DBXC SOLUTION AND CREATION

WHITE PAPER Ver 5.0

2021. 05. 20.

디지털뱅크엑스씨앤지(주)
(DBXC&G)

Digital Bank eXchange C & G Co., Ltd.

UNIT 17, 9/F TOWER A NEW

MANDARIN PLAZA NO 14 SCIENCE

MUSEUM RD TST KLN HONG KONG

www.dbxc24.com

www.dbxg24.com

INDEX

7. DBXC 사업들은 현재 개발 중이며, 출시 전에 변화가 있을 수 있습니다.
8. 때에 따라 DBXC에서 귀하에게 e-mail을 발송할 수 있음을 인정합니다. 그리고 이러한 e-mail 통지는 귀하의 기밀정보를 요구하지 않습니다. 따라서 이와 관련하여 사기, 피싱 시도 및 악의적인 의도의 접근 가능성이 있습니다. 이에 비공식적인 문의에 대해서는 응답하지 마십시오.
9. DBXC에서는 DBXC 사업의 운영 기간을 보증하지 않을 수 있습니다. DBXC 사업은 대중의 관심 부족 또는 솔루션 개발을 위한 자금 부족과 같은 여러 가지 이유로 중단될 수 있습니다.
10. DBXC 소지자는 결코 DBXC에 대한 어떠한 유가증권이나 지분도 소유함을 의미하지 않습니다.

귀하 및 DBXC의 상호 이익과 분쟁을 방지하기 위하여 상기의 법적 면책 조항을 명확하게 이해하시고 이를 합의 인정하시기 바랍니다.

-(끝)-

Coin DBXC의 모든 지침을 준수해야 합니다. 참가자는 Coin DBXC을 대표하는 척하는 사기를 일으킬 수 있으므로 www.dbxc24.com 외에 외부 게시된 계약 주소를 사용해서는 안 됩니다.

참가자는 Coin DBXC의 지시에 따라 모든 보안 모범 사례를 따라야 합니다.

11.04. 세금 및 규제 위험 요소

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

11.05 환불

환불은 처리되지 않습니다. 일단 판매가 되면 취소할 수 없습니다.

12. 법적 고지 사항

COIN DBXC는 유가증권이 아니며, 소유권을 나타내지 않습니다. 따라서 이 백서의 내용은 금융 프로모션의 용도로 사용되지 않습니다. 백서에 기술되어 있는 내용을 기반으로 계획에 맞도록 COIN DBXC를 운영할 예정입니다(객관적이고 합리적인 의사결정에 따라 개발 변경 사항이 적용될 수 있습니다)

귀하가 DBXC 사업에 참여하기 위해서 다음과 같은 내용을 정확히 확인, 완벽히 이해하시고 아래의 내용에 대하여 합의하시기 바랍니다.

1. DBXC는 어떤 관할권에서도 유가증권을 구성하지 않습니다.
2. 이 백서의 모든 내용은 어떠한 형태로든 투자 활동을 유도하거나 초청의 용도로 사용하지 않습니다.
3. 본 백서의 내용을 임의적으로 해석하고 이해해서는 안 됩니다(DBXC, ICO, 거래소 및 관련 Platform 포함)
4. 본 백서에 포함된 모든 정보를 비롯해 Coin DBXC로부터 현재 또는 미래에 공지되는 내용은 발생 시점과 관계없이 어떠한 형태로의 이익 또는 이익의 보장으로 해석되어서는 안 됩니다.
5. 큰 가격 변동성, 암호화폐 시장이 가지는 특유의 위험성 등 암호화폐와 연관된 위험이 있음을 인정하며, 이는 자금적 손실도 포함합니다.
6. DBXC 사업 운영, 가상자산 판매 등과 관련하여 위험이 있을 수 있습니다.

1. 서론

1.1 COIN DBXC

COIN DBXC는 대한민국 내 최고의 보안기술팀의 기술 탑재로 발행된 암호화폐이며, 블록체인 생태계의 미래를 준비하기 위한 다양한 수단과 방법의 제공을 위해 기획되고 발행됐습니다.

당초 DBXC는 홍콩에서 기반을 잡고 암호화폐 발행을 준비해 오던중 대한민국 내 블록체인 분야의 우수한 기술력을 접하게 되었고, 이어서 이 기술팀과 DBXC 핵심 관계자들이 몇차례 가진 미팅 이후 암호화폐를 발행하기로 결정하게 됐으며, 이에 개발에 착수한지 6개월만에 메인넷을 갖춘 완벽한 암호화폐 DBXC를 발행하게 됐습니다.

COIN DBXC는 발행에 이어서 대한민국내 거래소(DBX24.COM)에 상장했으며, 2021년 3월부터 2~3개의 유명 국제 거래소에 상장을 준비중인 명품 암호화폐로 자리 잡아가고 있습니다. 이는 DBXC가 글로벌화 되고 있고, 또한 국제적으로도 수준 높은 암호화폐로 자리를 잡아가고 있음을 입증하는 것입니다.

현재 COIN DBXC는 블록체인의 높은 보안성과 안정성을 바탕으로 일반 소비자들과 기업, 그리고 중소농 · 상공인들과 연계함으로써 소비자의 이익을 보호하고 극대화할 수 있는 실물 경제 인프라의 바탕을 제공하고자 노력하고 있습니다.

COIN DBXC는 다양한 암호화폐가 상장되어 거래되는 대한민국 내 가장 우수한 기술력을 보유하고 있는, 디비엑스(www.dbx24.com) 거래소의 솔루션 내에서의 기본적인 거래 단위가 되고 있으며, 단순히 DBX 솔루션 내에서 COIN DBXC를 사용하는 것만으로도 이에 상응하는 부가가치가 발생되도록 구현해 놓고 있습니다.

따라서 거래소 DBX24.COM 솔루션에서의 Coin 기여도에 의해서 코인 홀더의 자산 가치는 정비례 이상 증대가 가능할 것으로 내다보고 있습니다.

또한, COIN DBXC는 실물 거래 기반의 가상자산으로써 탈중앙화된 웹은 물론 다양한 앱과 데이터센터 기술을 중심으로 서버 서비스와 호스팅 서비스를 비롯한 많은 웹서비스를 지원하고 있으며, 최종적으로 국내 블록체인의 표준이 되는 지위를 통해서 전 세계 시스템 확충 및 글로벌 마켓 형성을 실현하고자 합니다.

<높은 보안성>

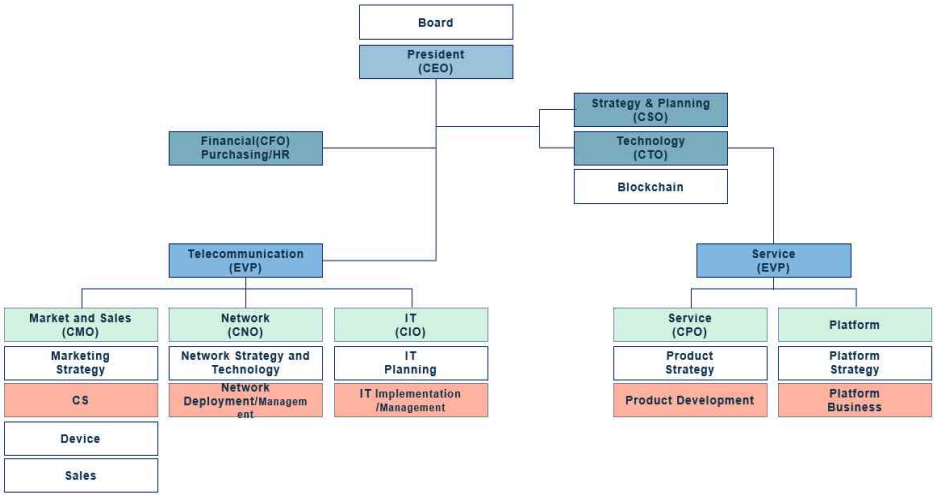
<높은 확장성>

<높은 자산성>

1.2 비전

COIN DBXC 프로젝트는 암호화폐 거래소에 금융기관의 커스터디 서비스를 도입하여 코인 거래 시스템에 대한 해킹 시도 및 공격은 물론 내부 범죄로부터 완벽에 가까운 보안을 실현해 주는 신개념

10.2 조직도



11. 코인 판매 및 환불

11.01 코인

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

11.02 기술적인 위험

Coin DBXC 계약은 CryptoNote 표준을 기반으로 합니다. 계약서에 기술적 오류가 없도록 모든 노력을 기울이고 메인넷 3.0을 준비하였습니다. 참가자는 이 위험을 이해하기 위해 블록체인 기술을 숙지해야 합니다. 참가자는 개인키 저장 및 전송과 관련된 위험을 이해해야 합니다.

