AERGO 백서

기업 자율화 Autonomous Business 를 위한 블록체인 플랫폼

최신 업데이트: 2018 년 10 월 1 일, AERGO

초록

블록체인은 기존 데이터베이스가 가진 고질적인 단일 장애점(Point of failure)등의 보안 문제점을 뛰어넘기 위해 암호화 디지털 거래 장부라는 개념을 최초로 도입해 탄생한 기술입니다. 블록체인 기술을 기반으로 한 상품이나 서비스는 금융 서비스나 제조, 유통, 보험, 보건, 정부, 사물인터넷 등 다양한 업계에서 비지니스 모델을 혁신적으로 변화시킬 수 있는 무한한 가능성을 가지고 있습니다. 특히, 블록체인 기술은 기업들에게 가장 중요한 세 가지 특성을 제공하는 것을 목표로 합니다.

보안(Security) - 투명성(Transparency) - 신뢰(Trust)

이러한 특성은 고차원적인 암호화를 통해 데이터가 안전하게 배포되고 저장되는 P2P(peer-to-peer) 분산형 컴퓨터 네트워크를 통해 확보됩니다. 전(☒) UBS 최고운영책임자(COO)는 블록체인 기술을 두고 다음과 같이 말하기도 했습니다. *"블록체인은 향후 20 년간 우리 삶에 엄청난 영향을 미칠 수 있는 혁신 기술입니다. 지난 20 년간 인터넷이 그래왔던 것 처럼 말입니다."*[1]

블록체인 기술의 장점이 주목받으면서 많은 블록체인이 실제로 구현되기도 했습니다. 대부분 누구나 쉽게 참여 가능한 분산형 컴퓨터 네트워크를 기반으로 하며, 이러한 비허가형(Permissionless) 구조는 흔히 '퍼블릭 블록체인 프로토콜'이라고 불리기도 합니다. 대표적으로 비트코인이나 이더리움을 꼽을 수 있습니다. 하지만 기업들이 현재 구현된 블록체인 프로토콜을 실무에 도입하기 위해선 다양한 문제점을 먼저 해결해야 합니다. 이들 프로토콜의 기능과 개발을 직접 통제하기가 불가능에 가깝기 때문입니다. 허가형(Permissioned) 블록체인 역시 기업 맞춤형(Fit-for-Purpose) 프로토콜을 추구하지만, 관련 인프라 구축에 엄청난 비용이 수반된다는 점과 오픈소스 프로젝트에 비해 개발 속도가 뒤처진다는 문제점을 안고 있습니다.

퍼블릭이나 프라이빗 블록체인을 활용한 대다수 프로젝트는 아직까지도 개발 초기 단계이며, 1 세대 비트코인과 2 세대 이더리움을 넘어 현재는 3 세대 기술이 적용되고 있습니다. 하지만 주로 특정 시장이나 업계에 중점을 두어 개발되기 때문에 단순한 개념증명(PoC) 수준에 머무는 경우가 대부분입니다. 이렇듯 많은 프로젝트가 진행됨에도 블록체인 기술 혁명은 지지부진합니다. 기존 IT 시스템과의 통합이 어렵다는 점과 개발자 친화적인 개발툴이 적다는 것이 주된 이유입니다. 지금껏 선보인 블록체인 적용 사례들 역시 실제 비지니즈 어플리케이션 운영에 필수적인 엔터프라이즈급 성능을 충족시키지 못한 경우가 대부분입니다. 블록체인 기술의 상용화를 위해선 핵심 기술의 발전과 기술 진입 장벽을 낮춰야 하며, 다양한 서드파티 서비스 역시 필요합니다.

기존 기업용 IT 시스템과의 호환성을 지원하고, 개발자 친화적이며, 풍부한 서드파티 생태계를 먼저 구축하는 프로토콜은 블록체인 네트워크와 "서버리스(Serverless) 유틸리티 컴퓨팅"의 핵심 프로토콜로 거듭날 수 있을 것이라고 생각합니다. 마치 TCP/IP 가 핵심 프로토콜로서 인터넷 네트워크의 발전을 견인해 온 것처럼 말입니다.

AERGO 는 고차원적인 기술을 활용하는 IT 플랫폼과 결합된, 기업용(Enterprise-ready) 4 세대 블록체인 프로토콜입니다. 분산형 어플리케이션과 보안 클라우드 서비스 제공자를 포괄하는 생태계 구축을 목표로 합니다. 진정한 개방형, 분산형 시스템 구축을 위해 AERGO 의 핵심 기술은 오픈 소스로 제공될 예정입니다.

AERGO 는 이러한 생태계를 만들어 갈 **개발자**들과 **다양한 기업들, IT 서비스 공급자**들을 위한 플랫폼입니다.

[1] Alex Batlin, et al.(2016). *Building the trust engine*. Available: https://www.ubs.com/microsites/blockchain-report/en/home.html

기업이나 개발자는 AERGO 플랫폼을 통해 클라우드 위에서 독자적인 블록체인 어플리케이션을 손쉽게 설계하고, 구축하며, 배포할 수 있게 됩니다. AERGO 는 다양한 개발 환경에 따른 각각의 요구사항에 맞춰 퍼블릭과 프라이빗을 넘나들며 블록체인 네트워크/어플리케이션을 개발할 수 있도록 새로운 가능성을 제공합니다.

기업과 개발자가 두 가지 블록체인 구조의 서로 다른 특장점을 고려해 목적에 맞는 구조를 선택할 수 있도록 함으로써 블록체인 어플리케이션 설계에 필요한 높은 유연성을 확보할 수 있습니다. 또한, 안전한 클라우드 기반 분산 네트워크를 통해 모든 리소스를 제공해 블록체인 어플리케이션 운영을 위한 물리적 인프라를 직접 구축해야 하는 필요성을 없애 업체들이 부담해야 하는 간접비를 상당 수준 줄일 수도 있습니다.

AERGO 의 핵심 기술은 블록체인 기술 및 엔터프라이즈 IT 통합 서비스 제공사인 블로코의 코인스택(COINSTACK)[2]을 기반으로 하고 있습니다. 코인스택 기반의 블록체인 시스템은 한국과 영국, 홍콩에서 20 개 이상의 실사용 사례에서 활용되고 있으며, 2500 만 명이 넘는 사용자들이 이용하고 있습니다.

현재 블로코는 AERGO 의 핵심 기술을 개발하고 있으며, 블록체인 기반 신규 비지니스 서비스를 기획하는 기업 고객을 대상으로 포괄적인 IT 통합/지원 서비스를 제안하고 있습니다. 제안된 신규 기술에는 고성능, 고효율 블록체인 프로토콜과 강력한 SQL 기반 스마트 컨트랙트 엔진, 발전된 IT 통합 API, 접근성 높은 개발도구 등이 포함되어 있습니다. 이러한 기술 지원은 분산형 어플리케이션 통합 및 적용(Orchestration and deployment) 프레임워크를 통해 이루어지며, 기업과 개발자는 복잡한 과정없이 설치-관리-운영을 통해 바로 사용할 수 있게 됩니다.

AERGO 는 블록체인 기술 대중화 시대를 열어 기업 블록체인 시장을 진일보시키고자 합니다. 기업은 새로운 서비스의 설치, 관리, 운영에 집중하며, 퍼블릭과 프라이빗 블록체인의 이점을 모두 누릴 수 있는 그런 시대를 열고자 합니다.

다시 말해,

1. 기업 및 개발자를 위한 사용자 친화적이면서도 편리한 고차원적 기술과,

2. 안전하고 속도 빠른 기업용 퍼블릭/프라이빗 블록체인 클라우드 아키텍처를 제공하며,

3. 기업과 서드파티를 연결하고 협력을 가능하게 하는 개방형 생태계를 구축하는 것,

기업 자율화를 위한 블록체인 플랫폼 AERGO 의 목표입니다.

[2] A 3rd generation blockchain platform(including developer tools, blockchain operating system, integration APIs) www.blocko.io

면책 조항

본 백서 및 이와 관련해 배포된 기타 문서들의 경우 AERGO 의 개발 및 활용과 관련이 있습니다. 이들 자료는 정보 제공만을 목적으로 하며 향후 그 내용이 변경될 수 있습니다.

본 백서는 향후 진행될 프로젝트에 대한 설명입니다.

본 백서에는 프로젝트를 위한 지속적 지원의 일환으로, 본 백서를 작성한 블로코의 신념을 바탕으로 한 미래 예측이 포함되어 있습니다.

본 백서에 언급된 AERGO 는 현재 개발 진행 중인 프로젝트로, 주요 거버넌스 및 기술적 기능을 비롯해 다양한 내용들이 지속적으로 업데이트되고 있습니다. AERGO 토큰은 본 백서에 명시된 목표 달성이나 성과로 이어지지 않을 수도 있는 실험적 플랫폼(소프트웨어)과 관련 기술의 개발 및 활용에 기반합니다.

AERGO 가 완성될 경우, 본 백서에 명시된 네트워크와는 상당히 차이가 있을 수도 있습니다. 모든 계획, 향후 예상 또는 전망의 달성이나 합리성과 관련해 어떠한 보증도 하지 않으며, 본 문서의 어떠한 내용도 미래에 대한 약속이나 표시로 간주하지 않고 간주되어서도 안 됩니다.

적법한 구매자

본 백서의 내용은 향후 특정 구매자들에게 직접 제공되며, 이들 구매자 외에는 누구도 백서의 수령이나 열람 대상이 아닙니다. 적법성은 보장되지 않으며 참여에 제한이 있을 수 있습니다.

규제 대상 품목

AERGO 플랫폼, AERGO 토큰이나 해당 플랫폼상에서 운영되는 모든 토큰은 유가증권이나 어떠한 법정관할 지역에서 규제 대상 품목으로 지정된 것을 의미하지 않습니다.

본 문서는 유가증권 또는 기타 규제 제품의 제공이나 권유, 투자 목적의 홍보, 초대 또는 권유를 위한 것이 아닙니다. 구매 조건은 금융 서비스 제공 목적의 문서나 그 어떤 투자설명서도 아닙니다.

AERGO 토큰은 플랫폼이나 소프트웨어 또는 기업의 자본, 수익, 소득 또는 수입에 대한 지분, 출자지분, 유닛, 로열티 및 권리, 또는 모든 관할구역의 플랫폼이나 기타 퍼블릭 또는 사설 엔터프라이즈, 조직, 기반이나 기타 독립체와 관련된 지식재산을 표시하는 것이 아닙니다.

본 백서는 구매 권고문이 아닙니다

본 백서는 AERGO 토큰 구매 권고문이 아닙니다. 본 문서는 계약이나 구매 결정과 관련된 것으로 간주되어서는 안됩니다.

리스크 경고

AERGO 토큰의 구매 및 판매 참여에는 상당한 리스크가 존재합니다.

AERGO 토큰을 구매하기에 앞서 다른 문서들에 언급된 리스크를 비롯해 모든 리스크에 대한 신중한 평가 및 고려가 이루어져야 합니다.

본 백서의 관점

본 백서는 블로코의 관점과 견해를 담고 있으며, 이는 어떠한 법정관할 지역의 정부나 준정부, 당국 또는 규제기관 등의 공공기관의 정책이나 입장을 반영하지 않습니다.

본 백서에 포함된 정보들의 경우 신뢰할 수 있는 출처를 통해 확보된 내용을 바탕으로 한 것이기는 하나, 그 정확성 또는 완전함에 대해서는 보증하지 않습니다.

본 백서의 공식 언어는 영어입니다

본 백서 및 관련 자료들은 영어로만 발행됩니다. 번역본은 참조용일 뿐이며, AERGO 나 기타 개인의 인증을 받은 것이 아닙니다. 번역본의 정확성 및 완전함에 대해서는 그 어떤 보증도 하지 않습니다. 본 백서의 번역본과 영어 버전의 내용 상 불일치가 존재하는 경우에는 영어 버전이 우선하는 것으로 합니다.

제삼자 제휴나 보증을 의미하지 않습니다

본 백서에서의 특정 기업 및 플랫폼에 대한 언급은 단순히 예시적인 차원에서 이루어진 것입니다. 기업이나 플랫폼의 명칭 및 등록상표의 사용이 해당 당사자의 제휴나 보증을 뜻하는 것은 아닙니다.

필요할 경우 전문가의 조언을 받으시기 바랍니다.

AERGO 토큰 구매 또는 AERGO 프로젝트 참여 여부를 결정하기에 앞서, 필요에 따라 변호사, 회계사, 세무사 또는 기타 전문가들로부터 상담을 받으시기 바랍니다.

본 백서와 관련해 관할 구역의 규제 당국이 검토한 것은 아닙니다. 본 백서 상, 특정 기업, 네트워크 또는 잠재적 활용 사례들에 대한 언급은 오로지 예시적 차원에서 이루어진 것입니다. 블로코 등 명확하게 언급된 파트너나 제공자를 제외하고, 기타 기업 또는 플랫폼 명칭 및 등록상표의 사용이 해당 당사자의 제휴나 보증을 뜻하는 것 또한 아닙니다.

모든 금액은 별도로 명시되지 않는 한, 미화(USD)를 의미합니다.

목차

초록 1

면책조항 3

전체 개요 6

엔터프라이즈 시장 기회

기회 7

장애요인 12

AERGO 15

AERGO 체인 20

AERGO 퍼블릭 및 프라이빗 저장소 29

AERGO 허브 31

AERGO 마켓플레이스 33

AERGO 토큰 35

토큰 분배 및 자금의 운용 36

개발 로드맵 37

실행계획 38

부록

부록-A: 블록체인 및 오픈 플랫폼 기초 40

부록-B: 블록체인 및 유틸리티 컴퓨팅 49

부록-C: 사설 및 공개형 엔터프라이즈 블록체인 56

부록-D: AERGO 팀 구성 및 자문 패널 59

부록-E: 용어정리 63

전체 개요

지난 2008 년 사토시 나카모토는 은행을 거치지 않고 개인 간 전자결제가 가능한 새로운 암호화폐, 비트코인을 선보였습니다. 10 년이 지난 지금, 다양한 업계 기업들이 비트코인의 혁신적인 핵심 기술을 기반으로 제품과 서비스, 비지니스 모델을 혁신하고자 부단히 노력하고 있습니다.

디지털 세상이 차세대 유틸리티 컴퓨팅 모델(개방형 네트워크와 분산 생태계에서 가치가 창출되는)로 향해감에 따라, 이러한 시스템과 생태계의 기반이 되는 블록체인 기술이 핵심 엔터프라이즈 플랫폼으로 거듭날 수 있는 가능성을 가지게 되었습니다.

새롭게 도래할 세상에서 개발자들은 복잡한 IT 아키텍처 구조와 관리, 운영 기능을 이해하는데 많은 노력을 기울일 필요가 없습니다. 대신 최종 사용자(및 수십억 개의 IoT 기기)들이 어플리케이션을 접하고, 이와 상호작용하는 프론트엔드(Front-End) 부분의 혁신과 가치 창출에 집중할 수 있습니다. 아키텍쳐 수준의 복잡함은 이러한 "서버리스 아키텍처"를 통해 추상화되거나 감춰지게 됩니다. 이렇게 설계된 어플리케이션은 다양한 클라우드 서비스 제공 파트너들이 제공하는 안전한 퍼블릭/프라이빗 클라우드 위에서 컨테이너와 마이크로서비스의 형태로 작동하게 됩니다.

이러한 형식의 유틸리티 컴퓨팅을 위한 주요 플랫폼으로 자리 잡기 위해서는, 블록체인 운영 시스템의 핵심 요소뿐만 아니라 완전히 새로운 "엔터프라이즈 블록체인 플랫폼"과 관련 생태계 창출을 위한 단계적인 접근이 요구됩니다. 이는 블록체인상에서 새롭고 안전한 분산형 마이크로서비스 기반 어플리케이션을 제작, 배포, 운영하는데 필수적인 요소를 모두 제공하기 위함입니다. 다양한 기업과 서드파티가 가치를 창출할 수 있는 주요 플랫폼으로 거듭나기 위해선 견고하면서도 사용이 쉽고, 비용이 낮은 핵심 기술과 개발도구, 개발방법론을 확보해야 합니다.

