

# 레이븐코인(Ravencoin)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록  
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.  
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는  
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.  
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,  
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,  
투자 손실은 투자자에게 귀속됩니다.

## 레이븐코인(Ravencoin): 자산의 생성과 전송을 위한 P2P 전자 시스템

브루스 펜튼 (Bruce Fenton)

트론 블랙 (Tron Black)

[www.ravencoin.org](http://www.ravencoin.org)

2018년 4월 3일

가상의 세계 웨스테로스(Westeros)에서, 까마귀(Raven)는 진실의 메시지를 전하는 전령이다.  
Ravencoin은 “누가 어떤 자산을 소유하고 있는가”에 대한 진실의 메시지를 전달하기 위해 설계된,  
특정 사용 사례에 초점을 맞춘 블록체인이다.

비트코인의 창시자와 개발자들에게 깊은 감사를 드린다.

Ravencoin 프로젝트는 비트코인 코드 포크 시점까지 430명 이상의 비트코인 개발자들이  
14,000회 이상의 커밋을 통해 쌓아올린 노력과 헌신에 기반해 시작되었다.

우리는 안전한 네트워크를 구축하고 자유롭고 오픈소스 개발 문화를 지원한 그들의 헌신에  
영원히 감사한다. Ravencoin 프로젝트는 그들이 구축한 토대 위에 세워졌다.

---

### 초록 (Abstract)

**Ravencoin**은 토큰과 같은 자산을 한 보유자로부터 다른 보유자에게 전송하는 데 최적화된 블록체인이자  
플랫폼이다. 비트코인 프로토콜의 **UTXO(Unspent Transaction Output)** 모델을 광범위하게 개발·테  
스트한 결과를 바탕으로, Ravencoin은 비트코인 코드를 포크(fork)하여 구축되었다.

주요 변경 사항은 다음과 같다:

- **블록 생성 주기:** 1분
- **코인 발행량 조정:** 총 발행 수량은 변경되었지만, 분배 구조의 가중 스케줄(Weighted Distribution Schedule)은 동일하게 유지됨
- **기능 추가:** 자산 생성(Asset Creation)과 메시징(Messaging) 기능 추가

Ravencoin은 **완전한 오픈소스(Free and Open Source)** 프로젝트이다. 모든 **Ravencoin(RVN)**은 **x16r 알고리즘**을 사용하는 **작업증명(Proof of Work, POW)** 방식으로 공개적이고 투명하게 공정하게 발행·채굴된다. 사전 채굴(Pre-mine), ICO, 내부 할당(Founder/Developer Allocation)은 존재하지 않는다.

Ravencoin은 **보안(Security)**, **사용자 통제(User Control)**, **프라이버시(Privacy)**, **검열 저항성(Censorship Resistance)**을 최우선으로 한다. 또한, 어떤 관할권에서도 자유롭게 사용 및 개발할 수 있으며, 사용자의 필요에 따라 **간단히 확장 가능한 기능(Simple Additional Features)**을 제공한다.

## 1. 서론 (Introduction)

블록체인은 사용자가 통제하는 **무언가의 수량(Quantity of Something Controlled by a User)**을 기록하는 **원장(Ledger)**이다. 이는 디지털 표현물의 통제권을 다른 사람에게 **이전(Transfer of Control)**할 수 있도록 한다. 블록체인 기술의 수많은 활용 사례 중에서도, **누가 무엇을 소유하고 있는가(Who Owns What)**를 보고하는 기능은 그 핵심적 역할 중 하나이다.

이러한 이유로, 블록체인 기술의 **최초이자 현재까지 가장 성공적인 활용 사례**는 2008년 10월 31일 **사토시 나카모토(Satoshi Nakamoto)**가 발표한 **비트코인(Bitcoin)**이라 할 수 있다 [1].

이더리움의 **ERC-20 프로토콜** 및 기타 프로젝트들은, 다른 블록체인을 기반으로 다양한 목적과 구조를 가진 **토큰화된 자산(Tokenized Assets)**을 생성할 수 있음을 보여주었다. 토큰은 전통적인 주식이나 참여 방식에 비해 여러 가지 장점을 가진다.

예를 들어,

- 더 빠른 전송 속도(Faster Transfer Speed),
- 사용자 통제력 강화(Increased User Control) 및 검열 저항성(Censorship Resistance),
- 그리고 신뢰할 수 있는 제3자에 대한 의존성 감소 또는 제거(Reduction or Elimination of Trusted Intermediaries) 등이 있다.

비트코인 또한 **OmniLayer, RSK, Counterparty** 등의 프로젝트를 통해 토큰 발행의 기반(Rails)으로 사용될 수 있다. 그러나 비트코인과 이더리움은 **자산의 소유권 이전(Facilitating Ownership of Additional Assets)**을 위해 설계된 것이 아니며, 각 프로젝트의 사용자 및 개발 팀은 일반적으로 다른 기능적 우선순위를 가진다.

