레이븐코인: 자산 생성과 이동을 위한 피어 투 피어(P2P)방식의 전자 시스템

브루스 펜튼 (Bruce Fenton)

트론 블랙 (Tron Black)

www.ravencoin.org

작성일: 2018년 4월 3일

번역: Bradar (https://twitter.com/digitalwolfgamg)

웨스테로스('왕좌의 게임'의 주무대, 가상세계)에서, 까마귀들은 진실의 성명서를 전달하는 메신저 였습니다.
레이븐코인은 누가 어떤 자산을 소유하는지에 대하여 투명성을 전달하기 위해 디자인 되었으며,
현실에서의 실 사용 사례를 위한 블록체인 시스템 입니다

먼저 비트코인 설립자와 개발진들에게 감사를 표합니다. 레이븐코인 프로젝트는 레이븐코인 최초 포크일 기준으로 14,000 개 이상의 커밋을 만든 430 명의 비트코인 개발자의 노고와 지속적인 노력에 기반하여 시작 되었습니다. 우리는 안전한 네트워크 구축과 자유로운 오픈소스 소프트웨어 개발을 위한 모두의 노력에도 진심어린 감사의 말을 전합니다. 앞으로도, 레이븐코인 프로젝트는 여러분이 만들어 나가는 기반을 중심으로 하여, 발전해 나갈 것입니다.

개요. 레이븐코인은 토큰과 같은 자산(Asset) 전송에 최적화된 블록체인이자 플랫폼입니다. 비트코인 프로토콜의 UTXO 모델 기반의 광범위한 테스팅과 개발을 통해, 레이븐코인은 비트코인의 코드를 포크하여 탄생하였습니다. 주요 변화된 부분으로써, 블록 생성 시간(1분), 코인 발행량(210억개), 그리고 추가적으로 자산 생성 및 메시지 기능 추가가 있습니다. 레이븐코인은 비트코인과 같이 오픈소스 블록체인입니다. 모든 레이븐코인(RVN)은 공정하게 발행되며, 레이븐코인을 위해 개발된 'X16R' 합의 알고리즘을 증명하는 작업증명(PoW) 방식을 통하여, 공개적이며 투명하게 채굴이 가능합니다. 또한, 레이븐코인을 위한 자체적인 X16R이라는 합의 알고리즘도 있습니다. 또한 레이븐코인은 개인, 공개, 설립자 또는 개발자를 위한 별도의 할당량을 보관하지 않습니다. 레이븐코인은 보안, 사용자 제어, 개인 정보 보호, 그리고 검열 저항에 우선 순위를 둡니다. 필요에 따른 사용자를 위한 간단한 추가 기능 허용과 더불어, 어떤 방식으로도 사용 및 개발이 가능합니다.

1. 서론

블록 체인은 사용자에 의해 관리되는 무언가의 수량을 보여주는 일종의 원장입니다. 이것은 디지털화된 자산의 통제권을 타인에게 전달 가능하게 합니다. 블록체인 기술의 다양한 용도 가운데, 누가 무엇을 소유

하는지에 대한 보고는 가장 핵심적인 기능중 하나입니다. 이로 인해, 2008 년 10 월 31 일 사토시 나카모토 [1] 에 의해 발표 된 '비트코인'이 블록 체인 기술의 최초이자, 현재까지 가장 성공적인 사용 사례가 된 이유이기도 합니다.

이더리움 ERC20 프로토콜과 다른 프로젝트들은 다양한 목적들과 구조들로 이뤄진 다른 블록 체인을 사용하는 토큰화 된 자산을 생성할 수 있음을 보여줍니다. 토큰은 전통적인 지분 이나 다른 참여 메커니즘에 [빠른 전송 속도, 향상된 사용자 제어 및 검열 저항, 그리고 신뢰할 수 있는 제 3 자의 필요성 감소 또는 배제] 와 같은 여러 이점들을 제공합니다.

비트코인은 또한 옴니레이어, RSK 또는 카운터파티와 같은 프로젝트를 사용하여 토큰의 레일 역할로도 수행할 수 있습니다. 그러나 비트코인과 이더리움, 그 어느 하나도, 추가 자산의 소유권을 용이하게 하기 위해 특화 설계되지 않았으며, 사용자들과 개발팀들은 일반적으로 다른 기능에 우선 순위를 두었습니다.