본 백서는 차세대 엔터프라이즈 블록체인 프로토콜이자 플랫폼인 AERGO 를 소개합니다. AERGO 의 목표는 다양한 업계 어플리케이션 개발자와 엔터프라이즈 기업이 활용하는 핵심적인 IT 아키텍처 및 모델의 하나로서 자리잡는 것입니다. 우리는 앞으로 수천, 수만 가지의 혁신적인 제품과 서비스, 비지니스 생태계가 AERGO 를 기반으로 구축되고 운영될 것으로 예상합니다.

또한, 현재 및 미래의 목표 시장(기존 문제점 및 향후 사업 기회)에 대한 설명을 위해 다양한 기업 니즈와 급변하는 IT 기술/블록체인 트렌드를 요약했으며, 비지니스 친화적인 설명을 위해 기술 컨셉에 대한 내용을 단순화하여 표기했습니다. 각각의 핵심 주제에 대한 자세한 정보는 부록에서 확인하실 수 있습니다.

AERGO 의 핵심 요소들은 블로코가 개발한 기술을 바탕으로 구현됩니다. 블로코는 글로벌 기업들과 함께 블록체인을 기반으로 하는 실제 비지니스 시스템을 설계하고 배포해온, 블록체인 기술 전문 기업입니다. 블로코는 지난 4 년간 쌓은 경험을 바탕으로 이미 2,500 만 명 이상이 사용하는 검증된 기술력을 보유하고 있으며, 이를 기반으로 진일보한 엔터프라이즈 블록체인 플랫폼의 토대를 마련해왔습니다.[3]

블로코는 이러한 핵심 기술을 AERGO 에 제공하는 것은 물론, AERGO 기업 고객을 위한 컨설팅과 유지보수 등의 향후 서비스 제공을 준비하고 있습니다. 하지만 오픈소스 플랫폼이 발전하고, 많은 개발자와 기업 고객이 채택함에 따라 비슷하거나 보완적인 서비스를 제공할 수 있는 다양한 기업이 등장할 것이라고 기대합니다.

[3] Gil, Jae-sik(2018). *"Shinhan Financial Group to Build Blockchain-based Single Sign-On App."* ETNews.com, 22 Jan. 2018, Available: www.etnews.com/20180122000304.

기회

WWW(World Wide Web) 및 IT 기술 산업의 중요한 변화

IT 업계는 미래에 대한 약속이나 희망으로 가득합니다. “차세대 혁신” 등의 아무 의미 없는 버즈워드(Buzzwords) 역시 넘쳐납니다.

우리는 지난 30 년 동안 웹 1.0 이 웹 2.0 으로 점진적으로 발전하는 것을 봐왔습니다.

웹 1.0 시대에는 기본적인 인터넷과 전화식 모뎀, 단방향이고 정적인 웹사이트, 그리고 아주 기초적인 휴대전화 등이 등장했습니다.

웹 2.0 은 이를 더욱 발전시키고 변화시켰습니다. 아이폰 및 안드로이드 스마트폰의 출현으로 사용자들이 서로 소통하고 정보를 교환하는 방식에 큰 변화가 일어났습니다(페이스북 등 소셜미디어 네트워크, 또는 트위터, 스카이프 및 유튜브 같은 인스턴트 멀티미디어 메시지 및 영상 서비스). 아마존이 전자상거래 시장을 바꾸고, 구글이 검색과 광고 시장을 혁신했던 것처럼 기업이 시장과 소통하는 방식 또한 변해왔습니다.

웹 2.0 시대는 모두가 지식을 창출하고 공유하며, 소통하기 위한 방법으로 상호 작용적이고, 초연결 적이며, 다차원적인 가상의 디지털 온라인 생태계가 만들어졌습니다. 하지만 이러한 생태계들은 중앙집중적인 메가 플랫폼을 기반으로 만들어졌으며, 메가플랫폼을 소유한 몇몇 기업들만이 여기서 수집되는 방대한 양의 데이터(사용자 정보와 비지니스 데이터, 그리고 가장 중요한 메타 정보)를 활용할 수 있었습니다. 데이터는 새로운 석유로 각광받기 시작했지만, 가치를 창출해 낼 수 있는 기회는 몇몇 소수 기업에만 집중되었습니다.

대부분의 IT 서비스 제공업체들은 이 거대한 산업이 유지되는데 일조하고 있습니다. 메가플랫폼 기업들이 안전한 중앙집중형(데이터 베이스)시스템에서 이러한 데이터를 수집, 관리, 분석 및 자금화할 수 있게 해주는 기술과 툴을 구축하고, 판매합니다. 다시 말해, 웹 2.0 시대를 통해 새로운 비지니스 모델들이 구현됐지만 여기서 발생한 대부분의 이익은 소수의 글로벌 대기업에 집중되었습니다.

웹 3.0 과 흔히 말하는 ‘웹 4.0’ 역시 버즈워드입니다. 다만 여기서 나온 ‘지능형 웹(Intelligent Web)’이라는 미래 상황, 즉 사용자들을 위한 초개인화된(hyper-personalized) 제품과 개별 고객 상황에 맞는(Contextual) 서비스를 제공하는 상황은 중요한 개념입니다. 이러한 서비스 제공을 위해 수십억 개의 모바일 기기와 IoT 기기가 연동될 것이며, 점점 더 실시간에 가깝게 구현될 것입니다.

현재 IT 기술은 몇 가지 중요한 개선과 변화를 겪고 있습니다. 더욱 안전한 클라우드 서비스가 점점 대중화 되어가며, 오픈소스 기반 플랫폼(리눅스 운영체제 도입, 하둡/텐서플로우 빅데이터 분석 시스템 도입 등)이 실제 비지니스에서 활용되는 경우가 늘어나고 있기 때문입니다. 소프트웨어 개발자들이 가장 흔하게 사용하는 대부분의 개발 툴과 미들웨어 역시 오픈소스 프로젝트를 기반으로 하고 있습니다. 오픈 플랫폼 기반으로 운영되는 어플리케이션을 제작하고자 하는 개발 트렌드 역시 꾸준히 증가하고 있습니다.

이러한 기술적인 요인들로 인해 낮은 비용으로 손쉽게 접할 수 있는 IT 아키텍쳐를 기반으로 한 완전히 새로운 서비스의 개발이 가능해지고 있습니다. 우리는 이를 “유틸리티 서버리스(Serverless) 컴퓨팅”이라고 부릅니다.

'서버리스 아키텍처'는 복잡한 프로그래밍 언어를 이해해야 하는 개발자 및 업체들의 부담이 줄어들게 될 것입니다. 또한, 더 이상 복잡한 IT 아키텍처를 제작하고 관리하기 위해 필요 이상의 노력을 쏟아부을 필요가 없습니다.

IT 복잡성은 추상화되거나 숨겨질 것입니다. 이에 따라 개발자들이나 사용자들은 어플리케이션이나 서비스 그 자체에만 집중할 수 있어, 개발 초점과 방법론 자체가 변하게 됩니다.

올해 말까지 글로벌 IT 시장의 규모는 미화 약 3 조 7 천억 달러에 이를 전망이며, 3 년 이내에 4 조 달러 규모로 성장[4] 할 것으로 예상됩니다. 국제전기통신연합(The International Telecommunication Union)에서는 이와 별도로 올해 말까지 세계 인구의 거의 절반에 해당하는 약 32 억 명이 연결될 것이라고 추정하기도 했습니다. 이 중 약 20 억 명은 개발도상국 국민입니다.

이들 사용자는 디지털 대기업들이 인식한 바와 같이 대단히 가치 있는 방대한 양의 데이터를 만들어내게 될 것입니다. 구글, 아마존, 페이스북 및 트위터 등 대형 IT 기업들은 지난 20 년간 자사 중앙집중형 서버에 대량의 데이터를 축적해오고 있습니다. 사용자들은 이들 업체가 제공하는 서비스를 이용하기 위해 개인정보 및 데이터 소유권을 제공해 왔습니다. 개인정보, 브라우징 습관, 검색 및 온라인 쇼핑 정보가 최고(광고) 입찰자에게 판매되어 온 것입니다.

이러한 기술 및 인터넷의 혁신이 진행됨에 따라, 전 세계 소비자와 기업은 물론, 정부까지도 개인 정보나 비지니스 데이터가 수집되고 저장되며 이용되는 방식의 공개를 요구하고 있습니다. 일부 국가에서는 이와 관련해 이미 새로운 법규가 도입되었습니다(일반개인정보보호규정, GDPR 등)[5].

몇몇 디지털 대기업들은 중앙집중형이고 폐쇄적인 생태계와 데이터베이스를 기반으로 독점형 데이터 추구(Data-hungry) 서비스를 운영할 수 있는 토대를 마련해왔으며, 이를 통해 웹 2.0 시대가 낳은 불균형의 혜택을 누려왔습니다.

그러나 데이터의 가치에 민감한 차세대 서버리스 유틸리티 컴퓨팅의 시대가 찾아왔습니다. 공개 표준(Open and Trusted) 분산 생태계에서 가치를 찾아내 새로운 제품과 서비스를 만들어낼 수 있는 신규 기업들에게는 엄청난 기회가 열려있습니다.

구조적인 발전을 통해 모든 산업 분야에서 데이터를 비롯한 다양한 형태의 디지털 자산 교환을 다루는 수많은 신규 비지니스 프로젝트가 등장할 것으로 예상합니다. 글로벌 리서치 회사인 에베레스트 그룹은 향후 수 년 안에 은행산업 내 블록체인 채택 사례가 급속히 늘어날 것이라고 예측하기도 했습니다(53 페이지 그림 25 참조).

그리고 인터넷은 다음 단계인, 인간 중심의 분산형 인터넷(Human-centered decentralized internet)으로 발전할 것입니다.

[4] Anon.(2018). *Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018*. Available: https://www.gartner.com/newsroom/id/3845563
[5] EU Parliament.(2018). *The EU General Data Protection Regulation*. Available: https://www.eugdpr.org/

블록체인의 역할

블록체인은 기술적인 측면에서 여전히 발전 초기 단계임에도 불구하고, 개발자와 기업들이 공개 표준 분산 생태계에서 가치를 찾아낼 수 있는 가장 혁신적이고 안전하며, 투명한 혁신 기술일 것 입니다. 여기서 가장 핵심적인 개념은 데이터 주권의 민주화(Democatization)이며, 블록체인은 이를 위한 기반을 제공합니다.

우리는 제삼자(중개자)의 개입 없이 모든 네트워크 참여자가 신뢰와 데이터 무결성, 가버넌스 등 합의(Consensus) 전반을 안전하고 효율적으로 도출할 수 있는 분산 인터넷 아키텍쳐를 만들었습니다.

블록체인이 적용된 시스템은 디지털 자산 및 관련 거래에 대해 전적으로 신뢰할 수 있으며 파기할 수는 없는 하나의 보편적인 단일 공유 원장을 작성할 수 있게 됩니다.

이는 현재 활용되는 도구들에 비해 보다 개선되고 효율적인 방식을 통해 이뤄집니다. 블록체인 기술은 암호화된 거래 내역이 분산 저장된 분산 원장을 통해 단일 취약점(Central point of failure)과 기타 보안 이슈를 해결하지 못한 전통적인 중앙집중형 마스터 데이터베이스를 대체할 수 있습니다. 블록체인의 핵심적인 기능은 안전한 검증 메커니즘으로 연결된 여러 원장에 거래를 기록해 거래의 적합성을 보장하는 것입니다.

블록체인 기술이 2 세대로 접어들며 집단 네트워크가 각자의 스마트 컨트랙트, 즉 블록체인을 기반으로 특정 조건에서 중개자 없이 실행되는 컴퓨터 프로그램을 관리하는 것이 가능해졌습니다.

이는 플랫폼 수준에서 디지털 생태계의 많은 부분을 간소화하고 비용을 절감하는 것은 물론, 더 안전하고 투명하게 만들 수 있는 잠재력을 가지게 된다는 것을 의미합니다. 사용자 및 비지니스 데이터가 안전하게 분산 저장되기 때문입니다. 또한, 현존하거나 추후 생겨날 몇몇 거대 기업들이 자신들의 경제적 이익을 위해 데이터를 비축히거나 남용하는 일이 없도록 할 수 있습니다.

그러나 가장 흥미로운 개발 분야는 블록체인 시스템상에서 운영되는 분산형 어플리케이션(dApp)일 것입니다. dApp 은 분산형 어플리케이션(Decentralized Application)의 약자로, 분산된 P2P 네트워크에서 운영되는 백엔드 소프트웨어 코드를 의미합니다. 중앙화된 서버에서 운영되는 기존 어플리케이션과 비교되는 개념입니다.

아직 분산형 어플리케이션이 특정 산업에 대해 가지는 장점은 잘 알려져있지 않지만, 그 전망은 상당히 밝습니다.

분산형 어플리케이션(dApp)을 활용하면, 사용자와 고객이 각자 자신의 데이터와 신분 및 디지털 자산을 소유하는 사용자 및 비지니스 중심형 웹 제작이 가능해집니다. 분산형 어플리케이션(dApp)의 잠재적인 이점으로는 다음과 같은 것들을 들 수 있습니다.

- 공급 및 가치 사슬의 극적인 간소화(중개자 존재 필요성 제거)
- 자동 거래정산 및 계약 체결
- 정확도 높은 사용량 기반(pay-as-you-go) 수익 비지니스 거래
- 저장 데이터 및 어플리케이션의 보안 개선(비가역성 측면에서)
- 사업 성과 향상(보다 신속하고 신뢰도 높은 거래)
- 간접비 절감(인력 및 시설 등)

- 거래사기 예방(궁극적 신뢰 기구)
- 평균 거래 비용 감소(전반적으로 단순한 아키텍처)

서버리스 유틸리티 컴퓨터 구현과 관련해서는, 상당히 많은 분산형 어플리케이션(dApp) 활용 가능성이 존재합니다. 서버리스 분산형 어플리케이션(dApp) 채택은 아직 진행 중이며, 초기 지표들에 따르면 분산형 어플리케이션(dApp)은 업체들이 안전한 분산형 클라우드 기반 서비스를 통해 신규 서비스를 제공하는데 있어서 중요한 요소가 될 것으로 전망됩니다.

블록체인의 개념 증명(Proof-of-concept) 및 일부 간단한 실상용화 사례를 언급하는 자료는 많습니다. 하지만 블록체인 기술이 엔터프라이즈 규모 비지니스에 적용되기에는 넘어야 할 장벽이 많습니다.

- 개발자 및 IT 계약업체가 블록체인을 위한 어플리케이션을 제작하기 어렵다.
- 선택해야 할 구현 모델들 중에서 서로 충돌하는 모델들이 지나치게 많다.
- 분산형 어플리케이션(dApp)의 확장 및 운영에 있어서 설계, 테스트, 배포 및 관리 능력이 매우 중요하다.
- 비지니스 실무상 필요한 성능이나 데이터 제어가 부족한 경우가 많다.
- 신규 블록체인 프로젝트를 기존 IT 시스템으로 통합하는 데 있어 많은 어려움이 존재한다.
- 엔터프라이즈 기업 내에서 여러 개의 블록체인을 구축해야 할 필요가 있을 수도 있다.

요약하자면, 업체들은 다양한 블록체인 솔루션을 활용하고 지원하는 것이 어렵다고 판단할 수도 있습니다. 부록-B 에서는 이러한 서버리스 유틸리티 컴퓨팅 세계에서의 블록체인에 대해 더욱 자세히 다루고 있습니다.

AERGO 설명에 앞서,

앞서 강조한 바와 같이, 오늘의 블록체인은 넘어야 할 도전과제가 많습니다. 하지만 우리는 블록체인의 투명하고 분산화된 비지니스 생태계의 장기적인 가능성을 믿습니다.

기업들과 개발자들에게 필요한 것은 사용이 간편하고 강력한 기능을 갖춘, 수평 개방형 블록체인 "플랫폼"입니다. 이는 단순한 블록체인 프로토콜을 넘어, 여러 이해관계자 간 협력을 활성화할 수 있는 완벽한 생태계입니다.

