

## PoK (Proof of Key)

### 1. Introduction

R2X의 PoK (Key of Proof of R2X)는 이전의 Blockchain Consensus Protocol / Algorithm의 새로운 개념입니다. 키를 사용하여 네트워크를 활성화 한 사람들에게 자격을 부여하는 새로운 방법입니다. 각 키 보유자는 스마트 노드가 될 수 있습니다. 보안, 조직 자산, 효율성 및 기타 분야에서 R2X의 시스템은 파괴하기 어려운 구조를 가지고 있습니다.

컴퓨터 ("마ining"이라고 함)를(을) 통해 작업하는 POW(작업 증명)는 간단하고 정확한 증명을 자랑하지만 작업에 많은 에너지를 소비하는 값비싼 컴퓨터를 필요로 하며, 너무 많은 시간이 걸리고 비효율적입니다.

POS (Stack of Proof of Stack)는 몇 개의 코인 더미로 작동하며 PoW 의 부정적인 요소를 개선하기 위해 만들어졌습니다. PoS 의 장점은 높은 보안, 빠른 트랜잭션 및 에너지 효율성입니다. 하지만 PoS 의 단점은 POW (Proof of Work)에 비해 부정확한 증명과 부자와 빈자 사이의 격차를 초래할 수 있다는 것입니다.

POK (Key of Proof of Key)는 POW (Proof of Work) 및 POS (Stack of Proof)의 장점을 보강하고 단점을 보완하기 위해 만들어졌습니다. R2X 키를 인터넷에 연결된 모든 기기와 호스트에 삽입하기만 하면 됩니다. 또한 채광 중 POK 의 하드웨어 보안은 안전합니다 (이 백서의 뒷부분에서 보안 작업 과정에 대해 설명합니다). POK 는보다 정확하고 효율적인 작업을 제공하고 더 나은 결과를 도출하려고 노력합니다.

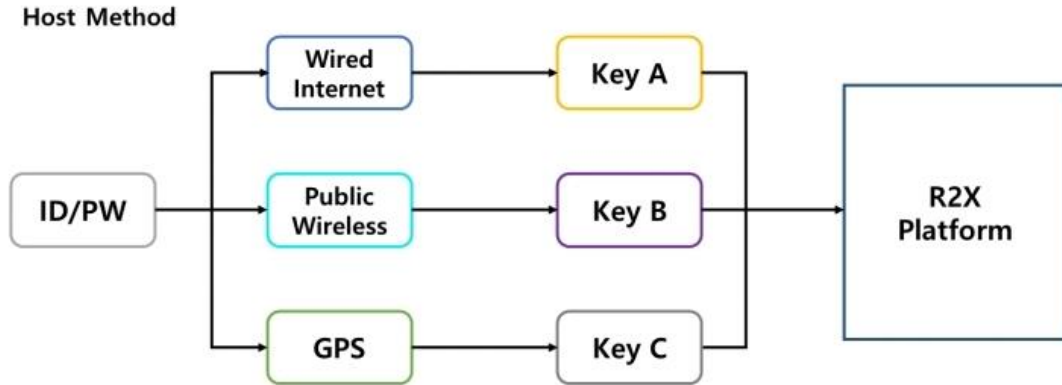
### 2. Operation Method

#### • R2X 플랫폼 액세스 방법

위에서 설명한 바와 같이 POK (Key of Proof of Key)는 POW (Proof of Work) 및 POS (Proof of Stack)에 대한 향상된 증명 방법입니다. 우리는 POK를 통해 R2X 플랫폼을 연결하기위한 호스트 방법을 선택합니다 : 매우 간단하며 호스트를 통해 연결하고 사용자 ID와 암호를 입력하면됩니다. 두 가지 방법 모두 장점이 있으며 사용자는 편리하고 효율적인 방법을 선택할 수 있습니다.

