TECHNICAL WHITEPAPER V1.0

6 December 2018

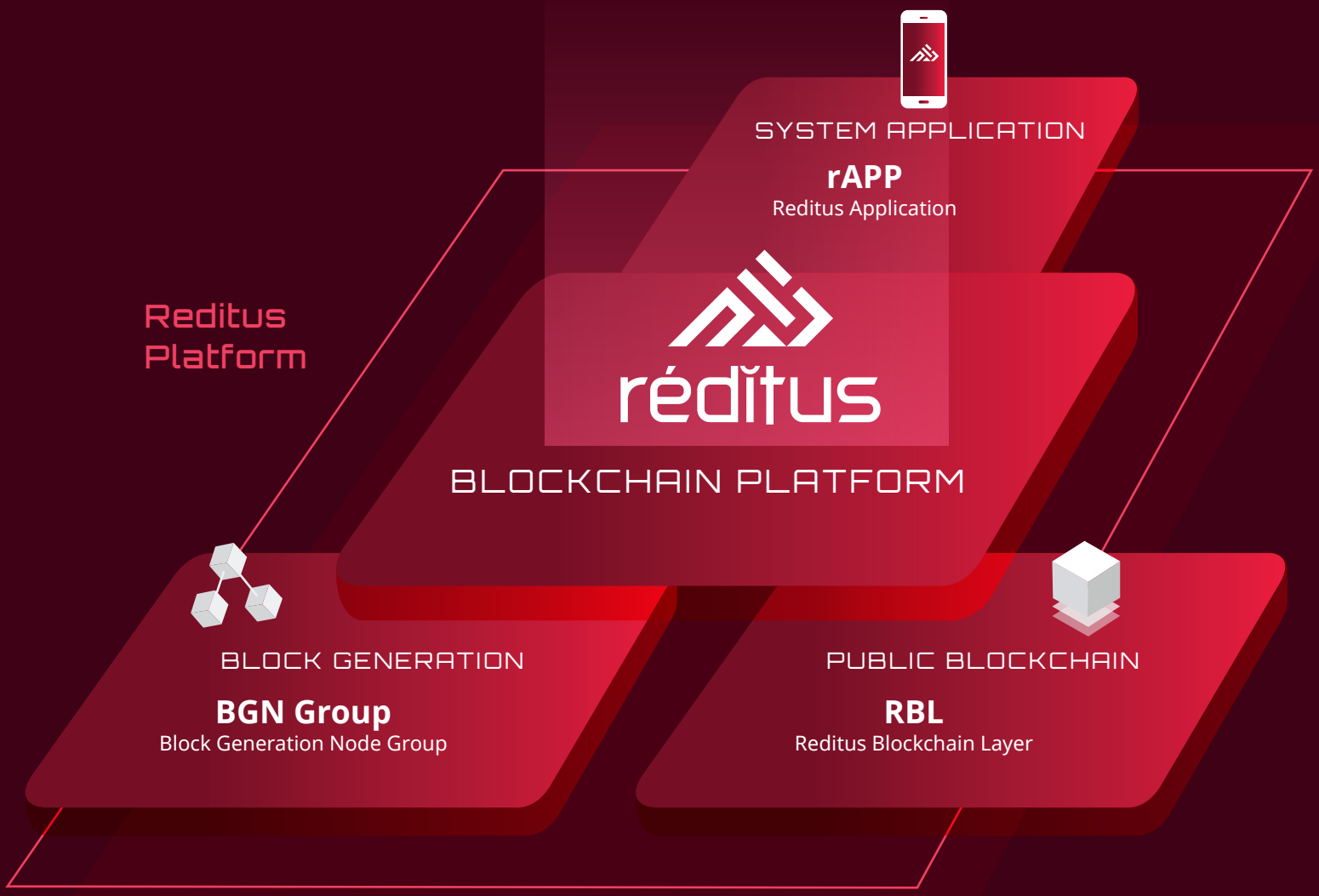
Contents

1. TECHNOLOGY

1.1. PLATFORM INTRODUCTION

Reditus® Platform은 '블록체인과 블록체인 네트워크에서 이용되는 프로토콜, 그리고 이를 통해서 운영되는 애플리케이션'이 복합되어 있는 시스템이며, Reditus® 의 레디투스 어플리케이션(rAPP)인 RMS와 Reditus® Platform이 처리하는 업무는 다음과 같다.