기업과 개발자, 시스템 통합사업자(SI)를 포함해 분산 생태계에서 핵심적인 역할을 담당하는 서드파티를 위한 플랫폼을 구축하기 위해선 기존 IT 소프트웨어와 새로운 분산형 서버리스 블록체인 시스템을 끊김없이 연결하는 "미들웨어 및 정규화 레이어(normalization layer)"가 필수적입니다.

우리는 이러한 과정이 향후 3~5 년간 블록체인 생태계에서 가장 어려우면서도 흥미로운 개발 분야가 될 것이라고 생각합니다. 글로벌 IT 소비 규모가 미화 기준 약 40 억 달러에 달하는 가운데, 엔터프라이즈 블록체인 플랫폼은 기업 및 그 제작자들 입장에서 상당한 가치를 창출할 수 있기 때문입니다.

이는 AERGO 프로젝트의 주된 목표이자 핵심 전략입니다.

장애요인

퍼블릭/프라이빗 블록체인 시스템을 채택하고 이를 활용하고자 하는 엔터프라이즈들 입장에서는 몇 가지 장애물들이 존재합니다. 블록체인을 활용해 실제 상용화된 시스템을 아직까지 보기 어려운 이유이기도 합니다.

신뢰성 결여

IT 인프라에 대한 완벽한 통제가 힘든 경우, 기업들은 다양한 운영상의 문제를 경험하게 됩니다. 퍼블릭 블록체인은 종종 "하드포크(기반 기술의 수정을 위해 원본으로부터 완전히 새로운 소프트웨어를 만드는 것)"를 겪었습니다. 퍼블릭 블록체인이 하드포크되는 경우, 이를 기반으로 한 dApp 들이 새로운 프로토콜 위에서 계속 동작하는 것이 전제되기도 합니다. 하지만 거미줄처럼 얽힌 엔터프라이즈 솔루션의 관계를 고려할 때, 단순한 사용자 어플리케이션의 하드포크라도 잠재적으로 큰 사업 실패로 이어질 수 있습니다.

하드포크는 IT 네트워크가 네트워크 재생이나 서비스 거부(DDoS) 공격에 매우 취약한 상태가 되게 만들 수도 있습니다. 한 가지 사례로 이미 원본 비트코인 블록체인 프로토콜은 다양한 하드포크가 존재합니다(그림 1 참조). 머지않아 하드포크는 더욱 늘어날 전망입니다.

블록체인 사용이 확대되는 상황에서 확장성을 비롯한 기반 기술 역시 발전을 거듭해야 할 필요가 있습니다. 이를 위해서는 소프트웨어를 운영하는 모든 노드(node)가 프로토콜 소프트웨어의 최신 버전으로 업그레이드 되어야 합니다. 블록체인 기술 수요 증가로 인해 하드포크를 시도하는 사례는 더욱 늘어날 것으로 예상됩니다. 이는 블록체인 기술 도입의 걸림돌이 되며, 안정적인 IT 시스템이 필수적인 기업에서는 도입 자체가 불가능할 수도 있습니다.

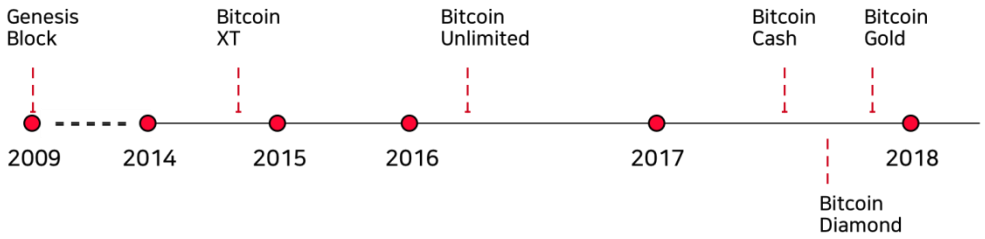


그림 1. 현재까지의 비트코인 블록체인 포크

또 한 가지 문제는 거래 수수료의 변동성이 상당히 높다는 것입니다. 비트코인의 90 일간 평균 거래 가격은 미화 110 달러 96 센트까지 상승하였습니다[6]. 2018 년 3 월 18 일 기준, 약 1 천 건의 거래가 대기 중입니다. 이러한 변동성으로 인해 블록체인의 비지니스 어플리케이션은 예측할 수도 없고 지속될 수도 없습니다. 일반적으로 업체들은 운영비가 불확실한 경우를 선호하지 않기 때문에 아무리 전망이 밝더라도 신규 기술을 거부하는 경우가 많기 때문입니다.

[6] Blockchain Info.(2018). Average over 90 days from 2017.12.19 to 2018.03.18. Available: https://www.blockchain.info

IT 통합의 어려움

수십 년간 다양한 규모의 기업들이 디지털 기술을 활용해 비지니스를 극대화하고 변모시켜 왔습니다. 이들의 경우 주로 다양한 시스템 계층을 테스트하고 구현한 관계로 운영 및 작업 흐름이 매우 복잡하게 구축되어 있습니다. 기업 인프라가 다양한 기술 및 프로세스에 의존하는 경향이 많은 이유입니다.

블록체인과 같은 새로운 혁신 기술을 전통적이고 복잡한 시스템과 통합하는 것은 매우 어려우면서도 상당한 비용이 소요되는 작업일 수 있습니다. 보안보장생성언어("SAML") 등 공개 표준이나 인증을 위한 웹 접근 위임 표준 및 참조 아키텍처(OATH)가 도움이 될 수도 있으나, 새로운 IT 시스템이 액티브 디렉터리, 오라클 또는 SAP 등 널리 사용되는 제품과의 호환성을 갖고 완벽하게 작동되게 만드는 것은 매우 복잡한 작업입니다.

소프트웨어 개발의 어려움

블록체인 같은 신규 기술의 경우 새로운 프로그래밍 프레임워크와 언어를 도입하는 경우가 많습니다. 신규 기업들은 프로젝트 중심적인 경향이 많기 때문에, 개발자들이 새로운 언어 및 툴을 실험하고 학습할 수 있는 여유가 거의 없다고 할 수 있습니다.

솔리디티(Solidity)를 비롯한 일부 개념은 이해하기도 어렵습니다. 개발자들은 솔리디티(Solidity)로 스마트 컨트랙트에 내재된 자체 시행 비지니스 로직을 구현하는 어플리케이션을 제작함으로써 특정 거래와 관련해 반박이 불가능한 신뢰할 수 있는 기록을 남겨둘 수 있습니다. 그러나 많은 기업들이 이러한 유형의 새로운 언어를 이용할 수 있는 소프트웨어 개발자 관련 유연성 및 역량을 갖추지 못한 실정입니다.

기업들은 주로 파트타임 계약업체를 통해 IT 프로젝트 작업을 진행합니다. 이들 계약업체들은 프로젝트 별로 새로운 언어를 습득하거나 학습해야 하는 상황을 원치 않을 것입니다. 이러한 업무들이 "아웃소싱" 되는 경우, 블록체인의 주요 비지니스 로직 및 규칙의 생성과 문서화 업무를 아웃소싱 계약을 체결한 제삼자에게 전적으로 의존하는 것은 바람직하지 않습니다.

개발자들이 스마트 컨트랙트를 작성하기 위해 새로운 언어를 학습하는 것에 비해, 엔터프라이즈 블록체인에 대한 이해 및 프로그래밍이 더욱 용이해야 할 것입니다. 따라서 개발자들은 익숙한 툴체인(C++, 고랭(Golang), 자바스크립트(Javascript) 및 파이썬(Python) 등)을 이용해 기존의 전문지식 및 경험을 활용할 수 있을 것입니다.

SQL 역시 널리 쓰이고 있는 데이터 프로그래밍 및 관리 언어이지만, 블록체인 구현 단계에서는 거의 활용되지 않는 실정입니다.

개인정보보호 문제

다양한 업계에서 현재 퍼블릭 블록체인이 제공하는 수준 이상으로 개인정보보호 요건을 강화하고 있습니다. 퍼블릭 블록체인에서 개인정보보호 및 보안을 개선하는 한 가지 방법은 어플리케이션 수준에서 암호화 및 암호해독 계층을 구현하는 것이나, 엔터프라이즈 블록체인 구현의 경우에는 특히 민감하거나 합법적으로 보호 받는 정보와 관련이 있을 경우 더욱 포괄적이고 강력한 데이터 보안을 제공해야 하는 사례가 많습니다.

2018 년 5 월 유럽 전역에 걸쳐 더욱 엄격한 내용의 GDPR 표준이 새로 발효될 예정입니다. 이와 관련해 비지니스 목적으로 블록체인을 이용하는 기업 등 모든 기업들은 사후 고려 차원이 아니라 시스템 설계 과정에서 개인정보보호 관련 문제를 고려하여 보안 및 개인정보보호 시스템을 구현해야 합니다.

확장성 문제

현재 많은 블록체인이 단순한 확장성 문제에 집중합니다. 그러나 대규모 사용 사례와 관련해서 서비스 사용자의 점진적 수요 증가나 갑작스러운 수요 증가를 자동으로 처리할 수 있는 IT 시스템이 필요합니다.

이러한 수요로 인해 수직 확장 시스템이라고 하는 환경에서 더욱 즉각적인 로컬 컴퓨터 리소스가 필요하게 됩니다(예. 처리량이 많은 특정 업무를 위한 로컬 메모리, 저장, 컴퓨팅 또는 네트워크 역량 확장). 가능한 최단 시간 내에 실행해야 하는 비지니스 거래가 그 한 가지 예라고 할 수 있습니다(즉, 특정 시간 내에 규제 대상인 거래소에서 거래되는 주가의 포착).

사용자 수요가 급증하는 경우, IT 인프라는 즉각적으로 추가 업무량을 공유하기 위해 분산 시스템 전체적으로 컴퓨터 리소스를 추가해야 할 필요가 있습니다(수평 스케일 아웃(Scale-out) 시스템이라고 하는 환경에서 추가해야 함). 인터넷으로 전체 공지된 주문형(On-demand) 이벤트의 티켓을 구매하려는 즉각적인 대량 수요가 한 가지 예라고 할 수 있습니다(즉, 이미 판매된 세계 최고 인기 팝 그룹의 콘서트 티켓의 추가 판매 날짜가 발표된 경우 등).

상호운용성 제약

관련 시장은 아직 초기 발전 단계이지만, 현재 100 가지 이상의 다양한 퍼블릭 블록체인 프로토콜-주로 비트코인 및 수많은 기타 암호화 “알트코인”-이 운영되고 있습니다. 이와 동시에 200 여개가 넘는 프라이빗 블록체인이 대형 기업들에 의해 개발되고 운영됩니다. 각각의 블록체인의 구현 요건이 다양하기 때문에 서로 융합되지 못하고, 규모의 경제를 통해 얻을 수 있는 잠재적 이익 역시 줄어듭니다.

지난 10 년간 클라우드 컴퓨팅과 리눅스의 발전에서 볼 수 있듯이, 시장이 발전하고 성숙하면서 이러한 블록체인 구현 시스템 중 대부분이 점차 사라질 것으로 전망됩니다. 그리고 일부 시스템은 소규모의 전문적 사례들에만 적용될 것입니다. 결과적으로 가장 성공적인 프로젝트들이 통합되면서 보다 더 큰 규모의 블록체인 “생태계” 및 플랫폼이 형성될 것입니다.

블록체인과 관련해 이루어지는 혁신과 상용화 사례의 대부분은 프라이빗 블록체인이 아닌 퍼블릭 블록체인을 중심으로 이루어질 것입니다.

이렇게 남겨진 블록체인 플랫폼 및 생태계 모두 각각의 전문적인 툴과 IT 통합 노하우 및 배포 기술을 필요로 하게 될 것입니다. 많은 기업들이 다양한 프라이빗 블록체인의 상호운용성과 관리 문제를 지속적으로 다루게 될 것이기 때문입니다.

앞서 언급한 바와 같이, 퍼블릭 및 프라이빗 블록체인을 통합하고 이들을 활용해 작업을 하는 것은 매우 어려운 일입니다. 어느 한 쪽 시스템의 성능이 저하되거나 중요한 특성이 사라질 수도 있기 때문입니다.

AERGO, 기업 자율화를 위한 블록체인 플랫폼

AERGO 는 혁신적인 개념의 오픈소스 프로젝트입니다.

AERGO 플랫폼

AERGO 는 클라우드 아키텍쳐를 기반으로 퍼블릭과 프라이빗 블록체인의 개념을 확장하고 각각의 장점을 모두 활용합니다. 우리는(dApp)개발자와 선별된 클라우드 서비스 제공 파트너와 기업들로 구성된 생태계를 지원하는 기술 및 운영 프레임워크를 구축하고자 합니다. 다시 말해, 참여자 모두가 혁신적이고 신뢰할 수 있는 비지니스 서비스를 제작할 수 있는 플랫폼을 만들고자 하는 것 입니다.

AERGO 는 빠른 성능과 안전성, 쉬운 사용성을 두루 갖춘 퍼블릭 블록체인(AERGO 체인)을 중심으로 구축된 분산형 모던 생태계를 지향합니다.

AERGO 의 주요 기능은 아래 그림 2 과 같습니다.

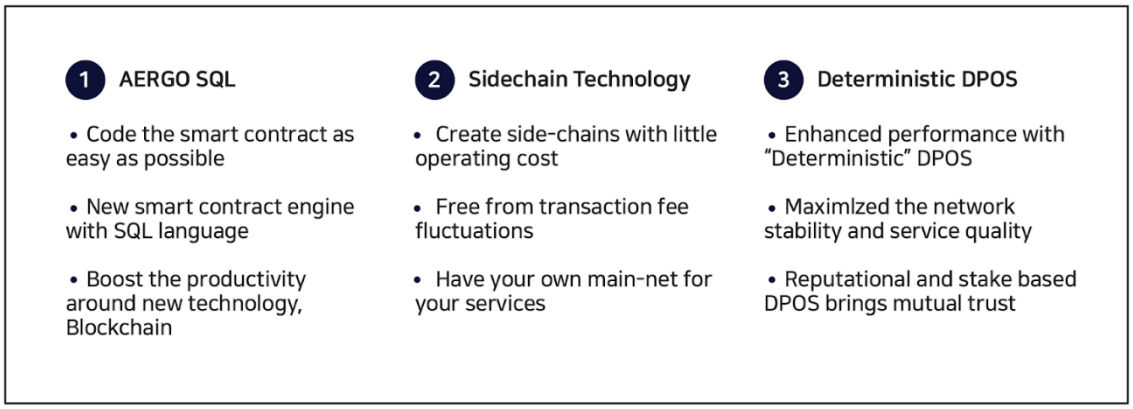


그림 2. AERGO 의 주요 기능

지난 10 년 동안 "하이브리드 클라우드"와 관련 생태계가 개발되고 진화되어 온 것 처럼, AERGO 는 하이브리드 블록체인을 기반으로 하는 다양한 제품과 비지니스 모델이 만들어질 수 있도록 지원하고자 합니다.

AERGO 는 최신 기술을 활용해 사용이 편리하고 실용적인 블록체인 프로토콜을 구현하고자 합니다. 이 프로토콜은(i)퍼블릭,(ii)프라이빗 또는(iii)퍼블릭 및 프라이빗 통합 블록체인 아키텍처 구성의 모든 조합으로 사용할 수 있도록 설계되었습니다. 아래 그림 3 에 이와 관련된 내용이 구체적으로 나와 있습니다.

AERGO 는 퍼블릭 및 프라이빗 네트워크 간의 갭을 해소하는 업계 표준(de facto) 엔터프라이즈 블록체인 구축을 목표로 합니다. 이를 위해 블로코가 이미 구축하고 상용화시켜온 블록체인 플랫폼의 핵심 기술과 구축 청사진을 활용하게 됩니다.[7]

[7]Blocko has successfully delivered 23 in-production blockchain systems (for 20 companies) supporting over 25 million users

나아가, AERGO 는 개발자 친화적이며, 풍부한 기능을 갖춘, 다중 패러다임 구조의 일관성있는 플러그인 기반 스마트 컨트랙트 구조 제공을 목표로 합니다. 이는 다양한 실사례 구축과 프로그래밍을 위함입니다.