레이븐코인은 '상호간의 자산 전송' 이라는 한 가지 특정 기능을 효율적으로 잘 처리하도록 설계되었습니다. 레이븐 프로토콜의 목표들중 하나는 비트코인 또는 다른 프로젝트에서 사용할 수있는 오픈소스 코드를 기여함과 동시에, 사용 사례에 중심화된 블록체인 형성과 특정한 사용 사례를 위한 이점들을 제공하기 위한 코드 작성을 위한 개발 노력을 이끌어 내는 것입니다.

세계 경제가 다양한 블록체인들을 사용하는 배우(의역: 사용자)들의 영향을 받는다면, 오늘날 자본 시장이 작동하는 방식 또한 바뀔 수 있습니다. 더욱 많은 자산이 거래 가능하게 됨으로, 국경이나 관할권의 관련이 더 적어 것이며, 국경을 넘어서는 거래는 자연스럽게 증가할 것입니다. 사람들이 비트코인을 사용하여 상당 부분의 자산을 즉각적으로 이전할 수 있는 시대가 도래하면, 소비자들은 유가 증권 및 유사한 자산들에 대해 동일한 효율성을 요구하게 될 것입니다.

2. 토큰과 기타 자산에 대한 배경

비트코인은 2009년 1월 3일, P2P 전자 현금 시스템으로 출시 되었습니다. 몇 년 후, 주목할 만한 수준의 보안 시스템이 검증 된 후에, 자산(Asset)들이 비트코인 블록 체인의 "상단에" 생성되거나 포함 가능함을 확인할 수 있었습니다. 새로운 자산은, 자산 발행 및 전송에 대한 정보를 전달하는, 안전하며 서명되어진 불변의 '비트코인 트랜잭션'을 통해 블록 체인에 추가될 수 있습니다.

비트코인 블록체인에 토큰을 추가한 여러 개의 프로젝트들이 있었습니다. 첫 번째는 J.R Willett의 의해 개발된 마스터코인 (Mastercoin) [2] 이였으며, 카운터파티 (Counterparty) [3] 와 다른 프로젝트들이 그 뒤를 이었습니다. 비트코인 블록체인에 기준한 자산 생성을 용이하게 하기 위해 개발된 프로토콜 중 하나로써, Colored Coins [4] 이 있습니다. Colored Coins를 통해 비트코인 프로토콜에서 주석란(Comment Field)의 역활과 같은 OP_RETURN [5]에서 특수하게 생성된 트랜잭션을 비트코인 트랜잭션에 표시할 수 있게 되었습니다.

비트코인 블록체인에 자산을 내장함으로 얻는 이점은 높은 수준의 보안성입니다. 비트코인은 각 블록을 "높은 난이도의 해시" [6] 로 보호하는 엄청난 양의 분산 채굴력이 있기 때문에, 많은 사람들에 의해 가장 안전한 블록체인으로 여겨집니다. 분산된 비트코인 노드들은 높은 난이도 해시를 생성하려는 레벨을 인식하기 때문에 굉장한 규모의 채굴 투자없이는 블록체인 장부를 재작성하거나 수정하는 것이 거의

불가능한 것입니다. 비트코인 블록체인을 변경하기 위해 장부를 재작성하거나 수정하기 위해서는, 한 국가의 운영 자금에 버금가는 개인 투자자의 상당한 노력을 필요로 하게 됩니다.

비트코인 블록체인에 자산들을 내장할 때, 비트코인 규칙들은 원본과 같이 작성되어져야 한다는 점과, 비트코인 노드들은 자산들이 내장되어 지고 있음을 인식하지 못한다는 단점이 있습니다. 즉, 비트코인 트랜잭션은 모든 자산 거래시에 필요하며, 거래의 우선 목적은 자산을 보내는 것이지만, 유효한 거래로 인식되기 위해서는 충분한 비트코인 트랜잭션이 이뤄져야 한다는 점입니다. 이는 불편하지만, 더욱 큰 단점은 내장된 자산 트랜잭션을 인식하지 못한 비트코인을 사용하는 비트코인 클라이언트는, 자산을 파괴한다는 점입니다. 예를 들어, 거래 상대방의 자산을 보유한 비트코인의 비트코인 개인키 (Private Keys) 보유자는 실수로 비트코인을 거래소나 다른 지갑으로 전송 후 그 자산을 잃을 수 있다는 점입니다. 이 문제를 위한 부분적인 해결책으로, 자산을 위해 사용되는 특수 주소 형식을 생성할 수 있지만, 이 또한 자산을 파괴하는 실수를 예방할 수는 없습니다. 다만, 트랜잭션에 자산이 내장되어 있다는 더욱 많은 단서를 제공할 뿐입니다.

