CyberMiles: 비즈니스 거래를 위한 차세대 블록체인 프로토콜

5xlab 제작

기술 백서

v1.5

[상업적 이용 시나리오 및 토큰 판매 관련 사항은 별도의 문서에서 다뤄집니다]

면책고지

이 문서는 저희가 제안해 드리는 CyberMiles 블록체인 프로토콜과 이 프로토콜의 네트워크 전개를 위해 나아갈 방향에 대해 설명해 드리는 개념서("**기술 백서**")입니다. 이 문서는 언제든지 수정되거나 대체될 수 있습니다. 그러나 본 "기술 백서"를 업데이트하거나 이를 받는 사람에게 추가적인 정보를 제공할 의무는 없습니다.

독자들은 다음과 같은 내용의 고지를 받습니다:

모든 사람들이 이용할 수 있는 것이 아닙니다: CyberMiles 플랫폼과 CyberMiles 토큰은 모든 사람들이 이용할 수 있는 것이 아닙니다. 참여의 방식은 특정한 정보 및 문서의 제공을 요구하는 등의 규정된 여러 절차에 따라 달라질 수 있습니다.

특정 사법권 내에서 규제되는 상품의 제안이 아닙니다: CyberMiles 토큰(본 "기술 백서"에 설명되어 있듯이)은 특정 사법권 내에서의 유가증권 또는 특정 사법권 내에서 규제되는 상품이 아닙니다. 이 "기술 백서"는 사업안내서가 아님은 물론 특정한 종류의 문서를 제공하는 것이 아니며 특정 사법권 내에서의 거래의 제안 또는 특정 사법권 내에서의 유가증권 또는 기타 규제되는 상품에 대한 모객행위가 아닙니다. 이 "기술 백서"는 어떠한 사법권 내에서도 그 종류를 막론하고 어떠한 규제당국으로부터의 심사를 받은 적이 없습니다.

자문이 아닙니다: 본 "기술 백서"는 CyberMiles 플랫폼에 대한 참여나 CyberMiles 토큰에 대한 구매에 대한 자문이 아니며 어떠한 계약 또는 구매결정과 관련하여서도 의존되어서는 안됩니다.

의존가능한 진술 또는 보증이 아닙니다: 이 문서에 설명되었거나 기타 본 프로젝트와 관련하여 전달되는 정보, 서술, 의견 등의 내용은 그 정확성 또는 그 완전성과 관련하여 의존가능한 진술 또는 보증이 아닙니다. 그 정도에 관계없이 향후의 일 또는 개념에 대해 서술된 내용의 달성 또는 합리성에 대해서 어떠한 의존가능한 진술 또는 보증을 제시하는 것이 아닙니다. 이 문서의 어떤 내용도 미래에 대한 약정이나 의존가능한 진술이 아니며 의존되어서는 안됩니다. 본 "기술 백서" 또는 그 일부에 의존하여 행동하는 사람으로부터 또는 그러한 사람과 관련하여 발생하는 손실 또는 피해에 대한 모든 책임은 태만, 불이행, 부주의의 유무와 관계없이 관련 법이 허용하는 한 최대한 면책됩니다. 책임이 제한되지만 완전히 면책되지 않는 경우 그 책임은 관련 법이 허용하는 한 최소한의 책임으로 제한됩니다.

기타 회사들: CyberMiles Foundation Limited("재단")과 5miles LLC("5miles")를 제외한 어떠한 회사명, 플랫폼명, 상표명의 사용도 해당 관련자와의 제휴, 그 관련자로부터의 후원을 나타내는 것이 아닙니다. 본 "기술 백서"에서 언급된 특정 회사 또는 플랫폼은 예시만을 목적으로 합니다.

귀하는 세금 및 회계 관련하여 전문가로부터 필요한 모든 내용에 관련하여 자문을 받으셔야 합니다. 저희는 CyberMiles 프로젝트가 크게 성공하는 프로젝트가 되기를 바랍니다. 그러나 성공은 보장되지 않으며 디지털 자산 및 플랫폼에는 리스크가 뒤따릅니다. 귀하는 이러한 리스크와 이 리스크를 부담할 수 있는 귀하의 능력에 대해 평가해 보셔야 합니다.

운영개요

블록체인 기술은 비즈니스 어플리케이션 분야에서 상당히 유망한 기술로 여겨지고 있습니다. 그러나 현 세대의 블록체인들은 낮은 실행효율 및 낮은 개발자 생산성의 문제를 겪고 있습니다. 결과적으로 이 블록체인들은 일반적인 비즈니스 거래에 있어서 폭넓게 채용되지 않고 있습니다. 이 백서에서 저희는 CyberMiles 블록체인이라고 불리는 비즈니스 계약 거래에 특화되어 있는 새로운 블록체인 네트워크 프로토콜을 제안합니다.

저희가 제안해 드리는 솔루션은 기존의 입증된 비즈니스 미들웨어 기술 스택이 블록체인 상의 분산화된 가상머신에 접근할 수 있도록 해주는 혁신적인 프로토콜입니다. 이 새로운 블록체인은 높은 성능을 보여줌은 물론 초당 10,000 회가 넘는 거래가 가능한 확장성을 지원합니다. 또한 이 블록체인은 기업들이 비즈니스 규칙과 그 절차를 코드화하는 분산화된 미들웨어 어플리케이션인 "스마트 비즈니스 계약"을 작성할 수 있도록 해줍니다. 본 네트워크의 네이티브 암호화 화폐인 CyberMiles 토큰(CMT)은 거래를 정산하거나 네트워크 검증자("스마트 비즈니스 계약"을 실행하는 자)에게 보상을 지급하거나 커뮤니티 구성원들이 서로 간에 서비스를 제공하도록 인센티브를 제공하는 데 사용될 수 있습니다.

CyberMiles 블록체인만의 이점은 1 천만명이 넘는 미국 기반 등록 이용자들과 30 억달러가 넘는 연간 거래액 추산치를 자랑하는 5miles 의 기존의 전자상거래 망의 지원에 사용될 수 있다는 것입니다. 이 블록체인은 곧 전세계에세 가장 큰 규모의 블록체인 기반 거래망을 만들 것입니다. 본 네트워크는 분산된 이용자 신분 및 신용 정보 관리, 분산화된 정산 및 어음교환소, 개인 대 개인 투표 및 합의도출 등의 서비스를

제공합니다. 본 네트워크 플랫폼 상의 어플리케이션의 예로는 분산화된 개인정보 "지갑", 개인 대 개인 중소기업 대출, 개인 대 개인 분쟁조정 등이 있습니다.

목차

1. 시작하며

1.1 비트코인과 이더리움

비트코인은 블록체인 기술 최초의 인기 어플리케이션입니다. 블록체인 1.0 이라고 알려져 있는 비트코인 네트워크는 간단히 말해서 분산화된 합의 메커니즘을 내장하고 있는 분산된 출납부 시스템입니다. UTXO 기술을 이용해 비트코인 네트워크 상에서 실행되는 프로그램을 만들 수 있지만 낮은 수준의 UTXO 프로그램은 그 수용력이 매우 제한적입니다. 이러한 프로그램은 튜링 불완전한 프로그래밍 환경이라고 할 수 있으며 그 사용이 매우 어렵습니다. 결과적으로 비트코인 네트워크란 커뮤니티 개발 어플리케이션을 매우 적게 이용하여 비트코인 거래를 기록하는 분산된 출납부 시스템이라고 할 수 있습니다.

이더리움 프로젝트는 블록체인 2.0 을 구축하는 것을 목적으로 만들어 졌습니다. 이더리움 블록체인은 튜링 완전한 가상머신(이더리움 가상머신 또는 EVM)을 덧붙여 특정 조건이 만족될 경우 계정 간에 토큰/암호화 화폐를 이동시킬 수 있는 "스마트 계약"라고 불리는 써드파티 스크립트를 지원함으로써 "전세계의 컴퓨터"가 되려는 큰 목표를 가지고 있습니다(활용사례 중 하나를 예로 들면 "스마트 계약"이 에스크로 계정의 역할을 하는 것입니다). 이러한 "스마트 계약"들은 이더리움 노드들에 의해 실시간으로 실행됩니다. 그 결과물은 유효성 인증을 거친 후 채굴자(또는 검증자)들의 블록체인에 저장됩니다.

또한 이더리움은 블록체인의 외부에서 동작하지만 블록체인 내의 "스마트 계약" 방식에 요청을 보낼 수 있는 분산화된 앱(일명 DApp)의 개념을 지원합니다. 일반적인

조건의 환경에서 DApp 은 해당하는 "스마트 계약"에 대해 UI 를 제공하는 웹 어플리케이션인 경우가 많습니다.

1.2 주요 문제들 및 관련 작업

한편 블록체인 기술이 오늘날 낮은 효율 및 낮은 개발자 생산성이라는 2 가지 밀접한 관련이 있는 문제들을 겪고 있다는 사실은 널리 알려져 있습니다.