11.03 해커와 형사상의 개입

Coin DBXC 계약 주소는 www.dbxc24.com을 통해 제공됩니다. 그간에 따르면 범죄로 사람들을 속여 잘못된 주소로 돈을 보내도록 컴퓨터와 이메일 서버를 인수하려는 시도가 있었습니다. 여기에는 사회 공학이 포함될 수 있습니다. Coin DBXC는 잠재적인 공격을 막기 위해 모든 모범 사례 보안 조치를 구현합니다. 참가자는 올바른 계약 주소를 다루는 모든 합리적인 노력을 기울여야 하며,

을 막을 계획입니다. 코인이 가상자산으로 활용되는 동안 그 가치가 보장될 전망입니다. 시장 가격이 합산되고 비정상 값이 제거되어야 올바른 결과를 얻을 수 있습니다.

9.3 카드결제

코인의 경우 현재 일반 매장에서 사용할 수 있는 인프라 구축이 부족한 상황입니다. 가상자산이 실제로 시장에서 통화로서 가치를 지니기 위해서는 통용이 되어야 할 것입니다. 때문에 점진적으로 화폐가 실물자산에서 가상자산으로 이동하는 과도기에서 사용자들이 현금과 가상자산을 모두 사용할 수 있도록 시스템을 구축할 예정입니다. 즉 은행을 통해 코인 사용자에게 카드를 발급해주고, 일반 매장에서 카드 결제시 사용자가 보유한 코인 만큼 거래소에서 코인과 현금이 자동 거래되어 실시간으로 현금 결제도 가능하도록 할 수도 있으며, 일반 신용카드와 거래소를 연계, 코인이 실물 거래에 활용되는 시스템을 구축할 것입니다.

10. 주요 멤버 및 조직도

10.1 경영진(운영진)

	- 김광주 - 전, 엘림에듀 총괄이사		- 김대식 - 전, 한국투자증권
	- 나정식 - 켈리포니아 빅터대 박사 - 건양대 IT공학부 교수 - (사)국회입법정책연구회 수석연구위원 - (사)대한블록체인조정협회 기술심의위원회 위원장		- 이상민 - ㈜엑트아이 중앙연구소 책임연구원
	- 김장남 - 전, 대검찰청		- 김병욱 - 전, 식약청장

가상자산 보안 솔루션입니다. 이러한 Coin DBXC 프로젝트의 보안 서비스는 기존 시스템의 보안 강화를 위한 솔루션을 제공하여 안정성 및 효율성을 높임으로써 향후 블록체인 보안에서의 표준화의 초석이 될 것으로 보여집니다.

특히 COIN DBXC가 상장되어 있는 거래소 DBX24.COM에서는 COIN DBXC가 “가장 신뢰성 있는 블록체인 인증기관을 기반”으로 한다는 점을 주목할 수 있습니다. 이는 거래소 DBX가 COIN DBXC와 함께 대한민국 최고의 블록체인 기술을 그대로 녹여 놓고 있는데에 따른 자연스러운 해석입니다. 다시말하면, 대한민국 표본이 되는 명실상부한 명품 암호화폐 거래소 DBX에 최고의 보안기술을 탑재하고 발행된 COIN DBXC도 함께 하고 있음을 의미합니다.

한편, COIN DBXC가 상장되어 있는 거래소 DBX는 국내 · 외의 양질의 암호화폐를 선별하여 상장하고 있는 거래소이며, 이는 무분별한 암호화폐를 거래하도록 해 발생할 수 있는 사용자의 피해를 사전에 막을 수 있는 최적의 거래소 운영의 기본이 될 것으로 판단하고 있습니다.

또한, COIN DBXC가 상장되어 있는 대한민국 암호화폐 거래소 DBX는 컴퓨터 모니터 안에서만 거래되고 있는 현재의 암호화폐 단점을 보완하기 위해 실물코인으로 전환할 수 있는 신용카드와 연계 준비를 하고 있으며, 신용카드 연계를 통해 라이프 스타일까지 변화할 수 있을 것으로 전망하고 있습니다.

이는 일부 코인을 얹어 실물 코인이라고 하는 체크카드와 전혀 다른, 실제 국내 · 외에서 사용할 수 있는 신용카드와 연동되도록 하는 기술로서 세계에서 독보적이라고 할 수 있습니다.

이에 따라 Coin DBXC는 거래소 DBX24.COM의 기축통화 수단으로 활용될 것이며, 거래소에서 가장 먼저 금융권 신용카드와 연동되어 사용할 수 있는 암호화폐가 될 것입니다.

1.3 주요 핵심 멤버

직위/직책	성 명	주 요 경 력	비 고
대표이사	김광주	전, 엘림에듀 총괄이사	
이사	김대식	전, 한국투자증권	
이사	나정식	현, ㈜엑트아이 대표이사	
이사	이상민	현, ㈜엑트아이 중앙연구소 책임연구원	
고문	김병욱	전, 식약청장	
고문	김장남	전, 대검찰청	

2. 코인의 특징

2.1 CryptoNote 란

“비트코인은 p2p 전자 화폐를 성공적으로 현실화한 사례입니다. 전문가들과 대중들은 public transaction과 proof-of-work 방식을 신뢰할 수 있는 모델로 평가했습니다. 현재 사용자 기반의 전자 화

폐는 꾸준히 성장하고 있습니다. 일반 소비자들은 전자화폐의 낮은 수수료와 익명성에 이끌리고 있으며, 상인들은 예견이 가능하고 분산화된 화폐 발행을 긍정적으로 생각하고 있습니다. 비트코인은 전자화폐가 지폐처럼 단순하고 신용카드처럼 편리하다는 사실을 효과적으로 입증하고 있습니다.

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

따라서 비트코인의 주된 단점에 대한 해결책을 제시할 수 있는데, 이를 통해서 전자 화폐 시스템은 건전한 경쟁을 할 수 있을 것으로 볼 수 있는 것입니다.

2.2 비트코인의 단점들과 가능한 해결책들

2.2.1 트랜젝션의 추적 가능성

전자화폐에서 프라이버시와 익명성은 가장 중요한 측면들입니다. 개인 간 거래는 제3자로부터 숨겨질 것이며, 이는 전통적인 은행의 거래 방식과 대조됩니다. 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 전자화폐 개념을 충족하기 위해서 2가지 특성을 이끌어 내고 있습니다.

○ 비추적성 : 각각의 수신 트랜젝션에서 누가 보냈는지 알 수 없음

○ 비연결성 : 임의의 2개의 발송되는 트랜젝션에 대해서, 같은 사람에게 전송되었다는 것 입증 불가

안타깝게도 비트코인은 비추적성에서 벗어납니다. 네트워크의 참가자들의 트랜젝션이 모두 공개되기 때문에, 발송자와 최종 수신자가 모두 공개될 수 있습니다. 만약 간접적으로 거래를 하더라도, 경로 추적 기술을 이용하면 발송자와 수신자를 확인할 수 있습니다.