ERC20, ERC721 및 ERC223 과 같은 기타 토큰 표준은 이더리움 또는 스마트 계약(Smart Contract)를 지원하는 다른 블록체인을 기반으로 합니다. 하지만, 스마트 계약 또한 다른 문제를 지니고 있습니다. 이더리움 네트워크는 이러한 스마트 계약 토큰들을 기본적으로 인식하지 못하기에, 몇몇 기본적인 문제들로부터 보호하기가 어렵습니다. 스마트 계약은 동일한 이름을 지닌 여러 개의 ERC20 토큰들의 형성을 가능하게 함으로, 사용자들에게 혼동을 줄 수 있습니다. 동일한 이름들을 지닌 계약들 사이의 유일한 구별점은 계약 해쉬 뿐입니다.

3. 완전 자산 인식 프로토콜 체계

누가 비둘기를 까마귀로 대체하는 것을 거부할 것인가? 그의 의지는 그의 논리에 의해 흔들렸다.
-윌리엄 쉐익스피어의 '한 여름밤의 꿈' 으로부터-

앞에서 언급된 문제들의 해결책은 완전히 자산을 인식하는 비트코인과 같은 유사한 시스템을 만드는 것입니다. 이러한 자산 인식 시스템은 두 가지의 큰 이점들을 제공합니다. 첫째, 클라이언트 및 RPC 명령을 통해 실수로 파괴될 수 있는 자산을 보호할 수 있습니다. 둘째, 단일 기본 클라이언트가 자산의 발행, 추적 및 이전을 실행할 수 있습니다. 추가적으로, 기본 자산에 보안성을 제공하기 위해, 비트코인과 같은 유사한 시스템은 시장성의 가치, 탄탄한 채굴 커뮤니티, 광범위한 분배의 전제하에 작동이 가능 합니다.

자산(Asset)
자산은 별도의 채굴없이, 레이븐 프로토콜 사용자에 의해 발행될 수 있는 일종의 토큰입니다. 레이븐 프로토콜 사용자는 이러한 자산을 생성하고, 해당 자산 프로토콜의 독립적인 목적 및 규칙을 결정합니다. 실험 계획안. 이러한 자산 또는 토큰은 레이븐코인 블록 체인에 존재하며 발행자(자산 생성자)가 원하는 어떠한 이름, 단체, 또는 목적성을 지닐 수 있습니다. 이 토큰들은 거래 가능하며, 비트코인 또는 유사하게 작동되는 암호화폐들과 같이 용이하게 이동이 가능합니다. 레이븐코인 블록체인에서, 한 자산은 제한된 수량과 고유한 상징성을 지니며, 어떤 레이븐코인 주소로도 이동이 가능합니다. 자산들은 오픈 에셋, 마스터코인, 카운터파티 같은 플랫폼들과 그리고 이더리움(Ehtereum)[9] 블록체인의 ERC20[7]와 ERC223[8]을 통하여 생성되어 왔습니다. 레이븐 프로토콜에서 생성된 자산들을 여러 이점들을 지니고 있습니다. 더욱 더

사용하기 편리하며, 기존의 코인과 긴밀하게 통합되며, 평등한 POW(작업증명) 방식의 채굴과 탈중앙화된 오픈소스 코드를 통해 보안성을 지닌다는 것입니다.

자산의 용도
자산 또는 토큰은 발행자의 상상력이 이끌어 낼 수 있는 모든 곳에 사용되어 질 수 있습니다. 이하 실제로 사용될 수 있는 아이디어 입니다.

실제 보관된 현실 세계의 물리적 자산 또는 디지털 자산의 토큰화

- 골드바
- 유로화 지폐
- 땅문서
- DC 코믹스 #26 (만화)
- 에너지 자산(전기,목재,가스,오일,풍력)

프로젝트의 지분 토큰화

- **증권 토큰:** 주권 서류 대신, 토큰 지분화를 통한 회사의 지분 또는 증권 배분
- 증권 또는 파트너쉽 이자 지불 시 레이븐코인으로 배당금 지불 (많은 자유 시장 국가에서는 합법)
- 조합, 제한된 파트너쉽, 로열티 또는 수익 분배 플랫폼을 위한 토큰
- 아이템을 이전하거나 재판매 할 수 있는 기능을 지닌 크라우드 펀딩 아이템을 위한 토큰