블록체인 네트워크는 분산화된 시스템으로 동일한 연산을 반복하여 "진실"이 무엇인지에 대한 합의에 도달하기 위해 많은 서로 독립되어 있는 비협조적 노드들을 필요로 합니다. 네트워크의 규모에 따라 연산에 들어가는 노력이 기하학적으로 증가하므로 이 작업은 시스템을 매우 비효율적으로 만드는 것은 물론 확장이 어렵도록 만들게 됩니다. 이러한 확장성/성능 관련 문제들로 인해 블록체인 네트워크 상에서 허용된 써드파티 연산작업 역시 매우 제한적입니다. 결국 이것은 매우 불량한 개발자 경험과 낮은 생산성을 야기합니다. 결과적으로 이더리움 "스마트 계약" DApp 은 오늘날 널리 사용되고 있지 않습니다.

최근 블록체인 기술의 성능 및 확장성 문제에 대응하고자 하는 몇가지 솔루션들이 제안되어 주목을 받고 있습니다.

- 새로운 합의 메커니즘. 기존의 비트코인과 이더리움 블록체인들은 모두 네트워크를 신뢰할 수 없는 참여자로부터 지키기 위해 작업증명(PoW)이라고 불리는 매우 비효율적인 합의 메커니즘을 사용하고 있습니다. 지분증명(PoS)라고 불리는 훨씬 더 효율적인 메커니즘으로 PoW 를 대체하기 위해 많은 노력이

이루어졌습니다. 이 분야를 선도하고 있는 것은 Tendermint 의 Byzantine 결함허용(BFT) 합의 엔진과 이더리움의 자체적인 CASPER 솔루션입니다.

- 네트워크의 파편화. 네트워크를 확장하기 위해 일반적으로 사용되는 접근법은 네트워크를 몇개의 하위네트워크로 파편화시키는 것입니다. 이로써 전체 네트워크는 하위네트워크들을 더 추가함으로써 수평적으로 확장을 할 수 있습니다. 그러나 분산화된 블록체인 네트워크에서는 하위네트워크들이 서로 정보를 교환해야 하며 그들의 상태에 대해 합의를 해야 합니다. 이것은 일반적인 데이터베이스 파편화와 비교해 훨씬 더 다루기 어려운 문제입니다. 이 분야를 선도하고 있는 솔루션으로는 Cosmos Internet of Blockchains 와 Polkadot 네트워크가 있습니다.

- 체인 외부 연산. 성능문제에 대한 보다 더 직접적인 솔루션은 상당한 부담을 발생시키는 대량의 연산작업을 체인 그 자체로부터 분리시켜 블록체인 합의 메커니즘을 연산결과를 기록하는 목적으로만 사용하는 것입니다. 이 분야에서도 Lightning Network 의 체인 외부 상태 채널, Plasma 의 사기방지 사이드 체인, TrueBit 의 체인 외부 이더리움 "스마트 계약" 거래 플랫폼 등의 많은 실험이 이루어졌습니다.

저희는 이 백서를 통해 블록체인 확장성과 관련된 근본적인 문제의 해결을 시도하지는 않을 것입니다. 저희는 시간이 지남에 따라 커뮤니티 합의에 의해 훌륭한

솔루션이 나타나게 될 것이라고 믿고 있습니다. 미래의 블록체인 네트워크는 높은 성능과 확장성을 겸비하기 위해 3 가지 접근법들을 모두 내장하게 될 것입니다.

그러나 블록체인 네트워크는 이러한 문제들이 해결된 뒤에도 상거래 분야에서의 유용성을 확보하기 위해서 엔터프라이즈 어플리케이션 개발자들을 끌어모으고 지원해야 합니다. 이 프로젝트에서 저희가 달성하고자 하는 목표는 블록체인 상의 써드파티 엔터프라이즈 어플리케이션들을 더욱 강력하게 만드는 동시에 더욱 쉽게 개발할 수 있도록 해주는 아키텍처적 솔루션을 제안하는 것입니다.

1.3 더 나은 스마트 계약

1 세대 기술로서 그리고 위에서 언급해 드린 확장성/성능 관련 이유로 인해 이더리움 EVM 과 DApp 은 사용하기가 어렵습니다. 저희는 EVM 과 그와 관련된 소프트웨어 스택을 획기적으로 개선하여 보다 개발자 친화적이고 엔터프라이즈 관련 작업에 보다 신속히 투입할 수 있도록 만드는 것을 목표로 하고 있습니다.

- "스마트 계약"은 종종 블록체인 외부의 이벤트에 의해 촉발되어야 하는 경우가 있습니다. 이더리움에서는 외부 세계의 권한있는 결정적 상태 정보를 제공하기 위해 "오라클"을 필요로 합니다. 오라클은 표준화되어 있지 않으며 "스마트 계약" 모르게 변할 수 있기 때문에 취약한 솔루션이라고 할 수 있습니다.

- "스마트 계약"은 DApp 미들웨어와 느슨한 관계밖에 맺을 수 없다고 할 수 있습니다. "스마트 계약"은 DApp 내의 어떠한 것들을 활용할 수 있는지에 대한 "알지" 못하는 상태에서 DApp 의 소프트웨어 파트에 콜을 보낼 수 없습니다. 튜링 완전한 절차적 프로그래밍 언어를 사용하여 복잡한 규칙을 프로그래밍하는 것은 난이도가 높은 작업이므로 대부분의 "스마트 계약"들은 단순한 비즈니스 거래 규칙만을 실행합니다.

- DApp 미들웨어는 캡슐화되거나 재사용될 수 없습니다. DApp 개발자들은 아키텍처 관련 결정을 내린 후 일회성 어플리케이션들을 만들어야 합니다.

- DApp 미들웨어는 블록체인 암호화 화폐 인센티브 시스템과 결합되지 않습니다. DApp 노드들은 상당한 양의 연산자원을 기여하여야 하지만 암호화 화폐를 보상으로 받을 수 없습니다. 이 때문에 DApp 들이 기업들에 의해 중앙집중식으로 운영되게 되었습니다.

2. 제안해 드리는 솔루션

저희는 이더리움의 단점에 대한 대응은 물론 비즈니스 계열 개발자들에 의한 분산화된 어플리케이션의 제작에 적합한 "가상머신" 기반의 블록체인의 제작을 위해서 저희가

"스마트 비즈니스 계약"이라고 명명한 기능을 지원하는 새로운 블록체인 프로토콜을 제안해 드리려고 합니다. 이 프로토콜은 가상머신을 포함하고 있을 뿐 아니라 블록체인 외부의 미들웨어 소프트웨어 스택을 규정합니다(오늘날 비표준 방식으로 DApp 에 의해 다뤄지고 있는). 블록체인의 각 노드는 블록체인 출납부를 운용하는 것뿐 아니라 표준화된 미들웨어도 지원합니다.

과거의 성공적인 엔터프라이즈 소프트웨어의 방식을 빌려온 이 방식의 주요 특징은 엄청나게 강력한 가상머신 또는 프로그래밍 언어를 만드는 대신 재사용이 가능한 소프트웨어 파트로 이루어진 대규모 라이브러리를 구축하는 것입니다. 리눅스 운영체제가 바로 좋은 예입니다. 이 운영체제는 커뮤니티가 수천개의 비즈니스 친화적 소프트웨어 패키지를 통해 핵심 OS 의 사용성을 확장시키는 것은 물론 Fedora/Red Hat 이 스택을 표준화하기 위해 참여한 뒤에서야 엔터프라이즈 사용자들에게 널리 채택되었습니다. 이외에도 다른 과거의 예로는 자바 2 엔터프라이즈 에디션 플랫폼, LAMP 스택, Ruby on Rails 플랫폼 등이 있습니다. 이러한 엔터프라이즈 플랫폼들의 강점은 표준화된 라이브러리 및 프레임워크에 있습니다.

소프트웨어 캡슐화 및 재사용은 엔터프라이즈 소프트웨어에 있어서 가장 중요하고 가장 훌륭한 기능이라고 할 수 있습니다. 이제 저희가 이러한 최고의 기능들을 블록체인 플랫폼에도 적용시킬 차례입니다.

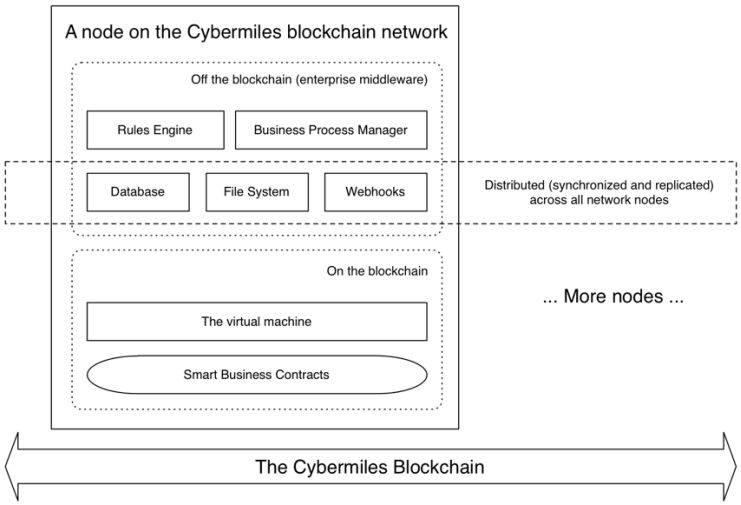

도표 1 이 CyberMiles 블록체인의 전반적인 아키텍처의 예시를 보여주고 있습니다. 보시는 것처럼 상당한 수의 재사용가능한 소프트웨어 파트들이 블록체인 밖에 위치하고 있습니다.