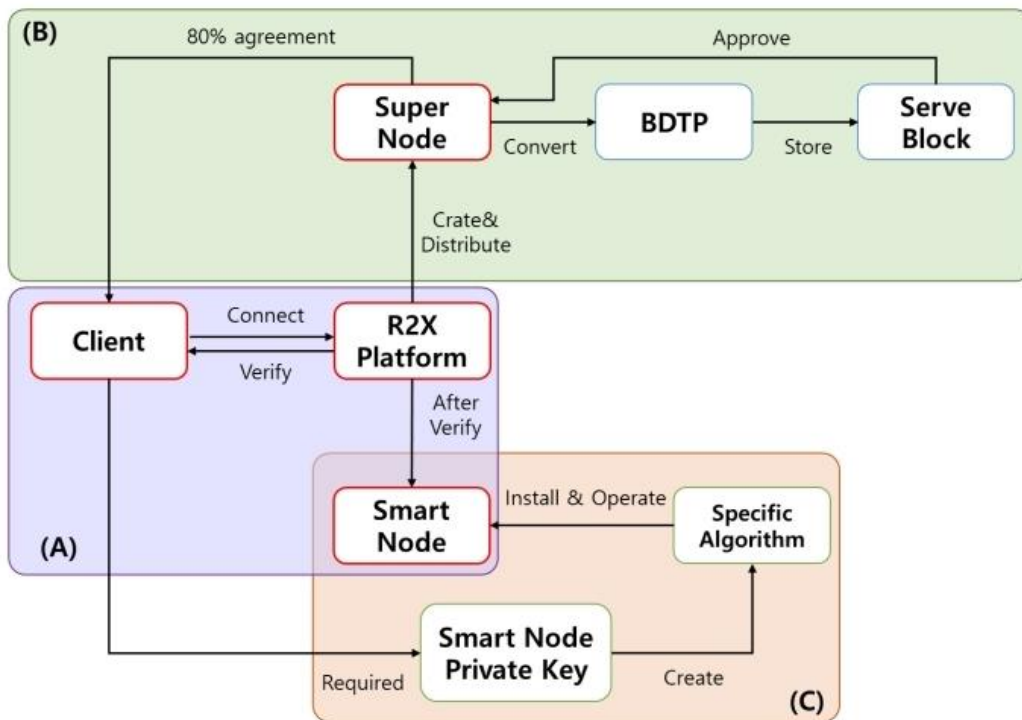
호스트 방법은 다음과 같습니다 : 가입하고 R2X 플랫폼을 입력 한 다음 자신의 키를 받으십시오. R2X 플랫폼의 로그인 섹션에 ID와 비밀번호를 입력하면 키가 확인되고 자동으로 인증 활성화에 참여할 수 있습니다. 이 방법은 매우 간단하며 PC, 스마트 폰, 태블릿 및 기타 네트워크 사용 가능한 기기를 통해 로그인 할 수 있으므로 매우 유연하고 편리한 방법입니다. 언제 어디서나 R2X 플랫폼과 커뮤니티를 쉽게 연결할 수 있습니다.

호스트 방법은 장소 및 커뮤니티 방법에 따라 다릅니다. 예를 들어, 집에 로그인하여 A 키를받습니다. 공용 Wi-Fi를 사용하는 공용 장소에서 R2X 플랫폼에 액세스하면 B 키가 수신됩니다. 운전 중에 GPS 서명을 사용하고 차 안에서 R2X 플랫폼에 액세스하면 키 C가 수신됩니다. 다른 시간과 장소에서 호스트로 R2X 플랫폼에 액세스 할 때 로그인 세션이 변경되기 때문에 동일한 키를 가질 수 없습니다. 키는 액세스 세션에서 새로 생성되며 이는 정보와 세션의 보안에 기여할 수 있습니다.