가상 상품 토큰화

- 재판매가 가능한 발티모어 레이븐스 게임과 같은 경기 티켓
- 특정 활동을 허용하는 라이선스
- 특정 서비스를 사용하기 위한 접속 토큰
- 게임 플랫폼 외부로 전송 가능한 게임 화폐 또는 아이템

크레딧 토큰화

- 기프트 카드
- 항공 마일리지
- 보상 포인트

사토시 나카모토는 비트코인을 중앙 집중식 시스템보다 사용자에게 더 많은 제어, 보안 및 개인 정보 보호 기능을 제공하는 웨이 다이의 비머니(bmoney) [10]를 구현한 블록체인으로 설명 하였습니다. 비트코인 소유자가 비공개로 남아 있으므로 인해, 폭력과 범죄를 막을 수 있는 잠재력을 지닌 체계를 만든 것입니다. 레이븐코인은 현금 대신 자산에 초점을 맞춤으로써 이러한 이점들을 유지하며, 사용자들은 안전한 블록체인에 그들이 만든 규칙들과 더불어, 사용자들이 관리하는 '자산'을 쉽게 발행할 수 있는 플랫폼을 제공합니다.

4. 레이븐코인 출시와 알고리즘

레이븐코인은 2017 년 10 월 31 일 [11] 에 발표되었으며, 비트코인의 발표 및 출시 9 주년인 2018 년 1 월 3 일, 채굴을 위한 바이너리를 출시했습니다. 레이븐코인은 사용자들이 자산을 발행하여 블록 체인에 통합할 수 있게 하는 비트코인과 유사한 시스템입니다. 이는 서로 연관성을 지니는 단계적인 개발을 통해 이루어집니다.

완료 사항

- 채굴풀들과 아식(ASIC)장비의 지배를 방지하기 위한 새로운 채굴 알고리즘 x16r [13]를 적용한 비트코인과 유사한 플랫폼 개발.
- 프리마인(Pre-mine) 미제공 및 넓은 배포를 위한 공정한 코인 출시.
- 채굴량의 증가, 레이븐코인의 자연스러운 가치 성장 그리고 플랫폼의 가치를 이해하는 소유자들에게 점진적인 지출 허용.
- 단순히 전기를 소모하거나 컴퓨터 하드웨어 업그레이드를 위해서가 아닌, 새로운 레이어로부터 오는 검열과 사용자 데이터 보호를 위한 큰 방어벽을 형성하는 가치있는 일에 중점을 두기 위한, POW(작업 증명) 방식의 채굴 활용.

5. 자산 발행 & 전송

그 어두움을 깊이 들여다 보면서, 나는 오랫동안 방황과, 두려움과, 의아함속에 어떤 인간도 감히 꿈꾸고자 하지 못했던 꿈을 꾸었다; 그러나 그 침묵은 깨어지지 않았고, 그 고요함은 어떤 것도 남기지 않았다.
– 에드거 앨런 포의 '까마귀' 로부터-

토큰명은 고유성이 보장 됩니다. 누군가 특정 토큰 이름을 먼저 발행할 때, 그는 해당 토큰의 소유자가 됩니다.

토큰 발행자는 레이븐코인(RVN)을 태우며, 고유한 토큰 이름을 제공해야 합니다. 발행자는 발행 수량, 소숫점 자리, 그리고 추후 동일 토큰의 추가 발행 허용 가능 여부를 결정하게 됩니다.

마스터코인(Mastercoin), 카운터파티(Counterparty) 또는 코인스파크(CoinSpark)와 유사한 방법을 사용한 다른 토큰 발행 허용합니다 [14].

GUI 지갑과 자산의 완벽한 통합 과 이해하기 쉬운 자산 관리를 제공하는 새로운 RPC 호출 작성이 가능하며, 쉬운 신규 자산 발행, 현재 잔액 보고 그리고 다른 사용자들에게 자산 전송의 편리성을 지니고 있습니다.

블록체인 기반의 토큰에 의해 사용 가능한 오픈소스와 공유 인센티브 메커니즘(인센티브 기법)의 결합은 전통적인 구조들이 할 수 없는 방식으로 이익(Interest)을 조정할 수 있게 합니다.

공정하며, 공개된 오픈소스 토큰 프로젝트는 사장, 지도자, 직원들 그리고 기업 구조를 참여자들의 이익 및 경제적 선택에 맞게 대체할 수 있습니다.

