

퀀텀(Qtum)

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.

서문

비트코인이 등장하기 전까지, 글로벌 정보 전달은 고속 저비용 전송을 달성하기 위해 인터넷의 TCP/IP (전송 제어 프로토콜 / 인터넷 프로토콜) 프로토콜을 통해 이루어졌다. 그러나 통신 기술(인터넷, IoT, VR / AR)의 발전에 따라 사람과 장치 간 상호작용 방식이 다양화되었고, 더 많은 자산이 디지털화 또는 토큰화되었다. 단순한 정보의 공유와 전달만으로는 경제 및 사회 발전의 요구를 충족할 수 없기 때문에, 자산이 디지털화되거나 토큰화될수록 사람들은 자산 및 가치의 전송, 특히 포인트 투 포인트 방식의 가치 전송에 점점 더 많은 관심을 가지게 되었다.

2008년 10월 31일, 사토시 나카모토는 최초의 비트코인 백서 "Bitcoin: A Peer-to-Peer Electronic Cash System"을 발표하였고, 분산된 비트코인 네트워크를 통한 가치 전송 개념을 제시하였다. 비트코인 시스템에서는 네트워크 전반의 참여자들이 거래를 직접 통제하며, 거래 당사자 모두가 신뢰 관계를 형성하지 않고도 거래를 완료할 수 있다. 블록체인 기술은 정보의 획득과 공유 방식을 변화시켰고, 새로운 분산형 피어 투 피어 생태 사회를 형성하게 되었다.

비트코인 코드가 2009년에 오픈소스로 공개된 이후, 커뮤니티 내에는 많은 블록체인 프로젝트들이 등장하였다. 일부 프로젝트는 범용 스마트 계약 및 탈중앙화 애플리케이션 플랫폼이 되는 것을 목표로 하고 있으며, 블록체인 산업은 이러한 신기술들을 산업적 응용 관점에서도 발전시키고 있다. 블록체인의 성장은 여러 도전에 직면하고 있으며, 이는 주로 다음과 같은 측면에서 나타난다:

1. 서로 다른 블록체인 플랫폼 간의 호환성이 부족하다. 예를 들어, UTXO (미사용 거래 출력) 모델을 기반으로 한 비트코인 생태계는 계정(Account) 모델을 기반으로 한 이더리움 생태계와 호환되지 않으며, 블록체인 간 상호운용성도 강하지 않다;
2. 핵심 기술 매개변수의 온체인 거버넌스를 달성하기 어렵다. 대부분의 탈중앙화 플랫폼에서는 메인넷이 배포된 이후, 업그레이드 및 블록체인 거버넌스가 주요 과제가 된다;

3. 합의 메커니즘의 유연성이 부족하다. 작업 증명(PoW) 합의 메커니즘은 에너지 요구 사항 및 채굴자와 토큰 보유자에 대한 인센티브 측면에서 한계가 있으며, 채굴 컴퓨팅 파워의 중앙집중화 위험이 존재한다;
4. 새로운 스마트 계약 플랫폼의 부족. 대부분의 블록체인 프로젝트는 현실 세계와의 연결 고리가 부족하여 다양한 산업에의 광범위한 적용이 제한된다.

Qtum 체인: 블록체인 과제에 대한 대응

블록체인 기술과 산업 응용의 다양한 문제에 대응하기 위해, Qtum 체인 개발팀은 커뮤니티 개발 역량을 결집하고, 기반 기술을 심층적으로 탐구하였으며, "가치 전송 프로토콜(Value Transfer Protocol)" 업그레이드 및 기타 혁신적 솔루션들을 통해 지속 가능한 퍼블릭 블록체인을 구축하기 위한 일련의 기술들을 개발 및 구현하였다.

AAL(Account Abstraction Layer)을 도입함으로써, UTXO 모델과 스마트 계약 계정 모델 생태계를 통합하여 서로 다른 블록체인 간 호환성 부족 문제를 효과적으로 해결하였다;

Qtum x86 가상 머신의 혁신적인 연구 개발은 프로그래밍 개발 역량을 더욱 풍부하게 하였고, 운영체제를 가상 머신으로부터 분리시켜 스마트 계약 개발을 주류로 끌어올렸다;

PoS(지분 증명) 합의 메커니즘을 혁신적으로 도입하여, 전 세계에 분산된 PoS 노드들을 통해 글로벌 PoS 피어 투 피어 네트워크의 효과적인 협업을 가능하게 하였다;

온체인 거버넌스를 위한 최초의 DGP(탈중앙화 거버넌스 프로토콜)를 개발하여 전체 시스템의 안정적인 운영을 유지할 수 있도록 하였다.

