는데, 왜냐하면 node는 모든 새로운 블록의 proof-of-work에 대하여 체크할 의무가 있기 때문이다. 만약 node에서 각각의 해쉬 평가에 대해 상당한 시간을 소모한다면, 임의 작업 데이터로 가득찬 가짜 오브젝트들로 인한 Ddos 공격에 취약해진다. (nonce value)

5. 더 많은 장점들.

6. 안정적인 통화량 발행

크립토노트 전자 코인의 상한값(upper bound)은 MSupply = 2^54 -1 원자단위(atomic units)이다. 이러한 것은 기술적인 제한값이며 “N개의 코인이 충분하다” 라는 직관적 방식에서 계산된 것이 아니다.

발행 과정을 안정적으로 유지하기 위하여 블록 리워드에 대해 다음과 같은 공식을 사용한다.

BaseReward = (MSupply − A) >> 18

여기에서 A는 이전에 생산된 코인의 양을 의미한다.

2.3.7 수정 가능한 파라미터

2.3.7.1 난이도

크립토노트에서는 모든 블록마다 난이도를 변경시킨다. 네트워크 해쉬레이트가 급격하게 성장하거나 감소할 때에 대한 반응시간이 낮아질 수밖에 없

고, constant block rate로 고착된다. 원래의 Bitcoin 방식에서는 마지막 2016개의 블록간의 목표 기간과 실제 기간을 비교하게 되고, 이를 현재의 난이도에 대한 배수(multiplier)로 적용한다. 이러한 비트코인의 방식에 따르면 난이도가 급증 급락한다는 점이 단점이다.

크립토노트의 기본적인 알고리즘은 node에 의하여 계산된 모든 work를 합하고, 그들이 소비한 시간으로 나누는 것이다. 일의 단위는 각각의 블록의 난이도 값에 상응한다. 하지만 time stamp에서의 부정확성과 비신뢰성 때문에 블록 사이의 정확한 시간 간격을 알아내기는 어렵다. 만약 한 유저가 time stamp를 미래로 전환한다면 다음의 interval은 감소하거나 심지어 음수가 될 것이다. 이러한 사례가 거의 없을 것으로 생각되며, 단지 time stamp를 정리하고 초과분을 소거할 것이다.(20퍼센트 정도) 나머지 값들의 범위는 80퍼센트의 상응하는 블록에 대하여 소비한 시간 값이다.

2.3.7.2 사이즈 제한

사용자들은 블록체인을 저장하는 것에 대하여 지불하며, 사이즈에 해당하는 투표 권한을 가진다. 모든 채굴자들은 수익과 지용의 균형 사이에서 절충을 선택해야 하는데, fee와 블록을 만드는 것에 대한 자신만의 “soft-limit”에 대한 균형이다. 또 위조 트랜젝션을 막기 위해서 최대 블록 사이즈에 대한 핵심 규칙은 필수적이다. 하지만 이러한 값은 수정할 수 있어야 한ᄃᆞ.

Mn이 N블록 사이즈에 대해서 중간 값이라고 가정하자. 그러면 블록을 받아들이는 데에 대한 “hard-limit”은 2 · MN이 된다. 이러한 것을 통하여 블록체인의 bloating을 방지하며, 시간에 맞게 서서히 성장하도록 허락한다.

트랜젝션 사이즈는 명시적으로 제한될 필요가 없다. 블록의 사이즈에 따라 달라지며, 만약 누군가가 수백개의 input / output을 이용하여 거대한 트랜젝션을 보내고자 한다면 (혹은 ring signature에서 큰 추상성을 가질 경우), 충분한 수수료를 지불함으로써 트랜젝션을 진행할 수 있다.

2.3.7.3 트랜젝션 스크립트

크립토노트는 굉장히 최소화된 스크립트 서브시스템을 가지고 있다. 송신자는 특정한 표현 Φ = f (x1, x2, . . . , xn)을 규정하는데, n은 destination 공개 키 C:\Users\ddd\AppData\Local\Temp\Hnc\BinD 의 숫자이다. 5 binary의 오퍼레이터만 지원되며, min, max, sum, mul, cmp이다. 수신자들이 이 지풀을소비하게 되면, 0 ≤ k ≤ n 의 서명을 생산하고, 트랜젝션 input으로 전송하게 된다. 확인 과정은 단순히 s Φ with xi = 1를 평가하여 공개키 Pi 에 대한 유효한 서명을 체크하며, Xi=0임을 확인한다. 확인자는 만약 Φ > 0인 경우에 proof를 받아들인다.

