출처: http://earlz.net/view/2017/10/02/0801/thoughts-and-goals-on-qtums-x86-vm

Qtum x86 VM에 대한 생각과 목표

그 동안 우리는 더 많은 프로그래밍 언어 지원 말고는 Qtum의 x86 VM에 대해서 말을 아꼈다. 그 이유는 기본적으로 디자인 프로세스가 범용적인 버전을 만드는 것은 쉽지만 최적화가 잘 되어 있고 효율적이며 사용하기 쉬운 버전을 만드는 것은 쉽지 않기 때문입니다. 그래서 이 글을 통해 디자인의 세부사항에 수박 겉핥기식이 아닌 우리가 염두 해 두고 있는 목표를 기술 하고 싶습니다.

프로그래밍 지원 언어

물론 프로그래밍 언어 지원은 x86 VM을 빌드 해야 하는 가장 큰 이유입니다. 저는 개인적으로 2018년을 Rust로 작성된 스마트 계약의 해라고 쓰고 싶습니다. Rust는 믿을 수 없을 정도로 효율적이고 경량이며 무엇보다도 프로그래머의 실수를 피하고 안정성을 중요시 합니다. Rust 보다 좋은 언어들은 훨씬 더 많이 있습니다. C# 혹은 Go 와 같이 사용하기 쉬운 언어를 가져 오는 것 역시 목표입니다.

x86 VM의 힘의 기본 핵심은 기존의 컴파일러나 프로그래밍 언어를 거의 다 사용할 수 있고 Qtum 운영체제와 같은 환경에서 실행하 수 있도록 일부 수정만 하면 된다는 것입니다. 거의 모든 컴파일러가 x86을 지원하고 있으므로 실제 bytecode나 아키텍처 지원이 이미 존재 합니다.

표준 라이브러리

EVM(Ethereum Virtual Machine)에 대해 공통의 불만 사항은 표준 라이브러리가 없다는 점입니다. 이것은 개발자로 하여금 성가시게 하고 귀중한 블록체인 공간을 직접 소모한다는 점 입니다. 표준 라이브러리를 제공하면 Qtum 블록체인을 보다 경량화하고 효율적으로 만들 수 있을 뿐만 아니라 이런 표준 라이브러리 함수가 이더리움의 pre-compiled 계약과 같은 특별한 내부 코드를 가질 수 있습니다. 기 기능은 새로운 pre-compiled 계약에 대한 특별 지원을 추가하지 않고도 발생할 수 있고, 이 특수 기능을 사용하는 계약에 의존합니다. 대신에 계약서는 예전의 최적화되지 않은 코드를 사용 할 수 있으며, opaque code(외부 인터페이스로 노출 되지 않은 코드)를 호출 할 때 이 코드는 아무런 변경을 하지 않고서도 마음대로 최적화 할 수 있습니다. 이와 같은 표준 라이브러리의 최적화는 구현 세부 사항입니다. 그러나 생태계의 구현이 보다 효율적으로 이루어짐에 따라 가스 모델은 가스 비용이 실제 자원 비용을 반영하도록 하여 이런 기능을 조정할 수 있습니다.

게다가 표준 라이브러리는 확장하기 위해서 포크(fork)가 필요하지 않습니다. 보통의 함수는 분산

형 관리방식 프로토콜(Decentralized Governance Protocol, DGP)을 사용하여 전문화된 표준 라이브러리 메모리 공간에 쉽게 입력이 가능합니다. 이 메커니즘을 사용하면 표준 라이브러리의 문제점을 보완할 수 있지만, 스마트 계약은 올바른 기능을 수행하기 위해서 문제점이 있는 동작에 의존 할 수 있으므로 특별한 감시가 필요합니다. 따라서 표준 라이브러리 기능에 대한 잠재적인 업그레이드 작업은 사전동의 기능에 의해서만 가능할 수도 있고, 전혀 존재하지 않을 수도 있습니다. DGP의 목표는 항상 보수적인 자세를 유지하고 가령 완전한 타협이 있는 경우에도 스마트 계약이 영향 받지 않고 사용자의 자금을 안전하게 보장하는 것입니다.