다양한 사용자들의 운영 체제 및 개발 수요를 충족시키고 진정한 오픈소스를 유지하기 위해, Qtum 체인은 모바일 터미널 서비스를 포함한 다양한 버전의 Qtum 시스템을 제공하며, 상업적 경로 모듈을 출시하여 서드파티 개발자들을 독려하고 영향력 있는 글로벌 오픈소스 커뮤니티 생태계를 조성하고자 한다. 궁극적인 목표는 블록체인을 금융, 소셜 네트워킹, 게임, 사물인터넷 등 다양한 산업에 통합하는 것이다.

가장 유망한 블록체인 생태계로서, Qtum 체인은 비트코인과 이더리움의 장점을 완벽하게 결합하고 기존 블록체인 시스템의 고유한 한계를 해결한다. Qtum 체인은 기본 플랫폼 구축을 지속하는 동시에, 다양한 제품 개발 및 상용화 프로젝트의 개발과 반복을 통해 점차 블록체인 경제를 형성하고, 산업 효율성을 향상시키며, 블록체인 경제의 효율적이고 조정된 발전을 촉진할 것이다.

Qtum 체인의 거버넌스 모델

탈중앙화 퍼블릭 체인으로서, Qtum 체인은 블록체인 거버넌스를 지속 가능한 발전을 달성하기 위한 중요한 요소로 간주한다. Qtum 체인의 거버넌스 모델은 두 가지 주요 측면을 포함한다. 하나는 DGP를 사용하는 온체인 거버넌스이며, 다른 하나는 비영리 조직인 Qtum 체인 재단(Qtum Chain Foundation)을 설립한 오프체인 거버넌스이다. DGP의 도입과 Qtum 체인 재단의 설립을 통해, Qtum 체인은 퍼블릭 블록체인에 인간 중심의 거버넌스와 코드 기반 거버넌스를 동시에 적용하여 블록체인 거버넌스의 탈중앙화와 효과적인 의사결정 구조를 실현한다.

2.1 DGP 기반 온체인 거버넌스

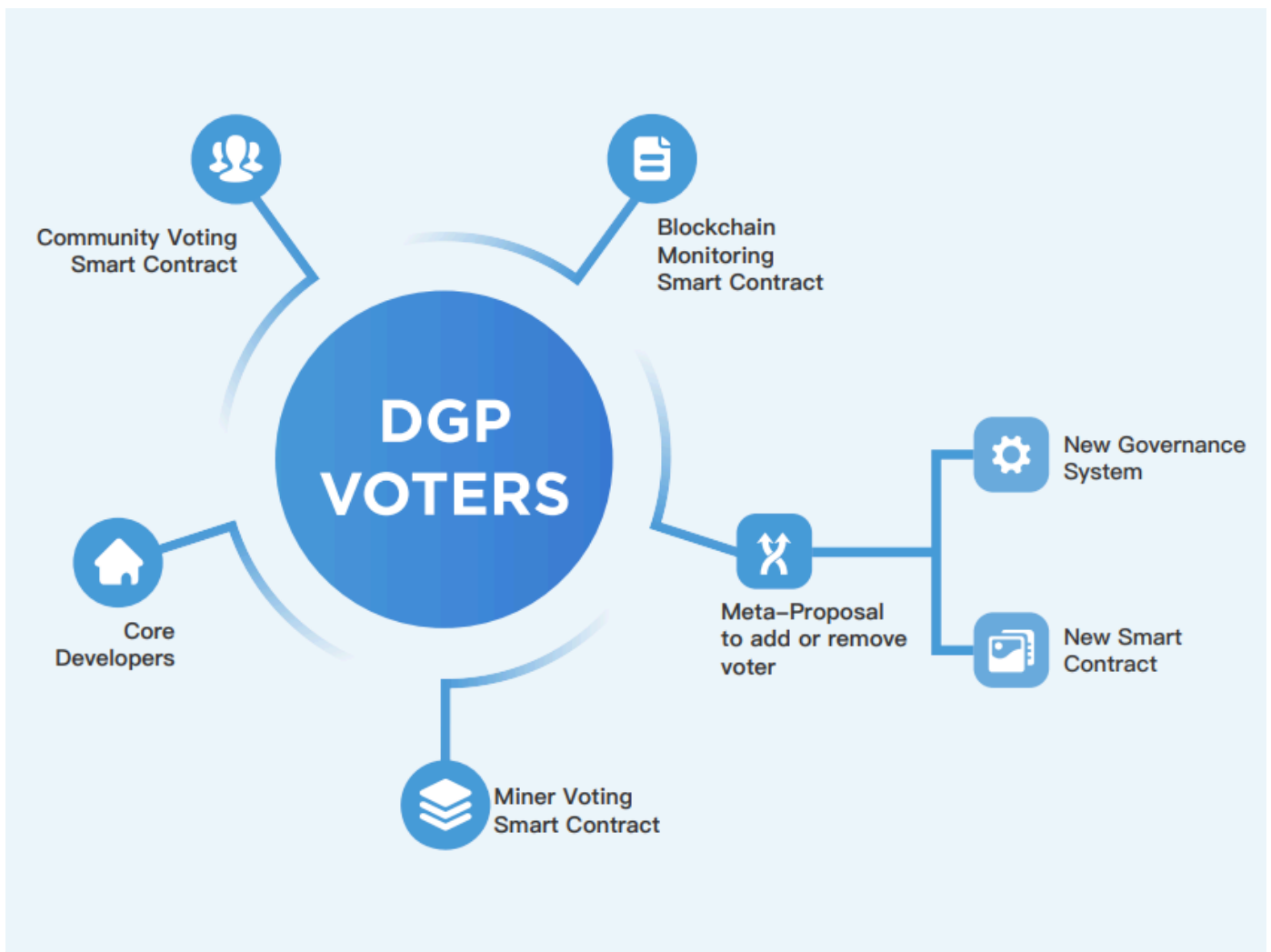
온체인 거버넌스는 Qtum 블록체인 시스템에 내장된 블록체인 네트워크 업데이트 프로토콜에 대한 협의 및 실행 절차를 의미한다. Qtum 체인은 DGP 설계를 통해 블록체인 네트워크를 위한 새로운 온체인 거버넌스 모델을 제공한다.