간단함에도 불구하고, 이러한 방식으로 가능한 모든 경우에 대처할 수 있다.

o multi-/threshold 서명. 비트코인 스타일의 “N 개중 M ro” multi 서명(수신자는 적어도 0 ≤ M ≤ N 의 유효한 서명을 공급해야 한다.) Φ = x1+x2+. . .+xN ≥ M 가중 threshold 서명(일부 키는 다른 키보다 중요할 수 있음)은 Φ = w1 · x1 + w2 · x2 + . . . + wN · xN ≥ wM로 표현될 수 있다. 마스터키는 Φ = max(M · x, x1 + x2 + . . . + xN) ≥ M에 상응한다. 이러한 방식으로 복잡한 상황을 간단하게 표현할 수 있다.

o 암호의 보호. 비밀 안호 s를 보유한 것은 개인 키에 대한 지식을 보유한 것과 동등하며, 확정적으로 암호 k=KDF(s)로부터 도출된다. 따라서 수신자는 k key 하의 또다른 서명을 제공함으로써 비밀번호를 안다는 사실을 입증할 수 있다. 송신자는 단순히 자신의 output에 상응하는 공개 키를 추가하며 s 된다. 이러한 방식은 Bitcoin에서 사용되는 “transaction puzzle” 보다 상당히 안전하다.

o Degenerate cases. Φ = 1 인 상황에서는 어느 누구든지 돈을 사용할 수 있다. Φ = 0 인 상황에서는 해당 output이 영원히 사용 불가능함을 나타낸다.

만약 공개키와 통합된 output script가 송신자에게 지나치게 클 경우에, 특별한 output type을 이용할 수 있다. 송신자가 단지 그것에 대한 해쉬를 공급하는 반면 수신자는 이 데이터를 그의 input으로 보내게 될 것이다. 이러한 접근은 Bitcoin의 "pay-to-hash"와 유사한 방식이다. 새로운 스크립트 명령을 추가하는 대신에, 데이터 구조 수준에서 이러한 케이스를 다룬다.

2.4 결론

비트코인의 주된 단점을 조사하였고, 가능한 대안을 제시하였다. 이러한 장점과 우리의 개발은 새로운 크립토노트라는 전자 화폐 시스템을 만들어 낸다. 크립토노트는 비트코인의 대항마가 될 것이다.

노벨상 수상자 Friedrich Hayek에 따르면 여러 독립된 화폐들의 공존이 긍정적 효과를 가져온다고 한다. 각 화폐의 발행인(혹은 개발인)은 기능을 개선함으로써 사용자들을 끌어들인다. 화폐는 재화와도 유사하다. 독특한 장단점이 존재하며, 가장 편리하고 신뢰받는 화폐가 최대의 수요를 얻게 될 것이다. 비트코인을 능가하는 코인이 있다고 가정해보면, 비트코인의 개발 속도가 빨라지고 개선된다는 것을 의미한다.

크립토노트가 비트코인을 완전히 대체할 것이라고 생각하지는 않는다. 강력한 화폐가 2개 혹은 이상이라는 것은 좋은 점이다. 전자 화폐 업계에서 다양한 프로젝트들이 동시에 진행되는 것은 자연스러운 현상이다.

3. PPP(INTEGRATION BUSINESS RELIABILITY) COIN 개발의 목적

피피피 코인(PPP) 개발의 목적은 그 많은 코인들과 다름없는 또 하나의 새로운 코인 상품을 개발하여 보급하자는 의미가 아니며, 화폐로서의 가치를 갖고 순기능을 할 수 있도록 하는 실질적인 P2P 피피피 코인 지불(PPP Coin)시스템 플랫폼을 구현하려고 하는 것이다.

이를 통하여 전자화폐가 가진 암호화폐의 장점들을 극대화하고 보다 효율적인 기술을 보강하여 더 많은 사람들에게 편리성과 안전성과 안정된 가치성을 부여하고자 한다.