• Key Activation

클라이언트가 키를 네트워크에 연결하고 처음으로 활성화하면 클라이언트는 R2X 플랫폼에서 플랫폼 관리를 호스팅 합니다. 시스템은 고유 한 해시 값을 받은 후 스마트 노드가 되는지 확인하고 허용합니다. 근처에 있는 슈퍼 노드는 R2X 플랫폼에 의해 생성되고 배포됩니다. 슈퍼노드는 입력값이 BDTP (Blockchain Digest Transmission Protocol)를 통해 변환 된 후 Subblock에 저장된 고유 해시 값의 일관성을 확인합니다. 그리고 슈퍼 노드에서 계약의 80 % 이상을 수신하면 클라이언트는 고유 한 스마트 노드 개인 키를 받습니다. 스마트 노드 개인 키는 원래 해시 값과 다른 알고리즘으로 만들어집니다. 키가 스마트 노드 개인 키에 접근하면 스마트 노드의 역할을 수행하기 위해 설치된 특정 알고리즘이 동작을 시작하고 스마트노드 역할을 수행합니다



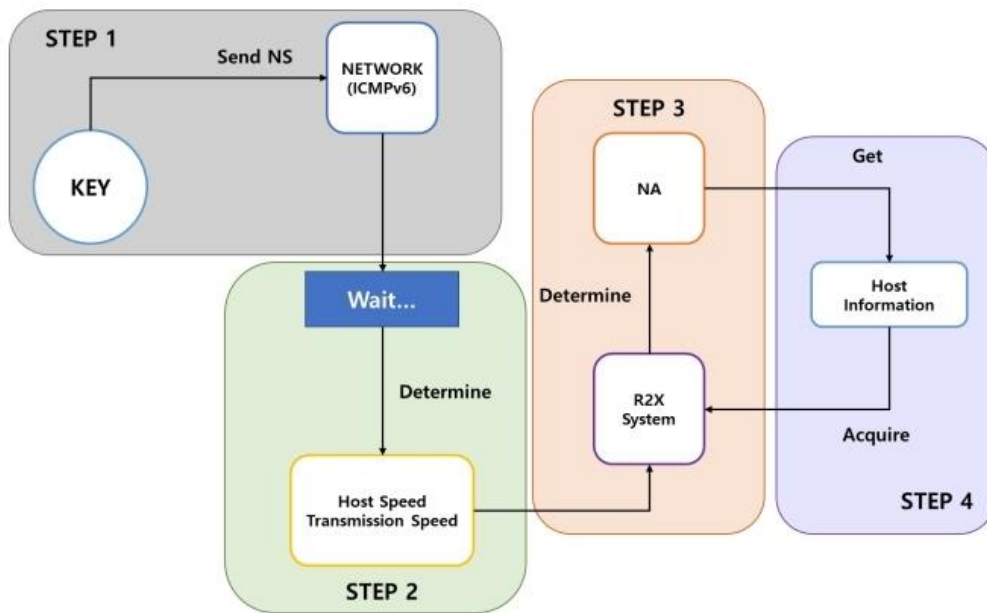
• **Communication step**

먼저, 키는 ICMPv6 (목표 IP 주소)로 설정된 네트워크에 NS (Neighbor Solicitation)를 보냅니다.

두 번째 단계는 호스트의 처리 속도와 네트워크에 따른 전송 속도를 고려하여 일정 시간 동안 대기하는 것입니다.

셋째로, R2X 시스템은 IP의 NA (Neighbor Advertisement) 패키지가 수신되었는지 여부를 결정합니다.

마지막으로 R2X 플랫폼은 NA (Neighbor Solicitation) 패키지에서 호스트 정보를 수집합니다.



• 핵심 관리

R2X의 모든 키는 키 관리에 대해 독점적으로 키 서버에 의해 관리됩니다. 해당 서버의 주요 역할은 다음과 같습니다.