2.1.1 다자 참여형 온체인 거버넌스

DGP의 핵심 특징은 QTUM 토큰 보유자가 블록체인 네트워크의 업그레이드 및 반복에 대한 투표 및 협상에 참여할 수 있도록 하는 것뿐만 아니라, 생태계 내의 다른 참여자들—예: 개발자, 커뮤니티 구성원 대표, 채굴자 등—도 온체인 거버넌스 제안을 발의하고 투표할 수 있는 경로를 제공한다는 점이다.

2.1.2 온체인 거버넌스를 위한 스마트 계약 기반 구조

DGP는 제네시스 블록에 내장된 스마트 계약을 통해 블록체인 네트워크의 다양한 매개변수를 관리하며, 각 당사자의 거버넌스 의식 수와 참여 비율을 명확히 한다. 어떤 참여자라도 제안을 발의할 수 있으며, 제안 유형에는 관리 또는 거버넌스 의식의 증가, 삭제, 공통 네트워크 매개변수의 수정 등이 포함된다. 거버넌스 의식을 보유한 참여자들은 해당 제안에 대해 투표하고, 승인 여부를 결정하며, 승인된 제안은 스마트 계약을 통해 실행된다.



2.1.3 공공성과 투명성을 갖춘 온체인 거버넌스

DGP 기반의 온체인 거버넌스 메커니즘은 강제적이며 자동화되어 있다. 이를 통해 Qtum 블록체인 시스템의 자동 업그레이드와 지속적인 업데이트 반복이 실시간으로 효과적인 의사결정 및 실행 메커니즘을 통해 실현될 수 있다. 동시에, 온체인 거버넌스 절차는 공개적이며 투명하며, 그 과정은 감사 및 추적이 용이하여 전체 거버넌스 절차의 공정성을 보장하고 의사결정 효율성을 향상시킨다. 이로 인해 소프트 포크 및 하드 포크가 네트워크나 커뮤니티에 미치는 영향을 걱정할 필요가 없다.