비트코인이 2번째 속성도 충족하지 않는 것처럼 보입니다. 일부 연구자들에 의한 블록체인에 대해 자세히 분석하면, 비트코인 네트워크의 이용자들과 트랜젝션 사이의 관계를 알게 될 가능성이 존재합니다. 많은 방법들이 부정되었지만, 공개된 데이터베이스로부터 숨겨진 개인정보가 알려질 가능성이 크다는 것입니다.

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

최근에, I.Miers는 새로운 계획을 제시하였습니다. “Zerocoin”은 단방향의 암호 축적 방식을 이용하며, 사용자들로 하여금 비트코인을 제로코인으로 바꾸게 하고, 디지털 서명 및 공개 키(KEY) 대신에, 익명 소유권 증명으로 전송됩니다. 그러나, 이러한 증명 방식은 상당히 많은 용량이 필요하며, 현재의 비트코인이 30kb인 것을 고려하면 실용적이지 않다는 것입니다. I.Miers는 이러한 방식이 대다수 비트코인 유저로부

처할 수 있는 기능을 제공합니다.

7.4.4 사용자가 제공

Coin DBXC의 콘텐츠는 주로 사용자가 생성하고 빠르게 확장 가능합니다. 공급자는 직접 목록을 추가하고 추가적인 서비스, 기술 및 라이센스를 요청할 수 있습니다.

7.5 자체 큐레이팅 및 자체 균형 유지

Coin DBXC는 진정한 능력주의이며, 따라서 자체 심사를 실시합니다. 좋은 기술과 리뷰를 가진 공급자는 더 많이 노출되고 더 많은 보상을 받을 수 있게 됩니다. 좋은 품질의 공급자 아이템은 수요가 더 많아지며 더 높은 요금을 부과할 수 있습니다.

새로운 공급자는 광고 노출을 통해 기존의 공급자 기반에 진입할 수 있습니다. 모든 공급자에게 최대한의 광고 노출을 보장하기 위해 그들의 프로필과 진행 업무 내용을 지속적으로 업데이트할 수 있는 기회를 제공합니다.

8. 자금 운용 계획

Coin DBXC의 법적 비용에는 법률 연구를 포함되어 있습니다. 기본적으로 각종 인증, 승인, 허가 등의 라이선스 비용과 실제 법률적 근거를 찾기 위한 연구비, 사례 연구비 등이 포함될 것입니다.

● 기부 및 후원 플랜

Coin DBXC는 DBX 솔루션과 함께 수익의 상당액을 세계에서 고통받는 이들과 함께할 것입니다. 이는 Coin DBXC 프로젝트에 참여하는 모든 멤버들과 어드바이저들의 의견을 통합하여 채택되었으며, 향후 방향성 논의를 거쳐서 확정할 예정입니다.

9. 생태계 성장 & 가상자산의 비전

9.1 생태계 성장

거래소 DBX를 통하여 초기에 이용하는 사용자에게는 다양한 방법으로 후한 보상 풀을 마련하고 있습니다. 보상 풀이 고갈되면 보상도 줄어듭니다. 사용자 기반이 커짐에 따라 공급자는 서비스 목록을 올리고 사용자가 더 많이 참여합니다. 공급자 기반이 성장함에 따라 일부 공급자는 자신을 구별하고 노출을 늘리기 위해 프리미엄 구독모델을 채택합니다. 거래 수익과 구독이 늘어남에 따라 보상 풀이 늘어나 더 많은 보상이 지급됩니다. 또한 은행의 신용카드 발급을 통해 결제까지 이어지도록 하는 생태계를 구축합니다.

9.2 변동성에 대한 보호

희소성을 가진 코인은 투기로 인해 발생되는 변동성 때문에 선호되는 가상자산이 아닙니다. Coin DBXC는 무보증 방식으로 입증된 가치를 지키고 Coin DBXC 의 가치를 유지하는 해지 계약을 활용하여 변동성

다.

* 판매가격 : - KRW[원화] 가격 변동으로 판매됩니다.

초기에 제공된 코인은 12개월(또는 규정에서 정한 기간) 동안(보호예수기간) 판매에 제한을 받습니다.

다양한 방법으로의 보상 풀은 플랫폼에서 사용자를 장려하기 위해 사용되며, 자세한 내용은 아래에서 자세히 설명합니다.

7.4 Coin DBXC 배포

Coin DBXC는 향후 플랫폼에서 사용할 수 있도록 DBXC를 공개적으로 배포합니다. 향후 코인의 목적은 로드맵에 통합되어 규제 승인을 받는 것입니다.

1) 공급자가 앱의 프리미엄(비지니스 업무 등) 기능에 접근하기 위해, 매달(또는 매번) 비용을 지불하기 위해 코인을 사용하도록 합니다.

2) 사용자가 생태계에서 특정 활동을 수행한 경우, 해당 사용자에게 보상으로 코인이 제공됩니다.

3) 모든 현지 법규를 준수하고, 적절한 라이센스가 있는 경우 공급자가 Coin DBXC으로 서비스 비용을 청구할 수 있는 가치 교환을 위한 매체입니다.

4) 공급자가 Coin DBXC Wallet에 결제금을 보관할 수 있도록 자산을 보관하는 기능을 합니다.

Coin DBXC는 현재 라이센스가 있는 제 3자를 통하여 KRW 화폐 단위로 결제가 가능합니다. 이 백서에서 제안된 Coin DBXC 생태계에 있는 결제 수단을 통합하려면 Coin DBXC을 통해 또는 제3자를 통해 추가 라이센스 및 규제 승인이 필요합니다.

5.4.1 플랫폼

Coin DBXC는 2020년 12월 2일 거래소 DBX24.COM 상장일로부터 유통됐습니다.

Coin DBXC는 곧 시장에서 성공적으로 유통할 수 있도록 기존 쇼핑 사용자 기반을 보유하도록 할 것입니다.

7.4.2 개인 대 개인

Coin DBXC는 고객이 제3자 대신 서비스를 제공할 사람을 직접 선택하고, 상호 소통하는 개인 대 개인 플랫폼입니다. 이 플랫폼은 안전하고 빠른 결제 서비스를 제공할 것입니다.

7.4.3 중립적인 서비스

Coin DBXC는 전문적인 서비스부터 단순한 시간당 서비스에 이르기까지 다양한 서비스에 적합합니다.

Coin DBXC는 다양한 서비스와 다양한 기술을 사용자에게 제공합니다.

Coin DBXC는 모바일 서비스, 오프라인 서비스, 일회성 작업, 주기적인 그룹 예약에 대해서 유연하게 대

터 외면받을 것이라고 예상했었습니다.

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 주장하였습니다. 이용자들은 트랜젝션 기록을 바탕으로 투표를 하게 되는데, 이 과정이 제대로 되어야 전체 시스템이 잘 작동할 수 있습니다.

이러한 모델의 보안은 두 가지 단점을 지니고 있는데, 첫째로는 정직한 유저의 통제하에 두려면 51퍼센트의 네트워크 마이닝 파워가 필요합니다. 두 번째로, 해당 시스템의 발전 과정(버그 수정, 보안 수정 등)을 하려면 대다수의 사용자가 변화에 지지하고 동의해야만 합니다.(사용자들이 지갑 소프트웨어를 업데이트 해야 하기 때문입니다)

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

비트코인의 경우 CPU 소유자보다 GPU 및 ASIC 채굴자들이 더 많은 투표력을 갖기 때문에, 실제 투표력과 차이가 발생합니다. “1CPU 1투표” 원칙을 어기기 때문입니다.

일부에서는 적지 않은 참가자들이 의사결정을 행사하기 때문에, 해당 문제가 보안과 관련된 사항은 아니며, 대신에 의사결정 참가자들의 정직성이 중요하다고 주장합니다. 이러한 주장에 대한 반론이 존재하는데, 값이 저렴하며 채굴에 특화된 하드웨어가 존재할 가능성 때문입니다. 예를 들어, 만약 악의적인 채굴업자가 값싼 하드웨어로 채굴을 하게 된다고 가정해보면, 그리고 전세계의 해쉬레이트가 감소했다고 가정해보면, 잠깐일지라도 그는 chain fork 및 double-spend가 가능해집니다. 이러한 상황의 가능성이 충분하다는 것을 이 글에서 설명할 것입니다.