최적화된 가스 모델

이번 파트는 조금은 까다로운 부분이라 예고합니다. 우리는 초기의 EVM(Ethereum Virtual Machine)과 비슷한 간단한 가스 모델로 x86 VM을 시작 할 것입니다. x86에서 사용할 수 있는 ISA(instruction Set Architecture)와 기능들이 훨씬 더 강력하기 때문에 이 공간을 발전시키기에 훨씬 간단한 방법이 있습니다.

간단하면서도 강력한 해결책 중 하나는 스마트 계약 및 전반적인 프로그램에서 사용되는 공통 기능을 갖춘 표준 라이브러리를 제공하는 것뿐만 아니라 이러한 표준 라이브러리 기능이 일반적인 계산에 사용되는 단순하고 일반적 가스 모델에 의존하는 것이 아닌 사람이 설정한 비용으로 만드는 간단한 방법이 있습니다. 예를 들어 단순한 가스 모델에서 `strlen`은 문자열에서 문자 하나당 90개의 가스가 필요할 수 있습니다. 그러나 개발자가 검사 할 때 `strlen`은 Qtum VM에서 매우 저렴하게 실행이 가능합니다. Qtum의 DGP는 이 함수에 대해서 특별 가스 규칙을 제안하는데 사용됩니다. 이제 이 함수를 호출하는데 드는 비용은 0개의 가스에 대한 초기 비용과 문자 하나당 1개의 가스를 합친 것입니다. 완벽하게 정확한 가스 모델을 만드는 것은 불가능 하기 때문에 Qtum에서 DGP 메커니즘을 활용하여 최적화되면서도 효율적인 근사 방식을 만들기 원합니다.

AAL(Account Abstraction Layer, 계정 추상화 계층)의 모든 권한 잠금 해제

현재 우리는 계정 추상화 계층(Account Abstraction Layer, AAL)을 "EVM(Ethereum Virtual Machine) 작업을 수행하기에 필요한 것"이라고 강조합니다. 그러나 AAL은 Qtum에서 EVM을 작동시키는데 필요한 것 이상으로 많은 숨겨진 성능을 제공합니다. Qtum은 처음부터 여러 개의 가상 머신을 지원하도록 설계 되어 있으며 EVM은 지원되는 가상 머신 중 첫 번째 입니다. 이 말은 계정 추상화 계층은 현재 EVM을 통해 쉽게 노출 될 수 있기 때문에 제한되고 있습니다. 우리가 설계하고 있는 x86 VM은 이런 한계에 직면 하지 않을 것입니다. 왜냐하면 우리가 드러내고 싶은 강력한 이유가 아래에 있습니다:

- P2SH(Pay to Script Hash, Bitcoin 스타일) 스마트 계약을 통한 송금 및 수취를 위한 일급 개체로써의 다중 서명(Multi-Signature)

- Qtum 스크립트 기능을 최대로 활용하기 위해 사용자 정보 거래내역을 보내는 원시 거래 내역 스크립트(Raw transaction script) 지원
- Segwit(증인 분리, Segregated Witness) 거래내역에 스마트 계약 포함 및 실행 허용

스마트 계약의 새로운 가능성

x86을 사용하게 되면 폰 노이만(Von Neumann) 컴퓨팅 아키텍처를 사용할 수 있습니다. 이것이 의미하는 바는 코드는 데이터이고 그 반대도 마찬가지라는 개념입니다. 하드웨어/소프트웨어 인터럽트와 같은 기능뿐 아니라 이런 특징은 구조 및 기능과 같은 잠재적인 운영 체제가 여러 개의 준 신뢰 관계가 있는 참가자가 단일 스마트 계약에 통합 되도록 합니다. 여기에는 협력 가능한 멀티 태스킹(Cooperative-multitasking), 일시 중지 및 다시 시작을 실행(다시 말하면 이후 거래내역에서 다시 시작) 그리고 워치독 타이머(Watchdog timer, "시간"대신 가스로 작동) 등이 포함됩니다. 물론 이런 개념은 새로운 계약에 자금과 데이터를 전송할 필요 없이 계약 bytecode를 업데이트 하는 직접적인 메커니즘을 포함합니다.