한 걸음 더 나아가 피피피 코인(PPP)을 이더리움 블록체인을 기반으로 한 장점을 극대화 하고, 통합 P2P 시스템 플랫폼을 적용하여 일원화 할 뿐 아니라 통합 보안 P2P 시스템 플랫폼을 탑재하여 개인은 물론 기업의 사유재산을 자유롭게 활용하고 사용할 수 있는 것은 물론 안정적으로 관리하게 함으로써 자신이 보유한 재산을 지키고 화폐시장의 무질서를 재편하는데 기여하고자 한다.

현재 우후죽순으로 늘어나 포화 상태인 코인들의 양에 비해 실질적으로 활용되고 있는 코인은 손에 꼽을 정도로 미미하다. 이것은 코인의 생산이 화폐로서의 순 기능을 목적으로 하기 보다는 투기를 위한 역기능이 많은 이유일 것이다. 코인은 코인으로써 가져야 할 순기능의 목적을 성취하지 못했을 때 미래 화폐발전에 대한 부정적 영향을 끼칠 뿐 아니라, 시각을 같이하는 사회 전반에 막대한 금전적 손실의 피해를 유발함은 물론 노동의 가치마저 상실하게 하고 가치에 대한 박탈감까지 유발하는 등의 문제점만 발생시킬 수 있는 점을 유의하여야 한다.

4. 코인 발행 및 채굴

피피피 코인(PPP Coin)발행과 채굴의 기능을 동시에 수행토록 구성 되었으며, 발행한 코인을 구매자에 의해 구매가 이루어졌을 시 코인이 생성되며, 채굴 또한 채굴 채득 방법에 따라 채득한 코인은 '거래자 고유코드'를 생성하여 보관한다.

피피피코인(PPP COIN)의 dApp 아키텍쳐는 운영주체에 대하여 신뢰가 필요없거나 최소화할 수 있도록 하며, 투명한 운영 원칙과 규칙 관철 용이할 뿐만 아니라 보안의 향상과 프라이버시 보호에 적합하도록 설계하였다. 또한 이미 투자된 자원의 활용도를 극대화 할 수 있도록 하고, 국가별 규제를 넘어선 글로벌 서비스에 용이하다는 강점도 갖도록 했다. 특히, 소수기업의 서비스(이윤)의 독점화 해소에 가장 큰 장점을 지닌다.

피피피 코인(PPP Coin)의 dApp을 이용, QR코드 또는 바코드 생성기를 이용하여, 부호를 생성한 후 편리하게 이용한다. 피피피 코인(PPP Coin)은 이더리움 블록체인 기반의 연동운영이며, 토큰으로 일괄 발행하고 발행된 일정의 피피피 코인(PPP Coin)을 다양한 채굴방식의 시스템 기반으로 조성하여 하기와 같은 방법으로 사회 환원의 환경을 조성하고 진행한다.

1) 모바일 기기을 이용한 채굴 [모바일 채굴]
2) 쇼핑몰을 통한 엄선된 상품 거래 활성화 [쇼핑몰 거래 코인]
3) 상거래시 거래량에 따른 코인 지급 [거래 채굴]
4) 광고 구독에 따른 보상을 채굴로 지불 [광고 채굴]
5) 개인 보유 코인을 회사에 맡겨서 이자 지급 [이자 채굴]
6) 개인간 코인 거래 활성화 [P2P거래]
7) 특화 단지의 거래 및 유통코인 [관광코인]
8) 코인 전문기업으로써의 각종 코인 채굴사업 지원 [각종코인채굴]

9) 모바일지갑을 이용한 개인간 모바일 통화 지원 [모바일 통화 컨텐츠]

10) 다양한 컨텐츠의 지속적인 업데이트 [컨텐츠 강화]

5. 거래 경로 정보

피피피 코인(PPP Coin)은 dApp을 이용하여, ‘거래자 고유코드’를 생성하여 보관하며, 그리고 상품을 중개 또는 구매하기 위하여, 결제 대금을 지급하고, 상품을 구입했다 는 증명을 위하여, 상품에 부착된 ‘생산품 주소’를 피피피코인 dApp의 ‘상품 이동’을 이용하여 저장 한다. 이 과정을 통해서, 블록체인에 저장된 정보를 통하여 확인이 가능하다.

6. 피피피코인의 가치 향상

피피피 코인(PPP Coin)은 개발 주체로부터 기 발행된 피피피 코인(PPP Coin)을 구매하거나 또는 채굴하여 채득하는 경우 다음과 같은 가치를 예상한다.

첫째, 블록체인의 보안기술을 기반으로 한 기술적인 미래 가치.