이에 비해, **Ravencoin**은 **자산을 한 사용자로부터 다른 사용자에게 효율적으로 이전(Transfer of Assets)**하기 위해 설계되었다. Raven 프로토콜의 목표 중 하나는 특정 기능에 최적화된 **사용 사례 중심 블록체인(Use-Case Focused Blockchain)**을 구축하는 것이다. 이를 통해 특정 사용 사례에 이점을 제공하는 코드를 개발하고, 동시에 비트코인이나 다른 프로젝트에서도 사용할 수 있는 **오픈소스 코드(Open**

**Source Code)** 발전에 기여하고자 한다.

만약 전 세계 경제가 여러 블록체인을 사용하는 다양한 행위자(Actors)의 영향을 받게 된다면, 오늘날의 **자본시장(Capital Markets)** 구조 역시 변화할 가능성이 높다. 더 많은 자산이 토큰화되고 국경 간 거래(Cross-Border Trading)가 점점 원활해짐에 따라, 국경과 관할권(Border and Jurisdiction)의 의미는 점차 줄어들 것이다. 비트코인을 통해 사람들이 거대한 부(Wealth)를 **즉시 이동(Instant Transfer)**할 수 있는 시대에는, 전 세계 소비자들 또한 자신들의 **증권(Securities)** 및 유사한 자산 보유에 대해서도 동일한 수준의 효율성과 편의성을 요구하게 될 것이다.

## 2. 배경: 토큰과 기타 자산 (Background: Tokens and Other Assets)

2009년 1월 3일, **비트코인(Bitcoin)**은 *P2P 전자 화폐 시스템(Peer-to-Peer Electronic Cash System)*으로 출시되었다. 수년 후, 비트코인이 일정 수준의 보안성을 확보한 뒤, 그 위에 자산을 “추가(온 톱으로 생성)”하거나 블록체인에 **임베딩(Embedded)**할 수 있다는 사실이 인식되었다. 새로운 자산은 비트코인 블록체인에 **안전하고 서명된 불변 거래(Secure, Signed, Immutable Transactions)**를 생성함으로써 추가할 수 있으며, 이 트랜잭션에는 자산 발행(Asset Issuance) 및 전송(Transfer)과 관련된 정보가 포함된다.

비트코인 블록체인에 토큰을 추가하려는 여러 프로젝트가 존재했다. 그중 **최초의 시도는 JR 윌릿(JR Willett)의 마스터코인(Mastercoin)**이었으며, 이후 **카운터파티(Counterparty)** 및 기타 프로젝트들이 뒤를 이었다. 비트코인 블록체인에서 자산 생성을 용이하게 하기 위해 개발된 프로토콜 중 한 부류는 **컬러드 코인(Colored Coins)**으로 알려졌다. 컬러드 코인은 비트코인 프로토콜의 OP\_RETURN 필드(주석 필드와 유사)에 특수한 트랜잭션을 삽입하여, 비트코인 트랜잭션에 **색을 입히듯 자산을 표시(Marking Transactions)**하는 방식으로 동작한다.

비트코인 블록체인에 자산을 임베딩하는 **가장 큰 장점은 높은 수준의 보안성(High Level of Security)**이다. 비트코인은 방대한 분산 채굴 파워가 존재하여, 각 블록을 “높은 난이도 해시(High Difficulty Hash)”로 보호하기 때문에 **가장 안전한 블록체인(Secure Blockchain)**으로 평가된다. 분산된 비트코인 노드들은 블록 생성에 요구되는 연산량(Proof of Work)을 인식하고 있기 때문에, 누군가가 막대한 채굴 자원 없이는 블록체인을 **재작성(Re-write)**하거나 **수정(Modify)**하는 것이 사실상 불가능하다. 비트코인 블록체인을 변조하거나 원장을 조작하려면 **국가 단위의 자금력(Nation-State Level Investment)**이 필요할 정도의 높은 난이도를 가진다.

그러나 자산을 비트코인 블록체인에 임베딩하는 데에는 **단점도** 존재한다. 비트코인의 규칙은 **원래 정의된 형태 그대로** 따라야 하며, 비트코인 노드들은 자산이 임베딩되었다는 사실을 인식하지 못한다. 즉, **모든 자산 거래(Asset Transaction)**는 반드시 **비트코인 트랜잭션(Bitcoin Transaction)**을 통해 수행되어야 하며, 자산 전송이 주된 목적이라 하더라도 해당 트랜잭션이 **유효한 비트코인 전송**으로 인정받기 위해서는 일정량의 비트코인을 함께 전송해야 한다.

이는 다소 불편할 뿐만 아니라, 더 큰 문제는 **비트코인 클라이언트가 임베딩된 자산을 인식하지 못하고 비트코인을 전송하면 자산이 소멸(Destroy)**된다는 점이다. 예를 들어, **카운터파티(Counterparty)** 자산을 보유한 비트코인 주소의 개인키를 가진 사용자가 이 비트코인을 거래소나 일반 지갑으로 전송하면, 해당 자산이 사라질 수 있다.

이를 부분적으로 해결하기 위한 방안으로, 특수한 **주소 형식(Special Address Format)**을 자산용으로 사용하는 방법이 제안되었다. 그러나 이는 자산 손실을 완전히 방지하지는 못하며, 단지 트랜잭션 내에 자산이 포함되어 있음을 식별할 수 있는 **단서(Clue)**를 제공할 뿐이다.