x86 명령어 세트는 시스템 호출뿐 아니라 특정 hem 공간, 페이징 및 메모리 매핑에 대한 특수 권한과 같은 것을 제어하는 많은 특수 기능을 포함합니다. Qtum에서 이러한 특수 시스템 수준의 지침을 대부분 공개하지 않을 것으로 예상합니다. 그들은 가스 모델 디자인을 크고 복잡하게 만들고 모든 것을 최적화 하기 더 어렵게 만듭니다.

그러나 이런 실망에도 불구하고, 해당 지침 내에서 스마트 계약과 관련된 것은 상대적으로 거의 없습니다. 하나의 스마트 계약 코드 내에 별도의 권한이 부여되 ring-0 코드와 권한이 부여되지 않은 ring-3 코드를 갖는 공개 블록체인데 대해 현실적으로 필요성이 거의 없습니다. 사용 케이스가 이런 기능에 대해 유행하는 경향이 있는 곳은 권한이 부여되거나 준권한이 부여된 블록체인에 있습니다. 그래서 Qtum의 엔터프라이즈 측면에서 초점을 맞추기 시작하면서 다시 검토 할 것입니다.

일급 오라클 데이터베이스

거래내역을 위한 x86 VM 모델에서 계약에 필요한 데이터를 알고 있는 경우 계약을 호출 할 필요가 없습니다. 외부 계약의 저장 공간에서 직접 다운로드를 할 수 있습니다. 이는 계약이 자신의 ABI(Application Binary Interface)및 API(Application Programming Interface) 메커니즘을 구축하여 저장 공간을 표준화 할 수 있는 일급 오라클 데이터베이스를 허용합니다. 그런 다음 계약서를 통해서 계약서 bytecode 전체를 불러오는 비싼 호출이 필요 없이 저장 데이터를 직접 불러올 수 있습니다. 이것은 스마트 계약의 기능에 의해 제한되는 대신 오라클 데이터베이스를 블록체인에서 일급객체로 만들 것입니다.

블록체인 분석

x86에서 사용할 수 있는 많은 메모리 공간과 일반적인 연산을 위한 효율적인 연산 코드 세트는 몽상과 같은 블록체인 분석의 잠재력을 실현 가능하게 합니다. 계약 분석을 위해 전체 블록체인 데이터를 드러내는 것이 가능합니다. 이를 통해 AI 기반 스마트 계약을 통해 스마트 계약이 현재 네트워크 상태에서 가능한 효율적으로 작동하도록 자신의 동작을 조정할 수 있도록 오라클 데이터베이스 역할을 할 수 있는 블록체인을 자동으로 모니터링 할 수 있습니다. 이 블록체인 데이터는 전체 거래 데이터 또는 블록체인 노드(합의-결정 방식)에 의해 계산 된 통계를 포함 할 수 있습니다. 이 데이터는 완전히 상수이며 추가 메모리 사용량이 수 메가 바이트 밖에 되지 않기 때문에 데이터를 노출하는데 불리한 점이 있습니다.