그렇게, 경우에 따라서는, 개인의 의견 또는 본의에 의해 동기부여와는 별도로, 오픈소스는 다른 구조들보다 새롭고 흥미로운 유형의 프로젝트들을 위한 더 나은 모델일지도 모릅니다. 레이븐코인은 한 프로젝트가 협동 조합, 기업, 또는 동업을 대표하는 토큰을 발행할 수 있게 합니다.

예를 들어, 협동 조합은 직원 및 참가자가 소유자인 일반적인 단체 입니다. 크레딧 에그리콜(Credit Agricole), REI, 랜드 오 레이크스(Land O' Lakes), 에이스 하드웨어(Ace Hardware), 고베 조합(Co-op Kobe), 썬키스트(Sunkist), 그리고 오션 스프레이(Ocean Spray)와 같은 대규모 단체는 협동 조합으로 구성되어 있습니다. 협동 조합은 참가자들에게 많은 이점들을 제공함에도 불구하고, 때때로 구조 및 유지면에서 어려움을 겪습니다. 협동 조합 이익을 토큰화함은, 이 구조가 자본 및 자원 할당에 사용될 수 있는 많은 새로운 방식을 열어줍니다. 각 토큰에 대한 규칙은 해당 토큰 발행자에 따라 달라질 수 있으며, 기록 보관은 작업이 분산된 레이븐코인 블록체인에서 이뤄지게 됨으로, 조직들은 다양한 종류의 참여 구조를 적용하고 효율적으로 사용할 수 있습니다.

게다가, 토큰은 발행자에 의해 고유하며, 제한적이며, 또는 대체 가능할 수 있으므로, 토큰 프로젝트 관리자들은 "클래스 A 주주," "소셜클럽 평생 멤버," "후원자," 또는 " OO 게임 아이템 소유자"와 같은 토큰 소유자 카테코리를 가질 수 있게 됩니다.

토큰은 소액 공공 기금의 발행을 더욱 용이하게 합니다.

"미래의 다국적 기업의 규모 분포는 지역 비즈니스의 규모(더 작은 단위를 뜻함) 까지 접근할 것입니다. 텔레콤 및 운송 비용이 "멜팅 포인트"를 통과하면서 다양한 새로운 다국적 소형 사업과 이 사업을 지지하기 위한 산업을 창조함으로, 이런 상태간의 상변화는 매우 빠를 수 있습니다." -소유자 권한 아래 안전한 재산 소유권(1998), 저자 닉 사보(Nick Szabo)-

경제학자 로버트 샤피로 박사는 토큰 발행을 통해 유치 사건으로 묶일 수 있는 월스트리트 사기 행위에 대한 중요한 증거를 마련함으로, 사기 행위를 줄일 수도 있다고 말합니다. [16]

오픈 프로토콜 만이 복잡하고 상충되는 규정을 지닌 여러 관할권이 있는 세계 경제에서 이용 가능 할 것입니다.

6. 보상

네이티브 토큰에 보상금 (또는 배당금) 지불 시스템을 접목시킬 수 있습니다. 단일 명령어로, RVN(레이븐코인)이 표시된 보상은 자동으로 균등하게 나눠지며, 자산 보유자들에 비례하여 나눠 집니다.

사례:

자산 발행을 허용하는 나라에 사는 한 어린 소녀는 레몬에이드 가판대 사업을 대표하는 토큰을 발행할 수 있습니다. 그녀가 10,000 개의 레몬에이드 토큰을 생성했다고 가정해 봅니다. 레몬에이드 가판대 사업을 위한 호주 달러 100 불(호주 달러 기준) 모금을 위해 한 레몬에이드 토큰당 호주 달러 0.01 불이라는 값을 제의할 수 있습니다. 이 토큰들은 사용자들에 의해 쉽게 판매되고 전송되어 질 수 있습니다. 이웃주민들이 이 사업을 위해 투자를 진행함으로, 이 레몬에이드 가판대가 성공적으로 진행되었다고 가정해 봅니다. 이제 이 가상의 8 세 소녀는 이 프로젝트를 지지해준 사람들에게 보상하기를 원합니다. 단일 명령으로, 그녀는 RVN 이 가질만한 어떤 가치로 표시된 이익을 레몬에이트 토큰 보유자들에게 보낼 수 있습니다. 그녀가 한 번도 만난적이 없는 새로운 토큰 보유자들이 있을수도 있습니다. 누구든 휴대폰이나 컴퓨터(윈도우, 맥, 또는 리눅스 운영체제)를 통하여 사용하기 편리한 내장기능을 전 세계 어디서든 이용할 수 있어야 합니다.