“설계”와 “배포”, “사용” 및 “관리”는 AERGO 프로젝트의 주요 설계 원칙들입니다. 이러한 원칙을 단순화, 간소화하는 것은 쉽지 않습니다. 특히, 현재 블록체인 기술 상황에서는 더욱 그렇습니다.

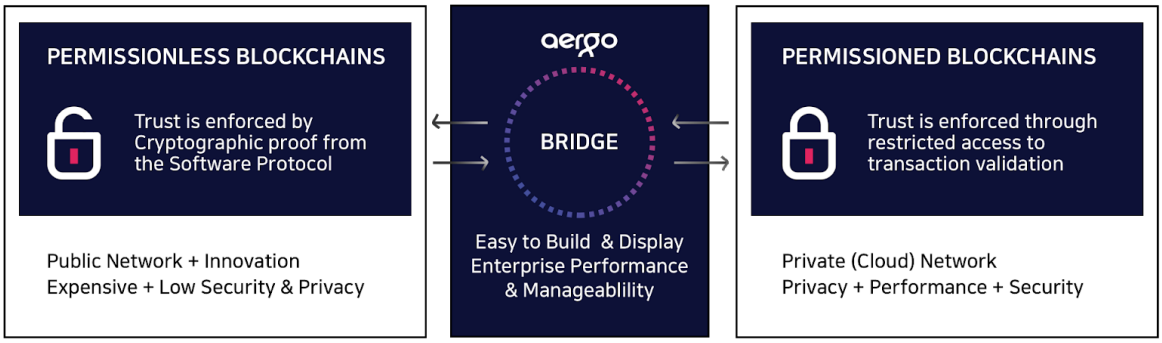


그림 3. AERGO 는 퍼블릭 및 프라이빗 블록체인 세계를 연결한 엔터프라이즈 IT 구축을 목표로 합니다.

AERGO 는 프라이빗 블록체인이 제공하는 성능 및 보안을 갖춘 퍼블릭 블록체인의 실용성 및 혁신을 통합하는 역할을 하게 될 것입니다.

우리는 클라우드 컴퓨팅처럼 기업들이 안전한 퍼블릭 인프라에서 자신들의(dApp)어플리케이션을 개발하고 운영할 수 있도록 하는 기술을 개발하고자 합니다. 해당 기업들은 필요에 의해 이러한 어플리케이션의 일부(또는 전부)를 보다 고성능의 프라이빗 블록체인으로 쉽게 이전할 수 있게 됩니다. 그렇더라도 기존 퍼블릭 블록체인 모델 구현의 이점이 사라지지는 않습니다.

이러한 포괄적인 하이브리드 블록체인 아키텍처, 혁신 기술 및 새로운 데이터 브릿징 프레임워크(Proxy)를 활성화하기 위해서는 다양한 유형의 시스템을 함께 작동시켜야 할 필요가 있습니다. 브릿징 프록시는 여러 개의 퍼블릭 및 프라이빗 블록체인 네트워크 간의 양방향 통신을 가능하게 할 수 있습니다.

또한 스마트 컨트랙트를 이러한 다양한 아키텍처로 개발, 편집 및 내장할 수 있는 기능도 필요할 것 입니다. 더불어 향후 보다 포괄적인 스마트 컨트랙트를 개발하기 위해서는 고성능, 고효율의 가상 머신(Virtual Machine)의 지원도 필요하다고 할 수 있습니다.

아래 다이어그램에는 이러한 원칙이 간략하게 설명되어 있습니다.

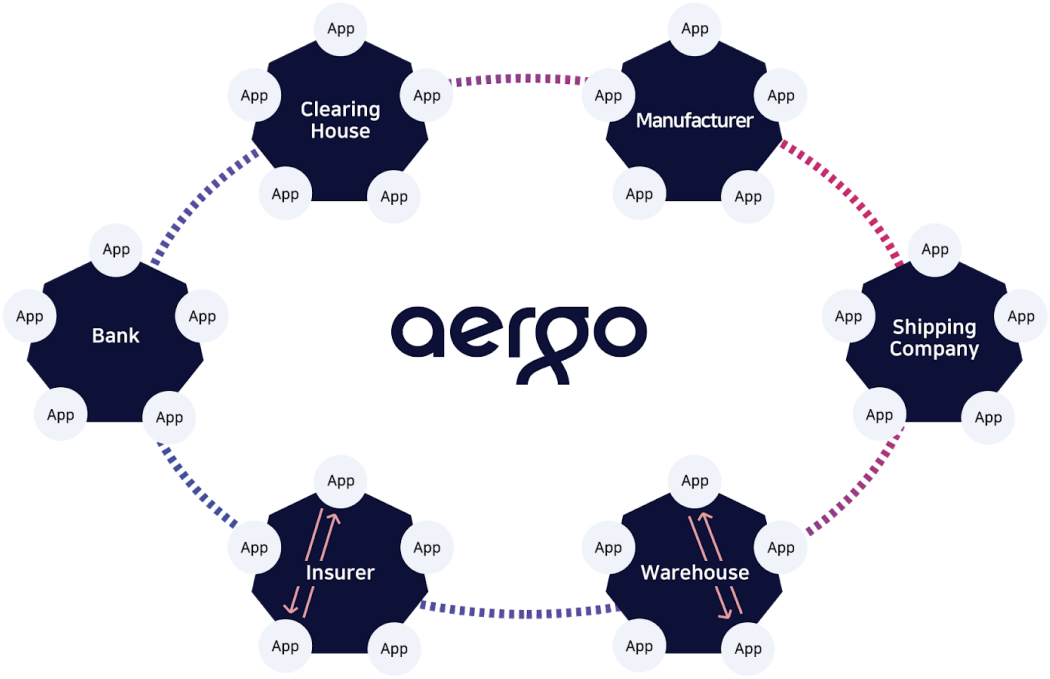


그림 4. 연결되어 있는 공개 및 프라이빗 체인을 나타내는 AERGO 의 생태계 네트워크

AERGO 구조 요약

AERGO 는 수많은 실구축 사례를 보유한 엔터프라이즈급 블록체인 플랫폼인 블로코의 코인스택(COINSTACK)을 토대로 개발될 예정입니다.

AERGO 의 목표는 안전한 고성능 클라우드 아키텍처의 개발, 조정 및 배포에 필요한 완벽한 프레임워크를 제공하는 것입니다.

블로코는 또한 기술 및 지원 파트너 “생태계”를 구축하는데도 일조할 계획입니다.

AERGO 생태계의 주요 이해관계자에는 블록체인과 그 개발자들뿐만 아니라 부가가치 서비스를 제공하는 IT 계약업체, 인프라 및 서비스 공급자를 활용하고자 하는 모든 유형의 업체들이 포함됩니다.

나아가, AERGO 는 AERGO 기술 스택 내 핵심 기능 및 프로젝트를 사용, 개발, 배양 및 확장하고자 하는 오픈 소스 개발자들도 지원하고자 합니다. AERGO 는 단순히 오픈소스 ‘친화적’이 아닌, 진짜 오픈소스 프로젝트가 될 예정입니다.

AERGO 생태계의 가치 및 활용성을 확대하기 위해 새로운 아이디어 및 프로젝트들을 도입하는 것이 본 이니셔티브의 주요 원칙입니다. 생태계 파트너들로는 이러한 혁신을 가능하게 하는 팀이나 연구 프로젝트를 지원하는 특별 프로그램을 들 수 있습니다.

다음은 AERGO 플랫폼을 구성하는 핵심 요소들입니다.

그림 5. AERGO 의 핵심 요소

(I) AERGO 체인: *블록체인의 퍼블릭 네트워크*

AERGO 체인은 노드 제공자가 운영하는 엔터프라이즈 블록체인의 글로벌 공용 분산형 네트워크로 구성된 신규 프로토콜입니다.

AERGO 체인은 혁신적인 비지니스 제품 및 서비스를 활성화하기 위해 고급 스마트 컨트랙트를 쉽게 제작할 수 있는 새로운 정규 스마트 컨트랙트 엔진이라고 할 수 있는 AERGOSQL 를 포함합니다.

요약하면, AERGO 체인은 개념 상 오픈소스 블록체인 운영 시스템으로 간주될 수 있습니다.

(II) AERGO 허브: *AERGO 체인을 위한 퍼블릭 인터페이스*

AERGO 허브의 목표는 AERGO 체인을 통해 안전한 dApp 과 연계해 업무를 수행하는 것입니다. 생성된 dApp 은 다음 두 가지 저장소 중 하나에 저장되게 됩니다.

- AERGO **퍼블릭 저장소(Public repository)**는 dApp 을 위해 공유되는 분산형 공개 인프라입니다(오픈소스 프로젝트 또는 퍼블릭 클라우드 컴퓨팅을 위한 자동화 구축 서버를 호스팅하는데 사용되는 GIT 공용 저장소와 유사).
- AERGO **프라이빗 저장소(Private repository)**는 dApp 을 위해 안전하게 제어되는 프라이빗 인프라입니다. 그 목표는 엔터프라이즈 IT 시스템에 필요한 접속 제어, 어플리케이션 보안 및 성능, 데이터 준수 및 서비스 품질("QoS") [8]을 달성하는 것입니다.

어떠한 방식의 저장소를 사용하더라도 전세계 클라이언트의 실구축 사례에서 이미 검증된 코인스택(COINSTACK)의 API 상호운용성과 구축 프레임워크를 확보할 수 있습니다.

[8] Wikipedia, The Free Encyclopedia.(2018). *Quality of service*. Available: https://en.wikipedia.org/w/index.php?title=Quality_of_service&oldid=836944975

dApp 을 포함해, 블록체인에 최적화 된 기타 지원 소프트웨어, 컴퓨팅 리소스 및 서비스 등을 AERGO 체인에서 사용하기에 앞서 자원들을 통합하고, 조성하며, 배포하고 관리하는 작업이 필요합니다.

이러한 과정은 AERGO **호드(Horde)**를 통해 이뤄집니다. AERGO 호드는 블록체인 노드 제공자나 소프트웨어 벤더 등 AERGO 허브 생태계에 참여하고자 하는 인프라 및 리소스 제공자를 위한 퍼블릭 통합(Orchestration)[9], 관리 및 소프트웨어 프레임워크입니다.

요약하자면, AERGO 허브는 현재 퍼블릭 클라우드 웹 서비스에 활용되는 기술과 유사한 개념이라고 할 수 있습니다.

(III) AERGO **마켓플레이스**: *AERGO 체인에 최적화된 소프트웨어 어플리케이션, 컴퓨팅 리소스 및 기타 서비스 등 필요한 핵심 요소를 모두 제공하는 원스톱 숍(One-Stop Shop)*

- AERGO 마켓플레이스 소프트웨어, 컴퓨팅 및 기타 서비스들은 AERGO 플랫폼을 지원하는 생태계의 일환으로 AERGO 체인 상에서 운영되거나 AERGO 체인과 함께 작동합니다
- AERGO 허브의 퍼블릭 인터페이스를 통해 파트너 서비스들을 이용할 수 있습니다
- 해당 서비스들은 AERGO 호드를 통해 관리됩니다.

AERGO 상세 기능 및 역량

아래에서는 앞에서 언급한 AERGO 플랫폼의 주요 기능들(및 기타 관련 기능들)과 관련된 기술적 역량에 대해 보다 상세하게 설명하고자 합니다.

본 백서가 일부 독자들에게는 지나치게 기술적인 내용일 수도 있으나, 이러한 핵심 기능들을 최대한 간략하게 설명함으로써 AERGO 만의 혁신적인 핵심 기능들을 파악할 수 있도록 하고자 합니다.

보다 자세한 정보는 웹사이트(www.AERGO.io)의 AERGO 기술 백서를 참조해 주시기 바랍니다.

[9] Wikipedia, The Free Encyclopedia.(2018). *Orchestration(computing)*. Available: https://en.wikipedia.org/w/index.php?title=Orchestration_(computing)&oldid=831362994

AERGO 체인

AERGO 체인은 현재 퍼블릭 블록체인에서 발견되는 문제점들을 줄이기 위해 설계된 퍼블릭 블록체인 프로토콜입니다. AERGO 체인은 위임지분증명("DPOS")[10] 거버넌스 모델을 채택하고, 새로운 평가 기반 자율 위임 알고리즘을 구현함으로써 신뢰도과 서비스 품질("QoS") 확보라는 목표를 달성하게 됩니다.

AERGO 체인은 SQL 기반 스마트 컨트랙트 플랫폼을 제공하여 그 유용성을 높이고자 합니다. 이는 블록체인 기술 도입 및 기존 시스템과의 통합 관련 문제를 해결하는데 가장 중요한 요소 중 하나입니다.

엔터프라이즈 기반 블록체인 프로토콜 계층에는 분산 버전 컨트롤(Distributed version control)과 병행제어(Concurrency control)를 비롯한 고급 기능들이 포함되어야 합니다. 이들 기능은 사용자들이 퍼블릭과 프라이빗 dApp 저장소(Repository)를 활용하는데 핵심적인 역할을 담당하며, 향후 엔터프라이즈 블록체인의 보안성을 높이는데 도움이 될 것입니다.

AERGO 체인은 스마트 컨트랙트의 새로운 병렬처리(Parallel processing) 역량을 바탕으로 초당 수백만 건의 거래를 처리할 수 있습니다. AERGO 는 블록체인 기반의 다양한 제품과 서비스 수요에 대응하기 위해 블록체인 네트워크에 최적화된 수직 확장(Scale-up) 및 수직 확장(Scale-out)을 지원하도록 설계될 예정입니다. 또한 병렬처리 네트워킹 패브릭(Parallel throughput networking fabric)은 물론, 멀티 코어 및 초고속 캐시 메모리 처리 환경을 위한 다중 쓰레드 아키텍처(multi-thread architecture)를 지원할 계획입니다.

현재 개발 중인 AERGO 체인의 핵심 기술은 블로코의 코인스택(COINSTACK) 운영 시스템을 기반으로 합니다. 대규모 엔터프라이즈 클라이언트를 대상으로 각 기업이 운영 중인 기존 컴퓨터 네트워크와 보안 데이터센터에 실제 블록체인 기반 시스템을 구축하며 얻은 경험과 노하우는 가장 중요한 자산입니다.

합의 알고리즘

블록체인의 가장 명확한 주요 특징 중 하나는 합의 알고리즘입니다. 합의 알고리즘은 블록체인에 추가되는 블록이 실제 버전인지의 여부를 확인하는 주요 프로그램입니다. 합의 알고리즘이 없을 경우, 누구나 블록체인에 정보를 추가할 수 있기 때문에 전체 시스템의 적법성에 문제가 발생할 수 있습니다.

이러한 합의 알고리즘에는 복잡한 수학 및 논리가 적용되지만, AERGO 플랫폼의 높은 성능을 위해 선택한 알고리즘의 기본 사항에 대한 이해가 필요합니다. 따라서 아래에서는 가장 관련성이 높은 기술들에 대해 간략하게 설명하고자 합니다.

AERGO 체인은 다양한 합의 알고리즘을 지원하고, 사용자들이 각자의 비지니스 요건에 가장 적합한 합의 알고리즘을 정의하고 선택할 수 있도록 지원합니다. 그러나 AERGO 의 기본적인 선택 합의 알고리즘은 위임지분증명("DPOS")입니다. 이 알고리즘 계층은 더 나은 확장성 및 경제적 운영 모델을 지원합니다. 또한 AERGO DPOS 알고리즘은 기업들과 중요한 노드 제공자들의 네트워크 참여를 이끌어 낼 수 있는 여러가지 이점을 제공하게 됩니다.

이를 통해 네트워크 전반의 장기적인 실행 가능성과 효율성, 지속가능성을 확보할 수 있게 됩니다.

---

[10] Mycryptopedia.(2017). *Delegated Proof-of-Stake(DPoS) Explained.* Available: https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/

작업증명(POW)

블록체인 커뮤니티에서는 작업증명("POW")이 블록체인과 관련해 가장 유용한 합의 알고리즘으로 여겨지고 있습니다. POW 의 이점은 간결하고 이해가 쉬우며 가장 민주적인 합의 방식이 될 수 있다는 것입니다.

그러나 POW 에는 매우 심각한 결함이 존재합니다.