2.2.3 불규칙적인 생성

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

문제점이 발생하면, 기존의 보상에 비해서 절반의 가치만을 얻게 됩니다. 12.5와 6.25 BTC의 차이(2020년에 예상)는 그래도 괜찮아 보였습니다. 그러나, 50과 25BTC의 차이는 2012년 11월 28일에 발생하였으며, 채굴 업계에서 상당히 부적절한 일로 비춰졌습니다. 그림에서는 11월 말 네트워크 해쉬레이트가 급격히 감소했다는 상황을 나타내며, 보상이 절반으로 감소한 직후 일어난 일이었습니다. 악의적인 개인이 double spending attack을 일으킬 완벽한 순간입니다.

Fig. 1. Bitcoin hashrate chart
(source: https://bitcoin.org/en/block_name% on 2018-11-01

2.2.4 수정의 어려움(Hardcoded Constants)

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

수정이 어려운(hardcoded) 문제점 중 하나는 블록 사이즈 리미트가 250kb라는 것입니다. 약 10,000건의 일반 거래를 감당하기에는 충분합니다. 2013년 초기에 거래량이 이 정도에 도달하였으며, 리미트를 올리고자 합의하였습니다. 지갑 버전 0.8에서 도입되었으며, 결과적으로 24-block chain split과 double-spend attack이 발생하게 되었습니다.

그리고 비트코인 프로토콜 자체에는 버그가 없었으나, 데이터베이스 엔진에 문제가 있었으며, 만약에 인위적인 블록 사이즈 제한이 없었다면 스트레스 테스트를 통해서 미리 알 수 있었을 것입니다.

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

2.2.5 방대한 스크립트

비트코인의 스크립트 시스템은 방대하고 복잡한 기능입니다. 잠재적으로 한 객체는 복잡한 트랜젝션을 만

적 불가능한 트랜젝션(Untraceable payment)으로 크립토노트(CryptoNote)는 링 시그니쳐(ring signature)라는 방식을 사용하며 보내는 사람이 누구인지 알 수 없도록 숨깁니다.

전 세계적으로 약 1조 달러로 예상되는 가치를 지닌 발전된 인적 서비스 가치가 뒷받침합니다. 코인은 플랫폼에서 교환될 수 있으며, 실제 세계의 숙련된 기술과 기능을 가진 아이템 또는 가치로 교환할 수 있습니다.

코인에 대한 지속적인 수요와 플랫폼에 대한 수익 흐름을 제공합니다. 점차적으로 전통화폐 결제 게이트웨이를 통합함으로써 Coin DBXC는 가상자산 시스템에 대한 합법적인 게이트웨이가 되어 전체 생태계를 강화하고 주류 채택을 가속화 하는 것을 목표로 합니다.

7.2 핵심 기능

Coin DBXC의 플랫폼은 Android 앱과 베타 웹으로 구성된 기업 대 기업 그리고 개인 대 개인 서비스의 모든 기능을 갖춘 비지니스 마켓 플레이스입니다. Coin DBXC에는 비즈니스 업무와 디지털 마케팅에서 사용되는 작업 등이 포함됩니다.

1) 고객은 Coin DBXC와 다양한 가상자산을 사용하여 Coin DBXC Wallet을 충전할 수 있습니다.

2) 고객은 수수료 없는 서비스(혹은 적은)를 로컬 및 전세계에 즉시 연결하고 비용을 지불할 수 있습니다. Coin DBXC는 비즈니스 업무 및 디지털 마케팅에 중점을 둔 대부분의 기업 대 기업뿐만 아니라 개인 대 개인 서비스를 지원합니다.

3) 서비스 공급자로서, 사용자에게 기술과 서비스를 제공하고 Coin DBXC을 받을 수도 있습니다. 서비스 공급자는 Coin DBXC을 앱에 사용하거나 교환하여 P2P 거래를 통한 개인 간에 즉시 보낼 수 있습니다.

4) 서비스 공급자로서, 사용자의 기능과 아이템을 BBS를 이용하여 글로벌 마켓 플레이스에 무료로 홍보하거나, 월별 구독료를 지불 하고 향상된 기능을 사용할 수 있습니다. Coin DBXC는 진정한 능력주의 시스템입니다. 즉, 최고의 사용자가 가장 많이 노력함으로써 최고의 보상을 받을 수 있습니다.

7.3 코인 판매

Coin DBXC는 정확하게 10,000,000,000개(100억개)가 발행됐습니다. 판매에 사용되는 Coin DBXC는 500,000,000개(5억개)가 될 것입니다.

7.3.1 Private 판매

본 프로젝트에 장기적인 가치를 보고 있는 전략적 투자자에게 판매됩니다.

Coin DBXC의 판매는 다양한 방법으로 Coin DBXC 커뮤니티에 기여하는 일반 대중, 지역 및 나라별 총판을 통하여 판매 진행됩니다.

DBXC 및 메인 판매는 소진될 때까지 진행됩니다. 마감 시에 판매되지 않은 코인은 자산으로 보내집니

주요 내용을 살펴보면,

● 통신망이 구축되지 않아 통신 서비스가 불가능한 지역에 전용 네트워크 설치

● 컨텐츠 소유권 및 원작자의 권리를 찾을 수 있는 유통망 구축 등의 사업을 진행할 예정입니다.

등록된 NGO에게 비현금 자산으로 기부가 이루어질 경우 참여자들 간에 그 가치를 평가하고 디비엑스 씨움 내에서 환전하여 기부를 진행할 수 있습니다. 통신 인프라 기부의 경우는 통신 환경이 낙후되거나 비용을 지불하기 힘든 집단 혹은 개인에게 통신망 사용권을 전달하여 정보의 사각지대에서보다 적극적인 경제활동이 가능하도록 지원할 계획입니다.

7. DBXC 발행 및 배포

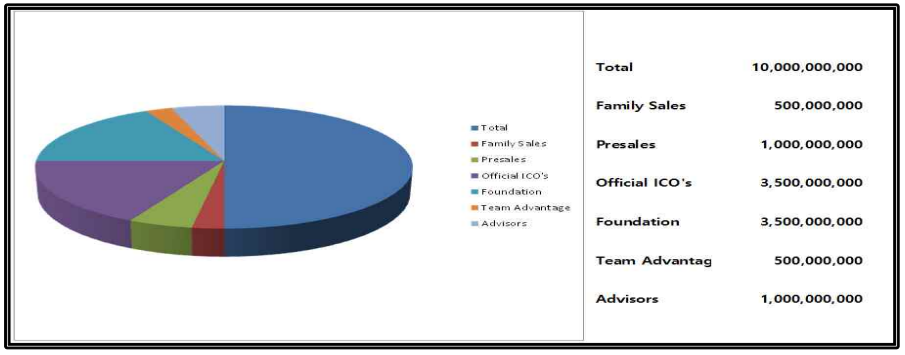
7.1 Coin DBXC

Coin DBXC은 총 100억개의 코인을 발행했습니다. 추후 적정한 기한이 도래하면 50%(50억개)는 소각할 예정입니다.

또한, Group-sale(기업, 기관, 단체, 협의체 등)과 Personal-sale(개인)로 구분하여 전략적으로 발행 및 분배될 계획입니다.

특히, 비즈니스와 접목하여 업무를 활용하는 동안에 다양한 아이템을 운영하도록 하여 컨텐츠의 공급과 수요를 창출하고, 향후 모든 업무 통합으로 인한 다목적이고 빅테이터로의 풍부한 플랫폼입니다.