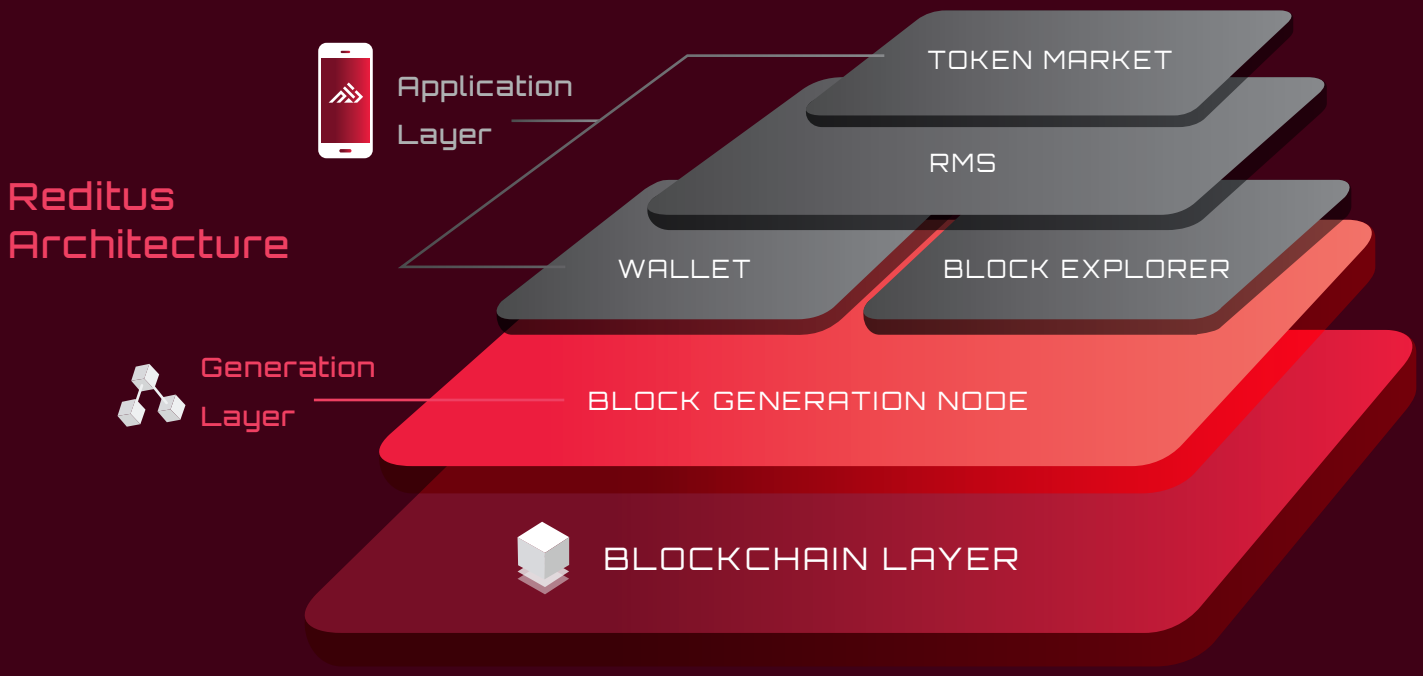
- 채권의 토큰화 (Tokenization) 및 토큰화 된 채권 (Reditus® Receivable Token)의 거래
- 채권 (Enrolled Receivables)의 회수 현황 및 채권 정보의 관리
- Reditus® RED Token, Reditus® IT Coin 의 거래 및 거래에 따른 수수료의 부과 및 정산



1. TECHNOLOGY

1.2. PLATFORM ARCHITECTURE

Reditus®는 계층적 구조의 Architecture를 가진다.



BLOCKCHAIN LAYER

Reditus®의 근간이 되는 모든 데이터가 분산 원장에 기록되는 데이터 레벨이다. 모든 블록은 해시 알고리즘(Hash Algorithm)으로 연결된다. 블록체인 레이어에서는 데이터의 무결성을 담보한다.

GENERATION LAYER

블록체인(Blockchain)의 범용성과 Application의 효율적인 운영을 위해 블록 생성 권한을 가진 Block Generation Node가 위치한다. 블록의 생성, Token Contract 검증 및 배포, 코인의 발행 및 소각 등 전체 NODE를 검증하며 거래의 정합성을 확보한다.