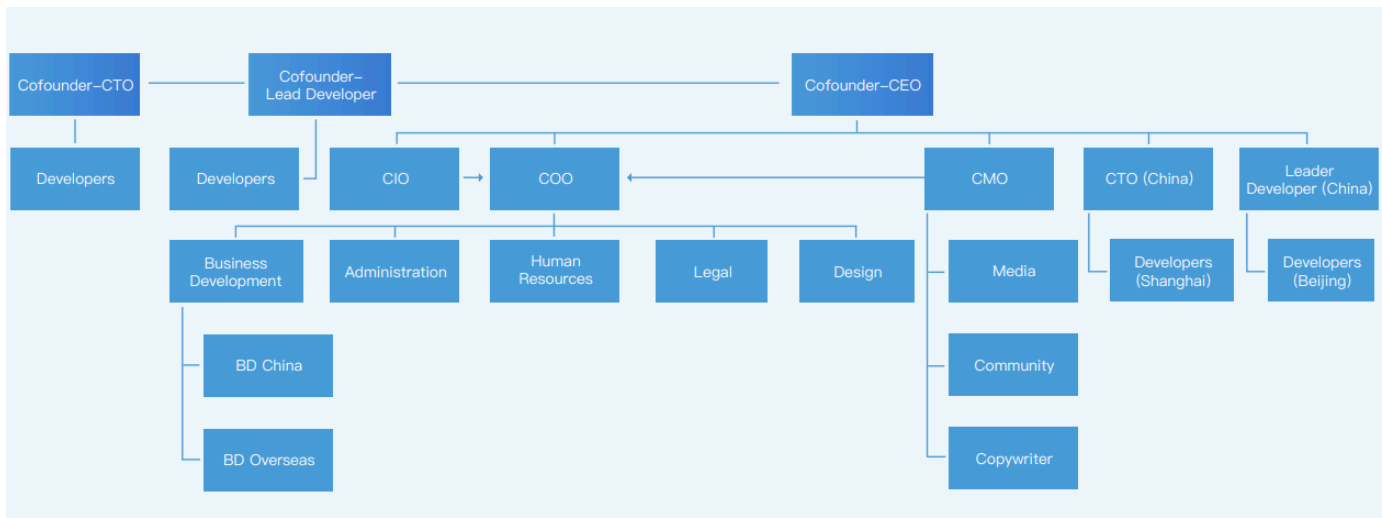
2.2 Qtum 체인 재단

Qtum 체인 재단은 2016년 11월 싱가포르에 공식 등록된 비영리 법인이다. Qtum 체인 재단은 건전한 거버넌스 메커니즘을 수립함으로써 오픈소스 커뮤니티 프로젝트의 전반적인 개발, 진행 상황 및 권한 관리를 지원한다. 본 재단은 Qtum 블록체인 프로젝트의 개발 및 구축뿐만 아니라 거버넌스 투명성의 옹호 및 촉진을 통해 프로젝트의 안전하고 조화로운 발전을 추구한다.

Qtum 체인 재단의 거버넌스 구조 설계 목표는 주로 오픈소스 커뮤니티 프로젝트의 지속 가능성, 관리의 효과성, 그리고 조달된 자금의 안전성을 고려한다.

2.2.1 Qtum 체인 재단의 거버넌스 구조

Qtum 체인 재단의 거버넌스 구조에는 일상 업무 및 특수 상황에 대한 운영 절차와 규칙이 포함된다. Qtum 체인 재단의 조직 구조는 다음과 같다:



Qtum 체인 재단은 세 명의 공동 창립자를 두고 있으며, 각각 최고경영자(CEO), 최고기술책임자(CTO), 수석 개발자(Lead Developer)의 역할을 맡고 있다. 이 세 명의 공동 창립자는 재단의 전반적인 전략 기획, 기술 프레임워크의 설계 및 기술 관리, 재단의 보안 감사, 코드 관리, 핵심 구성 요소의 리더십 개발, 전체 개발 진행 상황 감독을 담당하며, 재단 발전 방향을 공동으로 결정한다.

재단은 공동 창립자 하위에 COO, CIO, 중국 CTO, 중국 수석 개발자, CMO 등의 직책을 두어 재단의 정상적인 운영을 보장한다. 각 직책의 구체적인 기능은 다음과 같다:

COO

최고운영책임자(COO) – 재단의 관리 시스템 및 업무 프로세스의 구축과 표준화를 책임진다. 재단의 각종 계획을 추적하고 후속 감독을 수행하며, 부서 간 조정을 비롯해 요약 및 평가 업무를 진행한다. 또한 산업 및 시장 조사를 수행한다.

CIO

최고정보책임자(CIO) – 재단의 전략 기획에 협력하고, 그 실행 및 후속 감독을 수행한다. 해외 파트너와의 연결 및 후속 관리를 담당하며, 산업 및 시장 조사를 진행한다.

중국 CTO 및 중국 수석 개발자

Qtum의 기술 팀을 이끌며, 연구 개발 계획 수립 및 실행에 참여한다. 관련 분야의 기술 연구를 수행하며, 개발자 커뮤니티를 관리한다.

CMO

최고마케팅책임자(CMO) – 재단의 글로벌 홍보 관리 업무 계획을 수립 및 실행하며, 재단의 시장 확장 및 광고(이벤트 및 컨퍼런스, 커뮤니티 관리, 미디어 관계 유지, 정보 공개 등)를 책임진다. 위기 상황에 대한 홍보 대응을 담당하고, 제3자 홍보 대행사의 평가를 수행한다.

재단은 디자인, 인사, 홍보, 사업 개발, 관리 등 다양한 부서를 보유하고 있으며, 각 부서는 해당 업무 영역을 담당한다.

3.1 계정 추상화 계층 (Account Abstraction Layer)

UTXO 모델과 스마트 계약의 계정(Account) 모델을 결합하고, 가치 전송 계층과 계약 실행 계층을 분리하여 상호운용성을 달성하기 위해 Qtum은 계정 추상화 계층(AAL, Account Abstraction Layer)을 설계하였다.

Qtum은 스마트 계약 연산과 UTXO 연산 간의 인터페이스 및 변환을 최적화하였으며, 다음과 같은 네 가지 새로운 오퍼코드(opcode)를 개발하였다:

- **OP_CREATE:** 스마트 계약 생성
- **OP_CALL:** 스마트 계약 호출 (계약에 QTUM 전송)
- **OP_SPEND:** 스마트 계약 내 QTUM 지출
- **OP_SENDER:** 계약 호출자가 아닌 주소가 Gas 비용을 지불할 수 있도록 허용