이러한 글로벌 시스템이 작동하기 위해서는, 규제 관할권으로부터 독립적이여야 합니다. 이는 이데올로기적 신념을 위해서가 아닌, 실용성을 높이기 위함 입니다: 블록체인 자산 전송이 검열 저항적이며 관할권이 구속 받는다면, 주어진 어떤 관할권이라도 다른 관할권과 문제를 일으킬 여지가 있습니다. 기존의 시스템에서의 재산은 일반적으로 소유자의 관할권에 국한되었기에, 해당 관할권의 정책에 따른 통제가 수월했습니다. 블록체인 기술의 특성으로 인해, 재산을 통제하는 능력을 지닌 어떤 프로토콜이든 잠재적으로 관할권 충동을 일으키고, 공정하게 운영될 수 없을 것입니다.

7. 고유 토큰(Unique Tokens)

토큰 소유자들은 고유 토큰을 통하여 고유 자산을 생성할 수 있습니다. ERC721 토큰처럼, 한 고유 토큰은 단 하나의 유일한 자산으로 남게 됩니다. 고유 토큰은 이를 다른 사용자의 주소로 전송함으로 인해 소유권을 변경할 수 있습니다.

고유 토큰 사례:

- 한 미술품 매매업자가 ART 라는 자산을 발행했다고 가정해 봅니다. 매매업자는 특정 이름이나 일련 번호를 각각의 미술품에 기입함으로 고유 ART 자산을 만들 수 있습니다. 이 고유 자산은 예술 작품과 더불어 진품을 증명하기 위한 도구로, 새 주인에게 전송될 수 있습니다. 토큰 ART:MonaLis(모나리자) 와 토큰:VenusDeMilo(밀로의 비너스)는 다른 이름으로 대체될 수 없으며, 예술작품들이 진품임을 증명할 수 있습니다.

- 한 소프트웨어 개발자는 자신이 개발한 소프트웨어 ABCGAME(예시)라는 이름으로 자산을 발행하여, 각각의 ABCGAME 토큰에 고유 아이디 또는 라이센스 키를 지정할 수 있습니다. 각각의 토큰들은 라이센스 소유권 이전의 목적으로 사용될 수 있습니다. ABCGAME:398222 와 ABCGAME:423655 는 각각 고유한 토큰임을 의미합니다.

- ZYX_GAME 이라는 게임이 있다고 가정할 때, 이는 게임 플레이어가 소유하고 사용할 수 있는, 고유 한정판 게임 자산을 생성할 수 있습니다.
  예시: ZYX_GAME:SwordOfTruth005(진실의검 005) / ZYX_GAME:HammerOfThor(토르의 망치)

이러한 게임 자산들은 보관이 가능하며, QR 코드와 지갑을 통해 다른 플레이어들과 교환하거나, 게임의 다른 버전이나 업그레이드를 통해 업로드 될 수 있습니다.

- RVN(레이븐코인) 기반의 고유 자산은 현실 자산들과 연동할 수 있습니다. GOLDVAULT(골드볼트:금 보관소를 지칭)라는 자산을 만든다고 가정해 봅니다. 금고에 있는 각각의 금화 또는 골드바는 일련 번호를 지정과 더불어 감사될 수 있습니다. GOLDVAULT:444322 와 GOLDVAULT:55599 같이 연관된 고유 자산을 생성하여 실제 금 보관소의 특정 자산을 대체할 수 있습니다. 공개 가능한 블록체인의 특성상, 완전한 투명성을 보장할 수 있습니다.

- CAR 이라는 토큰의 소유자는 자동차 등록 번호를 포함하는 각각의 차를 위한 고유 토큰을 발행할 수 있습니다.
  예시: CAR:19UYA31581L000000

고유 자산의 실 사용 사례:

- 소프트웨어 라이센스
- 자동차 등록
- 위조의 가능성이 있는 품목과 함께 전달하는 진품 증명 토큰
- 한 채널에서 소통을 허가하는 토큰(8. 주주간의 메시지 전송 참고)

8. 주주간의 메시지 전송

"만약 런던타워의 까마귀들이 사라지거나 날아가버린다면, 왕과 더불어 영국도 사라질 것이다."
-무명-

토큰 및 자산의 공통적인 문제는 토큰 생성자가 토큰 소유자들과 소통할 수 없다는 점입니다. 토큰 소지자는 신원이 확인되는 것을 원치 않을 수도 있기에, 소통은 매우 조심스럽게 이루어져야 합니다. 소통은 항상 토큰 소유자에게 참여에 대한 의무가 아닌 자율권을 줄 수 있어야 합니다. 메시지 시스템은 스팸 메시지 방지를 위해, 선별된 단체들만 메시지 시스템을 사용할 수 있도록 허용해야 합니다.