다른 토큰 표준인 **ERC20, ERC721, ERC223** 등은 스마트 컨트랙트를 지원하는 **이더리움(Ethereum)** 또는 기타 블록체인을 기반으로 구축되었다. 그러나 이 경우에도 **다른 유형의 문제**가 존재한다. 이더리움 네트워크는 이러한 **스마트 컨트랙트 토큰을 기본적으로 인식하지 못하기 때문에**, 일반적인 오류나 취약점을 방지하는 보호 기능이 부족하다.

또한 스마트 컨트랙트는 사용자에게 혼란을 줄 수 있다. 예를 들어, **동일한 이름(Name)**을 가진 **ERC20 토큰이 여러 개 존재할 수 있으며**, 이 경우 토큰 간의 유일한 구분 요소는 **컨트랙트 해시(Contract Hash)**뿐이다. 이는 사용자가 잘못된 컨트랙트로 거래를 수행할 위험을 증가시킨다.

### 3. 자산 인식형 프로토콜 수준 시스템 (Full Asset Aware Protocol Level System)

“누가 까마귀를 비둘기로 바꾸지 않으랴? 인간의 의지는 이성이 이끄는 법이다.”  
— 윌리엄 셰익스피어(William Shakespeare)

해결책은 **완전한 자산 인식형(Asset-Aware)** 비트코인 유사 시스템을 구축하는 것이다. 이 시스템이 자산 인식형으로 동작할 경우 두 가지 주요 이점이 있다. 첫째, 클라이언트 및 RPC 명령이 **자산이 실수로 소멸되는 것을 방지**할 수 있다.

둘째, 단일 네이티브 클라이언트에서 자산의 **발행(Issuance), 추적(Tracking), 전송(Transfer)**이 가능하다. 마지막으로, 이러한 자산의 보안을 보장하기 위해 비트코인 유사 시스템은 **시장 가치(Market Value), 강력한 채굴 커뮤니티(Strong Mining Community), 광범위한 분포(Wide Distribution)**를 바탕으로 운영되어야 한다.

#### 자산(Assets)

자산은 Raven 프로토콜 사용자에게 의해 발행될 수 있는 **토큰(Token)**이며, 채굴(Mining)을 필요로 하지 않는다. 사용자는 **Raven 프로토콜**을 통해 이러한 자산을 생성하며, 그 **용도와 규칙(Rules)**을 프로토콜로부터 독립적으로 설정한다.

이러한 자산 또는 토큰은 **Ravencoin 블록체인** 상에 존재하며, 각 자산·코인·토큰의 **이름(Name), 단위(Denomination), 용도(Purpose)**는 발행자가 자유롭게 정할 수 있다. 이 토큰들은 비트코인(Bitcoin)과 마찬가지로 **손쉽게 전송 가능(Transferable)**하며, 동일한 속도와 효율성을 가진다.

Ravencoin에서 자산은 **고유한 심볼(Symbol)**을 가진 **제한된 수량(Limited Quantity)**으로 정의되며, 모든 Ravencoin 주소로 전송할 수 있다.

자산 발행 기능은 이미 **Open Assets, Mastercoin, Counterparty**, 그리고 **이더리움(ERC-20, ERC-223)** 등의 플랫폼에서 오랫동안 제공되어왔다. 그러나 **Raven 프로토콜**에서 생성된 자산은 다음과 같은 뚜렷한 장점을 가진다:

- **사용 편의성(Ease of Use)**
- **네이티브 코인(Native Coin)**과의 강력한 통합(Tight Integration)
- **공정한 POW 채굴 및 오픈소스 코드 기반 보안(Fair Proof-of-Work & Open Source Security)**
- **중앙화 조직에 의해 운영되지 않음(Decentralization)**

### 자산의 활용 사례 (Uses for Assets)

자산 또는 토큰은 **창작자의 상상력(Imagination)**이 허락하는 한 모든 목적에 사용할 수 있다. 아래는 그 예시이다.

#### 1. 실물 또는 디지털 자산의 토큰화 (Tokenization of Real-World or Custodied Assets)

- 금괴 (Gold Bars)
- 은화 (Silver Coins)
- 실물 유로화 (Physical Euros)
- 토지 소유권 증서 (Land Deeds)
- DC Comics Presents #26 (희귀 수집품)
- 에너지 크레딧 (Electricity, Wood, Gas, Oil, Wind 등)

#### 2. 프로젝트의 지분 표현 (Representing a Share of a Project)

- **증권형 토큰(Security Tokens):**  
주식이나 회사 지분을 실물 증권이 아닌 **토큰(Token)**으로 표현.
- **배당형 자산(Dividend-Enabled Assets):**  
RVN으로 배당금을 지급할 수 있는 **파트너십 지분** 또는 **증권형 토큰**, (자유시장 국가에서는 합법적인 구조).
- **협동조합(Co-op), 유한책임조합(Limited Partnership), 로열티/이익공유 플랫폼(Royalty or Profit-Sharing Platform)**의 지분을 표현하는 토큰.
- **크라우드펀딩 자산(Crowdfunded Item)**을 표현하며, **양도(Transfer)** 또는 **재판매(Resale)** 기능을 내장한 토큰.