APPLICATION LAYER

Reditus®의 애플리케이션들은 블록체인 레이어와 제너레이션 레이어 위에서 가동되며 주요한 애플리케이션은 다음과 같다.

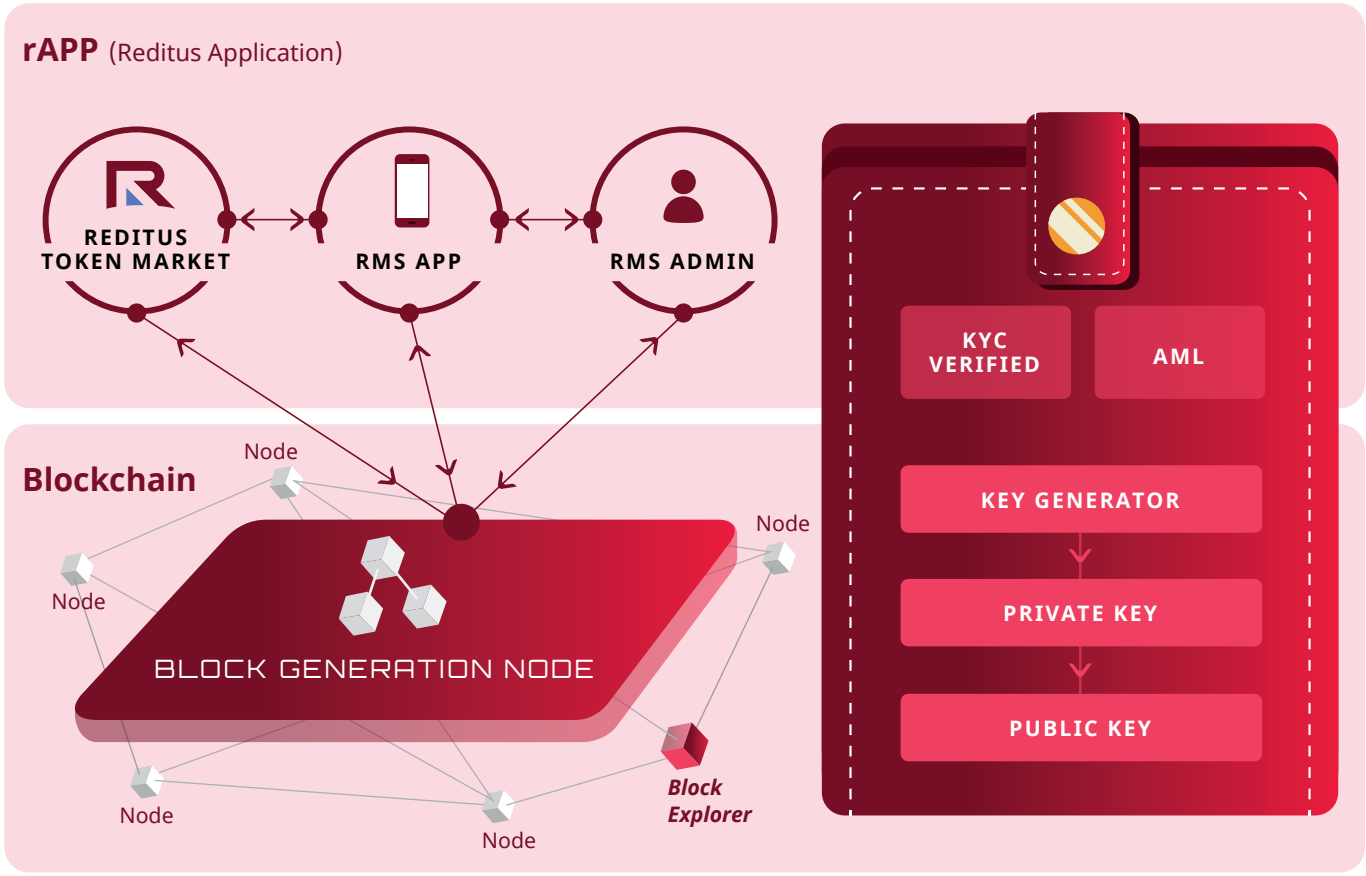
- Wallet – 암호화폐를 저장하고 전송할 수 있는 전자지갑
- Block Explorer – 블록체인에 기록된 내역을 검색, 확인할 수 있는 탐색기
- RMS – 채권을 토큰화 하여 관리 운영할 수 있는 시스템
- Token Market – RMS에서 생성된 토큰을 거래할 수 있는 시장

REDITUS PLATFORM STRUCTURE

Reditus Architecture Layer에서 플랫폼 구조는 BGN (Block Generation Node)에서 각 Application의 운영과 데이터의 검증을 담당한다.