둘째, 생산 발행되는 피피피 코인(PPP Coin)의 희소성과 쇼핑몰, P2P거래, 가맹점을 이용한 활성화 방안을 통한 확장성과 그 확장에 따른 보안 솔루션을 통한 특성에 따라 피피피 코인의 가치향상은 지속적으로 향상될 것으로 본다.

또한, 회사는 정책적으로 이를 관리 보완하며, 장기적으로 안정적 수익을 얻을 수 있도록 지속적으로 지원 보장할 것이다.

피피피 코인(PPP Coin)의 가치향상의 또 다른 하나는 코인의 시장성이다. 피피피 코인(PPP Coin)을 사용하는 유저의 성장은 곧 코인 가치의 향상에 기여하게 된다. 이에 통합 멤버십 솔루션을 통해 운영되는 인프라구성의 최적

화된 피피피 코인(PPP Coin)의 가치 향상에 막대한 영향을 끼치게 될 것으로 본다.

7. PPP 코인 제안

피피피 코인(PPP Coin)의 접근 방식은 일반 사용자가 쉽게 읽을 수 있으며, 구현의 메카니즘에 따라 계산적으로 결정 가능한지 수학적으로 증명할 수 있는 도메인 특화 언어를 적용하는 것이다.

그래서 우리는 피피피 코인(PPP Coin)을 통해 기술에 기반하여 안전하고 편리한 암호화폐의 표준 플랫폼을 개발하는 것을 목표로 한다.

추가적으로 피피피 코인(PPP Coin)을 통해 우리는 암호화폐와 관련해 공통적으로 반복되는 문제들을 해결하려고 한다. 피피피 코인(PPP Coin)은 이러한 제안들을 통해서 전체 코인 생태계의 발전을 위해 쓰일 수 있는 기술과 보안의 표준화에 개발의 초점을 두었다.

암호화폐의 생태계에서 대부분의 경우가 탈중앙형 화폐로써 제한된 실사용처로 인해 투기의 온상이 되는 경향이 있다.

우리는 화폐 가치에 대한 본질적인 접근을 시도하고, 화폐가 얼마나 유용하게 쓰여지고 있는가 하는 사실적이고 현실적인 연동적 성격으로 생각하기 때문에, 피피피 코인(PPP coin) 개발팀은 피피피 코인(PPP Coin)을 사용하는 어플리케이션을 다양한 부분에 접목할 수 있도록 지속적으로 출시할 예정이다.

새로이 개발된 어플리케이션은 코인의 거래 가치를 높이는 것은 물론 피피피 코인(PPP Coin) 사용자들이 상품을 구매 및 거래로 사용하는 실제 생활코인으로써의 확보하는데도 도움이 될 것이다.

8. Trust Contracts

1) 개 요

피피피 코인(PPP Coin)은 Web Ontology Language (OWL)8과 Timed Automata Language (TAL)로 구성된 Owlchain 기술을 사용하고자 한다. 이 아키텍처는 표현력을 확장하면서도 계약의 안전하고 정확한 실행을 지원할 수 있는 결정가능성을 유지하도록 설계되어 있다.

피피피 코인(PPP Coin)은 블록체인 위에 만들어진 OWL chain을 기반으로 한 계약을 Trust Contracts라고 한다.

2) 배 경

블록체인에서 계약을 개발하는 데는 두 가지 기본 접근 방식이 있다. 하나는 가상머신 위에서 유연한 프로그래밍 언어를 사용하는 것이고, 다른 하나는 다소 덜 유연하지만 결정가능성을 가진 도메인 특화 언어(domain-specific language)를 사용하는 것이다.
피피피 코인(PPP Coin) 팀은 두번째 방법을 선택했다. 가상머신에 기반을 둔 암호화폐와 달리, 추론 엔진은 시맨틱 웹 기술에 기반하므로 코드가 실행되기 전에 코드로부터 정보를 추론할 수 있다.

계약은 결정가능성을 가지고 있고, 계약의 결과는 분명히 확인된다. 이는 계약 기능을 가진, 안전하고 지속 가능한 통화를 구축하는 데 있어 핵심적인 개념이다.

Ethereum은 시장 매커니즘을 사용하여 이 문제를 해결하려고 복잡성에 가격을 적용했지만, 우리는 더엄격한 OWL 및 TAL 방식의 접근이 블록체인 기반의 계약을 개발하는데 있어서 보다 안전한 환경을 제공 할 것이라고 믿는다.