#### 3. 가상 상품의 표현 (Representing Virtual Goods)

- **이벤트 티켓(Tickets):**  
예: 볼티모어 레이븐스 경기 입장권 – 재판매 기능 포함.
- **라이선스(License):**

특정 활동을 허가하는 디지털 권한.

- **접근 토큰(Access Token):**  
특정 서비스 사용 권한을 제공.
- **게임 내 자산(In-Game Currency & Items):**  
게임 플랫폼 외부에서도 자유롭게 전송 가능한 아이템.

#### 4. 크레딧의 표현 (Representing a Credit)

- **기프트 카드(Gift Cards)**
- **항공 마일리지(Airline Miles)**
- **리워드 포인트(Reward Points)**

사토시 나카모토(Satoshi Nakamoto)는 비트코인을 **웨이 다이(Wei Dai)**의 *b-money* 구현체로 묘사했으며, 중앙화된 시스템보다 사용자가 더 많은 **통제(Control)**, **보안(Security)**, **프라이버시(Privacy)**를 가질 수 있도록 설계했다. 그 결과, 비트코인은 **사용자가 익명 상태로 자산을 보유할 수 있는 구조**를 통해 **폭력과 차별을 예방할 잠재력(Potential to Prevent Violence and Discrimination)**을 지닌 시스템으로 발전했다.

**Ravencoin**은 이러한 철학을 이어받아, **현금(Cash)** 외의 자산에 초점을 맞추고 있다. 사용자가 자신이 설정한 규칙에 따라 자산을 발행하고 통제할 수 있는 **보안성 높은 블록체인 플랫폼**을 제공함으로써, 누구나 자유롭게 **디지털 자산을 발행·관리·이전할 수 있는 환경**을 구축하는 것이 목표이다.

## 4. 라벤코인 출시 및 알고리즘 (Ravencoin Launch and Algorithm)

**Ravencoin**은 2017년 10월 31일에 발표되었으며, 비트코인 발표 및 출시 9주년 기념일에 해당하는 **2018년 1월 3일**, 채굴용 바이너리가 공개되었다. Ravencoin은 사용자가 자산을 **직접 발행(Issue)**하고 **블록체인에 통합(Integrate)**할 수 있도록 설계된 **비트코인 유사 시스템(Bitcoin-like System)**이다. 이는 단계적으로 진행되며, 각 단계가 이전 단계를 기반으로 구축되는 형태로 완성된다.

### - 진행 중(In Progress)

- **새로운 채굴 알고리즘 x16r**을 사용한 비트코인 유사 플랫폼을 구축한다. 이는 대형 채굴풀(Pool)의 즉각적인 지배와 ASIC 채굴기의 장기적 독점을 방지하기 위한 목적을 가진다.
- **사전 채굴(Pre-Mine)** 없이 **공정한 런치(Fair Launch)**를 통해 토큰을 광범위하게 분배한다.
- RVN의 채굴 속도를 점진적으로 늘리고, 토큰의 가치가 자연스럽게 상승하여 플랫폼의 가치를 이해하는 참여자에게 점진적으로 분배되도록 한다.
- **작업증명(Proof of Work, PoW)** 방식을 사용하지만, 이는 단순히 전기를 소비하거나 하드웨어 의존도를 높이기 위함이 아니다. Ravencoin은 “작업(Work)”의 가장 중요한 측면, 즉 **시간에 따라 누적되는 보안 벽(Time-based Security Wall)**을 구축하여 사용자 데이터를 미래의 조작과 검열로부터 보호하는 것에 초점을 맞춘다.

## 5. 자산 발행 및 전송 (Asset Issuance & Transfer)

“그 어둠 속을 깊이 들여다보며, 나는 오래도록 서서 궁금해하고, 두려워하고, 의심하며,  
인간이 전에 감히 꾸지 못했던 꿈을 꾸었노라,  
그러나 침묵은 깨어지지 않았고, 고요함은 아무런 징표도 주지 않았다.”  
— 에드거 앨런 포(Edgar Allan Poe), 『The Raven』

토큰의 이름은 **고유함(Unique)**이 보장된다.

즉, 동일한 이름으로 토큰을 최초 발행한 사용자가 해당 토큰 프로젝트의 소유자가 된다.

토큰 발행자는 **RVN을 소각(Burn)**해야 하며, 고유한 **토큰 이름(Token Name)**을 제공해야 한다. 또한 발행자는 다음을 직접 결정할 수 있다:

- 발행 수량(Quantity Issued)
- 소수점 자릿수(Decimals)
- 동일한 토큰을 향후 추가 발행할 수 있는지 여부

Mastercoin, Counterparty, CoinSpark 등과 유사한 방법으로 기타 자산의 발행을 허용한다.