1. TECHNOLOGY

Reditus Platform Structure



Wallet 은 Blockchain과 Application이 상호 연동되는 매개 이다.

BGN 는 Application에서 수집된 KYC, AML등에 관한 데이터를 검증, 합의 할 수 있다.

Reditus Blockchain 합의구조는 BG Node의 검증을 통해 블록의 생성, Token 및 Coin발행이 가능하며 이때 Verification Algorithm 은 PoV (Proof of Value) 이다. 가치 증명은 네트워크의 공헌도 또는 자산 가치를 확인, 증명하여 새로운 블록을 생성하거나, 토큰을 발행한다.

자산가치증명은 Reditus의 Application인 RMS 에서는 채권이 회수된 현금이 입금되고 그것을 BG Node가 확인 검증하는 것이다.

1.3. PLATFORM COVERAGE (TECHNICAL SPECIFICATION)

BLOCKCHAIN

Blockchain Layer 내부에 BG Node (Block Generation Node)가 Network 에서 상위의 Reditus Application을 실행하고 관장한다.

VERIFICATION ALGORITHM

Reditus의 검증 알고리즘 BG Node가 네트워크 기여도와 실질(경제)가치를 증명하는 PoV (Proof of Value) 이다.

TOKEN CONTRACT

Reditus의 Token Contract는 Reditus Application이 BG Node의 검증을 통하여 Blockchain에 새로운 블록을 추가하고 이를 통하여 Token을 발행 및 분배하는 계약의 기록이다.

TOKENIZATION

Reditus의 Token은 Reditus Application이 Token Contract를 통해 발행한 다양한 권리와 지분을 규격화한 거래의 수단이다. Reditus Application인 RMS를 통하여 발행되는 Token은 채권 최고액이 분할된 채권의 지분이다.

HASH ALGORITHM

Reditus Blockchain 에서는 <SHA-256> 해시 알고리즘을 사용하여 데이터와 블록의 연결을 암호화 한다.

전자지갑 주소체계

Reditus Platform에서 채택한 서명 및 서명 검증 알고리즘은 ECDSA(타원곡선전자서명알고리즘) 이다. 다음은 전자지갑 주소(Public key)의 생성과정을 설명한다.

- 256bit의 Private key 와 ECC(Elliptic Curve Cryptography) 알고리즘 함수들을 사용하여 만들어낸 Public key를 생성한다.
- Public key는 SHA256 과 RIPEMD160 를 이용하여 160비트의 해시값 (20 bytes)로 변환한다.
- 20 bytes 의 변환된 Public key 와 Checksum 4 bytes 와 합쳐져서 문자열(24 bytes)를 생성한다. 이를 16 진수로 변환하여 48자리의 문자열 앞에 '0r' 을 Prefix 는 넣어서50 bytes 의 주소값을 최종적으로 전자지갑 주소로 이용한다.
- * 함수예제 – concat("0r", hex(concat (20 bytes of hash value, 4 bytes of checksum))))
  예) 0r3ae893ae4b22d70432899a3471230face41fe912

1. TECHNOLOGY

NODE

Supervisor Node

BG Node의 인증, 관리 및 참여자들의 Node를 검증하는 역할을 한다. 또한 블록의 생성과 전파, Token Contract의 등록 및 배포 등 모든 기능을 할 수 있는 Node 이다.

BG Node

Block Generation Node 는Reditus Application Interface와 Token Contract를 배포, 실행하여 Token 및 Coin을 발행할 수 있다. PoV (Proof of Value)를 실행하는 핵심 Node이다.

Normal Privileged Node

Blockchain의 세부 거래내역을 조회하고, Coin 전송과 블록 전파가 가능하다. 일반 참여자와 제휴사를 위한 Node로 Application으로는 Block Explorer가 있다.