3) 개 발

웹 페이지를 제공하는데 사용되는 HTML, HTTP, RDF 및 OWL과 같은 표준 웹 기술을 기반으로 개발할 때, 이 기술들은 컴퓨터가 예측 가능하게 해석할 수 있는 방식으로 정보를 공유하도록 확장될 수 있다.

OWL과 RDF 모두 모호하지 않은, 구조화된 데이터 분류체계를 작성하는데 사용될 수 있다. Ian Grigg는 이러한 특성을 이용하여 지불 시스템의 모든 것과 연관된 계약인 Ricardian Contracts 개념을 제안했다9. OWL과 RDF가 비슷한 특성을 나타내지만, 현재 RDF 표준은 P-time 완전성을 지원하지 않는다. 그러나 이전에 제시된 사실 또는 공리의 집합에서 논리적인 결과를 추론하는 도구인 Reasoners를 사용하여 OWL 표준은 P-TIME 복잡성을 보장한다. 이것은 계약을 실행하는데 걸리는 시간을 사전에 결정할 수 있다는 것을 의미한다. 이 특성이 OWL을 Trust Contracts의 기반 언어로 선택하게 된 핵심 이유이다.

OWL DL(description logic)은 OWL의 하위 언어로, “계산의 완전성을 유지 보유 하면서도 가능한 최대 표현력을 제공하도록 설계되었다.“9 OWL DL은 ISO20022 사양과 같이 사전 정의된 방대한 어휘 및 분류체계 사전 위에서 작동한다. 거래와 같이 보스코인에 특화된 기능은 OWL 사전에서 제공되지 않기 때문에, 이와 관련된 어휘 및 분류체계는 계약 외부에서 호출해야 한다. 이러한 기술적인 문제를 해결하기 위해, 블록체인 위에 사전 정의된 네임 스페이스 도메인을 생성하는 방법을 제안한다. 이 네임스페이스 도메인은 계약에서 비표준 기본 타입(분류체계)을 호출 할 수 있다. OWL의 결정가능성 및 분류학적 복잡성 기능을 유지하기 위해 비표준 기본 타입이 신중하게 추가될 것이다.

블록체인에 대한 튜링-완전 계약의 또 다른 문제는 튜링-완전 언어는 비전문가들이 읽기 어렵다는 것이다. ’코드가 법’이라면 코드는 관련된 모든 당사자가 이해할 수 있어야 한다.

현재 계약용 튜링-완전 언어를 사용하는 통화는 코드를 읽을 수 있는 사람만 검사할 수 있다. PPP코인은 OWL 표준을 사용하고 SDLang10과 같은 언어에 문법을 매핑함으로써, 누구나 계약 내용을 읽고 그 계약이 의미하는 바를 정확하게 이해할 수 있게 하려고 한다.

Timed Automata Language 개념은 Andrychowicz의 논문인 'Timed Automata 에 의한 Bitcoin Contracts 모델링'11을 기반으로 한다. TAL은 Trust Contract에서 사용되는 프로그래밍 로직을 모델링하는 데 사용된다. OWL 및 TAL의 관계는 HTML과 Javascript의 궁합과 유사하다. OWL은 데이터 구조를 제공하고 TAL은 연산자처럼 작동한다. 프로그래밍 언어의 연산자는 더하기, 빼기 및 비교와 같은 특정 기능을 수행하는 구문이다. OWL은 정보를 제공하고 TAL은 컴퓨터에 데이터 처리 방법을 알려준다. TAL은 전역 시간 요소(global time factor)가 있기 때문에 다른 프로그래밍 언어와 약간 다르다.

즉, 계약을 실행하는 데 걸리는 시간을 사전에 테스트 할 수 있다. 가능한 모든 각각의 결과에 대해 사전에 자동화된 테스트를 실행함으로써 블록체인에서 버그 없는 계약을 구축할 수 있는 플랫폼을 제공할 수 있다.

9. 사전개발 어플리케이션 생태계

많은 암호화폐들이 그들의 플랫폼 위에 Application을 사용하고 구축하는 방법에 대한 예제를 제공하지만, 그들의 통화로 작동하는 어플리케이션을 제공한 암호화폐는 별로 없다.
암호화폐의 가치가 거래의 가치로 구성되는 정도와 투기적 가치로 구성되는 정도를 완벽하게 파악하기는 어렵지만, 피피피 코인(PPP Coin)의 목표는 경쟁 업체와 비교하여 통화의 거래 가치를 높이는 것이다. 장기적으로 볼 때 통화의 핵심 가치는 통화의 유용성이다.