Qtum 블록체인이 새로운 블록을 생성할 때, 거래 스크립트에 대한 일반적인 검사를 수행하는 것 외에도 해당 거래에 위에서 언급한 오퍼코드가 포함되어 있는지를 확인해야 한다. OP_CREATE는 계약 바이트코드를 가상 머신에 전달하는 데 사용된다. OP_CALL은 스마트 계약 실행에 필요한 데이터, gasPrice, gasLimit, VMVersion 등의 주요 파라미터를 거래 스크립트를 통해 전달하며, 최종적으로 이를 가상 머신에 전달한다. 이러한 설계에 기반하여, Qtum x86 가상 머신은 EVM(Ethereum Virtual Machine)과 병렬로 블록체인 상에서 실행될 수 있으며, 기본 프로토콜을 대폭 수정할 필요 없이 우수한 기능적 확장성을 유지할 수 있다. 향후 계정 모델 기반의 모든 가상 머신은 Qtum 블록체인 상에서 실행되도록 적응될 수 있다.

Qtum은 다양한 기능적 적응과 개선뿐만 아니라, 이더리움으로부터 Gas 개념을 차용하여 스마트 계약 실행에 Gas 모델을 적용하였고, EVM의 Gas 모델을 최적화하였다. Gas 모델의 사용은 오류나 악의적인 공격으로 인한 무한 루프를 방지할 수 있으며, 실제 작업량에 기반한 계산 수행에 대해 채굴자에게 보상을 제공하고, 계약 설계자와 사용자로 하여금 온체인 자원을 합리적으로 사용하도록 유도한다. 일반적으로 계약 호출자의 주소가 Gas를 지불하지만, OP_SENDER 오퍼코드는 분산 애플리케이션 서비스 제공자와 같은 제3자 주소가 Gas를 지불할 수 있도록 한다. EVM과 마찬가지로, "out of Gas" 상태에 대한 상태 롤백과 성공적인 실행 후 남은 Gas의 환불 기능도 존재한다. 이러한 상황들과 일부 드문 경계 케이스에 대응하기 위해 Qtum은 스마트 계약의 정상적이고 효율적인 작동을 보장할 수 있도록 적절한 처리를 제공한다.

3.2 x86 가상 머신

AAL의 강력한 확장성을 바탕으로, Qtum 체인은 기본 아키텍처를 변경하지 않고도 병렬로 실행되는 다중 가상 머신을 구현할 수 있다. Qtum은 새로운 설계의 Qtum x86 가상 머신을 개발 중이다. x86 가상 머신은 폰 노이만(Von Neumann) 컴퓨터 아키텍처를 사용하며, 이는 코드가 곧 데이터라는 개념으로, 현대의 주류 프로그래밍 모델과 일치한다. x86 가상 머신의 기본 원리는 간단한 수정과 다양한 기존 컴파일러 및 프로그래밍 언어를 활용하여 Qtum 블록체인에서 실행되는 스마트 계약을 작성할 수 있도록 보장한다. 현재 대부분의 컴파일러는 x86 아키텍처 명령어 집합을 지원하기 때문에, 실제 바이트코드 및 아키텍처 지원이 매우 완전하다.

Qtum의 x86 가상 머신은 i686 명령어 집합을 지원할 예정이며, 초기에는 Rust 언어를 지원한다. 따라서 x86 가상 머신은 상위 수준 언어 및 개발 도구의 지원을 자동으로 상속하게 되며, 이를 통해 Qtum은 EVM의 계산 한계와 Solidity 언어의 제약에서 벗어나 가변 길이 키 값, 선형 메모리, 실시간 온체인 데이터 분석과 같은 기능을 보다 효율적으로 구현할 수 있게 된다.

x86 가상 머신의 도입은 개발자에게 더 많은 표준 라이브러리를 제공할 수 있다. 이 표준 라이브러리들은 사전 컴파일된 계약(pre-compiled contract)처럼 존재하며, 해당 비용 및 가격은 DGP를 통해 관리될 수 있어, 스마트 계약 개발의 난이도와 운영 비용을 크게 줄일 수 있다. 가상 머신의 커널 외에도, Qtum x86 가상 머신은 블록체인의 과도한 성장 문제를 해결하기 위해 저장소 임대 모델(storage lease model)과 새로운 상태 저장 모델(state storage model)을 포함한 설계를 가지고 있다.