2.1 스마트 비즈니스 계약

CyberMiles 블록체인 상의 "스마트 비즈니스 계약"은 이더리움 블록체인 상의 "스마트 계약"과 유사합니다. 이 계약은 블록체인 노드에 의해 실행되며 새 블록이 생성될 때 채굴자에 의해 그 유효성이 인증됩니다. "스마트 비즈니스 계약"으로부터 얻어진 결과는 새 블록에 저장됩니다.

그러나 CyberMiles "스마트 비즈니스 계약"과 이더리움 "스마트 계약" 사이의 가장 두드러진 차이는 "스마트 비즈니스 계약"은 모든 어플리케이션을 처음부터 만드는 대신에 내장된 강력한 비즈니스 소프트웨어 미들웨어 스택에 접근할 수 있도록 했다는 것입니다. 따라서 "스마트 비즈니스 계약"은 쉽게 개발이 가능함은 물론 그 자체로 높은 재사용성을 가지고 있습니다.

"스마트 비즈니스 계약"이 블록체인을 구성하고 있으므로 외부 엔터프라이즈 미들웨어 스택 전체의 운용을 위해 필요한 자원을 비롯해 이러한 계약을 실행하기 위해 필요한 연산능력은 CyberMiles 시스템의 암호화 화폐인 CyberMiles 토큰(CMT)을 사용해 거래할 수 있습니다. 거래를 하고자 하는 네트워크 이용자들은 네트워크 검증자들에게 데이터 완전성 확보를 위해 노력해 준 것에 대한 보상으로 소정의 거래수수료를 CMT 로 지불합니다.

2.2 미들웨어 스택

"스마트 비즈니스 계약"은 블록체인 외부의 비즈니스 소프트웨어 프레임워크에 접근할 수 있습니다. 이러한 소프트웨어 프레임워크들은 블록체인을 운용하는 노드들 하나하나에 내장되어 있습니다. 이러한 프레임워크들은 "스마트 비즈니스 계약"이 실행될 때 또는 블록체인 채굴자들이 그 결과에 대해 유효성 인증을 할 때마다 작동합니다. CyberMiles 시스템에 포함된 엔터프라이즈 미들웨어 프레임워크 스택은 다음의 요소들로 구성되어 있습니다.

- 규칙엔진. 대부분의 비즈니스 계약은 특정한 규칙에 따라야 합니다. 일반적인 용도의 절차적 프로그래밍 언어와는 달리 전용 규칙엔진은 쉽게 사용할 수 있으며 또 효율적이라는 것이 입증되었습니다. 이러한 규칙엔진은 이미 많은 기업들에 의해 사용되고 있습니다.

- 비즈니스 프로세스 관리자(BPM). BPM 시스템은 다단계 계약의 실행 상태를 모방하는 상태머신입니다. 이것은 계약 당사자에 의한 외부 행위에 의해 조종되며 BPM 은 일반적으로 다음 단계를 결정하기 위해 규칙엔진을 사용합니다.

- 분산된 데이터베이스. 분산된 데이터베이스는 복잡한 어플리케이션 프레임워크를 지원하고 어플리케이션 데이터를 저장하기 위해 필요합니다. 이 데이터베이스는 블록체인 상의 모든 노드들에 걸쳐 복제되며 동기화됩니다. 거래의 결과에 대한 정보는 블록체인 자체에 저장되므로 이 데이터베이스는 거래결과를 저장하지 않습니다.

- 분산된 파일 및 데이터 저장소 서비스. "스마트 비즈니스 계약" 및 관련 미들웨어 서비스는 의사결정을 위해 필요한 대용량 파일을 관리하기 위해 파일 서비스로의 접근을 필요로 합니다.

- 분산된 웹훅 서비스. 비즈니스 시스템은 계약 의무(예를 들어 전자상거래 어플리케이션용 FedEx 배송 알림)를 완전히 달성하기 위해 외부 업체와의 상호작용을 필요로 하므로 저희는 "스마트 비즈니스 계약"과 관련된 외부 이벤트를 수신할 수 있는 분산된 웹훅을 내부에 구축할 예정입니다.

"스마트 비즈니스 계약"은 복잡한 규칙, 절차, 데이터, 웹훅 등을 포함하고 있습니다. 하지만 이 모든 요소들을 하나로 합쳐 그 작업들을 지휘할 프로그램이

필요합니다. 이는 일반 및 튜링 완전한 프로그래밍 언어를 필요로 합니다. CyberMiles 가상머신이 블록체인 소프트웨어와 함께 각 네트워크 노드로 전달되도록 함으로써 이것을 지원할 수 있습니다.

2.3 비즈니스에 바로 투입가능한 계약 템플릿

"스마트 비즈니스 계약"의 주요 특징은 이 계약들은 재사용이 가능한 소프트웨어 파트 위에 추가로 구축된다는 사실뿐만 아니라 그 자체를 재사용할 수 있다는 사실입니다. 대부분의 비즈니스 거래 시나리오들은 제대로 규정되어 있으므로(법적 또는 사업적 관점 모두에서) 주요 사항 및 변수(예를 들어 계약당사자명, 일시, 액수 등)들을 변경하는 것만으로 재사용할 수 있는 "스마트 비즈니스 계약" 템플릿을 만드는 것이 가능합니다. 이 템플릿 라이브러리는 비즈니스 어플리케이션을 구축하고 배치하는 데 드는 비용을 절약하고 네트워크 자체의 가치를 증대시켜 줄 것입니다.

2.4 분산화된 앱들과 스마트 비즈니스 계약

CyberMiles 블록체인 시스템 내에는 여전히 분산화 앱의 개념이 존재합니다. CyberMiles DApp 은 기밀 또는 성능을 이유로 블록체인 내에 저장되어서는 안되는 모든 데이터 및 로직을 관리합니다. 비즈니스 거래와 관련된 비즈니스 로직에 대한 부담을 "스마트 비즈니스 계약"에 완전히 넘겨줄 수 있습니다.

3. 기술

CyberMiles 블록체인의 미들웨어 스택을 위한 기술 솔루션을 선택하는 것은 상대적으로 간단한 일입니다. 왜냐하면 이러한 솔루션들은 모두 비즈니스 미들웨어 분야에서 이미 폭넓게 사용되고 있는 실효성이 입증된 솔루션들이기 때문입니다. 저희는 이러한 기술들을 블록체인 프레임워크에 내장시킬 수 있는 공학적 솔루션을 구축하고 있으며 시스템이 적절히 기능할 수 있도록 도와주는 경제적 인센티브 제도를 구상하고 있습니다.

이 백서에서 다뤄진 구체적인 기술 프레임워크는 예시만을 목적으로 합니다. 추후 커뮤니티가 기술운영위원회의 구성원을 선출하기 위해 토론회 및 선거 등을 개최할 수도 있습니다. 그 후 위원회가 전원의 의견을 취합하여 CyberMiles 미들웨어 스택과 관련하여 구체적인 기술적 결정을 내릴 것입니다.

3.1 규칙 엔진

CyberMiles 시스템은 자체 블록체인 검증자 소프트웨어에 순방향 추론 규칙엔진을 내장시킬 예정입니다. 이 규칙엔진 자체는 블록체인의 외부에 위치하지만 "스마트 비즈니스 계약"을 실행하기 위해 검증자에 의해 사용됩니다.

이 규칙엔진은 패턴들(비즈니스 행위에서 발생한 사실)을 규칙과 매칭하고 잠재적 충돌을 해결하기 위해 Rete 알고리즘을 실행합니다. Rete 알고리즘은 복잡한 구조를 가지고 있으며 이 백서가 다루는 범위에서 벗어나 있습니다. 저희는 다만 오늘날 많은 기업들이 폭넓게 채용하고 있으며 상당히 수준으로 발달되어 있는 성공적인 Rete 기반

순방향 추론 규칙엔진들이 존재한다는 사실을 강조해 드리고 싶습니다. 이러한 규칙엔진들의 예로는 Drools 와 Jess 가 있습니다.