다양한 컨텐츠(업무) 및 디지털 마케팅의 생태계에서 비지니스와 유관 회사 그리고 이용자가 투명한 형태로 비즈니스와 콘텐츠(또는 아이템)를 활용하고 수익을 창출할 수 있도록 하는 코인으로 사용하려 합니다.



Total	10,000,000,000
Family Sales	500,000,000
Presales	1,000,000,000
Official ICO's	3,500,000,000
Foundation	3,500,000,000
Team Advantag	500,000,000
Advisors	1,000,000,000

Coin DBXC는 점차 플랫폼에 결제 시스템을 강화하고 분산화된 서비스를 가능하도록 하며, 다양한 가상화폐 사이의 다리 역할을 하도록 할 뿐만 아니라, 네트워크 효과를 강화하기 위한 강력한 보상 시스템을 만들고, 인센티브를 받을 수 있는 사용자 큐레이션 및 사용자-중재를 활성화할 예정입니다.

Coin DBXC는 암호화폐와 현실 세계 사이의 궁극적인 연결 고리입니다. CryptoNote 기반을 통하여 추

들어낼 수 있으며, 일부 기능은 보안상의 이유로 제한되었고, 일부는 전혀 이용된 적이 없습니다(송신자와 수신자 부분을 포함하여) 비트코인의 대다수의 트랜젝션은 다음과 같이 사용됩니다.

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

이 스크립트는 164 바이트의 길이 이지만, 유일한 목적은 수신자가 그의 서명을 확인하기 위한 암호 키를 가지고 있는지를 체크하는 것입니다.

2.3 크립토노트 기술

2.3.1 추적 불가능한 트랜젝션

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

2.3.2 타원곡선 파라미터(Elliptic curve parameters)

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

일반적인 파라미터는 아래와 같습니다.

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 유사합니다. 트랜젝션 아웃 풋이 가능하며, 대응하는 개인 키로 서명하여 다른 주소로 보낼 수 있습니다.

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

2.3.4 비연결성 지불

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

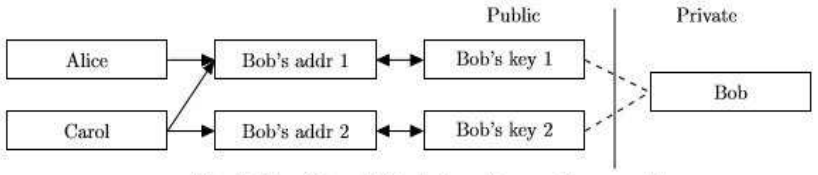
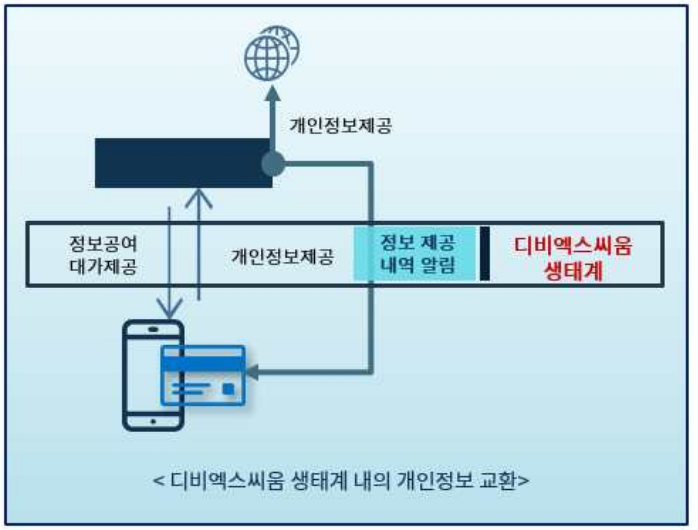


Fig. 2. Traditional Bitcoin keys/transactions model.

씨움'은 이러한 개인정보 및 거래 정보를 포함한 모든 활동 정보를 개인이 직접 저장하고 소유하도록 지원합니다.



< 디비엑스씨움 생태계 내의 개인정보 교환>

이러한 정보는 개인이 직접 소유하지만, 수정, 삭제는 불가능합니다. '디비엑스씨움'을 통해 본인의 정보 사용처를 확인할 수 있으며 오사용 되는 정보는 즉시 회수가 가능합니다. 기업에 제공한 정보가 사용기한이 경과하는 경우 정보는 자동 회수됩니다. '디비엑스씨움'을 통한 정보 저장은 디비엑스씨움에서 제공하는 온라인 영역과 개인의 모바일 폰의 데이터 영역 두 곳에 같이 저장하게 됩니다. 한 곳에만 저장된 정보는 의미가 없으며 두 개의 정보를 매치하여야 사용이 가능합니다. 정보가 있어야 하는 기업은 용도와 사용 기간, 사용범위를 고객에게 정확하게 알려주고 정당한 비용을 지불해야 합니다. 디비엑스씨움에 참여한 기업은 기본적으로 초기에도 개인정보를 수집하지 않으며 필요시마다 개인에게 구매하여 사용하는 것을 원칙으로 합니다.

6. 기부 활동

디비엑스씨움은 함께 공존하는 사회를 지향합니다. 정보로부터 소외된 지역의 통신 네트워크 설치, 네트워크 사용 지원 등을 사용자 간의 협력으로 이루고자 합니다. 디비엑스씨움 사용자는 자신이 보유한 자원을 제삼자 혹은 기관에 기부할 수 있고 기부 자원의 정확한 사용처를 확인할 수 있습니다. 디비엑스씨움에 참가한 NGO를 통해 오프라인 기부 사업에 참여도 가능하며 디비엑스씨움 자체의 정보 확장 자선 사업에 참여할 수도 있습니다.

자체 정보 자선 사업이란 정보의 사각지대를 없애고 특권층이 독점하고 있는 지역 혹은 사업에서 사용자를 해방시키는 정보 인권 사업입니다.

자(판매자)가 판매 물품을 진열할 경우 여러 개의 배송업체가 배송에 참여하는데 소비자는 구매 물건을 선택함과 동시에 배송업체를 지정하게 되고 배송업체를 선택한 이후 대금 결제를 진행합니다. 그리고 배송업체가 물건을 소비자에게 전달한 후 소비자가 구매 완료를 확인하는 즉시, 판매자와 배송업체에게 대금이 지불됩니다. 물품이 배송되는 상황은 배송업체에 탑재된 크루드(엘리시움) GPS를 통해 실시간으로 경로를 확인할 수 있습니다.

이런 거래 방식을 통해 온라인 구매에서 발생하는 문제점에 대해 직접적인 책임소재를 확인할 수 있으며 가격 면에서는 거품이 제거될 것으로 기대됩니다. 또한, 거래 품목의 정보는 생산자가 직접 등록하여 정확한 제품 정보를 실시간으로 확인 가능하며 구매자 간 협업 시스템에서는 판매자와 배송업체의 감시자 역할을 하게 됩니다. 상품에 대한 광고는 가능하지만, 그 광고를 희망하는 사용자에게만 전달되어 광고비의 일정 부분은 소비자에게 혜택으로 돌아가게 됩니다.

5. 개인 정보 거래

모바일 환경에서 사용자는 특정한 서비스를 사용하기 위해서는 가입을 위한 개인 정보, 신용정보 등을 제공하여야 하며 서비스를 받는 동안은 개인 사용 정보, 특정 거래 정보, 본인의 현재 위치 정보 등 여러 가지 정보를 사용의 편의성이라는 명목 하에 모두 제공하여야 합니다. 어떤 경우는 정보 제공 등의 동의가 없이는 서비스 자체를 받지 못하는 때도 있습니다. 이렇게 제공된 개인의 모든 정보는 실질적으로 특정 기업의 소유가 됨으로써 기업 간 데이터를 매매하거나 새로운 상품 혹은 기존 상품의 판매를 높이기 위한 다양한 상업적 활동에 활용되게 됩니다.