소수의 대규모 채굴자들이 권한 및 통제력을 장악할 수 있다는 점 입니다. 네트워크의 예측가능성, 안정성, 지속가능성은 기업들이 IT 기술을 활용하기 위한 기본 요소이며, 대형 IT 시스템의 운영 서비스 퀄리티(QoS)에 직접적으로 영향을 미칩니다.

기업들을 위해 설계된 퍼블릭 블록체인의 경우, 외적 요인들로 인해 QoS 가 저하되거나 소수(혹은 악의적인) 참여자들이 통제하는 상황이 벌어지지 않도록 막을 수 있어야 합니다.

지분증명(POS)

지분증명("POS") 기반의 다양한 알고리즘이 등장하고 있습니다. 이더리움 플랫폼 역시 추후 지분증명 기반으로 개발될 예정입니다. 하지만 아직 대다수가 아직 개발 중이거나 구현조차 이뤄지지 않았습니다. 현재 POS 와 관련해 가장 중요한 기술적 문제들(nothing-at-stake 등) 중 일부를 해결하는데 주력하고 있는 상황입니다.

또한, POS 가 주요 합의 방식으로 자리잡기 위해선 브랜치 해프닝(branches happening)이나 소위 '코인 슬래싱(coin slashing)' 같은 특정 문제를 해결해야 합니다. 예를 들어, 에러(또는 버그)가 POS 규칙을 위반하는 경우, 코인 슬래싱(coin slashing)이 발생하면서 블록체인과 관련해 최악의 하드포크가 생성될 수도 있기 때문입니다.

퍼블릭 네트워크의 하드포크는 네트워크 신뢰성에 직접적인 영향을 미치며, 퍼블릭 네트워크 기반으로 운영되거나 이와 연동된 기업체 혹은 서비스의 보안 리스크가 커질 수 있습니다. 지금까지의 비트코인 하드포크 사례는 본 백서 13 페이지, 그림 1 에서 확인하실 수 있습니다.

위임지분증명(DPOS)

위임지분증명("DPOS")은 효과적인 대안 합의 알고리즘입니다. DPOS 는 EOS 나 스팀(Steem) 등 여러 블록체인 프로젝트에서 활용하는 진보적이며 네트워크(에너지) 효율적인 모델입니다.

DPOS 는 분산(Decentralizaion)을 장려합니다. 중앙 집중형의 대규모 컴퓨터 마이닝 팜이 필요치 않기 때문입니다. 또한, DPOS 는 네트워크 이해관계자들이 악의적 행위자들을 네트워크에서 퇴출시키는 것을 가능하게 해 줍니다. 이러한 사회적, 기술적 형태가 통합된 분산 시스템은 네트워크에서 가치 있는 참여자를 인정함으로써 선의의 행위를 지원하게 되며, 이를 통해 자정 작용과 선순환이 가능하게 됩니다.

DPOS 는 이해하기도 쉽고 하드포크가 생성될 가능성도 매우 낮습니다. 또한, 기업과 인프라 제공자가 노드 역할을 담당하게 된다면 하드포크 발생 가능성은 더욱 낮출 수 있습니다. 기업 프로세스의 QoS 와 관련한 주요 요건들도 개선될 수 있습니다.

요약하자면, POW 는 순수하게 경제적 인센티브만 제공하는 반면, DPOS 는 사회적 합의와 경제적 인센티브를 동시에 제공합니다. AERGO 가 DPOS 를 선택한 이유입니다.

스마트 컨트랙트

AERGO 체인은 이더리움 버추얼 머신(Ethereum Virtual Machine)을 포함, 이미 검증되고 사용성 높은 다중 패러다임(Multi-paradigm) 스마트 컨트랙트 인프라를 지원하고자 합니다. 복합적 접근 방식을 통해 다양한 스마트 컨트랙트 간 의미있는 수준의 상호 운영성을 확보할 수 있습니다.

AERGOSQL

AERGOSQL 은 AERGO 체인 상에서 운영되는 스마트 컨트랙트를 지칭합니다. AERGOSQL 은 스마트 컨트랙트 작성을 위한 관계형 데이터 모델이며, 데이터와 SQL 을 비롯한 스크립트 언어를 저장하고 엑세스하는데 활용됩니다.

전통적이지만 시장 이해도가 높고, 사용이 간편한 SQL 기술을 활용하는 새로운 접근 방식을 통해 더 많은 개발자들과 기업들이 블록체인 기술이 제공하는 이점을 누릴 수 있도록 하고자 합니다.

아래 내용은 이와 관련해 간단한 한 가지 코딩 모델 사례입니다.

```
CREATE  IF NOT EXISTS accounts  (
        owner VARCHAR NOT NULL PRIMARY KEY,
        balance NUMERIC (15, 2)
);

CREATE OR REPLACE FUNCTION
transfer (sender TEXT, to TEXT, amount NUMERIC)
RETURNS text
AS
$$
DECLARE
        sender_bal NUMERIC ;
BEGIN
        SELECT balance INTO sender_bal FROM accounts WHERE owner = sender ;
        IF NOT FOUND THEN
            RETURN 'Sender not found' ;
        END IF
        IF sender_bal < amount THEN
            RETURN 'Not enough balance' ;
        END IF
        UPDATE accounts SET balance = balance + amount WHERE owner = to ;
        IF NOT FOUND THEN
            RETURN 'Receiver not found' ;
        END IF;
        UPDATE accounts SET balance = balance - amount WHERE owner = sender ;
        RETURN 'OK' ;
END;
$$
```

그림 6. AERGOSQL 코딩 모델 예시

AERGOSQL 은 최고의 성능을 구현하기 위해 LLVM 컴파일러 인프라(지능형 JIT 컴파일[11] 제공) 및 고성능 b-트리 데이터구조 구현(데이터 저장 오픈소스 WiredTiger[12] 등)과 같은 고급 혁신 기술을 채택하고 있습니다.

스마트 컨트랙트 실행은 AERGO 내부의 유틸리티입니다(AERGO 체인의 네이티브 디지털 자산으로 지정). AERGO 에서 스마트 컨트랙트를 실행하는 경우(이러한 업무에 필요한 연산력 포함) 러닝코스트가 발생합니다.

브랜칭(Branching) 및 머징(Merging)

분산 버전 관리시스템(Distributed version control systems)과 관련된 가장 복잡한 개념 중 하나는 브랜치 머징(Branch merging) 프로세스입니다. 실시간 데이터 처리가 필수인 블록체인의 경우, 머징의 난이도는 더욱 높아집니다.

AERGO 는 비파괴 프로세스(Non-destructive process)를 통해 브랜칭(branching)을 간단하고 직관적으로 실행할 수 있습니다. 단, 머징은 아래의 두 가지 방식으로 진행됩니다:

(I) 자동 머징(Automated Merging)

- 기본적으로 자동 머징(Automatic Merging)은 두 개의 브랜치를 병합하는 프로세스입니다. 자동 머징은 블록체인의 블록 재구성 프로세스와 유사합니다. 이 경우, 머징 소스(merging source)의 블록은 거래 별로 나뉘어져 머징 타깃(merging target)의 머징 풀(merging pool)로 흡수됩니다. 궁극적으로, 머징 풀(merging pool)은 머징 타깃(merging target) 중 베스트 블록에 새로운 블록을 추가합니다. 이 프로세스에서 머징 타깃 브랜치(merging target branch)와 일치하지 않는 거래는 자동으로 새로운 블록에서 제외됩니다.

(II) 일관된 머징(Consistent Merging)

- 일관된 머징(Consistent Merging)은 브랜치가 특정하게 일관적인 머징(merging) 로직을 통해 생성될 때에만 발생합니다. 일관된 머징(Consistent merging)은 Git 과 같은 버전 관리 시스템의 병합 기능과 유사합니다[13]. 기본적으로 일치하지 않는 트랜젝션은 폐기하는 자동 머징(automatic merging)과 달리, 일관된 머징(consistent merging)에서는 사전 정의된 갈등 해결 로직에 따라 일치하지 않는 거래를 관리합니다. 갈등 해결 로직은 시스템 차원의 스마트 컨트랙트로 구현됩니다.

[11] Wikipedia, The Free Encyclopedia.(2018). *LLVM*. Available: https://en.wikipedia.org/w/index.php?title=LLVM&oldid=841209654
[12] Michael Cahill.(2015). *A Technical Introduction to WiredTiger*. Available: https://www.mongodb.com/presentations/a-technical-introduction-to-wiredtiger
[13]Wikipedia, The Free Encyclopedia.(2018). *Git*. Available: https://en.wikipedia.org/w/index.php?title=Git&oldid=841769346

AERGO 체인은 Git 과 같은 버전 관리시스템에 익숙한 사용자들에게 친화적인 구문(Syntax)과 의미(Semantics)를 제공합니다. AERGO CLI 클라이언트 및 원격 절차 호출(Remote Procedure Call) API 를 통해 해당 기능들을 이용할 수 있습니다.

AERGO 체인의 목표는 개발자 친화적인 시스템으로 자리잡는 것입니다. 개발자들은 AERGO 체인을 통해 자신에게 익숙한 기술과 개발 도구와 방식을 이용할 수 있습니다.

병행 제어(CONCURRENCY CONTROL)

병행 제어는 블록체인 네트워크의 중요 기능입니다. 블록체인 네트워크 대표자(Delegates)들이 블록 생성 트랜잭션을 결정할 경우, DPOS 합의 알고리즘을 통한 결정성 확보를 가능케 하는 기능입니다.

AERGO 체인의 목표는 블록 수준과 풀(pool) 수준의 트랜잭션 직렬화 메커니즘을 제공하는 것입니다.

(I) 블록 수준 직렬화

- 블록체인의 각 브랜치는 일련의 블록으로 구성되어 있기 때문에 각각의 블록을 순차적으로 연결해 트랜잭션을 직렬화할 수 있습니다.
- AERGO 는 블록의 높이(Block height)를 토대로 멀티 버전 병행 제어(MVCC) 기능을 제공하게 됩니다. 브랜치와 블록의 높이가 판별되면, 저장소의 다양한 노드에 걸쳐 일관성 있는 리드(Reads)를 제공할 수 있습니다.
- AERGO MVCC 의 기능은 행 또는 문서 버전 관리를 통해 일관적인 리드(reads)에 사용되는 스냅숏 격리(Snapshot isolation)와 일종의 비선점 잠금(Optimistic locking)을 제공하는 것입니다. MVCC 기능은 블록 수준 직렬화를 위해서만 쓰입니다.

(II) 풀 수준 직렬화

- AERGO 노드에 접속하는 사람들은 대표들이 생성하려는 블록의 결정성을 활용할 수 있습니다. 이것은 핵심 DPOS 합의의 특성이며, 거래 완료성(Finality)을 강력하게 보장함으로써 트랜잭션 동기화를 가능하게 합니다.
- AERGO 네트워크에서 위임된 노드들은 신규 거래를 메모리 풀로 처리하고 균일한 직렬화 배열을 활용해 신규 블록을 생성합니다. 클라이언트들은 거래 결과를 검색하기 위해 블록 배치가 완료될 때까지 기다릴 필요가 없습니다. 결과적으로, 거래 실행 지연속도가 수 초에서 수 밀리 초 수준으로 줄어듭니다.

아래 도표에 풀(pool) 수준 직렬화가 간략히 설명되어 있습니다.

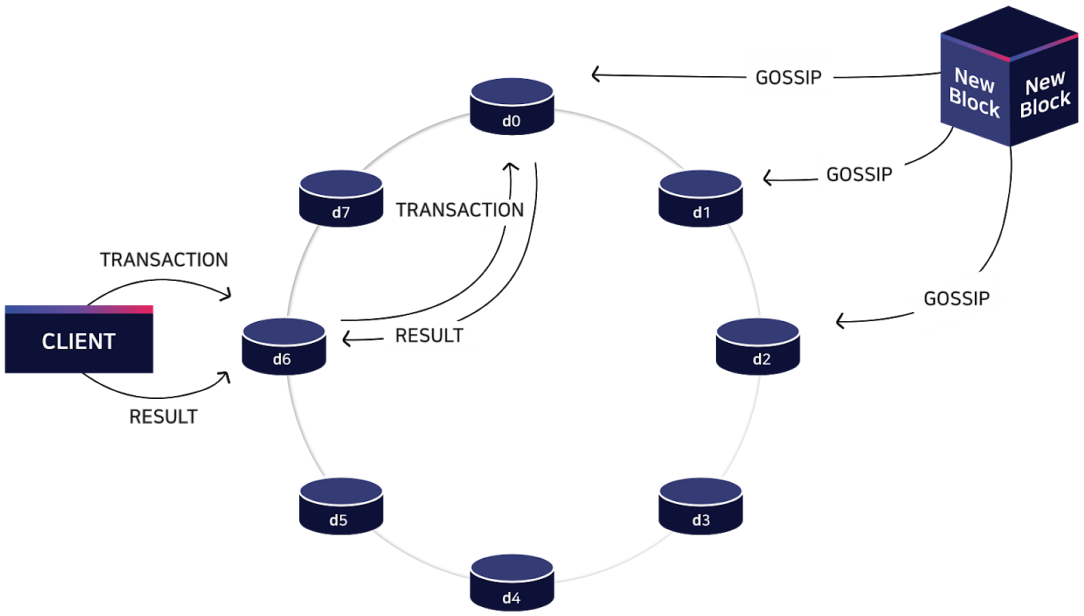


그림 7. AERGO 체인에서의 풀 수준 직렬화

병렬화(PARALLELISM)

AERGO 의 성능은 거래 및 블록 수준 병렬처리의 조합을 통해 극대화되게 됩니다.

블록체인 시스템의 성능은 주로 다음 항목들에 의해 좌우됩니다:

(i) 신규 블록의 효율적인 생성과 공유,

(ii) 각 노드가 신규 블록을 처리하는데 걸리는 시간

분산 합의 프로토콜은 블록체인의 블록 생성 프로세스에 대한 방법론입니다. 분산 합의 프로토콜에 대해 다방면의 연구가 진행되어 왔으며, 분산 합의에 대한 다양한 블록체인 프로젝트들이 주목 받기도 했습니다. 하지만 이러한 기존 시스템들은 노드의 실제 블록 생성 프로세스 설계와 구현이 미흡한 경우가 많습니다.

비트코인이나 이더리움을 비롯한 소비자용(Consumer grade) 블록체인에서는 제 성능을 내지 못하는 노드라도 어느정도 용인될 수 있었습니다. 그러나 AERGO 와 같은 산업용 수준(Enterprise grade) 블록체인은 실시간 처리가 가능할 정도의 견고한 성능을 요구합니다. 결과적으로, 블록체인의 전반적인 성능 향상을 위해선 합의 프로토콜 자체만큼이나 효과적이고 효율적인 노드 구현이 필수적입니다.

AERGO 체인의 경우, 시스템 성능을 극대화하기 위해 블록 프로세싱의 다양한 단계에서 병렬화(PARALLELISM) 개념을 도입하게 됩니다.

블록체인 시스템의 병렬(PARALLELISM) 처리를 위해서는 각 블록에 포함되는 트랜잭션 간의 상호 의존성에 대한 면밀한 분석과 이해가 요구됩니다. 또한, 단계별 이벤트 기반 아키텍처(SEDA, Staged Event Driven Architecture) [14]를 근거로 하는 효율적인 아키텍처가 필요합니다.

이러한 병렬(PARALLELISM) 형태는 다음과 같습니다.