개념 면에서 보자면 순방향 추론 규칙은 IF 와 THEN 서술문으로 구성된 복잡한 구조의 세트입니다. 이 규칙엔진은 소프트웨어 개발자와 대척점에 있는 비즈니스 분석가들이 비즈니스 규칙을 표현할 수 있도록 해주는 특수한 "프로그래밍 언어"를 제공합니다. 아래의 예제는 가짜 규칙언어로 작성된 규칙세트입니다. 이 예제는 구매자의 프로필에 기반하여 상품의 가격을 결정하는 방법을 보여주고 있습니다. 이 경우에 구매자의 FICO 점수가 740 이 넘는 경우 그는 가격에 대해 80%의 할인을 받게 됩니다.

```
Rule “Pricing”
  dialect “mvel”
  when
    m : Message(status==Message.GET_PRICE)
  then
    when
      m.fico_score > 740
    then
      m.price = m.listed_price * 0.8
End
```

"스마트 비즈니스 계약"은 이제 DApp 로부터의 신호를 받아 규칙을 실행합니다. "구매자 프로필"과 제품의 가격결정에 필요한 데이터가 CyberMiles 플랫폼 상의 분산된 데이터베이스로부터 얻었다는 사실에 주목해 주시기 바랍니다. 이 부분에 대해서는 3.3 장에서 저희가 더욱 심도있게 설명해 드리겠습니다.

```
engine = load_rules(“pricing.rl”);

m = new Message ();
```

```
m.status = Message.GET_PRICE;
m.fico_score = 741; // Get from profile DB
m.listed_price = 100; // Get from product DB

engine.send(m);
return m.price; // Returns 80 to Dapp caller
```

이 예제는 단순하지만 명확하게 설명해 주고 있습니다. "스마트 비즈니스 계약"이 복잡한 규칙을 다루는 방식은 물론 시스템 내의 대부분의 비즈니스 로직을 캡슐화하는 방식에 대해 쉽게 이해할 수 있습니다.

3.2 비즈니스 프로세스 관리자 (BPM)

대부분의 비즈니스 시스템 내에서 규칙들은 특정 조건들이 만족되었을 때만 반사적으로 적용됩니다. 예를 들어 제품가격을 결정하는 규칙은 잠재 구매자가 가격을 요청할 때만 적용됩니다(예를 들어 제품상세 웹페이지의 로딩을 통해). 이처럼 규칙엔진은 "주문에 따라" 기동하며 시스템은 대부분의 시간을 "대기" 상태로 있게 됩니다. 이러한 동작은 유한 상태 머신(FSM)에 의해 모델화될 수 있습니다.

폭넓게 사용되는 FSM 을 실행하는 엔터프라이즈 소프트웨어 제품으로는 "비즈니스 프로세스 관리자(BPM)"가 있습니다. 또한 BPM 은 비즈니스 분석가들이 프로세스를 특정할 수 있도록 자체 선언형 언어를 제공하고 있습니다. 각 상태는 다음 상태를 촉발하는 방식을 결정하는 비즈니스 규칙에 응답할 수 있습니다. 꽤 많은 BPM 언어들이 XML 을 기반으로 이루어져 있습니다. 아래의 예제는 일반적인 전자상거래 시나리오에서 BPM 이 다루게 될 가능성이 있는 상태들의 하위세트의 예시를 보여주고 있습니다.

```
<process-definition name=”purchase process”>

  <start-state name=”request a purchase”>
    <transition to=”evaluate”/>
  </start-state>

  <state name=”evaluate”>
    <!--...-->
    <transition name=”approve” to=”approved”/>
    <transition name=”disapprove” to=”done”/>
  </state>

  <fork name=”approved”>
    <transition to=”decrement inventory” />
    <transition to=”credit seller” />
    <transition to=”deduct from buyer” />
  </fork>

  <state name=”decrement inventory”>
    <!--...-->
    <transition to=”done” />
  </state>

  <state name=”credit seller”>
    <!--...-->
    <transition to=”done” />
  </state>

  <state name=”deduct from buyer”>
    <!--...-->
    <transition to=”done” />
  </state>

  <end-state name=”done” />
</process-definition>
```

이 BPM 스크립트는 변수들을 조정하거나 변수화된 작업을 시작 또는 종료시키거나 심지어 외부 규칙 엔진를 참조할 수 있습니다.

"스마트 비즈니스 계약" 스크립트 내에서의 프로그래밍은 이제 FSM 상태를 체크하는 선언형 서술문들의 집합으로 단순화될 수 있습니다.

```
// pid is the ID of a process
// associated with a shopping session
// It is stored in the distributed DB
if (pid) {
  process = load_process (pid);
} else {
  process = start_process(“purchase.bpm”);
  pid = process.id;
  // Save pid to the DB
}

while (process.next()) {
  if (process.state == “credit seller”) {
// Do the transaction …
  }
  if (process.state==”deduct from buyer”) {
// Do the transaction …
  }
  … …
}
```

폭넓게 사용되는 엔터프라이즈 미들웨어 BPM 솔루션에는 jBPM, Enhydra Shark, OpenSymphony OSWorkflow 등이 있습니다.

3.3 분산된 데이터베이스

규칙엔진과 BPM 모두 효율적으로 동작하기 위해서는 내부 데이터를 데이터베이스에 저장해야 합니다. 비즈니스 어플리케이션의 복잡성이 증가하면서 어플리케이션도 자체적으로 블록체인 내의 거래기록만이 아닌 외부의 데이터를 관리해야 합니다. 이는 모든 블록체인 노드들에 내장되어 있는 데이터베이스를 필요로 합니다. 블록체인 어플리케이션들의 분산되어 있는 특성으로 인해 이 노드는 모든 블록체인 노드들에 걸쳐 복제되고 동기화되어야 합니다.

다행히도 분산된 데이터베이스 기술은 최근 몇년간 상당한 진보를 이루어 내었습니다. 이제 기존의 오픈소스 소프트웨어를 사용하여 인터넷 규모의 분산된 데이터베이스를 구축하는 것이 가능합니다. 그러나 이를 위해서 포기해야 하는 것은 이러한 데이터베이스들은 일반적으로 NoSQL 이며 시스템의 일관적인 동작을 보장할 수 없다는 것입니다. 대신에 이러한 데이터베이스들은 시스템이 단계적으로 잠재적인 충돌들을 해결하는 "결과적 일관성"을 목표로 하고 있습니다. 이러한 데이터베이스들은 블록체인과는 상당히 다르지만 유용한 충돌해결 전략을 채택하고 있습니다.

저희는 CyberMiles 를 위한 기본적인 분산된 데이터베이스로서 인기 있는 Apache Cassandra 를 사용하기로 이미 결정을 내린 상태입니다.

3.4 분산된 파일 시스템

"스마트 비즈니스 계약"은 종종 블록체인과 데이터베이스 기록 외에도 데이터의 파일 또는 블랍들을 관리해야 합니다. 이러한 파일들은 블록체인 상의 모든 노드들에 걸쳐 복제되어야 하는 동시에 접근이 가능해야 합니다. 따라서 분산화된 파일 및 데이터 저장소 시스템이 필요합니다.

CyberMiles 시스템은 이더리움 Swarm 혹은 IPFS 등과 같은 블록체인 친화적 분산된 파일 시스템 기술을 기본 파일 저장소 기능으로서 사용하게 됩니다.

3.5 분산된 웹훅

위에 언급된 것과 같이 이 비즈니스 시스템은 외부의 이벤트에 대해 반응합니다. BPM 은 계약 당사자들(외부 상태를 위한 "오라클")로부터의 입력을 기다립니다. 그리고 다음에 무엇을 할 것인지를 결정하는 규칙을 실행합니다. 일단 다음 상태에 도달한 후에는 다시 입력을 기다립니다. 전자상거래 인프라가 인터넷 상에 위치하고 있으므로 CyberMiles 시스템은 인터넷으로부터 이벤트를 수신할 수 있는 인터페이스를 가지고 있어야 합니다.

이러한 목표를 달성하기 위해서 각 CyberMiles 블록체인 노드는 외부 메시지를 수신하고 BPM 이벤트를 촉발시킬 수 있는 웹서버스를 내장하게 됩니다. 각 "스마트 비즈니스 계약" 어플리케이션은 외부 이벤트를 수신하기 위해 1 개 이상의 웹훅 URL 을 발행할 수 있습니다. 블록체인 상의 활성 노드들은 DNS 시스템 상에서 자체적으로 스스로를 등록시킬 수 있는 것은 물론 모두 들어오는 HTTP 요청을 수신할 수 있습니다.

4. 블록체인

"스마트 비즈니스 계약"은 모든 비즈니스 미들웨어 파트들을 하나로 묶어주는 한편 이것들을 블록체인에 의해 유지되는 거래 출납부와 연결시켜 줍니다. 이 분야를 선도하고 있는 이더리움의 뒤를 이어 CyberMiles 도 블록체인에 추가된 튜링 완전한 가상머신을 구축하고 있습니다. 이 가상머신은 자바 스크립트와 유사한 스크립트 작성 언어(이더리움의 Solidify 프로그래밍 언어와 유사)를 통해 프로그래밍이 가능합니다. 이것은 또한 웹훅 이벤트들을 BPM 프로세스들과 연결하거나 비즈니스 규칙을 로딩하거나 공유된 데이터베이스에 접근하는 등(도표 1 참고)의 작업을 완전히 수행할 수 있습니다.