모바일 환경에서 사용자는 정보 제공자이자 활동 정보 생산자이며 정보에 의해 특정 상품을 재구매하는 소비자가 됩니다. 결국, 내 정보를 무상으로 주고, 무상으로 나를 계속 알려주며, 기업을 위해 상품을 구매해 주는 대상이 되는 것입니다. 이런 구조에서 벗어나려고 한다면 아마도 굉장히 서비스 이용에 제한을 받을 것입니다. 한국에서 신용카드를 신청하여 받는 경우를 예를 들어 본다면, 우선 신용카드 신청을 위해 개인의 모든 정보를 제공하여야 합니다. 정보를 제공하고 발급 승인을 받은 후 실물 카드나 앱 카드를 수령할 때 개인정보 활용에 승인하지 않으면 카드를 수령할 수 없습니다. 상당히 많은 부분에 정보 활용 동의를 해주어야 하고 그렇게 승인된 내 정보가 도대체 어느 곳에 사용되는지 기업은 사용 후에도 전혀 알려주지 않습니다.

최근에는 사용과 소지의 편리함 때문에 신용카드 정보를 모바일 폰이나 앱에 연동해서 O2O 환경 모든 곳에서 사용하고 있기 때문에 결국 나의 거래 활동 정보가 신용카드사에만 남는 것이 아니라 연관된 생태계 전체에서 수집되고 활용되고 있는 것입니다. 최초 가입 시에 평가해야 하는 개인 정보는 일회성으로 필요하지만, 기업은 자신의 위험요소 관리라는 명목으로 이를 파기하지 않고 계속 업데이트해서 관리하고 있으며 개인의 변화되는 신용정보만 아니라 개인의 거래 정보도 모두 수집하고 있는 것입니다. 디비엑스씨움의 생태계에서는 기업에 대한 정보 제공을 반대하지는 않습니다. 원칙적으로 기업의 생태계 유지를 위해서 최소한의 정보만을 제공하고 기업이 그 개인 정보를 활용해서 수익을 창출할 경우 정보 제공자에게 정당한 대가를 지불하게 하고 개인의 정보가 정확하게 어느 곳에 사용됐는지 본인에게 알려주는 정책을 정착시키고자 합니다. 즉, 이는 사용자는 소비자이면서 공급자의 역할을 하는 경우 정확한 공급자의 권리를 가져야 한다는 것을 의미합니다. 뒷장에서 설명할 '디비엑스

사용자가 단일 주소를 공개할 수 있으며, 무조건적으로 비연결성의 지불을 받을 수 있는 단일 주소를 발행할 수 있는 방식을 제안합니다. 각각의 크립토노트 output은 기본적으로 공개 키 방식이며, 수신자의 주소와 송신자의 랜덤 데이터로부터 발생합니다. 비트코인과의 주된 차이점은 모든 destination key가 기본적으로 독특하다는 것입니다.(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 없습니다.

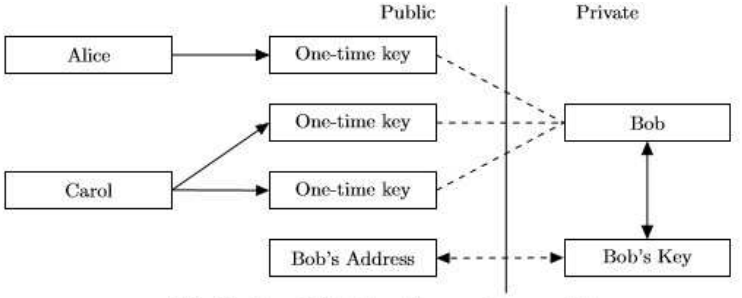


Fig. 3. CryptoNote keys/transactions model.

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

일반적인 거래 과정은 다음과 같습니다.

1. Bob은 표준 주소를 공개하였으며, Alice가 Bob에게 전자화폐를 보내고자 합니다. Alice는 주소를 분석하고 Bob의 공개키를 얻습니다.(A,B)

2. Alice는 랜덤의 r(1,-2 중 하나)을 만들어내고, 1회용 공개키를 계산해 냅니다. 공개키 P = Hs(rA)G + B.

3. Alice는 output에 대해서 P를 destination key로 사용하고, R 값을 해석합니다. R=rG(Diffie-Hellman 교환의 일부) 또 다른 공개 키를 활용하여 다른 output을 만들어낼 수도 있습니다(수신인의 키가 다르면 (Ai, Bi), 동일한 r에 대해서도 서로 다른 Pi가 도출됩니다)

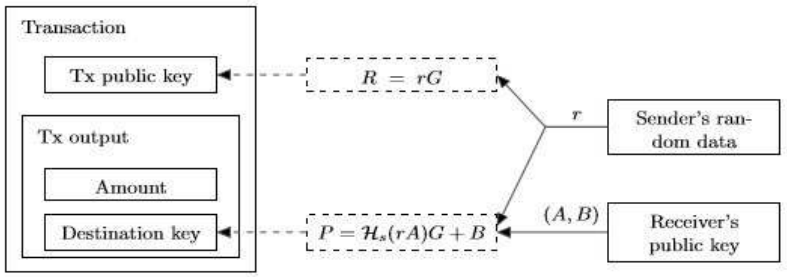


Fig. 4. Standard transaction structure.

4. Alice는 트랜젝션을 전송합니다.

5. Bob은 개인키(a,b)를 이용하여 트랜젝션을 체크하며, P0 = Hs(aR)G + B라는 내용을 계산합니다.

만약 Alice와 Bob의 트렌젝션이라면 aR = arG = rA and P' = P.

6. Bob은 상응하는 1회용 개인 키를 얻을 수 있습니다. x = Hs(aR) + b. 따라서 P = xG가 되며, x로 서명함으로써 원할 때에 output을 전송할 수 있게 됩니다.

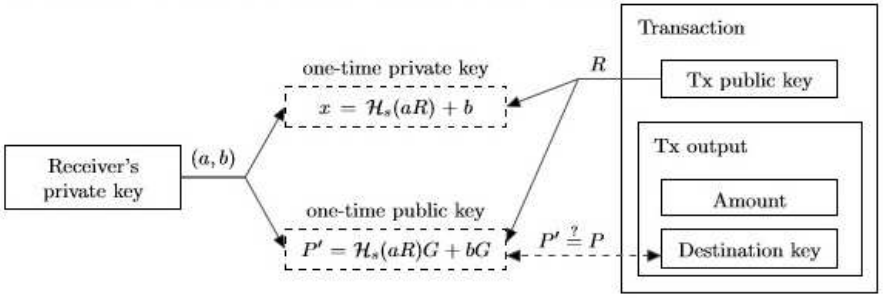


Fig. 5. Incoming transaction check.

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

추가적으로,

*Bob이 스스로의 Transaction을 "인지"하면(step 5) 실질적으로 그의 개인정보의 절반만을 이용합니다 (a, B). 이 한 쌍은 또 tracking key로 알려져 있으며, 제3자 (Carol) 에게 전달될 수 있습니다. Bob은 새로운 트랜젝션에 대한 진행을 Carol에게 위임할 수 있습니다. 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 됩니다.

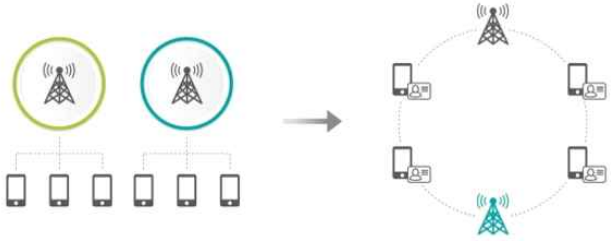
을 추가하는 대신에, 데이터 구조 수준에서 이러한 케이스를 다룹니다.

3. DBXC PORT(생태계)

DBXCSEUM ZOON에는 DBX PORT가 있습니다. DBXC PORT는 DBXC PORT 상에서 경제활동을 하는 참여자 간의 계약 및 거래가 이루어지는 공간입니다.