Ravencoin은 **GUI 지갑과 자산 관리 기능을 긴밀하게 통합**하며, 이를 위한 새로운 RPC 호출 기능을 제공한다. 이를 통해 사용자는

- 새로운 자산을 손쉽게 발행(Issue New Assets)하고,
- 현재 잔고를 보고(Report Balances),
- 다른 사용자에게 전송(Transfer to Users)할 수 있다.

블록체인 기반 토큰이 제공하는 **오픈소스(Open Source)**와 **공유 인센티브 메커니즘(Shared Incentive Mechanisms)**의 조합은 전통적인 시스템으로는 불가능한 방식으로 **이해관계의 정렬(Aligned Interests)**을 가능하게 한다.

공정하고 오픈소스 기반의 토큰 프로젝트는 기존의 **고용 구조(Employers/Employees)**, **회사 형태(Corporate Structures)**, **지배 계층(Rulers)** 등을 참여자의 경제적 선택(Economic Choice)과 이 해관계로 대체할 수 있다.

따라서, 이타적 동기(Selfless Motivation)든, 이기적 동기(Selfish Motivation)든, 오픈소스 모델은 다양한 새로운 형태의 프로젝트를 위한 **보다 효율적이고 유연한 조직 모델**이 될 수 있다. Ravencoin은 **협동조합(Co-op)**, **법인(Corporation)**, **파트너십(Partnership)** 등 다양한 형태의 조직이 토큰을 발행하여 이를 대표할 수 있도록 지원한다.

### 협동조합(Co-ops)의 예시

협동조합은 **참여자(Participants)**와 **직원(Employees)**이 **공동 소유자(Owners)**가 되는 일반적인 조직 형태이다. 대표적인 예시로는 다음과 같은 대형 조직이 있다:

- Credit Agricole
- REI
- Land O' Lakes
- Ace Hardware
- Co-op Kobe
- Sunkist
- Ocean Spray

이러한 구조는 참여자에게 많은 이점을 제공하지만, 기존 방식으로는 설립 및 유지가 어려운 경우가 많다. **협동조합의 이익을 토큰화(Tokenizing Co-op Interests)**함으로써, 자본 및 자원의 배분 구조를 새롭게 효율적인 방식으로 구현할 수 있다.

Ravencoin 블록체인은 분산된 작업(Distributed Work)에 의해 관리되므로, 각 조직은 토큰의 규칙을 자체적으로 변경하고, 다양한 참여 구조를 손쉽게 배포할 수 있다.

또한, 토큰은 발행자의 의도에 따라 **고유(Unique)**, **한정(Limited)**, 혹은 **대체 가능(Fungible)**하게 만들 수 있다. 따라서 토큰 프로젝트 관리자는 다음과 같은 다양한 카테고리의 토큰 보유자를 정의할 수 있다:

- “A등급 주주(Class A Shareholders)”
- “평생 회원(Lifetime Social Club Members)”
- “후원자(Benefactors)”
- “게임 내 특정 아이템 보유자(Holders of \_\_\_\_\_ In-Game Item)”

## 소규모 공개 발행(Small-Scale Public Offerings)

토큰은 **소규모 기업공개(Micro IPOs)**를 훨씬 간단하게 수행할 수 있도록 한다.

“미래에는 다국적 기업의 규모 분포가 지역 비즈니스와 유사해질 것이다.  
통신 및 운송 비용이 ‘융점(Melting Point)’을 지나면서  
스타트업에서 성숙한 기업으로의 전환 속도는 매우 빨라질 것이며,  
이로 인해 새로운 형태의 다국적 중소기업과  
이를 지원하는 다양한 산업이 등장하게 될 것이다.”

— 닉 재보(Nick Szabo), 「Secure Property Titles with Owner Authority」, 1998

이러한 구조는 **사기(Fraud)** 감소에도 기여할 수 있다. 경제학자 **로버트 샤피로(Dr. Robert Shapiro)**는 **월가(Wall Street)**에서 발생한 사기의 상당수가 **자산 보관(Custody)** 문제와 연관되어 있음을 지적했다 (패트릭 번, PhD의 연구에 의해 뒷받침됨).

글로벌 경제에는 복잡하고 상충되는 **규제(Regulations)**가 존재하는 여러 관할권이 있기 때문에, **전 세계적으로 작동하기 위해서는 오픈 개방형 프로토콜(Open Protocol)**만이 효과적으로 기능할 수 있다.

## 6. 보상 (Rewards)

Ravencoin은 네이티브 토큰(RVN)으로 보상 또는 배당금(Rewards or Dividends)을 지급할 수 있다.

단 하나의 명령으로, RVN으로 표시된 보상 금액이 자산 보유자에게 비례(pro-rata)로 자동 분배된다.

---

## 예시 (Example):

한 어린아이가, 해당 행위를 허용하는 국가에서, 레모네이드 가판대 사업(Lemonade Stand Business)을 나타내는 토큰을 만들었다고 가정하자. 그녀는 10,000개의 LEMONADE 토큰을 발행하고, 개당 AUD\$0.01로 판매하여 총 AUD\$100을 모아 사업을 시작할 수 있다.