"스마트 비즈니스 계약"에 있어서 개발자는 어플리케이션 코드, BPM 설정 파일들, 웹훅 설정, 비즈니스 규칙 파일 등을 함께 묶음으로 만들어 단일 보관소 내에 보관해야 합니다. 일단 "스마트 비즈니스 계약"이 채용되면 외부 시스템들은 블록체인 주소를 통해 접근할 수 있습니다. 예를 들어 DApp 은 어플리케이션을 위한 UI 를 구축할 수 있으며 이는 모든 비즈니스 로직을 처리하기 위해 "스마트 비즈니스 계약"을 활용하고 그 결과로 도출된 토큰 거래들을 블록체인 내에 기록되도록 합니다.

4.1 블록체인과 합의

CyberMiles 시스템의 블록체인 레이어에 있어서 저희가 목표로 하는 것은 기존의 시스템을 완전히 새로 만드는 것이 아닌 기존의 블록체인 프레임워크 위에 추가로 구축하는 것입니다. 이 시스템의 근본이 되는 기술에 있어서 저희가 중요하게 생각하는 조건은 다음과 같습니다.

- 커뮤니티에 의해 주도되어야 하며 활발하게 개발되는 오픈소스 프로젝트여야 합니다. 이는 CyberMiles 가 인프라 소프트웨어를 변경하고 소프트웨어가 향후 나아갈 방향에 영향을 주고 커뮤니티 내로 다시 역기여를 할 수 있도록 해줍니다.

- 소프트웨어 아키텍처가 거래에 대한 유효성의 인증을 위해 핵심 블록체인 로직(예를 들어 합의로직)과 어플리케이션 로직 간의 완벽한 분리를 지원해야 합니다. 합의엔진은 체인 상에서 새로운 블록을 제안하고 그에 대해

커밋합니다. 커스텀 어플리케이션들이 "스마트 비즈니스 계약"의 실행을 비롯해 거래들의 유효성을 인증하고 어느 거래가 블록체인 상에 기록되어야 하는지를 결정합니다. CyberMiles 가상머신과 "스마트 비즈니스 계약"을 위한 전체 소프트웨어 스택이 블록체인 상의 커스텀 어플리케이션으로서 만들어 집니다.

- 블록체인 합의엔진은 수백만명의 사용자를 가진 일반소비자용 품질등급의 어플리케이션으로서 입증된 확장능력을 가지고 있어야 합니다. 이더리움 확장성에 있어서 이미 그 능력을 인정받고 있는 주요 솔루션들 중 하나가 채택되는 것이 가장 이상적일 것입니다. 다시 말해 공학적 발달 정도에 있어서 시장을 선도하는 위치에 있어야 합니다.

CyberMiles 팀은 기존의 블록체인 인프라 솔루션들을 비교하는 연구에 상당한 노력을 기울여 왔습니다. 저희는 Tendermint/Cosmos 플랫폼 상에서 CyberMiles 블록체인의 첫번째 버전을 구축하는 것으로 잠정적인 결론을 내었습니다. 도표 2 는 CyberMiles 블록체인 상의 각 검증자 노드에 대해 제안된 소프트웨어 아키텍처의 예시를 보여주고 있습니다. 실제로 CyberMiles 는 이미 Tendermint/Cosmos 플랫폼에 관련하여 기술적으로 기여하고 있습니다.

- Tendermint 프로젝트는 Byzantine 결함허용(BFT) 합의엔진을 만듭니다. 본 프로젝트는 매우 활발하고 상당한 자금을 제공받고 있는 오픈소스

프로젝트(성공적인 자체 ICO 후)입니다. 블록체인 자체적으로 1/3 의 노드 실패(충돌 또는 전복)까지 견딜 수 있습니다. DPoS(위임된 지분증명)의 환경에서는 개별 검증자들이 네트워크의 전복을 방지하는 것에 대해 강력한 인센티브를 가지고 있으므로 Byzantine 실패가 매우 드물게 발생되게 됩니다.

- Tendermint 는 현대적인 모듈 방식의 아키텍처를 가지고 있습니다. 합의엔진은 다른 종류의 블록체인들에 대해 독립적으로 결합될 수 있습니다. 예들 들어 이더리움 프로젝트는 이더리움의 규모를 확장하기 위해 Tendermint 합의엔진을 사용합니다. ABCI(어플리케이션 블록체인 인터페이스)는 CyberMiles 가 자체 가상 머신과 어플리케이션을 개발할 수 있도록 해주는 간단하고 깔끔한 어플리케이션 로직이라고 할 수 있습니다. 새로운 거래가 들어오면 블록체인이 그것을 ABCI 를 통해 CyberMiles 어플리케이션으로 넘겨줍니다. 일단 관련된 "스마트 비즈니스 계약"이 실행되고 거래가 CyberMiles 어플리케이션에 의해 그 유효성이 인증되면 기록보관을 위해 블록체인 합의엔진으로 다시 넘겨집니다.

- Tendermint 는 DPoS(위임된 지분증명)에 기반한 고성능 블록체인 시스템입니다. 이 시스템은 이더리움의 확장성 솔루션 중 하나로서 이더리움이 정식으로 후원하고 있습니다. 테스트 시에 이 시스템은 초당 10,000 회의 거래를 안정적으로 지원할 수 있기 때문에 가장 진보된 공학적 솔루션 중 하나로 여겨지고 있습니다.

시스템의 근본이 되는 Tendermint DPoS 메커니즘으로 인해 CyberMiles 블록체인은 10 초 미만의 블록 생성시간을 가지게 되며 일단 블록이 커밋되면 블록의 거래들은 즉시 확정됩니다.

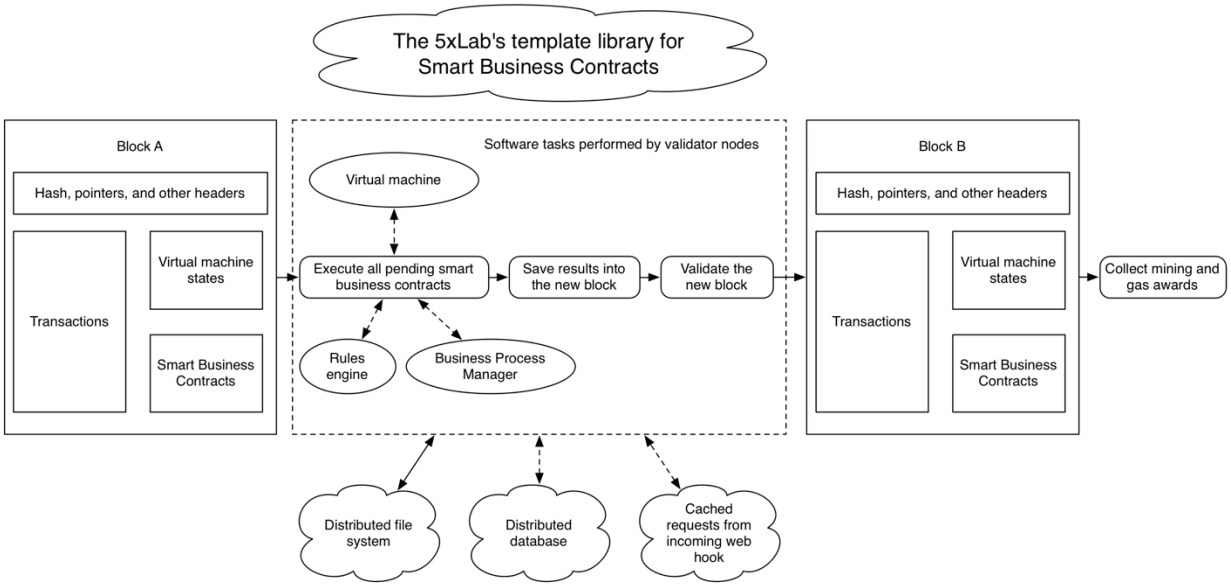

도표 2. CyberMiles 블록체인 검증자가 수행하는 작업을 보여주고 있습니다.

4.2 암호화 토큰

CyberMiles 블록체인은 CyberMiles 토큰(CMT)이라고 불리는 네이티브 암호화 토큰을 만들고 기록합니다. CMT 의 용도는 2 가지가 있습니다. 커뮤니티 구성원들에게 그들이 제공한 서비스에 대해 보상해주는 것과 네트워크 상의 금전적 거래가 더욱 용이하게 것입니다. 정산된 각 거래로부터 획득한 "수수료"가 해당 거래를 가능하도록 해주는 서비스를 제공한 검증자들에게 지불하는 데 사용되므로 이 2 가지 용도는 서로

관련되어 있습니다. 그럼, 이 2 가지 사례들에 대해 더욱 자세히 알아봅시다. 일 네트워크 참가자들은 서비스의 제공을 통해 CMT 를 획득할 수 있습니다.