3.3 상호화 지분증명(MPoS) 합의 메커니즘

Qtum의 또 다른 혁신은 MPoS(Mutualized Proof-of-Stake, 상호화 지분증명) 합의 메커니즘이다. 일반적인 지분증명(PoS) 메커니즘은 컴퓨팅 파워 경쟁 문제가 없고, 하드웨어 요구 수준도 낮아 노드의 탈중앙화된 분산에 더 유리하다. Qtum의 MPoS 알고리즘은 PoS 3.0을 개선한 것이지만, 전통적인 PoS 합의 메커니즘과 스마트 계약의 결합은 "불량 계약(junk contract)" 공격과 같은 보안 위험을 초래할 수 있으므로 Qtum에서는 이를 직접 사용할 수 없다. 이에 대해 Qtum은 블록 보상 지급을 블록 생성 노드 간에 분배하고 지연시킴으로써 공격 비용을 증가시켰다. 각 새로운 블록 보상은 블록을 생성한 채굴자와 그 이전의 9명의 채굴자에게 각각 10%씩 균등하게 분배되며, 나머지 90%의 보상은 500 블록 후에 지연 지급된다. 이러한 수익 메커니즘의 개선은 PoS 3.0의 핵심 로직을 변경하지 않으며, 공격자가 얼마만큼의 블록 보상을 받을 수 있는지를 예측하거나 즉시 획득할 수 없게 하여, 불량 계약 공격의 비용을 크게 증가시킨다. (이는 이론적으로만 가능하며, 실제로는 실현 불가능하다.)

3.4 탈중앙화 거버넌스 프로토콜

블록체인 커뮤니티는 프로젝트의 발전 방향에 대한 의견 차이로 인해 종종 분열되며, 이는 논란이 많은 하드 포크를 통해 새로운 블록체인을 생성하는 결과를 초래한다. 이러한 의견 차이는 대체로 다음 세 가지로 나뉜다:

- 프로젝트 알고리즘 및 기능의 개발 방향에 대한 이견
- 핵심 취약점의 수정 및 성공적인 공격의 롤백
- 블록체인의 특정 매개변수에 대한 이견

상위 두 가지 문제는 대부분의 경우 하드 포크를 통해 해결해야 하지만, 세 번째 유형의 문제는 보다 완화된 방식으로 해결할 수 있다. DGP의 프레임워크는 제네시스 블록에 배치된 여러 스마트 계약을 통해 구현된다. 기본적인 거버넌스 구조는 생태계 내의 채굴자(스테이커), 개발자, 그리고 QTUM 보유자들이 블록체인 거버넌스에 참여하는 형태이다. 거버넌스 절차는 투표를 통해 진행되며, 블록체인은 이를 통해 자체 관리, 업그레이드 및 반복을 실현할 수 있다.

DGP의 핵심 로직 구현은 일련의 스마트 계약(프레임워크 계약 및 기능 계약 포함)으로 구성된다. Qtum 노드는 이러한 스마트 계약 매개변수를 포함한 코드를 탑재하고 있으며, 이를 통해 Gas 가격 및 블록 크기를 제어한다. 이러한 핵심 합의 매개변수는 하드 포크 없이 DGP 프로세스를 통해 온체인 소프트웨어 업데이트로 수정할 수 있다.

3.5 Qtum 2.0

메인넷이 2년간 안정적으로 운영된 이후, 최초의 Qtum 하드 포크를 통해 합의 알고리즘이 업그레이드되었고 새로운 오퍼코드가 추가되었다. 끊임없이 변화하는 블록체인 기술의 응용 시나리오에 적응하기 위해 Qtum은 기반 프로토콜을 점진적으로 업그레이드하고 Qtum 2.0을 출시할 예정이다. Qtum 2.0은 블록 간격 알고리즘의 업그레이드 및 최적화 외에도, 블록체인의 활용 경계를 확장하고 Qtum 블록체인의 기능을 풍부하게 하기 위한 일련의 새로운 기능을 포함한다. 향후 주요 기능으로는 프라이버시 자산, 오프라인 스테이킹, 체인-클라우드 통합이 포함될 예정이다.

프라이버시 자산 (Confidential assets)

Qtum은 스마트 계약을 통해 프라이버시 자산의 발행 및 유통을 지원할 계획이며, 사전 컴파일된 계약(pre-compiled contracts)을 배치하고 프라이버시 인증 데이터 구조를 최적화함으로써 Qtum 블록체인에서 프라이버시 자산 관련 계약의 개발 및 사용 비용을 절감하고자 한다. 최근 Qtum 2.0의 업그레이드에서는 btc_ecrecover 사전 컴파일 계약이 배포되었으며, 향후에는 secp256k1 타원 곡선 및 Schnorr 서명 기반의 더 많은 사전 컴파일 계약이 배포되어 프라이버시 자산 솔루션의 배포 및 운영 비용을 더욱 낮출 수 있을 것이다.

오프라인 스테이킹 (Offline staking)

표준 Qtum PoS 시스템에서는 스테이킹에 참여하는 노드는 반드시 온라인 상태를 유지해야 하며, 온라인 스테이커는 네트워크의 보안성과 운영을 향상시키지만, 이 설계는 일반 보유자에게는 제약이 될 수 있다. Qtum이 개발 중인 오프라인 스테이킹 메커니즘은 이러한 문제를 효과적으로 해결할 수 있다. 일반 사용자는 스테이킹 권한을 특별한 온라인 스테이킹 노드에 위임할 수 있으며, 자신의 노드를 항상 온라인 상태로 유지할 필요 없이 토큰은 오프라인 상태에서 안전하게 보관할 수 있고 언제든지 자유롭게 사용할 수 있다.