메시지 시스템은 고유 토큰을 사용하여 주 토큰 채널에서의 소통을 허용합니다. 예를 들어, COMPANY 토큰은 ~COMPANY 고유 토큰을 통하여 COMPANY 의 모든 소유자들에게 경보를 보낼 수 있습니다.

뉴스 레터, 게임 개발자, 비영리 단체, 활동가 단체, 기업 그리고 기타 독립체들은 특정 사용자들을 위해 토큰 발행이 가능할 것이며, 이메일이나 다른 메시지 전송 서비스와는 다르게, 토큰 소유자만이 사용 가능하며, 이를 통해 토큰을 전송할 수 있습니다.

승인된 발신자들이 토큰 소유자에게 전송하는 메시지는 고유 자산 위에 쌓이게 됩니다. 고유 자산은 채널 소유자에 의한 메시지 전송을 가능케 하는 "발언 막대기(talking stick)"의 역활을 하게 됩니다. KAAAWWW 프로토콜은 이 내용에 대한 별도의 추가 정보와 함께 공개될 것입니다.

9. 투표

기존 미국 금융 시스템의 많은 문제점 중 하나는, 모든 주식이 거리 이름(street name)으로 보유된다는 점입니다. 빠른 소통이 중요한 이 시대에, 이는 투표 실시를 굉장히 어렵게 하는 것입니다. 예를 들어, 나스닥(Nasdaq)에 주식을 발행하는 상장 기업은 주어진 시점에 단지 자사 주주들의 우편 주소를 받기 위해, 준독점회사에게 일정 비용을 지불해야 합니다. 그리고, 위임 투표 양식과 함께 토표 방법에 대한 정보가 있는 우편물(종이 양식)을 주주들에게 발송해야 합니다.

메시지 시스템을 사용하여, 토큰 소지자들은 투표에 대한 공지를 받을 수 있으며, 토큰 소지자들에게 투표 토큰을 자동적으로 부여함으로써, 클라이언트 또는 웹이나 레이븐코인에 내장된 프로토콜을 이용하는 모바일 인터페이스를 통하여 자동화 투표를 실행할 수 있습니다.

토큰은 투표권을 대체하기 위하여 생성됩니다. 레이븐코인은 정확한 수량의 투표(VOTE) 토큰을 발행할 것이며, 토큰 소유자에게 1:1 의 비율로 지급할 것입니다. 이 투표권은 프로토콜을 통하여 표수를 집계하는 주소로 전송될 수 있습니다. 투표 토큰이 자산과 동일한 방법으로, 전송될 수 있으므로, 때로는 위임 민주주의 또는 액체 민주주의 [17] 와 같은 방식의 '투표 위임'이 가능 합니다.

10. 개인 정보 보호

폭행 당사자들은 그들의 실명이나 소재지에 연계될 수 없기에, 폭력은 불가능하다.
폭력이 불가능하기에, 폭력 자체가 무력함을 뜻하는 공동체가 되는 것이다. (웨이 다이)

금융 시스템은 자산이 다른 것으로 대체 가능하며, 문제 없이 거래될 수 있을 때, 더욱 잘 기능 하기에 사생활 보호는 투자와 토큰의 핵심이라고 볼 수 있습니다. 메시지 전송, 자산, 보상과 같은 기능이 추가됨으로 인하여, UTXO 기반 암호화폐가 공개 주소로부터 신원(ID)를 분리하는 것과 동일한 방식으로, 개인 정보를 보호할 수 있습니다.