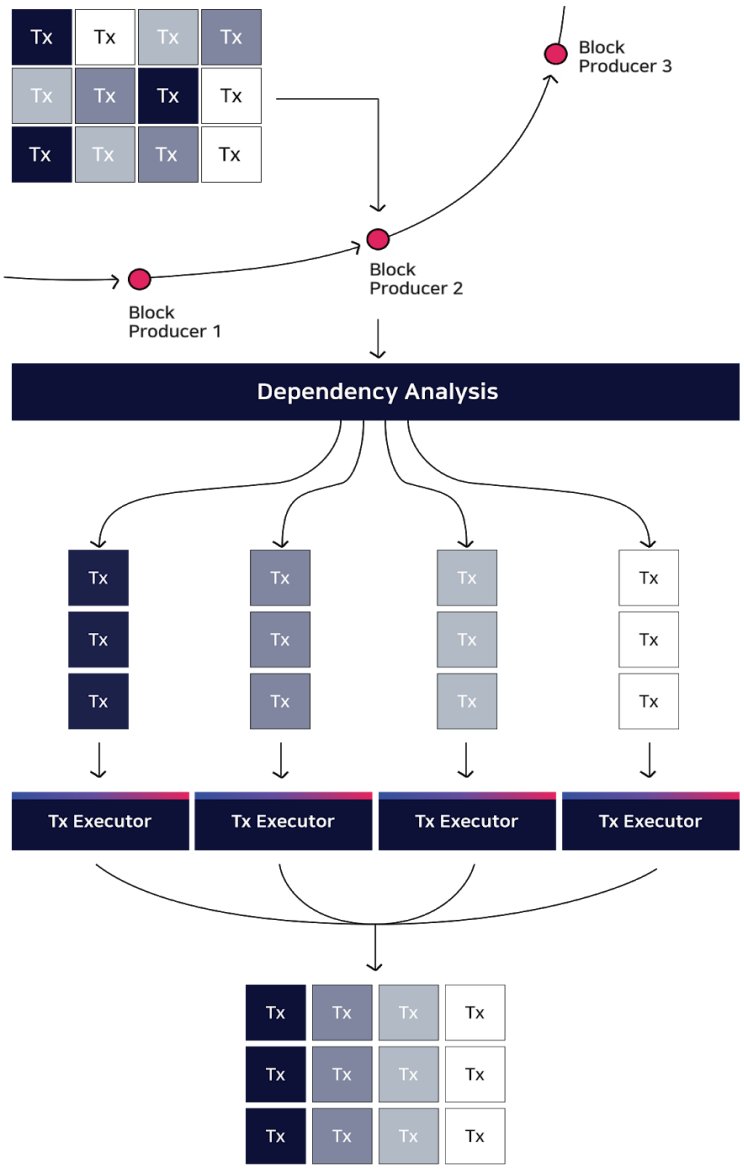


그림 8. AERGO 병렬(AERGO PARALLELISM)

[14] Wikipedia, The Free Encyclopedia.(2018). *Staged event-driven architecture*. Available: https://en.wikipedia.org/w/index.php?title=Staged_event-driven_architecture&oldid=812633632

종속성 분석(Dependency Analysis)

종속성 분석은 AERGO 의 병렬처리 역량을 가능케하기 위한 주요 요소입니다.

AERGO 는 트랜잭션 및 블록의 종속성 분석을 통해 실행 순서에 대한 데이터 구조를 생성하며, 트랜잭션의 영향을 받는 상태 기계(State Machine) 내의 결정적 결과값을 측정합니다. 이러한 데이터 구조 형식을 결정형 트랜잭션 트리(DTT, Deterministic Transaction Tree)라고 부릅니다. DTT 에 대한 자세한 정보는 AERGO 기술 백서에서 확인 가능합니다.

AERGO 파일 시스템

AERGO 의 고유 파일 시스템(AERGOFS)은 확장성, 특히 앞서 언급한 IT 시스템의 수직적, 수평적 확장성을 확대합니다.

AERGOFS 는 분산 파일 시스템처럼 작동합니다. 그 목표는 AERGO 체인을 위한 구조적, 비구조적 데이터 저장 역량을 제공하는 것입니다. 데이터를 덩어리(Chunk) 형태로 관리하는 하둡 분산 파일 시스템(HDFS, Hadoop Distributed File System)[15]과 달리, AERGOFS 는 다양한 형태와 사이즈의 파일을 서비스할 수 있습니다.

AERGOFS 는 페이스북의 헤이스택(Haystack)[16]기술을 기반으로 합니다.

AERGO 체인은 사용이 쉬운, Git 과 같은 프라이빗 저장소를 제공해 적절한 권한을 가진 개발자들과 사용자들이 기반 원장에 쉽게 접근할 수 있도록 설계됩니다.

이는 개발자들에게 매우 중요한 요소라고 할 수 있습니다.

도메인 기반 분할(DOMAIN-BASED PARTITIONING)

도메인 기반 분할(DOMAIN-BASED PARTITIONING)은 AERGO 의 확장성을 확보할 수 있는 가장 기본적인 방법입니다. 도메인 분할은 AERGO 의 분산 버전관리 기능을 통해 제공됩니다.

AERGO 는 기존의 블록체인 구현과 달리 브랜치를 통해 데이터를 자유롭게 포크(fork) 및 머지(merge)할 수 있습니다. 이를 분산 버전 관리(DVC, Distributed Version Control)라고 합니다. 분산된 원장이 다양한 저장소를 통해 논리적으로나 물리적으로 분할될 수 있습니다.

Git 이나 Mercurial 등 이미 광범위하게 이용되고 있는 다양한 분산 버전 관리 시스템들이 이러한 방식을 성공적으로 활용하고 있습니다. 예를 들어, 널리 배포된 Git 허브 시스템의 경우 수천만 개의 저장소를 호스트할 수 있습니다.

그러나, 도메인 기반 분할의 효과는 주로 데이터의 구조 및 사용 방식에 따라 달라집니다. 단일 저장소가 데이터를 무한 확장해야 할 경우, 브랜칭(branching)으로 데이터를 분할하기는 매우 어렵습니다.

---

[15] IBM.(2018). *Apache Hadoop Distributed File System*. Available: https://www.ibm.com/analytics/hadoop/hdfs.
[16] Peter Vajgel.(2009). *Needle in a haystack: efficient storage of billions of photos*. Available: https://code.facebook.com/posts/685565858139515/needle-in-a-haystack-efficient-storage-of-billions-of-photos/

따라서, AERGO 의 목표는 AERGO 파일 시스템(AERGOFS) 및 AERGO 허브를 바탕으로 추가적인 확장 방식 및 역량을 활용하는 것입니다.

분산 디렉토리(DISTRIBUTED DIRECTORY)

분산 디렉토리("DD")는 AERGO 구현 시스템의 블록 생성 시 필요한 핵심 요소입니다.

저장소의 각 DD 는 네임스페이스(Namespace)를 독립적으로 관리합니다. 각 네임스페이스에는 저장소에 포함된 다양한 브랜치 및 태그 관련 정보뿐 아니라 블록체인 관련 다양한 식별자들에 대한 검증 내용도 포함되어 있습니다.

각각의 DD 는 개별적인 블록체인으로서, 제네시스 블록과 베스트 블록을 갖고 있습니다. DD 블록은 기존 블록들과 달리 비교적 생성 간격이 길고 사이즈가 제한적이라는 특징을 갖고 있습니다. 또한, 메타데이터 관리를 위해 이용되기 때문에 사이즈가 작아야합니다.

그 역할 및 기능의 측면에서 DD 는 데이터 사전 즉, 하둡(Hadoop)의 주키퍼(zookeeper) 또는 CoreOS 의 etcd 와 비슷하다고 할 수 있습니다[17].

요약하자면, AERGO **체인**을 통해 강력한 *블록체인의 퍼블릭 네트워크*가 구현됩니다.

[17] Lawrence Hecht.(2018). *CoreOS, Red Hat and Kubernetes Competition*. Available: https://thenewstack.io/coreos-red-hat-kubernetes-competition/

AERGO 퍼블릭 & 프라이빗 저장소(REPOSITORIES)

AERGO 체인은 바로 사용가능 한(Out-of-the-box) 퍼블릭 및 프라이빗 저장소 생성을 지원합니다.

저장소는 개발자들을 위한 일종의 코드 호스팅 플랫폼으로서, 프로젝트를 위해 개발되는 실제 소프트웨어 프로그램 코드를 포함합니다. 또한, 버전 제어 및 협업을 위해서도 활용됩니다. 저장소를 통해 개발자와 다른 관계자들이 어디서든 신규 프로젝트를 진행할 수 있습니다. 실제로, 저장소는 시간이 지나면서 바뀌기 때문에 프로젝트나 파일 묶음을 관리합니다.

이러한 저장소들은 실제로 AERGO 체인에서 동작하는 가장 작은 형태의 블록체인이라고 할 수 있습니다. 저장소는 프라이빗 블록체인이거나, AERGO 체인과는 독립적으로 기능하는 퍼블릭 블록체인의 형태로 구현될 수도 있습니다.

AERGO 에서는 퍼블릿 및 프라이빗 저장소를 모두를 무료로 이용할 수 있습니다. 저장소에 대한 권한은 이들을 생성하는 독립체가 관리합니다. 일반적으로 퍼블릭 저장소는 퍼블릭 네트워크에서 식별된 모든 개인에게 공개됩니다. 프라이빗 저장소는 특정 프라이빗 네트워크에 접속할 수 있도록 허가받은 개발자 및 사용자들만 접속이 가능합니다.

이와 관련된 내용은 아래 표에 나와 있습니다.

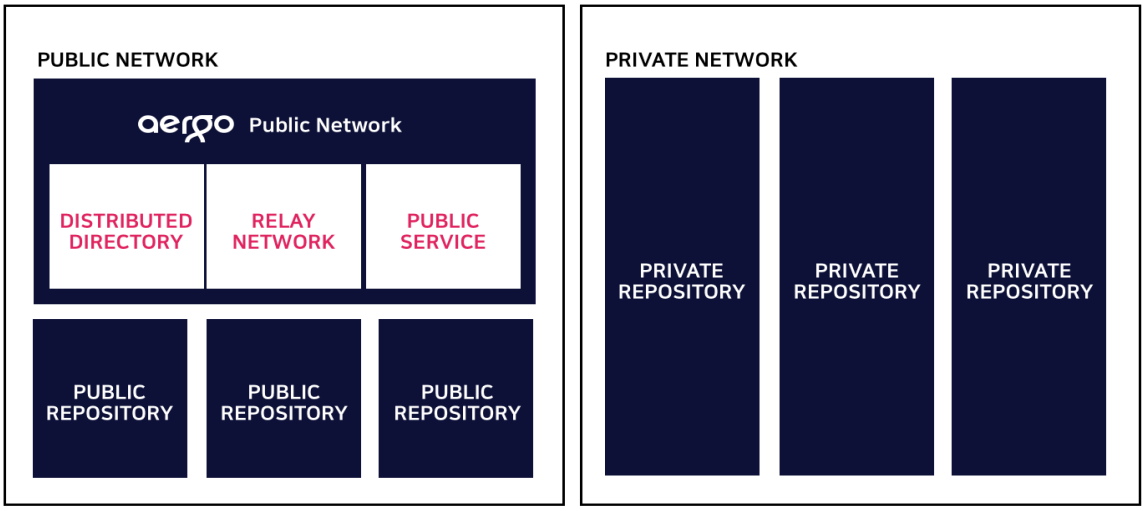


그림 9. AERGO 퍼블릭 및 프라이빗 저장소

AERGO 퍼블릭 저장소(AERGO PUBLIC REPOSITORY)

AERGO 퍼블릭 저장소의 목표는 dApp 을 위해 공유되고 공개된 분산 인프라를 구축하는 것이며, 이는 오픈소스 프로젝트 호스팅을 위해 사용되는 Git 의 퍼블릭 저장소나, 퍼블릭 클라우드 컴퓨팅에 쓰이는 자동 빌드 서버(Automated build server)와 비슷한 개념입니다.

퍼블릭 저장소는 읽기와 쓰기 엑세스가 모두 허용되며, 익명 사용자들에게 선택적으로 권한을 부여할 수도 있습니다. AERGO 퍼블릭 저장소의 일반적인 권한은 익명 사용자에게 읽기 전용(read-only anonymous access)으로 설정될 것입니다.

AERGO 프라이빗 저장소(PRIVATE REPOSITORY)

AERGO 프라이빗 저장소의 목표는 dApp 를 위해 제어되는 안전한 프라이빗 인프라 역할을 하는 것입니다. 이를 통해 엔터프라이즈 IT 시스템에 필요한 완벽한 액세스 제어, 어플리케이션 보안 및 성능, 데이터 컴프라이언스 및 QoS 가 가능하게 됩니다.

AERGO 프라이빗 저장소는 읽기 및 쓰기에 대한 완벽한 권한 제어를 보장합니다. 상위 브랜치(Parent branch)에서 새로운 브랜치를 생성해 퍼블릭과는 완전히 격리된 환경에서 블록을 관리할 수 있습니다. 해당 브랜치를 수용하는 특정 저장소에 대한 권한를 받은 경우에만 사용자들이 각 저장소의 블록에 접근할 수 있습니다.

AERGO 는 또한 Git 과 같은 중요 데이터 모델 및 명령 구조를 활성화함으로써, 블록의 브랜칭 아웃(branching out) 또는 머징(merging) 등의 기능을 실행합니다.

각 저장소에서 특정한 상태를 생성하기 위해서는 각각의 브랜치가 블록체인의 각기 다른 콘텐츠 스냅숏을 지칭해야 합니다. 새로운 브랜치의 생성도 가능합니다.

마지막으로, AERGO 에서의 “베스트 체인”이라는 개념은 마스터 브랜치(master branch)와 유사합니다.

퍼블릭과 프라이빗 두 유형의 저장소는 업계에서 검증된 블로코의 엔터프라이즈 솔루션인 코인스택의 구현 프레임워크와 API 호환성을 그대로 물려받았습니다.

AERGO 의 브랜칭(branching) 및 병합(merging) 개념은 다음과 같습니다.

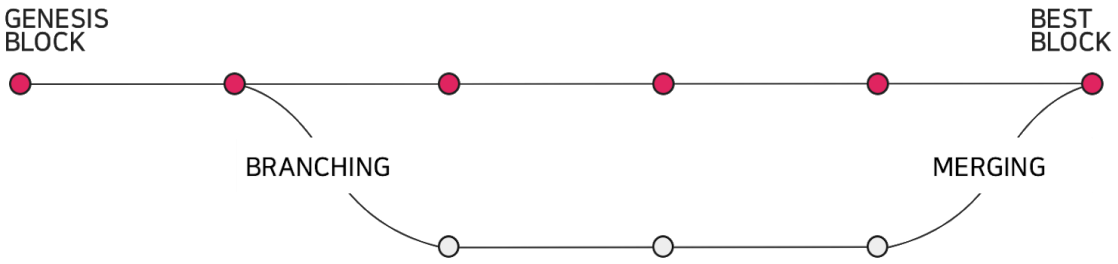


그림 10. 브랜칭(Branching) 및 머징(Merging)

사용자들은 AERGO 허브의 기능과 서비스를 활용해 AERGO 퍼블릭 저장소와 프라이빗 저장소를 생성하고 연결할 수 있습니다.

AERGO 허브(HUB)

AERGO **허브**는 기업 및 dApp 개발자들이 비지니스 또는 어플리케이션을 운용하기 위한 컴퓨팅 파워를 활용할 수 있는 퍼블릭 인터페이스입니다.

AERGO 허브는 AERGO 체인의 dApp 들과 연동됩니다. dApp 은 앞서 설명한 두 가지 저장소 중 하나에서 생성되고 저장됩니다. AERGO 허브는 아마존 AWS 처럼 검증된 퍼블릭 클라우드 웹 서비스와 비슷한 개념의 서비스를 제공하게 됩니다.

AERGO 허브는 아래의 기능 등을 포함해 다양한 고급 기능(아래 그림 11 참조)을 제공합니다.

1) 소프트웨어 마이크로서비스 지원

2) 콘텐츠 전송 네트워크(CDN)[18]

3) 서버리스 데이터베이스

4) 스마트 오라클 인터페이스(별도의 데이터베이스와 같은 외부 데이터 소스와 블록체인 연결)

5) 데이터 트래픽 / 메시지를 블록체인에 지능적으로 라우팅(route)하는 스마트 게이트웨이

그림 11. AERGO 허브 기능

요약하면, AERGO **허브**는 *AERGO 체인을 위한 퍼블릭 인터페이스*입니다.

[18] Wikipedia, The Free Encyclopedia.(2018). Content delivery network. Available: https://en.wikipedia.org/w/index.php?title=Content_delivery_network&oldid=841886968

AERGO 호드(Horde)

AERGO dApp 을 비롯해 블록체인에 최적화된 기타 지원 소프트웨어와 컴퓨팅 리소스 및 서비스는 통합과 공급, 배포, 관리가 필수적입니다.