A. 들어오는 다른 신호마다 새 키 생성

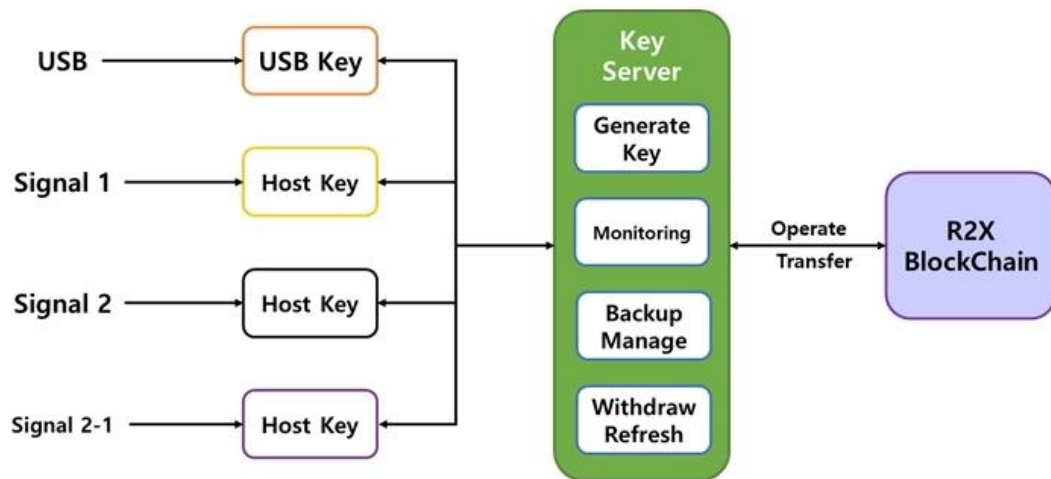
B. 시스템

및 로그 모니터링

C. 키 데이터베이스 백업 및 관리

D. 사용 된 키 철회 및 새로 고침

이 서버는 관리자가 운영하는 것입니다. 자신이 악의적으로 사용하는 경우 매우 위험하기 때문에 (예 : 관리자가 키 작동에 액세스 할 수 있는 경우 자신 또는 다른 사람과 관련된 키를 선택하여 사용할 수 있음) 이 서버는 키 조작에 액세스 할 수 없습니다. 이 서버는 키 생성 및 철회 및 데이터베이스 관리 및 백업과 관련된 작업에만 액세스합니다. 키 서버의 모든 부분은 R2X 블록 체인 시스템과 관련이 있으며, 운영 및 전송의 주요 부분입니다 (블록 체인 시스템 자체로 작업을 자동으로 수행).



- **Arrangement**

스마트 노드는 단일 노드에서 과부하를 피하기 위해 연결이 적은 슈퍼 노드와 일치합니다. 각 슈퍼 노드의 작업 부하의 균형을 유지하고 처리 속도를 향상시킬 수 있습니다.

키가 로그오프되고 다시 로그인하면 클라이언트가 이전 절차를 반복합니다. 각 정품 인증은 나중에 보상 기준으로 사용되는 요소 역할을 합니다.

- **Security**

고유한 코드가 하드웨어에만 있기 때문에 해커에게는 침투가 불가능합니다. 해커는 실제 키 없이 침투할 수 없으며 키의 소프트웨어를 복사할 수 없습니다.

USB 유형 키는 도난 및 키 손실시 추가 보안 조치를 위해 PIN 코드로 물리적으로 확인됩니다. PoK는 접근성, 참여, 비용 절감, 참가자 분포, 보상 및 보안과 관련하여 기존 플랫폼에 비해 장점이 있습니다.

### **3. The Advantages of PoK**

#### **-Accessibility**

스마트 노드가 되고자 하는 사용자는 키가 있어야 하며 어디에서나 네트워크에 액세스해야 합니다.

#### **-Participation**

누구나 지역, 성별, 나이 등을 구분하지 않고 쉽게 참여할 수 있습니다.

#### **-Expenses**

POW와는 달리 Key의 비용 이외에 많은 돈을 투자할 필요가 없으며 POS의 지분 확보를 위한 비용 입력이 필요하지 않습니다.

#### **-Distributed Participants**

세계 어느 곳에서나 참여할 수 있는 USB 유형 키이므로 인증 및 검증 방법에 대한 분산 시스템을 구현할 수 있습니다.

#### **-Compensation**

스마트 노드가 되는 데 소요되는 시간과 빈도에 따라 보상합니다. R2X 모델의 복잡성은 모든 참가자가 공정하게 설계되었습니다.

#### **-Security**

Key에는 제조 과정에서 실제 암호화된 해시 값이 포함되어 있어 해커에게 거의 통용되지 않습니다. Key없이 Smart 노드로 액세스하는 것은 불가능합니다.