이 토큰은 구매자 간 쉽게 전송 및 거래 가능(Transferable)하며, 만약 이 가상의 사업이 성공하여 동네 전체가 그녀의 프로젝트에 투자하게 되었다면, 이제 8살짜리 소녀는 자신을 믿어준 사람들에게 이익(Profits)을 돌려주고 싶을 것이다.

그녀는 단 한 번의 명령으로, RVN 단위의 이익금을 LEMONADE 토큰 보유자들에게 자동 분배할 수 있다. 그녀는 새로운 투자자, 즉 한 번도 만나본 적 없는 LEMONADE 토큰 보유자들에게도 보상을 줄 수 있다. 이러한 내장된 편의성은 전 세계 누구나, 모바일 폰이나 Windows, Mac, Linux 기반 컴퓨터를 통해 손쉽게 이용할 수 있도록 한다.

이러한 글로벌 시스템(Global System)이 작동하기 위해서는, 규제 관할권(Regulatory Jurisdictions)으로부터 독립적(Independent)이어야 한다. 이는 이념적 신념 때문이 아니라 실용적 이유(Practicality) 때문이다.

만약 블록체인 자산 전송 시스템이 검열 저항성(Censorship Resistance)과 관할 무관성(Jurisdiction Agnosticism)을 갖추지 못한다면, 하나의 관할권에서 허용되는 행위가 다른 관할권과 충돌하게 될 것이다.

기존 금융 시스템에서는 자산이 보유자의 관할 지역(Jurisdiction) 내에 한정되어 있었기 때문에, 해당 지역의 정책에 따라 자산을 통제하기가 쉬웠다. 그러나 블록체인은 국경을 초월한(Global) 기술이므로, 프로토콜 수준에서 자산을 통제하려는 모든 시도는 관할권 간 충돌(Jurisdictional Conflict)을 초래하며, 공정한 운영이 불가능하게 된다.

## 7. 고유 토큰 (Unique Tokens)

고유 토큰(Unique Tokens)은 토큰 보유자가 유일한 자산(Unique Asset)을 생성할 수 있게 한다. 이들은 ERC-721 토큰과 유사하게, 오직 하나만 존재하며 복제 불가하다. 고유 토큰은 다른 사용자의 주소로 전송하여 소유권(Ownership)을 이전할 수 있다.

### 고유 토큰의 예시 (Examples of Unique Tokens):

- 예술품 거래소의 활용 (Art Assets):

예술품 딜러가 ART라는 자산을 발행했다고 가정하자. 그는 각 예술 작품에 고유한 이름(Name)이

나 **일련번호(Serial Number)**를 부여하여 고유한 ART 자산을 생성할 수 있다. 예를 들어, **ART:MonaLisa**와 **ART:VenusDeMilo**는 서로 대체 불가능(Non-Fungible)하며, 각각 다른 작품을 나타낸다. 이러한 토큰은 작품의 **진위성 증명(Proof of Authenticity)**으로 사용될 수 있다.

- **소프트웨어 라이선스 (Software Licensing):**

소프트웨어 개발자가 **ABCGAME**이라는 자산을 발행하고, 각 게임 라이선스에 고유 ID 또는 키를 부여할 수 있다.

예: **ABCGAME:398222**, **ABCGAME:423655**

해당 토큰은 게임 라이선스의 이전(Transfer)에 따라 함께 이동한다.

- **게임 내 자산 (In-Game Assets):**

게임 **ZYX\_GAME**이 한정판 인게임 아이템을 생성할 수 있다.

예: **ZYX\_GAME:SwordOfTruth005**, **ZYX\_GAME:HammerOfThor**

이러한 자산은 QR 코드나 지갑을 통해 다른 플레이어와 교환 가능하며, 게임의 다른 버전으로 이전(Upgrade or Transfer)할 수도 있다.

- **실물 자산 연동 (Real-World Asset Backing):**

**GOLDVAULT**라는 자산을 만들고, 금고 내의 각 금화나 금괴를 일련번호로 관리할 수 있다.

예: **GOLDVAULT:444322**, **GOLDVAULT:555994**

이러한 고유 자산은 **실제 금고 내의 개별 자산을 대표**하며, 블록체인의 공개 특성으로 인해 **완전한 투명성(Full Transparency)**이 보장된다.

## 또 다른 예시 (Additional Example):

**CAR**라는 자산 보유자가 각 차량의 **차대번호(VIN)**를 이용해 고유 토큰을 발행할 수 있다.

예:

**CAR:19UYA31581L000000**

---

## 고유 자산의 주요 활용 사례 (Use Cases for Unique Assets):

- 소프트웨어 라이선스 관리 (Software Licensing)
- 차량 등록 (Car Registration)
- 진품 인증용 토큰 (Proof-of-Authenticity Tokens):  
위조 가능성이 있는 상품에 진위 인증 토큰을 함께 전송
- 통신 채널 접근 제어 (Messaging Access Tokens):  
특정 메시징 채널에 접근할 수 있는 권한을 제공

---

이처럼 Ravencoin의 **Unique Token** 시스템은 실물 자산에서 디지털 콘텐츠까지, 소유권, 진위성, 사용권이 필요한 모든 영역에서 **명확하고 검증 가능한 디지털 표현(Verifiable Digital Representation)**을 가능하게 한다.