이와 같은 기능은 AERGO 호드를 통해 제공됩니다. AERGO 호드는 인프라 제공을 위한 퍼블릭 통합(Public Orchestration)관리 및 소프트웨어 프레임워크입니다. 노드 제공자와 소프트웨어 벤더를 비롯해 AERGO 허브 생태계에 참여하고자 하는 서드파티 서비스 제공자들 역시 AERGO 호드를 활용합니다.

이러한 서비스 제공자들은 노드 역할을 수행하기 위해 AERGO 호드를 설치해야 하며, 이를 통해 각각의 자체 서비스를 AERGO 생태계와 연결할 수 있게됩니다. AERGO 호드는 오픈소스 기반의 퍼블릭 도메인 소프트웨어 프로젝트로 진행될 예정입니다.

AERGO 호드의 경우, 관리 및 효율성 확보를 위해 AERGO OS 라는 자체적인 운영체제와 함께 제공됩니다. 또한, 아래 그림과 같이 임베디드된 고성능 리눅스 커널과 관련 서비스를 연동시킬 수 있는 인터페이스와 구성 요소들을 제공하게 됩니다.

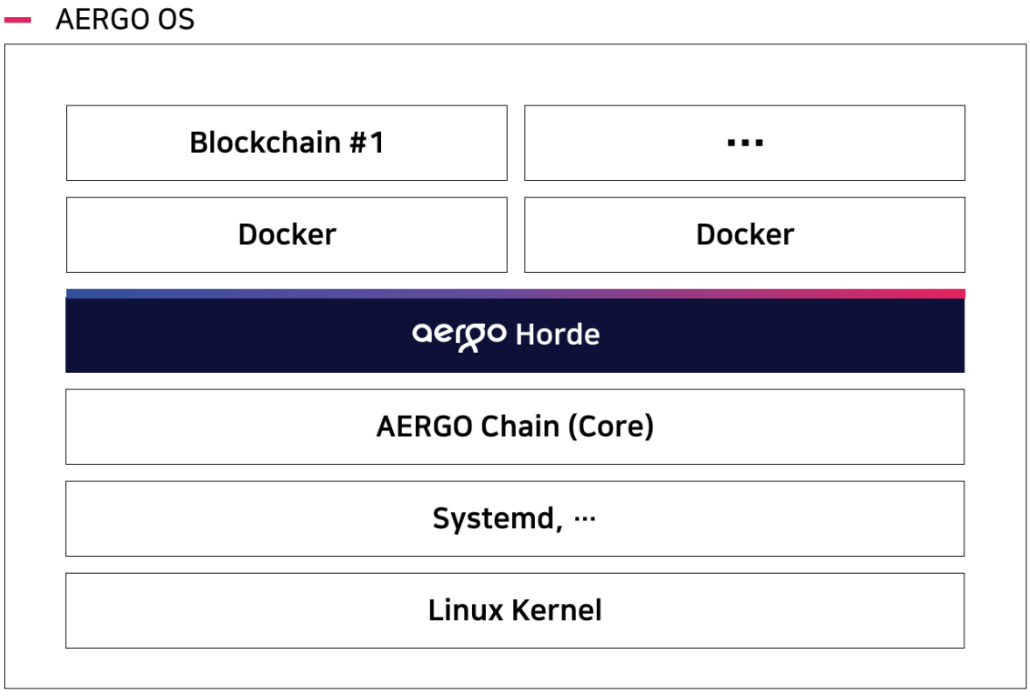


그림 12. AERGO OS 아키텍처

노드 제공자는 AERGO OS 를 통해 노드 정보를 체크하고, 리소스 사용과 생성된 블록 정보를 모니터링 하는 등 다양한 시스템 레벨 업무를 수행할 수 있습니다.

AERGO 마켓플레이스(Marketplace)

AERGO 마켓플레이스는 *AERGO 체인에 최적화된 소프트웨어 어플리케이션, 컴퓨팅 리소스 및 기타 서비스 등 필요한 핵심 요소를 모두 제공하는 원스톱 숍(One-Stop Shop)* 입니다.

AERGO 마켓플레이스 소프트웨어와 컴퓨팅 및 기타 서비스는 AERGO 체인과 호환됩니다.

AERGO 마켓플레이스는 AERGO 허브의 퍼블릭 인터페이스를 통해 접속이 가능하며, AERGO 호드를 통해 관리됩니다.

그 흐름은 아래 도표와 같습니다.

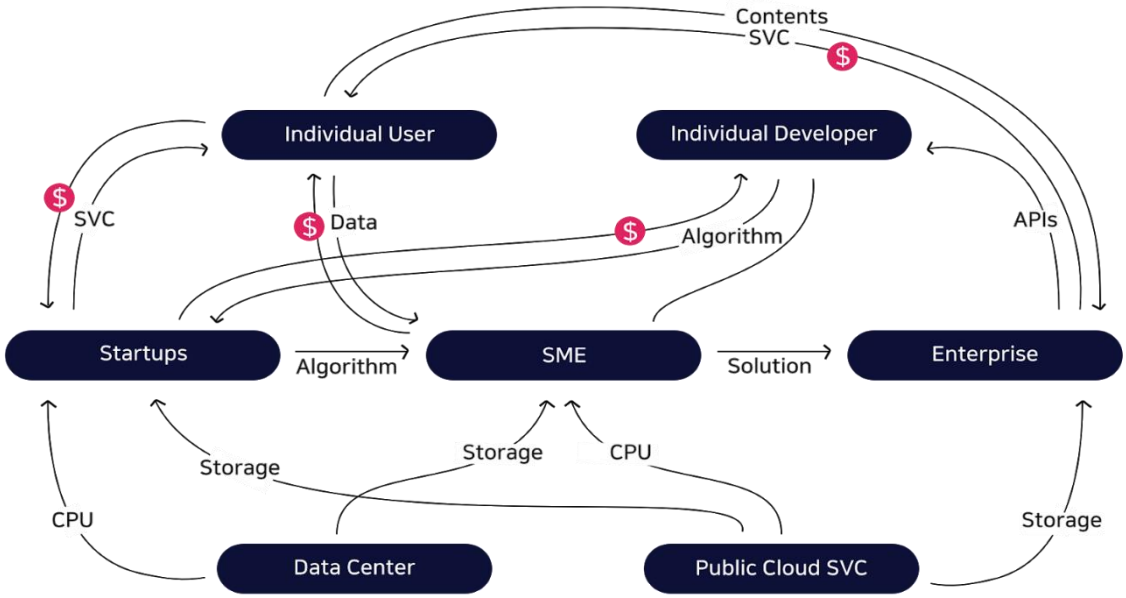


그림 13. AERGO 마켓플레이스

서비스 제공자, 개별 소프트웨어 벤더 및 클라우드 인프라 벤더 등 다양한 서드파티를 끌어들여 이들이 자체 제품 및 서비스를 AERGO 사용자들에게 제공할 수 있도록 하고자 합니다.

소프트웨어 개발자와 블록체인 프로젝트를 구축, 관리 및 운영하고자 하는 모든 유형 및 규모의 업체들이 AERGO 의 최종 사용자가 될 것입니다.

AERGO 마켓플레이스는 전통적인 클라우드 마켓플레이스와 유사합니다. 개인 소프트웨어 개발자, IT 계약업체 및 기업들(중소기업부터 다국적 엔터프라이즈 대기업)을 포함한 사용자들의 진입 장벽을 큰 폭으로 낮추는 것이 목표입니다.

또한, 구체적인 문제점 해결을 위해 AERGO 를 이용하고자 하는 국가 및 지역 정부기관도 지원할 계획입니다. 블록체인 기반의 안전하며 익명성이 보장되는 국민투표 시스템을 제공하는 것을 예로 들 수 있습니다. 블로코는 이미 코인스택을 기반으로 한국 지방 정부의 블록체인 기반 서비스를 구축하기도 했습니다.

AERGO 마켓플레이스는 비지니스 및 파트너 생태계로서 운영될 예정입니다. 혁신적인 블록체인 솔루션이 탄생하고, 상용화될 수 있도록 다양한 디지털 자원을 제공할 계획입니다.

추후 AERGO 마켓플레이스에서 제공될 디지털 자원은 다음과 같은 항목들이 포함될 수 있습니다.

- 연산력(CPU)
- 저장(확장 가능하며 초고속), 플래시 기반 메모리
- 콘텐츠 전송 네트워크(CDN)
- 기계학습 알고리즘
- 디지털 콘텐츠(신규 알고리즘 및 신규 소프트웨어 마이크로서비스)
- 전문 데이터베이스
- 스마트 컨트랙트 및 스마트 오라클(템플릿)
- 블록체인 IT 통합 설계도
- 디지털 신분 설계도
- 문서 타임 스탬핑(DTS 설계도)
- AERGO 블록체인 교육

AERGO 플랫폼에 더욱 다양한 모듈을 탑재할 계획이며, AERGO 생태계 참여 및 협력에 관심이 있는 사람들의 새로운 아이디어를 언제든지 환영합니다.

요약하자면, AERGO 마켓플레이스는 생동감 넘치고 개방적이며 지속가능한 생태계, 다시 말해 개인 개발자나 대형 소프트웨어 벤더들이 혁신적인 기술을 제공하는 곳으로 탄생할 예정입니다. 이러한 서비스들은 안전한 블록체인을 바탕으로 하는 차세대 비지니스 운영에 적합할 것으로 예상됩니다. 기반 IT 아키택처 역시 저비용의 분산 유틸리티 컴퓨팅 배포 모델을 기반으로 할 것입니다.

AERGO 토큰 [블록체인 네이티브 자산 및 토큰 모델]

AERGO 토큰은 AERGO 플랫폼에서 활용되는 유틸리티 토큰이며, 다양한 방식으로 활용될 수 있습니다. AERGO 토큰은 광범위하게 표현해 AERGO 생태계의 교환 매체라고 할 수 있습니다.

토큰 소지자는 AERGO 생태계에서 제공되는 특정한 서비스를 이용할 수 있는 권리를 갖게 됩니다.

토큰의 구체적인 용도는 다음과 같습니다.

- 스마트 컨트랙트 운영(AERGOSQL),
- DPOS 합의 알고리즘,
- 코인스택(COINSTACK) 4.0 상 블로코의 기술 지원에 대한 지불수단,
- AERGO 허브 서비스에 대한 지불수단,
- AERGO 마켓플레이스 서비스 및 자산에 대한 지불수단,
- AERGO 도메인에 대한 지불수단

또한, AERGO 토큰은 플랫폼에서 양도도 가능합니다.

AERGO 메인넷은 2019 년 초(현재 목표는 2019 년 1 분기)에 출시될 예정입니다.

우선 AERGO 토큰은 블로코의 코인스택(COINSTACK) V4.0 에서 제품 및 서비스를 이용하거나 구매하는데 사용할 수 있습니다.

AERGO 토큰의 유통 및 사용 사례를 보면 다음과 같습니다.

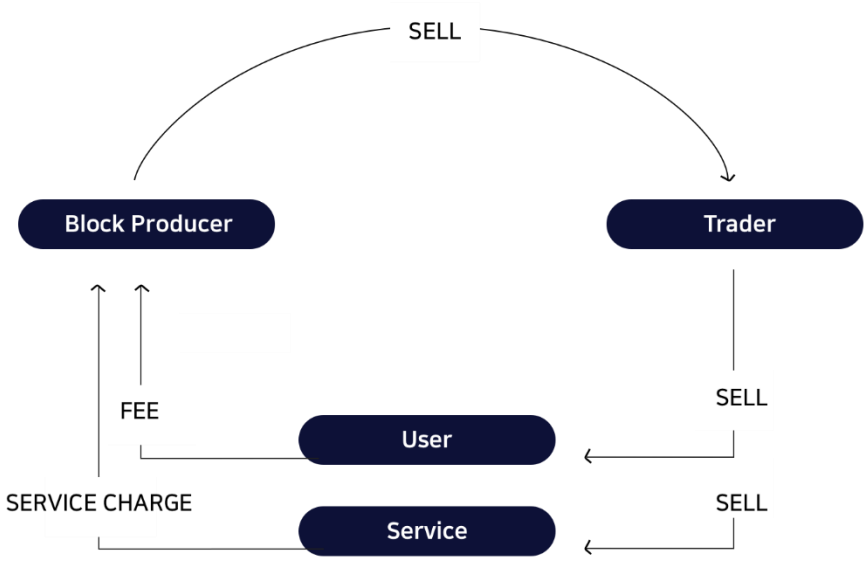


그림 14. AERGO 네이티브 자산 유통

AERGO 토큰 분배 및 자금의 운용

토큰 분배

총 500,000,000 개의 AERGO 토큰이 발행될 예정입니다. 토큰의 용도별 할당은 아래와 같으며, 상황에 따라 변경될 수도 있습니다.

Proportion of Tokens for Sale	30%
AERGO community incentives and strategic partners	30%
Reserved by token issuer	25%
Advisors and key backers	10%
Employees of token issuer and affiliates	5%

자금 운용

토큰 세일을 통해 모인 금액은 AERGO 의 기술 프로그램 및 파트너 생태계의 개발 및 발전에 사용될 예정입니다. 자금 운용 비율은 아래와 같으며, 상황에 따라 변경될 수도 있습니다.

R&D	40%
Ecosystem incubation	30%
Marketing	15%
Strategic alliances and business development	10%
Miscellaneous	5%

개발 로드맵

AERGO 체인, AERGO 허브 및 AERGO 마켓플레이스의 개발 로드맵 및 출시 일정은 아래와 같습니다.

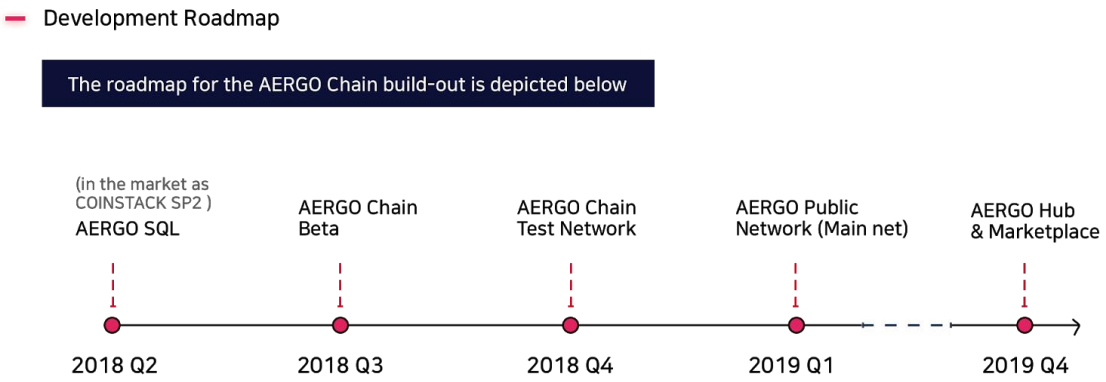


그림 15. AERGO 개발 로드맵

이 로드맵은 변경될 수 있습니다.

AERGO 기반 프로젝트 구축에 관심을 보인 초기 도입 기업 고객의 요구 등에 따라 일정이 변경될 수도 있으며, 상기 로드맵 상 제시된 일정과 비교해 일찍(또는 늦게) 특정 기능이 출시될 수도 있습니다.

실행 계획

AERGO 프로젝트는 매우 야심찬 장기적 목표를 토대로 진행되고 있습니다. AERGO 플랫폼의 핵심 기능들은 꾸준히 출시될 예정이며, 이미 상당한 수의 구성 요소들이 개발 진행 중에 있습니다.

AERGO 프로젝트를 본격적으로 시작하기 위해 다음과 같이 블로코의 핵심 역량을 활용할 예정이며, 이는 AERGO 전체 프로그램의 일환이기도 합니다.

블로코 코인스택(COINSTACK) 및 블로코 노하우 공유

블로코는 AERGO 플랫폼에 다양한 기존 제품과 서비스 및 노하우를 제공합니다. AERGO 의 발전 가능성에 관심을 표시한 기존 고객군 역시 활용할 계획입니다.