Certification Authority

Node와 Node간 검증을 위해 <RSA2048> 방식으로 키교환 및 검증체계를 운영한다. 전자서명을 위한 별도의 인증기관은 필요치 않다.

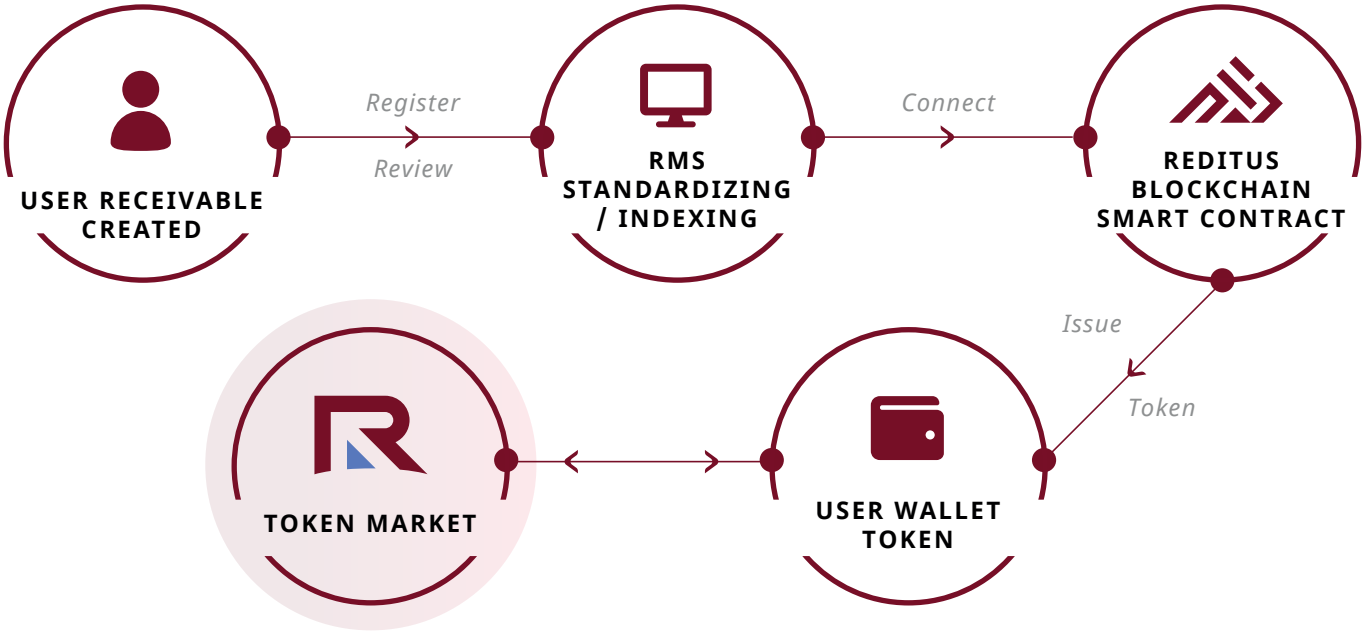
Signing Transaction

모든 거래의 전자서명은 공개키 암호기술인 ECDSA(Elliptic Curve Digital Signature Algorithm)을 사용한다.

2. REDITUS® RMS

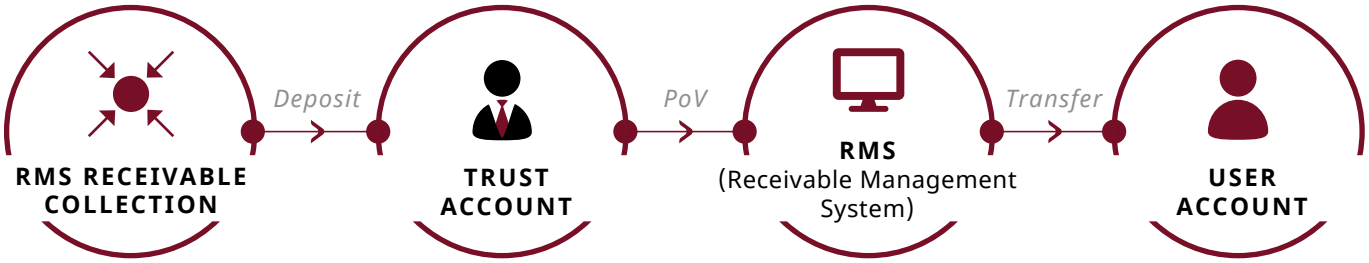
(RECEIVABLE MANAGEMENT SYSTEM)

RMS는 다양한 형태와 권리 구조를 가진 채권과 그것을 기반으로 발행한 Token의 권리와 권리에 대한 지분을 관리하는 시스템으로 채권자가 채권을 등록하는 Creditor Application과 채권의 발생, 양도, 회수, 토큰화에 이르는 일련 과정을 관리하기 위한 RMS Admin Tool 로 구성된다.