## 8. 이해관계자 메시징 (Messaging Stakeholders)

“런던탑의 까마귀가 사라지거나 날아가면, 왕관이 무너지고 영국도 함께 무너질 것이다.”  
— 익명 (Unknown)

토큰 또는 자산 시스템에서 자주 발생하는 문제 중 하나는, **토큰 발행자(Issuer)**가 **토큰 보유자(Token Holder)**와 직접적으로 소통할 수 없다는 점이다. 이 문제는 매우 신중히 다뤄져야 한다. 왜냐하면 토큰 보유자가 **신원 공개를 원치 않는 경우가 많기 때문이다**.

따라서 메시징 시스템은 다음 조건을 충족해야 한다:

- 토큰 보유자는 언제든지 **수신 거부(Opt-out)**를 선택할 수 있어야 한다.
- 메시징 채널은 **허가된 당사자(Authorized Parties)**만 사용할 수 있어야 하며, 스팸 전송 통로(Spam Conduit)가 되어서는 안 된다.

## 메시징 시스템 구조 (Messaging System Structure)

이 메시징 시스템은 **고유 토큰(Unique Tokens)**을 활용하여 메인 토큰 채널(Main Token Channel) 상의 통신을 가능하게 한다.

예를 들어, 회사가 **COMPANY**라는 토큰을 발행했다면, 해당 토큰에는 **~COMPANY:Alert**라는 고유 토큰이 연결되어 COMPANY 보유자 전원에게 **알림(Alert)**을 전송할 수 있다.

## 활용 예시 (Use Cases)

뉴스레터 발행자, 게임 개발자, 비영리 단체, 활동가 조직, 기업 등은 특정 사용자 그룹을 위해 토큰을 발행하고 그 보유자들에게 메시지를 전송할 수 있다.

단, 이메일이나 일반 메시징 서비스와 달리, 이 시스템에서는 **해당 토큰 보유자만 메시지를 수신할 수 있으며**, 이는 곧 **메시지 권한이 토큰과 함께 양도(Transferable)**됨을 의미한다.

## 프로토콜 동작 (Protocol Mechanism)

토큰 보유자에게 메시지를 보낼 수 있는 권한은 **인증된 발신자(Authorized Sender)**에게만 부여되며, 이는 **고유 자산(Unique Asset)** 계층 위에 구현된다.

고유 자산은 “**말하는 지팡이(Talking Stick)**”처럼 작동하여, 채널 소유자(Channel Owner)가 메시지를 보낼 수 있도록 한다.

이 시스템의 세부 구조는 **KAAAWWW 프로토콜(The KAAAWWW Protocol)**이라는 이름으로 별도의 문서에서 자세히 공개될 예정이다.

## 9. 투표 (Voting)

현재 미국 금융 시스템의 주요 문제 중 하나는 **모든 주식이 ‘Street Name’ 형태로 보관된다는 점**이다. 이는 신속한 통신이 가능한 현대 사회에서 투표 절차를 비효율적이고 복잡하게 만든다.

예를 들어, 나스닥(Nasdaq)에 상장된 공개기업이 주주 투표를 실시하려면, 먼저 특정 시점의 **주주 주소 목록**을 얻기 위해 거의 독점적인 제3기관에 비용을 지불해야 한다. 그 후, **종이 우편(Physical Mailing)**으로 투표 안내문과 위임장(Proxy Voting Form)을 발송해야 한다.

## Ravencoin을 활용한 개선 (Voting via Ravencoin)

Ravencoin의 **메시징 시스템**을 활용하면 토큰 보유자에게 **투표 공지(Notification)**를 자동으로 전달할 수 있다. 또한 각 토큰 보유자에게 **VOTE 토큰**을 자동 발행함으로써, 클라이언트·웹·모바일 인터페이스를 통해 **자동화된 투표(Automated Voting)**가 가능하다.

Ravencoin은 **정확히 동일한 수량의 VOTE 토큰**을 생성하고, 이를 **기존 토큰 보유자에게 1:1 비율(1:1 Distribution)**로 분배한다. 이후 투표자는 해당 VOTE 토큰을 프로토콜 내에서 지정된 주소로 전송하여 **투표 결과 집계(Tallying)**를 수행한다.

## 위임 민주주의(Delegative or Liquid Democracy)

Ravencoin의 투표 토큰은 일반 자산처럼 이동할 수 있기 때문에, **투표 위임(Delegation of Votes)**이 가능하다. 즉, 보유자가 자신의 투표권을 다른 사용자에게 위임할 수 있으며, 이는 흔히 **위임 민주주의(Delegative Democracy)** 또는 **유동 민주주의(Liquid Democracy)**로 불린다.

이를 통해 Ravencoin은 **투명하고 자동화된 디지털 거버넌스(Digital Governance)**를 블록체인 네이티브 환경에서 실현할 수 있게 된다.

# 10. 프라이버시 (Privacy)

“이곳은 폭력이 무의미한 공동체이다.

폭력이 불가능하기 때문에 폭력의 위협도 무력하며,

폭력이 불가능한 이유는 참여자들이 자신의 진짜 이름이나 물리적 위치와 연결될 수 없기 때문이다.”