체인-클라우드 통합 (Chain-cloud integration)

오늘날까지 블록체인의 발전은 여전히 비트코인의 “시간 기반 블록 생성 + 글로벌 동기화 검증”이라는 논리를 벗어나지 못하고 있다. 이는 가치 전송처럼 상호작용이 적은 작업에는 큰 문제가 되지 않지만, 애플리케이션 플랫폼에는 최적의 방식이 아닐 수 있다. 단순한 소규모 게임조차 이더리움, EOS 등의 플랫폼을 마비시킬 수 있다는 사실은, 대규모 상업용 애플리케이션에 있어서 기존 퍼블릭 블록체인 플랫폼이 불충분하다는 점을 보여준다.

Qtum 팀은 블록체인이 애플리케이션에 제공하는 가장 중요한 특성은 "탈중앙화" 그 자체가 아니라, 아래의 세 가지 "블록체인 특성"이라고 본다:

- 계정, 주소, 자금, 신원에 대한 ‘4-in-1’ 권한 관리 메커니즘
- 자연스러운 정산 및 결제 네트워크를 내장함
- 인센티브와 유동성이 가져오는 고속 성장성

이러한 특성은 기존 모든 인터넷 애플리케이션에 결합된 요소들이다. 대부분의 인터넷 애플리케이션은 클라우드에 배포되어 있으며, 가까운 미래에도 클라우드 기반 애플리케이션은 주류로 남을 것이다. Qtum 팀은 위에서 언급한 블록체인의 특성과 클라우드에 배포된 애플리케이션이 융합될 경우, 새로운 형태의 애플리케이션이 등장할 것이며, 이는 블록체인의 진정한 도입을 촉진할 것이라고 믿는다.

4.1 초기 QTUM 토큰 분배

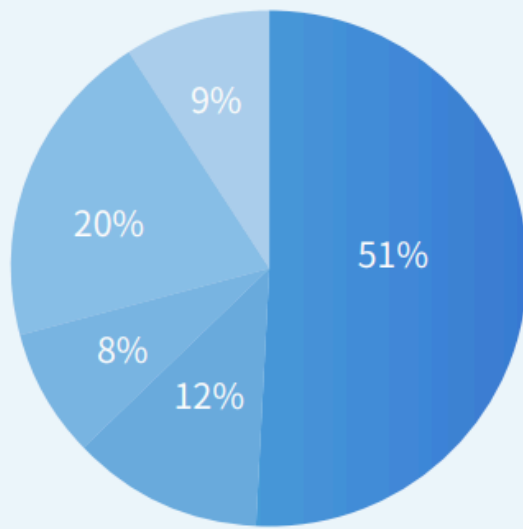
QTUM의 초기 발행량은 1억 개이며, Qtum 블록체인의 최초 5,000개 블록 동안 블록당 20,000 QTUM이 생성되는 코인베이스 거래(coinbase transaction)를 통해 발행되었다.

초기 생성된 토큰 중 **51%**, 즉 5,100만 QTUM은 2017년 3월에 대중에게 판매되었다. 해당 공개 판매를 통해 확보된 자금은 시스템 개발, 마케팅, 재무 및 법률 자문을 포함한 Qtum 체인 재단 운영에 사용된다.

20%, 즉 2,000만 QTUM은 창립 팀, 초기 투자자, 개발 팀에 할당된다. 이 중 **7%~8%**는 초기 투자자에게, **12%~13%**는 창립 팀 및 개발 팀에 할당된다.

29%, 즉 2,900만 QTUM은 상업 및 커뮤니티 개발, 학술 연구, 교육, 시장 확장에 사용된다. 이 중 **20%**는 산업 관련 애플리케이션 확장, DApp(분산 애플리케이션) 개발 지원, 비즈니스 지출(법률, 컴플라이언스, 회계, 컨설팅), 마케팅 및 PR, 토큰 스왑을 포함한 비즈니스 개발에 사용된다. 나머지 **9%**는 학술 연구, 개발자 교육, Qtum 체인 기술의 홍보 및 오픈소스 커뮤니티와의 협업을 지원하는 데 사용된다.

QTUM Token Distribution



- Public Sale
- Founding Team and Development Team
- Private Investors
- Business Development
- Academic Research, Education

투자자들의 이익을 보호하고 프로젝트의 건전하고 장기적인 운영을 보장하기 위해, QTUM 토큰의 사용 규정 외에도 Qtum 재단은 일부 개발 자금에 대해 락업(lock-up) 메커니즘을 설계하였다. 세부 내용은 다음과 같다:

Entity	Percentage	Amount	Lock-up
Qtum Community	51%	51,000,000	No lock-up
Early Supporter	8%	8,000,000	No lock-up
Team	12%	12,000,000	Distributed in four years
Academic Research, Education and Market Extension	9%	9,000,000	4-year lock-up. From March 2017 to 2021, each March unlock a quarter (2.25 million QTUM).
Business Development	20%	20,000,000	4-year lock-up. From March 2017 to 2021, each March unlocks a certain part. The unlock amounts for each year are 7 million QTUM 6 million QTUM 3.5 million QTUM 3.5 million QTUM respectively.