- 이들은 네트웨크에 서비스를 제공하는 검증자가 될 수 있습니다. 좀 더 구체적으로 말하자면 참가자들은 CMT(DApp 에 의해 지불된 GAS)의 획득을 위해 DApp(5miles 앱 등과 같은)을 위해 "스마트 비즈니스 계약"을 실행합니다. 또는 블록체인 상의 새로운 거래들에 대해 유효성을 인증하고 그것들을 기록하고 DPoS 합의 프로토콜로부터 CMT 를 획득할 수 있습니다.

- 이들은 네트워크 상에서 다른 개인들에게 서비스를 제공할 수 있습니다. 네트워크 상의 소비자들과 기업들은 서로 분쟁해결을 위한 조정 서비스는 물론 심지어 "스마트 비즈니스 계약"을 위한 개발 서비스 등에 대한 지불을 위해 CMT 를 사용할 수 있습니다.

참고: CMT 는 1 개의 GAS 의 전환된 가치가 안정적으로 유지될 수 있도록 동적 환율을 통해 GAS 로 전환됩니다. 그 후 GAS 는 "스마트 비즈니스 계약"을 실행하는 CyberMiles 에 대한 지불을 위해 사용됩니다. "스마트 비즈니스 계약"의 GAS 가격은 "스마트 비즈니스 계약"이 블록체인에 제출될 때 시스템에 의해 추산됩니다.

또한 CMT 는 CyberMiles 네트워크 어플리케이션 상에서 내부 정산화폐로서 사용될 수 있습니다. 예를 들어 중소기업 대출 어플리케이션(5 장 참고)이 기밀성, 투명성, 자금안전성 등을 확보하기 위해 중앙집중식 어음교환소의 개입 없이 CMT 를 이용해

대출금을 정산하거나 상환할 수 있습니다. 공급망 관리 어플리케이션은 CMT 를 이용해 도중에 발생되는 거래를 정산하고 하루를 마감할 때의 정산에 대해서만 명목화폐로의 전환을 허용할 수 있습니다. 이것은 거래 상의 불편과 비용을 감소시켜 줍니다. 이 2 경우 모두 네트워크는 해당 거래와 관련된 "스마트 비즈니스 계약"을 실행하는 검증자들에게 지불하기 위해 각 정산거래에 대해 소정의 수수료를 수취합니다.

CMT 의 이 2 가지 활용사례는 블록체인 기술 커뮤니티 내에서 상당히 좋은 평을 받고 있습니다. 저희는 현재 새로운 CyberMiles 블록체인 인프라를 구축하고 있기 때문에 새로운 블록체인의 네이티브 기능들에 대해 ETH 또는 BTC 를 그대로 사용할 수 없으므로 CMT 가 필요합니다. CMT 는 오늘날 존재하는 몇몇 인기 토큰들에 비유될 수 있습니다.

XRP 와의 비교

Ripple 네트워크와 같이 CyberMiles 네트워크는 거래의 분산화된 정산을 더욱 용이하게 만들기 위해 자체적으로 네이티브 암호화 화폐를 상용합니다.

Ripple 은 각 거래에 대하여 소액의 XRP 를 "연소"시키지만 CyberMiles 는 해당 거래와 연계된 "스마트 비즈니스 계약"을 실행하는 검증자에게 지불하기 위해 거래 수수료를 수취합니다.

ETH 와의 비교

이더리움 네트워크와 유사하게 CyberMiles 네트워크는 새로운 블록을 만들고 블록 내에서 "스마트 계약"을 실행하는 검증자들에게 보상을 제공합니다(GAS 수수료의 형식으로).

그러나 현 세대의 이더리움은 매우 느리며 이 때문에 복잡한 스마트 계약을 실행하는 비용은 상상할 수 없을 정도로 비쌉니다. CryptoMiles 는 복잡한 "스마트 비즈니스 계약"의 실행할 수 있도록 높은 성능과 확장성을 가지도록 설계되었습니다. 이와 더불어 이더리움은 일반적인 용도의 연산 네트워크가 되는 것을 목표로 하고 있는 반면 CyberMiles "스마트 비즈니스 계약"은 전자상거래 거래에 특화되어 있습니다.

4.3 네트워크 효과 촉발시키기

CyberMiles 네트워크가 시작되기 위해서는 네트워크 효과를 달성하고 기업 및 채굴자들이 네트워크에 참여할 수 있도록 충분한 가치를 제공하는 것이 필수적입니다. ICO 의 목적 중 하나는 네트워크 효과를 촉발시키기 위한 자원을 제공하는 것입니다. 저희는 CyberMiles ICO 를 통해 다음과 같은 목표들을 달성하고자 합니다.

첫째, 개발팀은 미국에서 가장 큰 전자상거래 웹사이트 중 하나를 운용해 본 5miles 의 가치 있는 경험으로부터 얻은 지식을 최대한 활용하여 "스마트 비즈니스 계약" 템플릿을 구축하려고 합니다. 5miles 에는 20 개의 주요 카테고리별로 나뉘어진 수천개의 계약 템플릿들이 있습니다. 이 템플릿들은 실제 사용 중인 어플리케이션들을 통해 테스트가 완료되었으며 바로 재사용할 수 있습니다. 더욱이 본 시스템은 써드파티 이용자들에 의해 개발된 "스마트 비즈니스 계약" 템플릿을 판매할 수 있는 어플리케이션이자 그 자체로 블록체인 상의 DApp 중 하나인 "스토어"를 운영하고 있습니다. 템플릿들은 CMT 또는 GAS 단위로 가격이 결정되어 있습니다.

둘째, 5miles 는 현재 보유하고 있는 1 천만명의 미국 기반 이용자들과 중소기업들 간의 중소기업 대출을 지원하는 새로운 어플리케이션을 만들 예정입니다. 이

어플리케이션 분산화된 신분 및 신용 정보 관리와 분산화된 대출/정산 기능을 지원할 것입니다(중앙집중식 어음교환소의 개입 없이). 이 프로젝트는 장기적으로 1 천만명의 미국인 이용자들의 신분정보 및 신용기록을 CyberMiles 블록체인으로 이동시키게 됩니다. 이 어플리케이션은 다른 개발자들에 의한 CyberMiles 상의 이용자들의 신분정보 및 신용기록의 활용은 물론 소비자 대상 어플리케이션의 자체적인 구축에 대한 청사진을 제공해 준다고 할 수 있습니다. CyberMiles 네트워크는 CMT 를 정산화폐로 활용함으로써 대출조건 관련 "스마트 비즈니스 계약"의 실행에 대해 검증자들에게 지불할 소정의 수수료를 수취할 수 있습니다. CyberMiles 상에서 구축되는 어플리케이션들이 많아질수록 CMT GAS 의 소비도 증가하게 됩니다.

마지막으로 5miles 는 현재 보유 중인 플래그십 C2C(소비자 대 소비자) 전자상거래 어플리케이션을 CyberMiles 블록체인으로 마이그레이션시킬 예정입니다. 이는 5miles 에 의해 관리되는 DApp 중 하나로서 CyberMiles 상의 "스마트 비즈니스 계약"에 의해 지원될 예정입니다. 이 조치는 장기적으로 3 억달러 상당의 거래를 CyberMiles 플랫폼으로 이동시킬 수 있습니다. 결과적으로 5miles 자체가 "스마트 비즈니스 계약" 운용에 대한 GAS 비용을 지불하기 위해 상당한 액수의 CMT 를 구매하고 소비하게 될 것입니다.

5. 어플리케이션들

CyberMiles 블록체인 플랫폼은 비즈니스 거래 어플리케이션을 위한 미들웨어 운용을 주요 기능으로서 지원합니다. 이에 따라 대부분의 경우에 이용자 대상 어플리케이션의 UI 를 받쳐주는 역할을 하게 됩니다. 그러나 분산화된 블록체인 고유의 특성으로 인해 이 플랫폼의 "스마트 비즈니스 계약"은 장기적으로 중앙집중식 전자상거래가 운용되었을

때 불가능하다고 여겨졌던 새로운 기능 및 어플리케이션들을 가능케 해줄 것으로 기대하고 있습니다.

5.1 분산화 신분정보 관리 플랫폼

Equifax 해킹 사건이 시사하듯이 (2017 년 1 억명이 넘는 미국인들의 신분정보 및 신용기록이 도난당했습니다) 중앙집중식 신분정보 관리는 소비자들에게는 상당한 리스크를 이러한 데이터를 보유하고 있는 기업들에게는 상당한 책임을 발생시킵니다. 이 문제를 해결하기 위해서는 신분정보 관리에 대한 완전한 패러다임의 전환이 필요합니다. 가장 명확한 솔루션 중 하나는 이용자에게 자신의 개인정보에 대한 완전한 통제권을 부여하는 것입니다. 이용자는 자신의 데이터에 접근할 수 있는 사람에 대해 개별적으로 결정할 수 있어야 합니다. 데이터에 대한 접근가능 시기, 접근가능 시간의 정도, 허용되는 용도가 모두 이용자에 의해 승인되어야 합니다. 이 경우 공격의 대상이 되는 개인정보의 중앙집중식 저장소가 존재하지 않게 됩니다. 그러나 블록체인 기반의 "스마트 비즈니스 계약" 없이 이러한 시스템을 운용하는 것은 매우 어렵습니다.