이를 통하여 채권에 대한 권리의 행사를 통해 유입된 실질 자산이 Token Economy 에 편입될 수 있도록 한다.

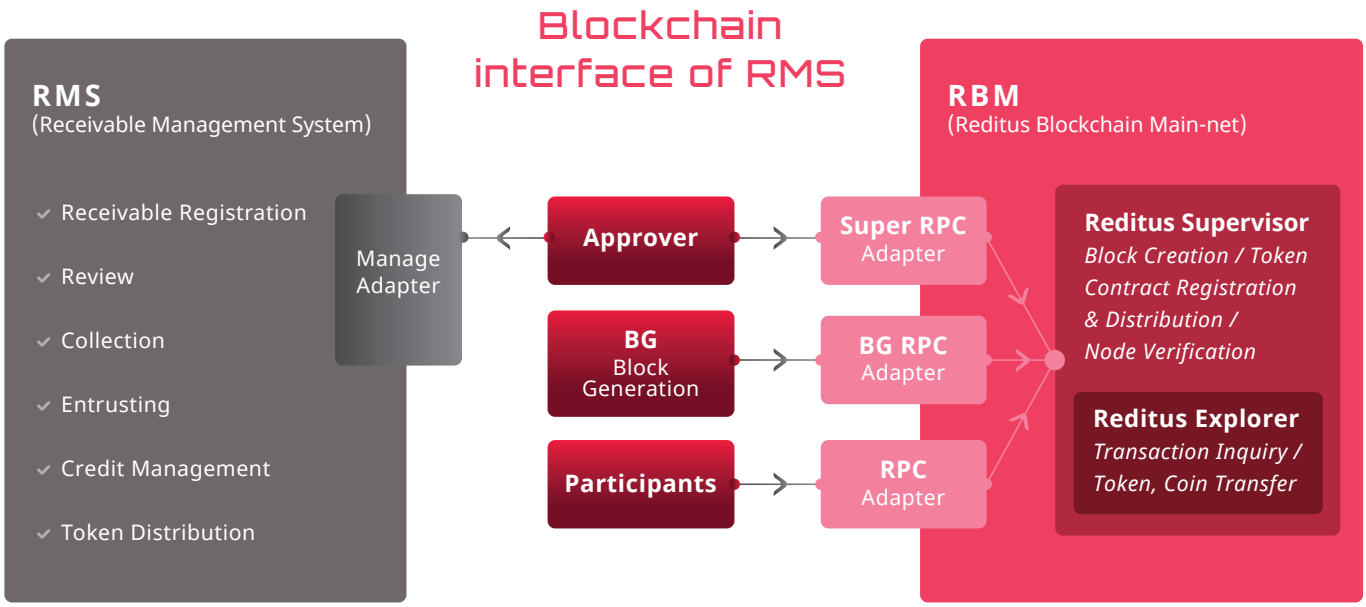
RMS를 운영하는 주체(회사)는 채권의 위임, 양도시점에서 Token 을 배분 받아 채권회수 활동에 대한 보상을 대신한다.



2. REDITUS® RMS
(RECEIVABLE MANAGEMENT SYSTEM)

RMS에서 회수된 대금은 RED Token의 보유량(지분)에 따라 RED Token 소유자에게 배분한다.

Reditus®의 Application인 RMS의 Blockchain Interface와 그에 영향을 주는 Node는 다음과 같다



APPROVER
매 채권이 생성될 때마다 채권에 대한 유효성 검증을 하여, Token 생성을 검증한다.

BLOCK GENERATION (NODE)
매 1 분마다 블록을 생성하여, 블록에 대한 내용 합의 및 검증한다.

PARTICIPANTS
Reditus® 의 블록체인을 조회 할 수 있는 참여자