대체 데이터 저장소

현재 EVM은 32바이트 데이터를 가리키는 데에 32바이트 키를 사용하도록 강제하고 있습니다. 특히 공간의 세분화와 유지 관리를 생가면 관리하기 상당히 어려울 수 있습니다. 게다가 이것에 대한 큰 이유도 없습니다. 따라서 x86 시스템에서 우리는 스마트 계약에 일반 목적의 키-값 저장소를 제공하려 합니다. 따라서 1부터 많은 수의 바이트를 키로 저장 할 수 있으며, 동일하게 변형된 값을 바라보도록 할 수 있습니다. 지금까지 이 기능에 대해 제안된 가스 모델은 기본적으로 데이터베이스에 쓰기/읽기에 대한 정액 요금을 지불하고 처리되는 바이트에 대한 요금을 포함합니다. 이 기능은 물론 stateRootHash 아래에 적용되므로 SPV(Simple Payment Verification) 지갑이 이런 데이터베이스를 사용하여 스마트 계약과 상호 작용 할 수 있습니다.

명시적 종속 계층

다소 이상적인 다음 목표는 명시적으로 선언되고 실행되는 스마트 계약의 종속성 계층을 허용하는 것입니다. 이것은 알 수 없는 스마트 계약에 관해서 여전히 가능하도록 하는 사전 동의 기능일 뿐입니다. 그러나 의존성을 정확히 알고 있는 계약의 경우 계약에 따라 일부 계약이 병행 될 수 있으므로 가스 비용이 절감되고 다른 혜택도 얻을 수 있습니다. 이 기능을 선택하는 x86 기반 스마트 계약의 경우 확장성의 큰 이점이 됩니다.

왜 x86인가? ARM이 안 되는 이유가 무엇인가?

나는 많은 사람들에게 "왜 x86인가? ARM이 안 되는 이유는 무엇인가" 라고 묻는 것을 들어왔습니다. 이런 질문은 아주 좋은 질문입니다. 우리는 x86이 가상 시스템과 에뮬레이터에 대해 가장 잘 이해하고 있는 플랫폼이라고 생각하고 있습니다. x86을 위해 효율적이면서 안전한 VM을 만들

기 위해 수십 년간 공통의 관심사가 있었습니다. 이에 대해 정말 연구하고 싶다면 답을 멀리서 찾지 말고 안드로이드 에뮬레이터를 합리적인 성능 수준으로 작동시키는 것에 대해 Stackoverflow에 올라와 있는 질문을 보시기 바랍니다. 기본적으로 대부분의 경우 해결책은 ARM 대신 x86 가상 머신을 사용하는 것 입니다. 물론 Qtum과 같이 형편없는 것으로 간주되지 않는 ARM VM을 위한 일부 프로젝트가 있습니다. 그러나 요점은 x86 에뮬레이션이 상당히 간단한 해결책으로 알려진 문제라는 사실입니다. 잘 알려진 Intel 설명서는 이와 같은 CPU 아키텍처에서 가장 잘 작성되고 명확한 문서로 간주됩니다. 재미를 위해서 x86 에뮬레이터를 사용하는 고등학생들도 있습니다(하하 바로 작성자 본인이다!). ARM에 대한 컴파일러 지원은 계속 향상되고 있지만 x86지원과 거의 비슷한 수준입니다.

이제 x86은 단순한 ISA(Instruction Set Architecture)가 아닙니다. 그것은 8008과 함께 70년대부터 존재했고, 8088/8086 이후로 하위 호환성을 유지하고 있습니다. 이것은 실제 디자인에 큰 타격을 주고 있으며 사용 가능한 방대한 양의 opcode가 있습니다. 그 중 일부는 쓸모가 없으며 지시를 따르지 않고 코드를 작성했다면 실제 하드웨어에서 더 느리게 실행됩니다. 제가 가장 좋아하는 예제는 80년대부터 인기가 없었던 저주받은 2진 코드화 된 10진수 입니다. 그러나 이것은 몇 시간의 추가 작업으로 인해 추가되는 복잡성입니다. x86 사용의 이점은 비용보다 훨씬 큽니다.

ARM은 여전히 사정권 안에 있습니다. 특히 ARM 프로세서에서 일반적으로 작동하는 IoT 사용 사례가 있습니다. 현재 우리는 x86에 초점을 맞추고 있지만 그 이후에는 특히 엔터프라이즈 및 허가된 블록체인에 대해 특별히 중점을 두고 있습니다.