디비엑스씨포트(DBXC PORT)에서 거래되는 대상은

- 통신망 인프라(네트워크)
- 개인이 소유하고 있는 탈중앙화 된 개인 정보
- 디지털 컨텐츠 및 실물 컨텐츠
- 개인이 구매한 유휴 인프라 등 다양한 품목이며, P2P 거래 방식을 기본으로 하여 다자간 거래(공동구매), 재판매, 기부, 환전 등의 다양한 거래 방식이 가능한 플랫폼입니다. 통신망 인프라 거래와 관련해서는 디비엑스씨 참여 통신망 사업자는 이제 가입자를 확보하기 위한 마케팅 활동을 하는 것이 아니라 통신 인프라를 판매하는 판매자 역할을 하게 됩니다. 사업자에 의한 네트워크의 벌크(BULK) 판매가 가능하고 개인이 구매한 여유/유휴 네트워크 자원의 재판매와 소유권 변경도 가능합니다. 또한, 네트워크의 공동구매와 공동소비도 가능합니다. 네트워크 거래는 사용량 기준이나 금액 기준으로 계약할 수도 있고 공동 소비를 위한 합산 구매도 가능합니다.



4. 실물 상품 거래

디비엑스씨포트는 실물 거래를 지원하여 판매자와 소비자 그리고 배송업체 간의 직거래 생태계를 구성합니다. 오프라인의 유통 단계를 단순화했던 온라인 쇼핑몰 및 오픈마켓도 이제는 대형화 혹은 특정 기업에 종속적인 구조로 인하여 또 다른 문제점을 양산하고 있습니다. 제품에 대한 소비자의 선택권이 상대적으로 제한되어 버렸고 대형 유통업자들이 만들어 놓은 생태계는 수많은 문제점을 야기하고 있습니다.

철저한 에스크로(ESCROW)제와 상품 확인제를 통해 온라인 쇼핑에서 발생하는 사기, 품질불량, 배송지연, 탈세 등의 문제점을 원천적으로 차단하게 됩니다. 즉, 판매 물품에 대한 정확한 인증 시스템과 배송 상태의 투명한 모니터링 그리고 거래에 대한 확실한 증빙과 거래 금액에 대한 정확한 분배가 이루어집니다.

실물 거래는 생산자와 소비자가 직접 연결되고 소비자가 가격 및 배송업체를 선택하게 됩니다. 생산

채굴자들은 수익과 비용의 균형 사이에서 절충을 선택해야 하는데, fee와 블록을 만드는 것에 대한 자신만의 “soft-limit”에 대한 균형입니다. 또 위조 트랜젝션을 막기 위해서 최대 블록 사이즈에 대한 핵심 규칙은 필수적입니다. 하지만 이러한 값은 수정할 수 있어야 합니다.

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

트랜젝션 사이즈는 명시적으로 제한될 필요가 없습니다. 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 있습니다.

2.3.7.3 트랜젝션 스크립트

크립토노트는 굉장히 최소화된 스크립트 서브시스템을 가지고 있습니다.

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, cmp 입니다. 수신자들이 이 지출을 소비하게 되면, 0 ≤ k ≤ n 의 서명을 생산하고, 트랜젝션 input으로 전송하게 됩니다. 확인 과정은 단순히 s Φ with xi = 1를 평가하여 공개키 Pi에 대한 유효한 서명을 체크하며, Xi=0임을 확인합니다. 확인자는 만약 Φ > 0인 경우에 proof를 받아 들입니다.

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

o multi-/threshold 서명. 비트코인 스타일의 “N 개중 M ro” multi 서명(수신자는 적어도 0 ≤ M ≤ N 의 유효한 서명을 공급) 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 있습니다. 마스터키는 Φ = max(M · x, x1 + x2 + . . . + xN) ≥ M에 상응합니다. 이러한 방식으로 복잡한 상황을 간단하게 표현할 수 있습니다.

o 암호의 보호. 비밀 암호를 보유한 것은 개인 키에 대한 지식을 보유한 것과 동등하며, 확정적으로 암호 k=KDF(s)로부터 도출됩니다. 따라서 수신자는 k key 하의 또 다른 서명을 제공함으로써 비밀번호를 안다는 사실을 입증할 수 있습니다. 송신자는 단순히 자신의 output에 상응하는 공개 키를 추가하면 됩니다. 이러한 방식은 Bitcoin에서 사용되는 “transaction puzzle”보다 상당히 안전합니다.

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

만약 공개키와 통합된 output script가 송신자에게 지나치게 클 경우에, 특별한 output type을 이용할 수 있습니다. 송신자가 단지 그것에 대한 해쉬를 공급하는 반면 수신자는 이 데이터를 그의 input으로 보내게 될 것입니다. 이러한 접근은 Bitcoin의 “pay-to-hash”와 유사한 방식입니다. 새로운 스크립트 명령

* 만약 Alice가 Bob의 주소로 보낸 트랜젝션을 확인하려면, r을 공개하거나, zero-knowledge protocol을 사용하여 그가 r을 안다는 것을 입증하면 됩니다(예를 들어 트랜젝션을 r로 서명할 수 있음)

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

2.3.5 일회용 ring signature

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

우선 전자화폐와는 별도로 ring signature 알고리즘을 설명하겠습니다.

1회용 ring signature은 4개의 알고리즘을 포함합니다.(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 단순합니다. 한 사용자가 1개의 특정한 공개키가 아니라 여러개의 공개키 세트로 체크될 수 있는 서명을 한 사용자가 생성합니다. 소유주가 동일한 열쇠 짝을 이용하여 두번째 서명을 발행하지 않는 한, 서명자의 아이덴티티는 공개 키의 동일한 세트 중에서 구별할 수가 없습니다.

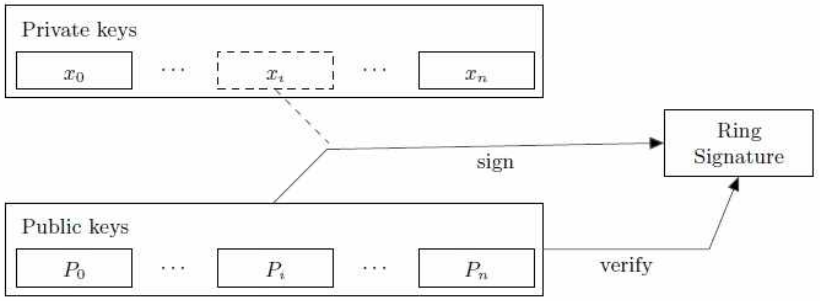


Fig. 6. Ring signature anonymity.

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

SIG : 서명인은 기술을 활용하여 1회용 ring signature를 비상호작용적인 zero-knowledge proof와 함께 생성합니다. 서명인은 다른 이용자들의 공개 키Pi, 자신만의 keypari (x,P), Key image I로부터 랜덤한 하위집합 S0를 선택합니다. S(그의 공개키는 Ps)에서의 서명인의 비밀 인덱스를 0 ≤ s ≤ n 라고 합니다.
서명인은 랜덤의 {qi | i = 0...n}를 선택하며 (1...l)로부터 {wi | i = 0...n,i 6= s}를 선택하며, 다음의 변환에 적용됩니다.