코인과 함께 공개되는 개발 어플리케이션을 통해 사용자는 피피피 코인(PPP Coin) 생태계 내에서 즉시 사용할 수 있는 세련된 서비스를 만나게 될 것이다.

이들 서비스들은 코인을 배포하는 채널 역할을 하는 동시에 피피피 코인(PPP Coin)을 사용하는 매장 역할을 할 것이다. 이러한 도구를 적절하게 사용하면 새로운 사용자를 유입시킴으로써 생태계를 성장시키는 데 도움이 될 것이다.

10. 코인 발행

피피피 코인(PPP Coin)은 총 7,700,000,000 [77억개] 의 코인을 발행할 계획이다. 피피피 코인(PPP Coin)팀은 다양한 암호화폐에 내재된 기술 상의 그리고 운영 상의 문제를 극복하는 것을 목표로 한다.

인센티브 제도 및 발행 계획은 권력의 중앙 집중화을 억제하면서 코인의 가치를 창출하는 것을 목표로 한다.

피피피 코인(PPP Coin)팀은 블록체인 기술을 통해 얻을 수 있는 안전하고 편리한 암호화폐의 표준을 창출하면서 위와 같은 목적을 달성하는 것을 목표로 하고 있다.

11. 자산 실사

PPP Coin은 세계 최고의 쇼핑 과 디지털 마케팅에서 불록체인 기반의 새로운 암호화페로 될 것이다. 활발한 사용자, 고급 매칭, 다국어 지원 및 분산화와 함께 보상을 제공하는 흥미진진한 보상 시스템인 PPP Coin은 공개 능력주의를 가상화폐와 결합한 최초의 진정한 글로벌 서비스 플랫폼입니다.

“PPP Coin은 가상화폐가 쇼핑에서 채택되는 것을 가속화할 것입니다.”

12. 코인 판매 및 환불

코인

PPP Coin은 증권, 주식 또는 이익 분배 메커니즘이 아닙니다. 코인 판매 참가자는 코인을 구입할 때 위험 요소를 이해하고 참여하기 전에 PPP Coin의 백서 전체를 읽어야 합니다. 코인 판매에 참여하는 것은 PPP Coin 판매 및 구매 약관의 적용을 받습니다.

기술적인 위험

PPP Coin 계약은 CryptoNote 표준을 기반으로 합니다. 계약서에 기술적 오류가 없도록 모든 노력을 기울이고 메인넷 1.0을 준비하였습니다. 참가자는 이 위험을 이해하기 위해 블록체인 기술을 숙지해야 합니다. 참가자는 개인 키 저장 및 전송과 관련된 위험을 이해해야 합니다.

해커와 형사상의 개입

PPP Coin 계약 주소는 http://www.PnPPcoin.com 를 통해 제공됩니다. 그간에 따르면 범죄로 사람들을 속여 잘못된 주소로 돈을 보내도록 컴퓨터와 이메일 서버를 인수하려는 시도가 있었습니다. 여기에는 사회 공학이 포함될 수 있습니다. PPP Coin은 잠재적인 공격을 막기 위해 모든 모범 사례 보안 조치를 구현합니다. 참가자는 올바른 계약 주소를 다루는 모든 합리적인 노력을 기울여야 하며, PPP Coin의 모든 지침을 준수해야 합니다. 참가자는 PPP Coin

을 대표하는 척하는 사기를 일으킬 수 있으므로 http://www.PPPcoin.com 외에 외부 게시된 계약 주소를 사용해서는 안됩니다. 참가자는 PPP Coin의 지시에 따라 모든 보안 모범 사례를 따라야 합니다.

세금 및 규제 위험 요소

코인 구매자는 자신의 관할권에 있는 가상화폐의 세금, 증권 및 기타 규정에 관한 모든 현지 법률을 준수하는지 확인하기 위해 자체 실사를 수행해야 합니다. PPP Coin 판매는 향후 추가 규제의 대상이 될 수 있습니다.

환불

환불은 처리되지 않습니다. 일단 판매가 되면 취소할 수 없습니다.