— 웨이 다이 (Wei Dai)

프라이버시는 **투자(Investments)**와 **토큰(Tokens)**에서 핵심적 요소이다. 금융 시스템은 자산이 **대체 가능(Fungible)**하고 **마찰 없는 거래(Frictionless Trading)**가 가능할 때 가장 효율적으로 작동한다. 따라서 Ravencoin 프로젝트는 향후 기술적 발전이 이루어짐에 따라 가능한 모든 방식으로 **프라이버시를 강화(Strengthen Privacy)**하는 방향으로 나아가야 한다.

메시징, 자산, 보상 등 새로운 기능이 추가되더라도, Ravencoin은 **UTXO 기반 암호화폐(UTXO-Based Cryptocurrencies)**처럼 **개인 신원(Identity)**과 **공개 주소(Public Address)**를 분리함으로써 프라이버시를 유지한다.

\*“우리가 프라이버시를 원한다면,  
거래의 각 당사자는 해당 거래에 직접적으로 필요한 정보만 알아야 한다.  
모든 정보는 공유될 수 있기 때문에, 우리는 가능한 한 적게 공개해야 한다.  
대부분의 경우, 개인의 신원은 본질적으로 중요하지 않다.

만약 거래의 근본적인 메커니즘이 나의 신원을 노출한다면, 나는 프라이버시를 잃는다.  
나는 선택적으로 나 자신을 드러낼 수 없으며, 항상 공개될 수밖에 없다.

그러므로 열린 사회에서의 프라이버시는 **익명 거래 시스템(Anonymous Transaction System)**을  
필요로 한다.

지금까지 현금(Cash)이 이러한 시스템의 대표적인 예였다.

익명 거래 시스템은 **비밀 거래 시스템(Secret System)**이 아니다.

익명 시스템은 개인이 원할 때, 그리고 원할 때에만 자신의 신원을 공개할 수 있게 해준다.

이것이 바로 프라이버시의 본질이다.”\*

— E. 휴즈 (E. Hughes)

## 11. 추가 사항 (Additional)

다른 프로젝트들도 **Ravencoin 체인**을 사용할 수 있다. 특히, **비트코인 코드베이스(Bitcoin Code Base)**를 공유하는 프로젝트들이 구축 중인 **2계층 솔루션(Second-Layer Solutions)**은 Ravencoin 위에서 구현될 수 있다.

예를 들어,

- RSK,
- 라이트닝 네트워크(Lightning Network),
- 컨피덴셜 트랜잭션(Confidential Transactions),
- 그리고 기타 확장성 개선 솔루션(Scalability Improvements) 등은  
오픈소스 생태계 전반의 발전에 기여하면서,  
Ravencoin 기반 프로젝트에도 직접적인 이익을 가져올 수 있다.

## 12. 결론 (Conclusion)

**Ravencoin**은 **비트코인 UTXO 모델(UTXO Model of Bitcoin)**을 기반으로 구축된 플랫폼형 코인이다. 비트코인 코드에 직접 기능을 추가하는 것은 현실적으로 불가능하기 때문에, Ravencoin은 **비트코인 코드 포크(Code Fork)**를 기반으로 새롭게 구축되었으며, 신규 채굴된 **RVN**을 발행한다.

Ravencoin은 앞으로 다음과 같은 기능을 단계적으로 추가할 것이다:

- 자산 발행(Assets)
- 보상 시스템(Rewards)
- 고유 자산(Unique Assets)

- 메시징(Messaging)
- 투표(Voting)

이러한 기능들은 **계획된 하드포크 업그레이드(Planned Hard Fork Upgrade)**를 통해 단계별로 출시된다. 코드베이스는 사용자와 개발자가 **보안성(Security)**, **탈중앙화(Decentralization)**, **변조 불가능성(Tamper Resistance)**을 유지할 수 있도록 설계되었다.

Ravencoin 프로젝트는 또한 새로운 **프로젝트(Project)**, **2계층 솔루션(Second-Layer Solutions)**, **실험(Experiments)**, **비즈니스 아이디어(Business Ideas)**의 **출발점(Base and Starting Point)**으로 활용될 수 있다. 비트코인 기반 코드베이스의 이점을 유지하면서, Ravencoin 고유의 기능을 더해 혁신적인 응용을 실현할 수 있다.

*\* 이누이트, 툰링킷, 타히티인, 족치족, 수족(Sioux), 하이다(Haida) 등 많은 민족은 까마귀(Raven)를 **비밀의 수호자, 교활한 장난꾸러기, 최초 인간의 친구, 그리고 세계의 창조자**로 여겼다.*

*즉, 무(無)로부터 무언가를 창조하고 변화시키는 힘을 상징한다.*

*오픈소스(Open Source)의 세계에서조차 마찬가지다.*

*군중의 힘(The Power of the Crowd)은 한 개인이나 조직이 결코 이룰 수 없는 성과를 만들어낸다.*

*Ravencoin은 모든 사람에게 열려 있다.*

*누구나 이 생태계에 기여할 수 있다.\**