2. 최신 ASIC 파이프라인에 대해서 1MB의 내부 메모리는 부적절합니다.
3. GPU의 uddn tnqor의 인스턴스를 동시에 처리할 수 있으나, GDDR5 메모리는 CPU의 L3캐쉬보다 느리고, 대역폭은 넓지만 랜덤 엑세스 속도는 낮습니다.
4. scratchpad가 확장되면 필연적으로 반복적 계산이 증가하게 되며, 전체적인 시간이 증가하게 됩니다. 신뢰성이 낮은 p2p 네트워크에서 많은 계산량은 심각한 취약점으로 남을 수 있는데, 왜냐하면 node는 모든 새로운 블록의 proof-of-work에 대하여 체크할 의무가 있기 때문입니다. 만약 node에서 각각의 해쉬 평가에 대해 상당한 시간을 소모한다면, 임의 작업 데이터로 가득 찬 가짜 오브젝트들로 인한 Ddos 공격에 취약해집니다(nonce value)
5. 더 많은 장점들
6. 안정적인 통화량 발행

크립토노트 전자 코인의 상한값(upper bound)은 MSupply = 2^54 -1 원자단위(atomic units)입니다. 이러한 것은 기술적인 제한값이며, “N개의 코인이 충분하다”라는 직관적 방식에서 계산된 것이 아닙니다.
발행 과정을 안정적으로 유지하기 위하여 블록 리워드에 대해 다음과 같은 공식을 사용합니다.

BaseReward = (MSupply − A) >> 18

여기에서 A는 이전에 생산된 코인의 양을 의미합니다.

2.3.7 수정 가능한 파라미터

2.3.7.1 난이도

크립토노트에서는 모든 블록마다 난이도를 변경시킵니다. 네트워크 해쉬레이트가 급격하게 성장하거나 감소할 때에 대한 반응시간이 낮아질 수밖에 없고, constant block rate로 고착됩니다. 원래의 Bitcoin 방식에서는 마지막 2016개의 블록간의 목표 기간과 실제 기간을 비교하게 되고, 이를 현재의 난이도에 대한 배수(multiplier)로 적용합니다. 이러한 비트코인의 방식에 따르면 난이도가 급증 급락한다는 점이 단점입니다.
크립토노트의 기본적인 알고리즘은 node에 의하여 계산된 모든 work를 합하고, 그들이 소비한 시간으로 나누는 것입니다. 일의 단위는 각각의 블록의 난이도 값에 상응합니다. 하지만 time stamp에서의 부정확성과 비신뢰성 때문에 블록 사이의 정확한 시간 간격을 알아내기는 어렵습니다. 만약 한 유저가 time stamp를 미래로 전환한다면, 다음의 interval은 감소하거나 심지어 음수가 될 것입니다. 이러한 사례가 거의 없을 것으로 생각되며, 단지 time stamp를 정리하고 초과분을 소거할 것입니다(20퍼센트 정도) 나머지 값들의 범위는 80퍼센트의 상응하는 블록에 대하여 소비한 시간 값입니다.

2.3.7.2 사이즈 제한

사용자들은 블록체인을 저장하는 것에 대하여 지불하며, 사이즈에 해당하는 투표 권한을 가집니다. 모든

각의 access 마다 다시 계산하는 것보다 저장하는 것이 유리해집니다. 이 알고리즘은 내부적인 병렬성(internal parallelism)을 방지해야 하며, 따라서 N의 동시적인 쓰레드는 N배 많은 메모리를 요구해야 합니다.

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

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

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

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

2.3.6.3 새로운 알고리즘의 제안

proof-of-work 가격 설정 함수에 대해서 새로운 메모리 기반(memory-bound) 알고리즘을 제안합니다. 느린 메모리에 대한 랜덤 엑세스에 의존하게 되며, 레이턴시 의존성을 강조합니다. 스크립트와는 다르게, 모든 새로운 블록(64바이트 길이)은 이전의 모든 블록에 의존적입니다. 결과적으로 메모리 절약기("memory-saver")는 계산 속도를 기하급수적으로 증가시킬 것입니다.

우리의 알고리즘은 다음의 이유로, 인스턴스당 2MB 정도를 요구합니다.

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

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

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

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 있습니다.

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

결과적으로, 확인자는 위 그림을 찾게 되며,
만약 등식이 성립한다면, 알고리즘 LNK를 작동하게 됩니다. 그렇지 않다면 확인자는 서명을 거부합니다.

LNK : 확인자는 I가 이전의 서명에서 사용되었는지를 조사합니다. 다중의 사용들에서 두 개의 서명들이 같은 비밀 키에서 만들어졌다는 것을 시사하게 됩니다.
프로토콜의 의미 : L 변환을 적용함으로써 서명자는 그러한 x가 적어도 Pi=xG라는 사실을 입증하게 됩니다. proof를 반복 불가능하게 하기 위해서 키 이미지를 I=xHp(P)로 설정합니다. 서명인은 같은 계수(ri,ci)를 활용하여 거의 동일한 명제인 "그러한 x가 적어도 Hp(Pi)=I·x^-1이라는 사실을 안다"는 것을 증명합니다.

만약 x에서 I로의 대응이 injection mapping이라면,

1. 어느 누구도 키이미지로부터 공개키를 복원할 수 없으며, 서명인을 알 수 없습니다.
2. 서로 다른 I들과 동일한 x를 가지고 두 개의 서명을 만들어낼 수 없습니다.

2.3.6 표준 크립토노트 트랜젝션

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

각 트랜젝션을 유효화하기 위해서, Bob은 추가적으로 단지 2개의 타원곡선(elliptic curve)을 다중 발행하고, Bob 소유의 트랜젝션인지를 확인하기 위하여 output 당 1개를 추가하게 됩니다. Bob은 각각의 output에 대하여 1회용 keypair (pi, Pi)를 복원하며, 지갑에 저장하게 됩니다. 단일한 트랜젝션인 경우에만 동일 소유주의 input으로 확인될 수가 있습니다.

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

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

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

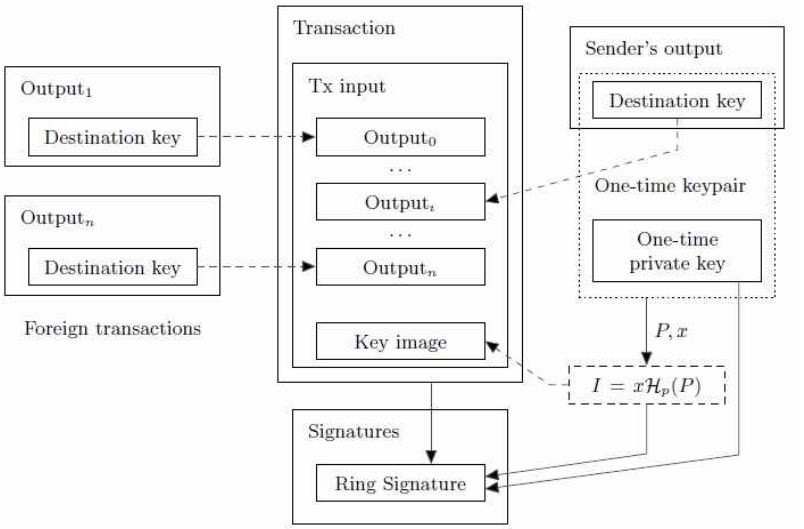


Fig. 7. Ring signature generation in a standard transaction.

2.3.6.1 평등화된 Proof-of-work

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

2.3.6.2 Related works

원래 Bitcoin의 proof-of work 프로토콜에서는 CPU에 중점을 둔 가격 결정 함수 SHA-256을 사용하였습니다. 주로 basic logical operators로 구성 되었으며, 프로세서의 계산 속도에 따라서 바뀌기 때문에 multicore/conveyer 의 적용에 완벽히 적절하였습니다.

하지만, 현대적인 컴퓨터의 경우 초당 operation 숫자에 의해서만 제한되는 것이 아니라, 메모리 사이즈에 의해서도 제한을 받습니다. 프로세서 간의 속도 차이가 상당할 수는 있으나 메모리 사이즈는 큰 차이가 없습니다.

메모리를 기준으로 가격을 결정하는 함수는 Abadi에 의하여 맨 처음 소개되었으며 “주로 메모리에 접속한 시간에 의하여 계산 시간이 결정되는 함수”라고 정의되었습니다. 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 것입니다. 블락이 충분히 커야만 각