블록체인 네트워크들은 암호 키를 통해 신분정보를 관리합니다. 비트코인 또는 이더리움 상의 이용자의 "지갑"은 분산되어 있으며 비공개 키를 통해 이용자에 의해 완전히 통제됩니다. 저희는 "스마트 비즈니스 계약"을 이용해 "지갑"의 개념을 암호화 토큰의 안전한 저장소의 역할뿐이 아닌 임의적인 개인정보의 저장소의 역할을 겸하는 것으로 확장할 수 있습니다. 암호화 화폐 지갑의 경우와 유사하게 네트워크 상에서는 많은 "개인정보지갑"들이 존재할 수 있습니다. 이용자의 요청(이용자의 비공개 키에 의해 서명된 거래)에 따라 지갑은 써드파티 어플리케이션이 OAUTH 프로토콜을 통해

데이터에 임시로 접근할 수 있도록 허가를 해줄 수 있습니다. 이용자는 오늘날 암호화 화폐 지갑이 이용되듯이 다양한 목적을 위해 다양한 지갑을 사용할 수 있습니다.

아래의 워크플로우와 도표 3 은 개인정보를 위한 "온라인 지갑"이 기능하는 방식을 예시로 보여주고 있습니다. 이 특수한 "지갑"은 이용자의 개인적인 금융 관련 정보를 저장합니다. 그리고 이용자는 CyberMiles 상의 금융 어플리케이션이 이것을 활용할 수 있도록 허가해 줄 수 있습니다. 한 가지 예로 5.2 장에 예시로 나와 있는 개인 대 개인 중소기업 대출 어플리케이션을 들 수 있습니다.

1. 이용자는 자신이 신뢰하는 "지갑" 앱을 선택합니다.
2. 이용자는 지갑을 통해 개인정보 및 금융 관련 정보를 등록합니다.
3. 지갑은 정부가 요구하는 자금세탁 방지 확인를 위한 AML/KYC 유효성 인증을 합니다.
4. 지갑은 공개/비공개 키 조합을 생성하고 기록을 위해 공개 키를 블록체인에 공표합니다.
5. 지갑은 금융 관련 링크를 허가하고 테스트합니다.

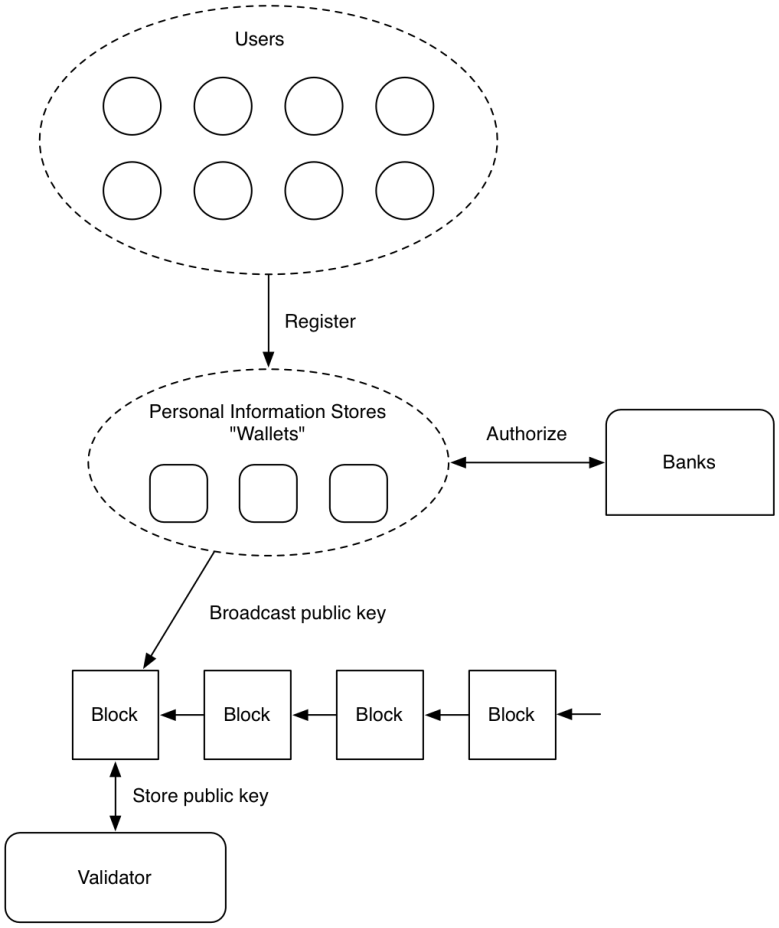

도표 3. CyberMiles 상의 분산화된 신분정보 관리 플랫폼

5.2 개인 대 개인 중소기업 대출 거래소

CyberMiles 블록체인 상에서 구축될 수 있는 어플리케이션 중 또 다른 예로는 개인 대 개인 중소기업 대출 거래소입니다. 5.1 장에 설명되어 있듯이 저희는 CyberMiles 상에서 분산화된 신분정보 관리 플랫폼을 구축할 것입니다. 이렇게 되면 공개 키를 통해 신분이 특정된 각 이용자에 대한 신용기록정보를 기록할 수 있습니다.

저희는 신분정보 및 신용기록을 통해 블록체인 상에서 대출 매칭 엔진(대출 "거래소")을 구축할 수 있습니다. 일단 대출조건이 일치하면 "스마트 비즈니스 계약"이

중앙집중식 어음교환소의 개입 없이 CMT 를 통해 각 당사자의 은행계좌로부터 자동으로 대출을 정산합니다. 아래의 워크플로우와 도표 4 가 대출을 매칭하고 정산하는 방식에 대한 예시를 보여주고 있습니다.

1. 이용자는 자신의 지갑으로부터 OAUTH 를 통해 거래소로 로그인합니다. 거래소는 개인정보를 캐싱하지만 저장하지는 않습니다.
2. 이용자는 자신이 원하는 대출조건을 제출합니다(대출하기 또는 대출받기, 대출기간, 이자).
3. 거래소는 매칭된 결과를 제안합니다.
4. 거래소는 매칭된 예비거래자들에 대한 상세한 신용 관련 점수 및 기록을 제공합니다.
5. 이용자가 특정 예비거래자를 선택하면 두 당사자는 합의해야 합니다.
6. 대출계약이 거래소에 의해 블록체인에 기록됩니다.
7. 거래소는 지갑들에 두 당사자들의 은행계좌들을 통한 정산을 요청합니다.

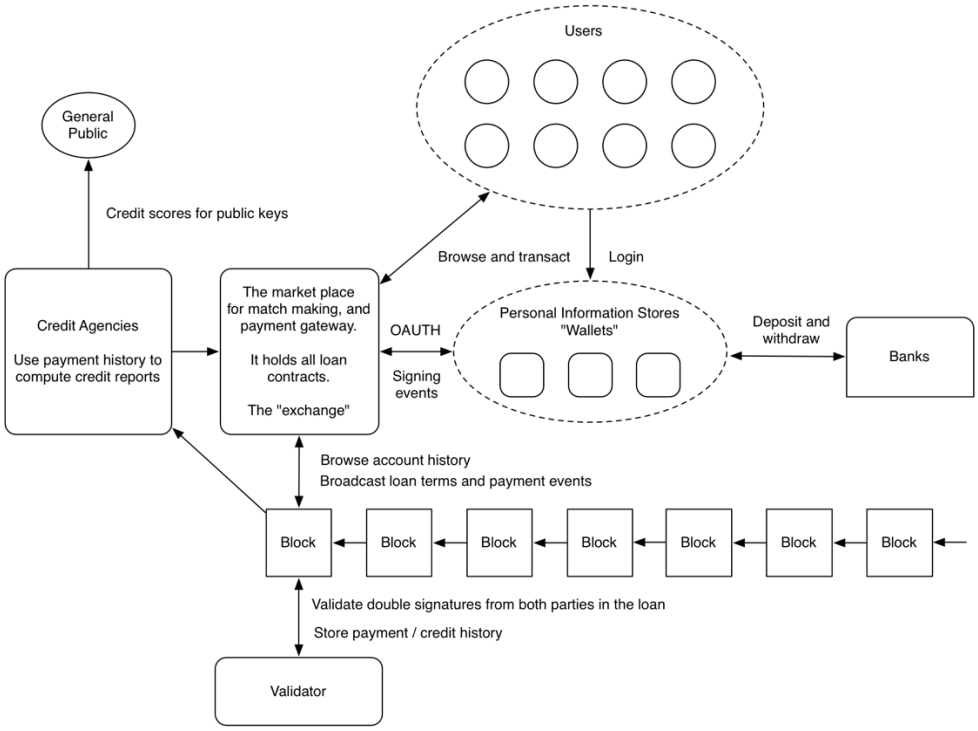

도표 4. 분산화된 대출의 매칭과 정산.