"우리는 프라이버시를 원하기 때문에, 거래 당사자는 해당 거래에 필요한 최소한의 지식만 가지고 있는지 확인하여야 합니다. 어떤 정보라도 노출될 수 있기에, 가능한 최소한의 정보만을 공개해야 합니다. 대부분의 경우 개인 신분은 주요한 문제가 아닙니다... 개인의 신원이 거래 기본 매커니즘에 의해 밝혀질 때, 우리는 프라이버시를 잃게 됩니다. 그로 인해, 당사자는 항상 자신을 노출할 수 밖에 없게 됩니다."
"그러므로, 열린 사회에서의 프라이버시는 익명의 거래 시스템을 필요로 합니다. 지금까지, 현금은 그러한 시스템의 표본으로 이어져 왔습니다. 익명 거래 시스템은 비밀 거래 시스템이 아닙니다. 익명 시스템은 개인이 원하는 때에 자신의 신분을 밝힐 수 있게 합니다; 이것이 바로 프라이버시의 본질입니다."
(에릭 휴즈) [18] .

11. 추가 내용

다른 프로젝트에서도 레이븐코인 체인을 사용할 수 있습니다. 특히, 비트코인 코드 기반을 공유하는 프로젝트를 위해 구축된 2 단계 프로토콜(second layer protocol)은 레이븐코인 프로젝트에서 구축될 수

있습니다. RSK, 라이트닝 네트워크(Lightening Network), 기밀 거래 그리고 다른 확장성 개선, 기타 등등의 다양한 오픈소스 프로젝트들은 레이븐코인 플랫폼에 구축된 프로젝트들을 위해서도 도움이 될 수 있습니다.

12. 결론

레이븐코인은 비트코인의 UTXO [19] 모델에 기반한 플랫폼 코인입니다. 여러 기능의 추가 목적으로 비트코인 코드를 수정하는 것은 실용적이지 않지만, 레이븐코인은 코드 포크와 새로 채굴 가능한 레이븐코인(RVN) 발행을 기반으로 구축된 플랫폼입니다. 레이븐코인은 자산, 보상, 고유 자산, 메시지 기능, 투표 기능을 추가할 것입니다. 레이븐 프로토콜의 기능들은 계획된 하드 포크 업그레이드를 통하여, 단계적으로 추가될 것입니다. 코드 기반은 사용자들과 개발자들이 안전성, 탈중앙화, 변조 방지를 유지할 수 있도록 설계 되었습니다.

레이븐코인 프로젝트는 조정된 비트코인 기반의 코드 베이스 또는 레이븐코인 블록체인에 추가된 네이티브 부가 기능들의 이점을 제공받을 수 있는 프로젝트, 2 단계 해결책, 실험, 그리고 비즈니스 아이디어들의 출발점 또는 베이스 역활을 할수 있을 것입니다.

이뉴잇족, 트링글리우스, 타히티인, 추치족, 수족, 하이다족 등 많은 민족들은, 사물을 변화 시키거나 무언가를 창조할 수 있는 아이디어 또는 힘의 상징이라고 여기는 까마귀(Raven)를 마력이 있는 비밀 책임자, 사기꾼, 창조주의 친구라고 부릅니다. 오픈소스에서 대중은 어느 한 사람이나 조직보다 더욱 많은 것을 이뤄낼 수 있는 힘이 있습니다. 레이븐코인 프로젝트는 여러분의 기여를 언제든지 환영합니다.

참고 문헌

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
[2] https://bravenewcoin.com/assets/Whitepapers/2ndBitcoinWhitepaper.pdf
[3] https://counterparty.io/
[4] https://en.bitcoin.it/wiki/Colored_Coins
[5] https://en.bitcoin.it/wiki/OP_RETURN
[6] https://bitcoinwisdom.com/bitcoin/difficulty
[7] https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[8] https://github.com/Dexaran/ERC223-token-standard
[9] https://www.ethereum.org/
[10] W. Dei, "B-Money" http://www.weidai.com/bmoney.txt
[11] B. Fenton, "Ravencoin: A digital peer to peer network for the facilitation of asset transfers." https://medium.com/@ravencoin/ravencoin-4683cd00f83c
[12] https://github.com/RavenProject/Ravencoin
[13] T. Black, J. Weight "X16R" Algorithm White Paper https://ravencoin.org/wpcontent/uploads/2018/03/X16R-Whitepaper.pdf
[14] http://coinspark.org/developers/assets-introduction/
[15] N. Szabo, "Secure Property Titles with Owner Authority" http://nakamotoinstitute.org/secure-propertytitles/#selection-7.7-7.50
[16] https://www.forbes.com/2008/09/23/naked-shorting-trades-opedcx_pb_0923byrne.html#63076e102e6c
[17] https://en.wikipedia.org/wiki/Delegative_democracy
[18] E. Hughes https://www.activism.net/cypherpunk/manifesto.html
[19] https://bitcoin.org/en/glossary/unspent-transaction-output