4.2 스테이킹 보상

앞서 언급했듯이, 스테이커(채굴자)에게 지급되는 블록 보상 인센티브는 세 가지로 구성된다: 새로 발행된 QTUM에 대한 보조금, QTUM 토큰 전송에서 발생한 거래 수수료, 스마트 계약 사용에서 발생한 Gas 수수료이다.

초기 발행된 토큰 외에도, 블록 보상으로 새로운 QTUM이 발행된다. 초기 블록 보상 보조금은 블록당 4.0 QTUM이며, 4년마다 반감되어 2045년에는 보조금이 완전히 사라진다. 따라서 초기 4년 동안 연간 발행률(인플레이션율)은 총 공급량의 약 1% 수준이다. 발행량이 증가하고 보상이 반감됨에 따라 발행률은 점차 감소하여 결국 추가 발행이 없게 된다.

Qtum 노드 코드에 따르면, 매 985,500 블록마다(관련 코드는 `qtum/src/chainparams.cpp` 참고) 블록 보상이 반감된다. 설계된 블록 생성 간격인 128초를 기준으로 계산했을 때, Qtum의 블록 보상은 4년마다 반감되며 총 7회에 걸쳐 반감된 후 0이 된다.

부록

용어 정의

비트코인 (Bitcoin)

최초로 성공한 피어 투 피어 전자 화폐 시스템이며, 전 세계 커뮤니티는 향후 전자 금 시스템으로 자리 잡을 것으로 기대하고 있다.

암호화폐 (Cryptocurrency)

1990년대의 크립토펙크 정신을 계승하여, 신뢰를 최소화하고 개인의 프라이버시 및 권리를 중시하는 모든 인터넷 사용자에게 서비스를 제공하는 암호화폐를 구축하려는 움직임. BTC(비트코인)는 이러한 암호화폐의 일종이다.

블록체인 (Blockchain)

IBM이 이 개념을 대중화하는 데 기여하였다. 2015년 IBM은 Permission Blockchain 및 상업용 블록체인 개념을 강력히 홍보하였으며, 이는 블록체인에 대한 일반적인 참조 개념이 되었다.

퍼블릭 체인 (Public chain)

이더리움을 기점으로, 단순한 토큰 시스템을 넘어 다양한 객체 지향 서비스를 제공할 수 있는 네트워크로 발전하길 기대하고 있다. 이상적인 퍼블릭 체인 플랫폼은 네트워크 노드 참여와 서비스 접근에 있어 진입 장벽이 없어야 하며, 위에서 운영되는 서비스는 실질적인 가치를 제공해야 한다. 이러한 기준에 따르면, 현재 산업 전반에 대중 시장을 위한 퍼블릭 체인은 존재하지 않지만, 다양한 형태의 “토큰” 분산 네트워크는 존재한다.

블록체인 핵심 기술 (Blockchain core technology)

원래는 비트코인 블록체인에 특정된 의미였지만, 현재는 전체 블록체인 산업을 지칭한다. 분산형 피어 투 피어 네트워크를 유지하기 위해 사용되는 핵심 기술들을 의미하며, 암호학, 합의 알고리즘, 가상 머신 기술, 게임 메커니즘, 피어 투 피어 네트워크 등을 포함한다.

블록체인의 가치 (Blockchain value)

정보화 시대에 있어 분업과 협업 인프라를 구축하는 것. 실물 자산과 시장성 있는 증권은 화폐 없는 블록체인 상에서 먼저 유통되고 거래될 것이다. 이때 신용은 여전히 현실 세계의 신용 투입에 의해 유지된다. 현실 세계의 신용에 의존하지 않는 것은 발행된 블록체인 네트워크이며, 이는 아직 초기 단계로, 진정한 공공 인프라가 되기에는 매우 어렵지만, 해당 방향은 지속적으로 진화하고 혁신 중이다. 여기서 공공 인프라란, 예를 들어 도시 내의 모든 상품 및 금융 정보를 하나의 네트워크에 올리는 것을 의미한다.

계정 추상화 계층 (AAL, Account Abstraction Layer)

계정 추상화 계층은 UTXO 모델의 계정 하위 계층과 스마트 계약 계층을 연결하는 구조이다. UTXO 모델 기반에서 실행되는 스마트 계약을 구현하기 위해 다양한 가상 머신을 느슨하게 결합된 방식으로 지원한다.

탈중앙화 거버넌스 프로토콜 (DGP, Decentralized Governance Protocol)

하드 포크 없이 스마트 계약을 이용한 동적 거버넌스를 실현한다. DGP를 통해 사용자는 온체인에서 네트워크 매개변수를 동적으로 수정할 수 있으며, 권한 관리 및 투표 기능을 구현할 수 있다.