대출기간 중 지불시기가 되면 "스마트 비즈니스 계약"이 다음을 자동으로 수행합니다.

1. 거래소는 두 당사자의 지갑들에 그들의 은행계좌를 통해 결제금액을 정산해줄 것을 요청합니다.
2. 거래결과가 블록체인으로 공표되며 신용기록의 일부가 됩니다.

5.3 공급망 현금유동성

CyberMiles 블록체인의 가상토큰(CMT)은 주로 네트워크로의 접근에 대한 보상에 사용됩니다(예를 들어 기업들은 자체 "스마트 비즈니스 계약"을 실행하고 블록체인 네트워크의 유효성의 인증을 위해 지불합니다). 또한 이것은 최종 소비자 및 판매자들을 비롯한 공급망 관계자들의 네트워크 내 정산 수단 중 하나로서 사용될 수도 있습니다.

CMT 는 디지털 토큰이므로 그 정산은 즉각적으로 무료로 안전하게 처리됩니다. "거래의 흐름"이 상품의 이동과 동시에 이루어질 수 있으므로 CMT 는 매우 효율적인 공급망 관리를 가능케 해줍니다. 당사자들은 네트워크 상의 거래소들을 통해 정기적으로 자신의 CMT 잔고를 다른 자산으로 전환하기만 하면 됩니다.

5.4 인증된 상품들

블록체인의 주요 특성들 중 하나는 불변성을 가진 안전한 디지털 기록을 저장할 수 있는 능력입니다. 이 특성은 전세계 전자상거래 업계의 가장 해결하기 어려운 문제 중 하나인 위조상품 문제를 해결하는 데 도움을 줄 수 있습니다.

"스마트 비즈니스 계약"은 상품 제조자/생산자가 제조하는 각 상품에 대한 정품인증서를 작성하는 데 사용될 수 있습니다(예를 들어 공장의 생산시스템과 CyberMiles 비즈니스 계약 간의 API 연결을 통해). 그 후 이러한 인증서는 상품이 판매자로부터 구매자로 공급망을 통해 움직이는 과정에서 투명하게 추적될 수 있습니다.

5.5 커뮤니티 기반 분쟁해결

중앙집중식 전자상거래 기업은 구매자와 판매자 간의 분쟁의 해결하기 위해서 고객서비스 담당자들을 고용해야 합니다. CyberMiles 블록체인 위에 추가로 DApp 을

구축하는 전자상거래 회사도 분명히 같은 방식으로 운영될 수 있습니다. 그러나 분산화된 플랫폼으로서 CyberMiles 는 또 다른 설득력 있는 솔루션을 제공합니다.

CyberMiles 커뮤니티 이용자들은 CMT 를 댓가로 받고 중재자로서의 역할을 자발적으로 수행할 수 있습니다. 거래의 주요 절차들은 블록체인 상에 기록되기 때문에 "스마트 비즈니스 계약"을 활용하면 판매자 및 구매자 모두의 허락을 받아 중재자가 이러한 기록이 있는 곳을 찾을 수 있는 메커니즘을 개발할 수 있습니다. "스마트 비즈니스 계약"은 합의의 도출을 기다리는 동안 판매자와 구매자로부터 CMT 로 금액을 받아 에스크로 계정으로서의 역할을 할 것을 서약할 수 있습니다. 중재자가 분쟁을 해결하고 양쪽 당사자 모두 만족하면 맡겨진 액수가 분쟁에서 "승리한" 당사자에게 지급되며 중재자는 일정 퍼센티지의 배분을 받게 됩니다.

용어해설

CyberMiles 블록체인: 비즈니스 거래에 최적화된 새로운 분산화된 블록체인 프로토콜.

"스마트 비즈니스 계약": CyberMiles 블록체인 상에서 실행가능한 비즈니스 어플리케이션.

CyberMiles 토큰 (CMT): 블록체인을 유지하는 것은 물론 스마트 비즈니스 계약을 실행하는 CyberMiles 블록체인 노드들을 호스팅하는 사람들에 대한 보상을 위해 사용되는 암호화 화폐/토큰. 네트워크 상에서 실행될 "스마트 비즈니스 계약"을 제출하는 기업 및 계약당사자들은 계약의 복잡성의 정도에 상응하는 액수의 CMT 를 지불해야 합니다.

CyberMiles 검증자: "스마트 비즈니스 계약" 실행을 포함한 CyberMiles 블록체인 인프라를 유지하기 위한 연산능력을 기여하는 사람 또는 업체. 이 사람이 전세계 어디에 있든지 관계없으며 이 사람은 5miles 와는 제휴를 맺지 않았을 수도 있습니다. 이 사람은 보상(네트워크를 유지하려고 노력한 결과로서 얻게되는 CMT)이라는 인센티브를 받습니다.

CyberMiles 어플리케이션: 어느 기업이나 CyberMiles 블록체인 상에서 어플리케이션을 구축하고 사용할 수 있습니다. 기업은 네트워크 상에서 실행될 "스마트 비즈니스 계약" 세트를 제출합니다. 기업은 접근을 위해 네트워크에 지불할 CMT 를 구매하여야 하며 내부 자금거래를 정산하거나 더욱 용이하게 하기 위해 CMT 를 사용할 수 있습니다.

최종 사용자: CyberMiles 에 대해서 전혀 알지 못해도 상관없는 5miles 어플리케이션 상의 구매자 및 판매자. "스마트 비즈니스 계약"은 거래의 직전과 직후 그들의 자금의 미국 달러와 CMT 간의 환전을 담당합니다.

5miles: 5Miles LLC 에 의해 개발된 C2C(소비자 대 소비자) 전자상거래 거래소 어플리케이션. 5miles 는 연환산 추산 거래액 30 억달러의 상당의 1 천만명이 넘는 미국의 고객들을 보유하고 있습니다.

감사의 말

5xlab 은 이 백서에 기여해 주신 Michael Yuan 박사와 Lucas Lu 박사님께 감사의 말을 전합니다.

참고문헌

[1] Nakamoto, S. 비트코인: 개인 대 개인 전자캐쉬 시스템. https://bitcoin.org/bitcoin.pdf 2008.

[2] 이더리움 팀. 차세대 스마트 계약 및 분산화된 어플리케이션 플랫폼. https://github.com/ethereum/wiki/wiki/White-Paper 2014

[3] Kwon, J. Tendermint: 채굴없는 합의. https://tendermint.com/static/docs/tendermint.pdf 2014.

[4] Popov, S. IOTA: 혼란. https://iota.org/IOTA_Whitepaper.pdf 2016.

[5] Zamfir, V. "친절한 유령" 캐스퍼를 소개합니다. https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/ 2015.

[6] Kwon, J and Buchman, E. Cosmos: 분산된 출납부 네트워크. https://cosmos.network/whitepaper 2016.

[7] Wood, G. Polkadot: 이기종 다중체인 프레임워크의 장래성. https://github.com/polkadot-io/polkadot-white-paper 2016.

[8] Poon, J., Dryja, T. 비트코인 Lightning Network:
확장가능한 체인 외부 즉시 결제. https://lightning.network/lightning-network-paper.pdf 2016.

[9] Poon, J., Buterin, V. Plasma: 확장가능한 자율적 스마트 계약.
http://plasma.io/plasma.pdf 2017.

[10] Teutsch, J., Reitwiebner, C. 블록체인을 위한 확장가능한 인증 솔루션.
http://bit.ly/2vIConl 2017.

[11] Forgy, C. Rete: 다패턴/다대상패턴 매칭 문제를 위한 빠른 알고리즘. 인공지능. 19: 17–37. 1982.

[12] Oracle. 자바 엔터프라이즈 에디션 플랫폼.
https://www.oracle.com/java/technologies/java-ee.html

[13] Redhat. Drools 비즈니스 규칙관리 시스템. http://drools.org/

[14] Sandia 국립연구소. Jess, 자바 플랫폼용 규칙 엔진. http://www.jessrules.com/

[15] Redhat. jBPM, 유동적 비즈니스 프로세스 관리 스위트. http://www.jbpm.org/

[16] Lazo, D. OS 워크플로우. http://shop.oreilly.com/product/9781847191526.do 2007

[17] DataStax. Apache Cassandra 데이터베이스. http://cassandra.apache.org/

[18] 이더리움 팀. Swarm, 개인 대 개인 저장소 및 컨텐츠 분산에 인센티브를 지급하는 무서버 호스팅. http://swarm-gateways.net/bzz:/theswarm.eth

[19] Benet, J. IPFS - 컨텐츠 주소화 및 버전관리가 된 P2P 파일 시스템.

[20] Protocol Labs. Filecoin: 분산화된 저장소 네트워크. http://filecoin.io/filecoin.pdf 2017.

[21] Civic Team. Civic 백서. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf
2017

[22] Thomas, S., Schwartz, E. 출납부를 초월한 결제를 위한 프로토콜.
https://interledger.org/interledger.pdf 2015