블로코는 AERGO 플랫폼의 발전에 다음과 같이 기여하게 됩니다.

- **코인스택(COINSTACK)을 통한 AERGO 프로토콜의 초기 핵심 기술 제공**
  AERGO 프로토콜은 코인스택에서 입증된 다양한 주요 기능을 이어받게 됩니다.
- **입증된 엔터프라이즈 구현 모델 확보**
  AERGO 는 향후 기업 고객들의 테스트 및 채택을 위해 개인정보보호 규정을 준수하는 안전한 구현 프레임워크를 제공합니다. 블로코는 실사례에서 검증된 구현 프레임워크를 AERGO 와 그 사용자들을 대상으로 공유하게 됩니다.
- **블로코의 기존 기업 및 향후 클라이언트 유치**
  블로코는 현재까지 20 곳 이상의 유료 고객을 확보했으며, 그 이상의 코인스택 기반의 블록체인 시스템을 구축해오고 있습니다. 블로코는 기존 고객을 대상으로 현재 구축된 것보다 상위 버전의 형태로 제안하고자 합니다. 이는 특히 운영 관리 미흡 및 개인정보 보호 등의 문제로 인해 퍼블릭 블록체인 활용을 꺼려하는 기업들에게 유용할 것입니다.
- **AERGO 기반 제품의 출시 및 직접적인 서비스 지원**
  블로코는 클라이언트들을 위한 자체적인 코인스택 COINSTACK) 솔루션을 구축하고 이것과 연결될 수 있는 효과적인 공개 프로토콜로서 AERGO 를 발표, 판매할 예정입니다. 또한, AERGO 기반 제품 및 서비스를 직접적으로 지원할 계획입니다.
- **AERGO 의 전략적 기술 파트너**
  블로코는 AERGO 와 관련해 기술 개발 뿐만 아니라 직접적인 기술 지원도 제공할 예정입니다. 또한 AERGO 는 한국과 홍콩, 런던 기반으로 진행 중인 블로코의 수준 높은 상용화 관련 연구 개발과 IT 통합 및 지원 역량을 활용하게 될 것입니다. 블로코는 전 세계적으로 지속적으로 사업을 확장해 다른 여러 국가들 및 지역에서 사업 기반을 구축해 나갈 예정입니다.
- **블로코의 기존 인프라 및 블록체인 파트너 활용**
  블로코는 AERGO 생태계의 확장을 지원합니다. 수많은 기술 파트너들이 AERGO 생태계 구축을

위해 협력하고 생태계 발전에 참여하겠다는 의사를 밝혔습니다. 여기에는 전문 SQL 개발 회사, 클라우드 인프라 제공자 및 글로벌 통신사가 포함되어 있습니다.

- **기타 서드파티 지원자 생태계 지원 활동**
  새로운 기술적 혁신을 만들고, 다양한 부가가치 파트너를 발굴하며, 오픈소스 및 소프트웨어 개발자를 지원하는 것이야말로 AERGO 생태계의 핵심 구성 요소입니다. AERGO 이해 관계자들을 발굴하고 협력하는 것은 프로젝트의 기반이 될 것이며, 주요 산업 및 정부 부문의 전략, 기술 및 IT 서비스 관계 개발도 포함됩니다.

  AERGO 이해관계자 생태계를 촉진하고 개발하기 위해 상당한 자금이 투입될 예정입니다. 이러한 노력들을 지원하고 이끌 수 있는 역량을 갖춘 자문 패널도 구성되었습니다. 이 패널에는 블록체인, 분산형 데이터베이스, 유틸리티 컴퓨팅, 디지털 통신, 클라우드 컴퓨팅, 빅 데이터, 머신 러닝/AI, 가상화, 오픈소스 기술, 오픈소스 라이선싱, 컴퓨터 프로그래밍, 보안, 오픈소스 비지니스 개발, 금융 및 투자 은행 거래, 정부 관계 및 전략적 파트너 사업 개발 부문 등에 있어서의 세계 최고 전문가들이 포함되어 있습니다.

AERGO 팀원 관련 정보는 부록-D 에서 확인 가능합니다.

부록(APPENDICES)

부록-A: 블록체인 및 오픈 플랫폼 기초

비트코인은 현재까지 가장 잘 알려진 가상 암호화 화폐라고 할 수 있습니다. 비트코인의 경우 퍼블릭부문 및 정부 규제당국으로부터 상당한 관심을 받아 왔습니다. 그 이유는 익명(또는 때로 불법) 거래가 자주 이용되고 가치 변동성이 높기 때문일 것입니다.

본 AERGO 백서는 시장에서 통용되는 비트코인과 수많은 기타 "알트코인" 화폐들이 아니라, 이러한 코인이 운영되고 존재하는 새로운 기술 아키텍처에 초점을 맞추고 있습니다. 블록체인이 바로 그 기술에 해당된다고 할 수 있습니다.

블록체인은 지극히 단순한 수준에서 분산되는 안전한 데이터베이스일 뿐입니다. 퍼블릭 블록체인은 리눅스나 하둡(Hadoop)의 경우처럼 오픈소스입니다. 즉, 하나의 소프트웨어 기업이 해당 기술을 소유하는 것이 아니라 개발자들이 전 세계적으로 개방적인 투명한 프로세스를 통해 기술을 개발합니다.

블록체인은 분산 원장 시스템에서 디지털 거래를 승인하고 수용하는 자율적인 방식을 보장하기 위해 정교하고 지능적인 암호화 기술(소위 알고리즘)을 활용하는 독창적인 기술입니다. 또한 합의 알고리즘은 블록체인 상에서의 거래와 데이터 공유, 컴퓨터에 대한 푸시 아웃(push-out) 방식 등에도 영향을 미칩니다. 블록체인 기술은 시스템에 기록되는 거래를 신뢰할 수 있게끔 쉽게 변경할 수 없도록 해 줍니다. 이러한 신뢰되는 서로를 거의(또는 전혀) 신뢰하지 않는 당사자들에게도 적용됩니다.

블록체인의 혁신적인 측면은 블록체인이 매개체 역할을 함으로써 인간이 없이도 작동하는 시스템이라는 점입니다. 데이터베이스 기술이 50 년 넘게 사용되어 왔음에도 불구하고, 이러한 기능은 예전에는 전혀 가능하지 않았던 새로운 차원입니다.

블록체인 활성화 시스템을 통해 디지털 자산 및 관련 거래들을 보편적이고 신뢰할만하며 전체적으로 파괴가 불가능한 단일 등록부 형태로 작성할 수 있게 됩니다. 블록체인은 디지털 자산(또는 단순한 데이터)이 교환되는 시스템에 있어 필수적인 기본 서비스를 제공하기 위해 사용될 수 있습니다. 현재 활용되는 도구들보다 더욱 효율적이고 개선된 방식으로 사용될 수 있는 것입니다. 그 중 한 가지가 블록체인 기술을 통해 실행 가능하고 분산된 암호화 거래 기록, 즉 분산된 수많은 데이터의 전통적인(잠재적으로 보안성이 떨어지는) 마스터 데이터베이스를 대체하는 분산된 분산 원장을 생성하는 것입니다. 이를 통해 여러 다양한 디지털 시스템들의 안정성과 신뢰성을 높이는 한편 그 절차나 관련 비용을 큰 폭으로 줄일 수 있는 가능성이 존재합니다.

또한 블록체인 기술을 통해 디지털 네트워크를 지속적으로 이용하면서 직접적이고도 명확한 가치의 이전을 위한 메커니즘을 제공하는 디지털 자산이나 토큰을 생성할 수도 있습니다.

그 외에도 현재 이용하는 것보다 훨씬 더 개선된 신원 확인 및 이용 수단을 제공합니다. 신원은 암호화되어 저장될 수 있기 때문에 블록체인 네트워크를 이용하는 개인들은 자신의 개인정보를 보호하는 동시에 신원을 인증할 수도 있습니다.

블록체인은 그 소유권에 대한 불가침 기록과 함께 위조 불가능한 고유의 신원을 제공함으로써 잠재적으로 물리적 자산의 직접적인 양도를 대폭 간소화하고 그 출처에 대한 신뢰를 높이는 역할을 할 수 있습니다.

블록체인의 프로그래밍 역량들은 소위 “스마트 컨트랙트”을 통해 활성화됩니다. 스마트 컨트랙트는 기본 가치 단위를 제어할 수 있는 능력을 가진 이벤트 기반 컴퓨터 프로그램입니다. 요약하자면, 스마트 컨트랙트는 자동 업무 실행 및 정산을 목적으로 설계된 프로그램입니다. 이것은 dApp 가 블록체인 시스템에서 가치의 대부분을 해제(unlock)하도록 만드는 어플리케이션 계층입니다(아래 그림 16 참조).

업체들은 스마트 컨트랙트를 통해 금융거래의 가치나 기타 디지털 협약을, 암호화를 통해 보장되는 비지니스 로직의 형태로 통합함으로써, 자율적으로 가치를 이행하고 이전할 수 있게 됩니다. 요약하자면 비지니스 업무들은 자동 실행, 자동 점검, 자동 집행 및 자동 기록을 위해 블록체인 자체에서 안전하게 암호화 및 내장됩니다.

따라서 스마트 컨트랙트는 블록체인을 통해 직접 작성, 편집됩니다. 즉, 요청이 있을 경우 자동으로 실행되게끔 블록체인 자체에 포함되어 있습니다.

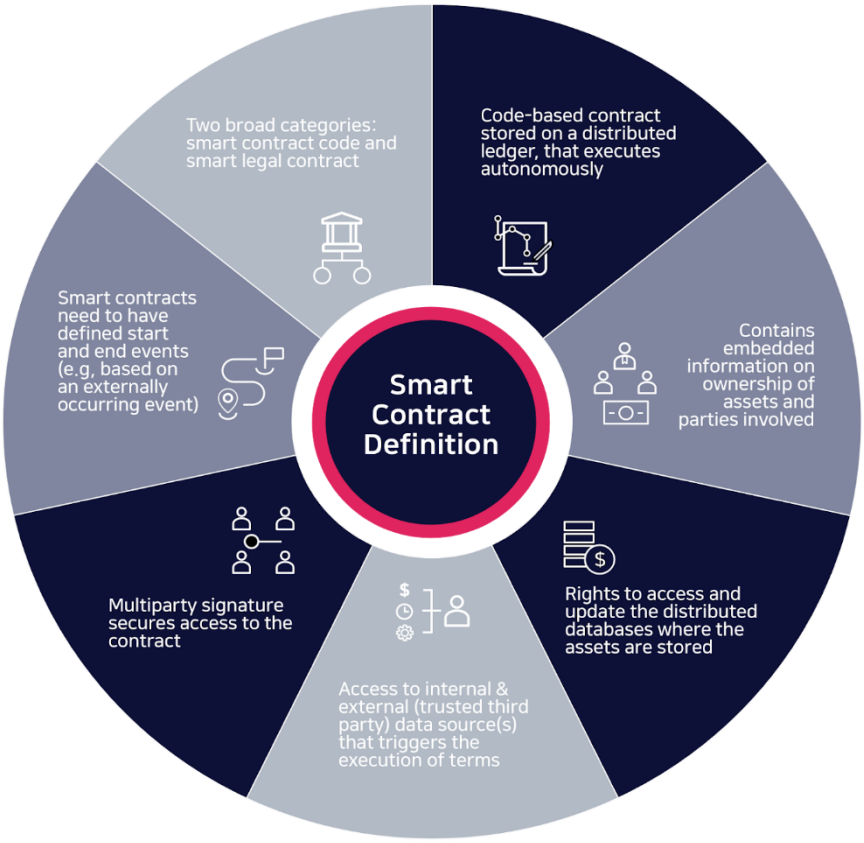


그림 16. 스마트 컨트랙트[19]

[19] Everest Group.(2016). Smart Contracts: Realizing the Benefits of Blockchain. Available: https://www.everestgrp.com/2016-10-smart-contracts-realizing-benefits-blockchain-36282.html/

블록체인의 경우 독립적인 네트워크 외부 데이터에 대한 접속이 불가능합니다. 따라서, “스마트 오라클”이라는 스마트 컨트랙트 관련 중요 기능이 추가적으로 제공됩니다.

(블록체인의 맥락에서) 스마트 오라클은 스마트 컨트랙트의 활용을 위해 실시간으로 발생 건을 찾아 확인하고 블록체인에 해당 정보를 제공하는 외부 에이전트이자 프로그램이라고 할 수 있습니다. 스마트 오라클은 외부 데이터를 제공하고 스마트 컨트랙트를 “유발” 합니다. 실제로 스마트 오라클은 서드파티 “데이터 피드” 입니다. 이것은 안전하고 신뢰할만한 방식으로 해당 정보를 제공합니다.

스마트 오라클은 실제로 소프트웨어 오라클, 하드웨어 오라클, 컨센서스 오라클, 인바운드 및 아웃바운드 오라클의 형태가 될 수 있습니다. 이것들의 경우 서드파티 서비스인 관계로 신뢰성 확보를 위해서는 추가적인 관리가 필요합니다.

블록체인에서 구축되는 시스템이 스마트 컨트랙트를 사용할 경우 시스템 사용자에게 신뢰할 수 있고 안전한 정보를 제공하는 것이 매우 중요합니다. 실수가 발생할 경우 심각한 결과를 초래할 수도 있습니다. 스마트 컨트랙트는 자율적으로 실행되며, 핵심적인 비가역성으로 인해 블록체인에 대한 롤백(rollback)은 없습니다.

요약하자면, 스마트 오라클은 실시간 데이터와 스마트 컨트랙트 사이의 “인터페이스”라고 할 수 있습니다.

전반적인 블록체인 정보 기술(“IT”) 스택은 아래 그림 17 의 내용과 같습니다.

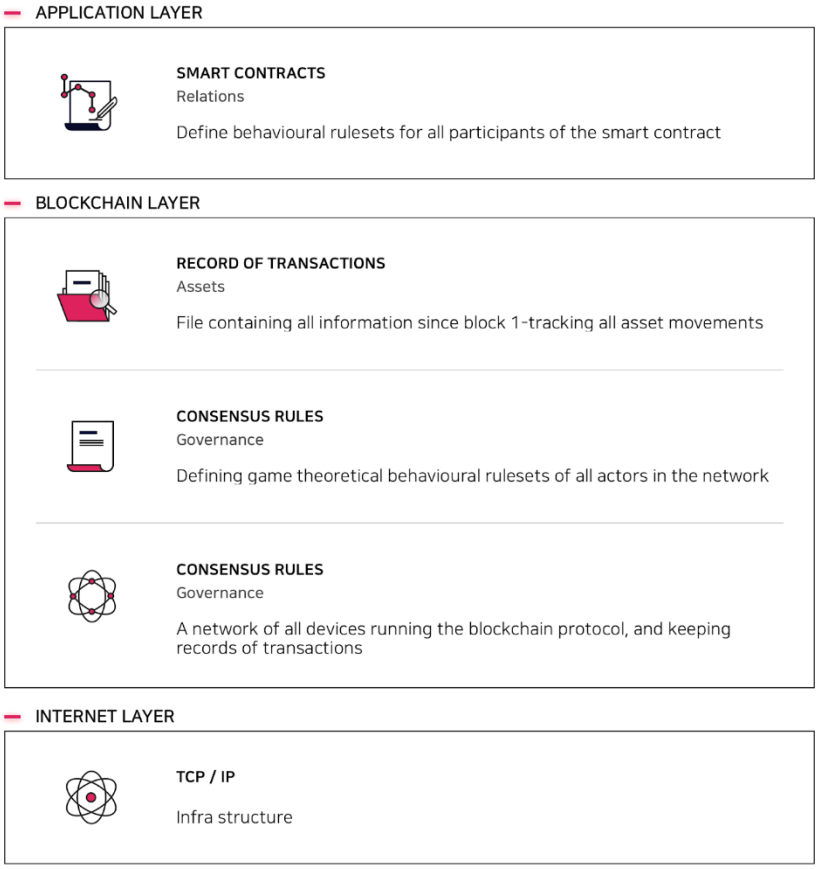


그림 17. 블록체인 IT 스택

블록체인의 주요 비지니스 기능은 아래 표-18 과 같습니다.

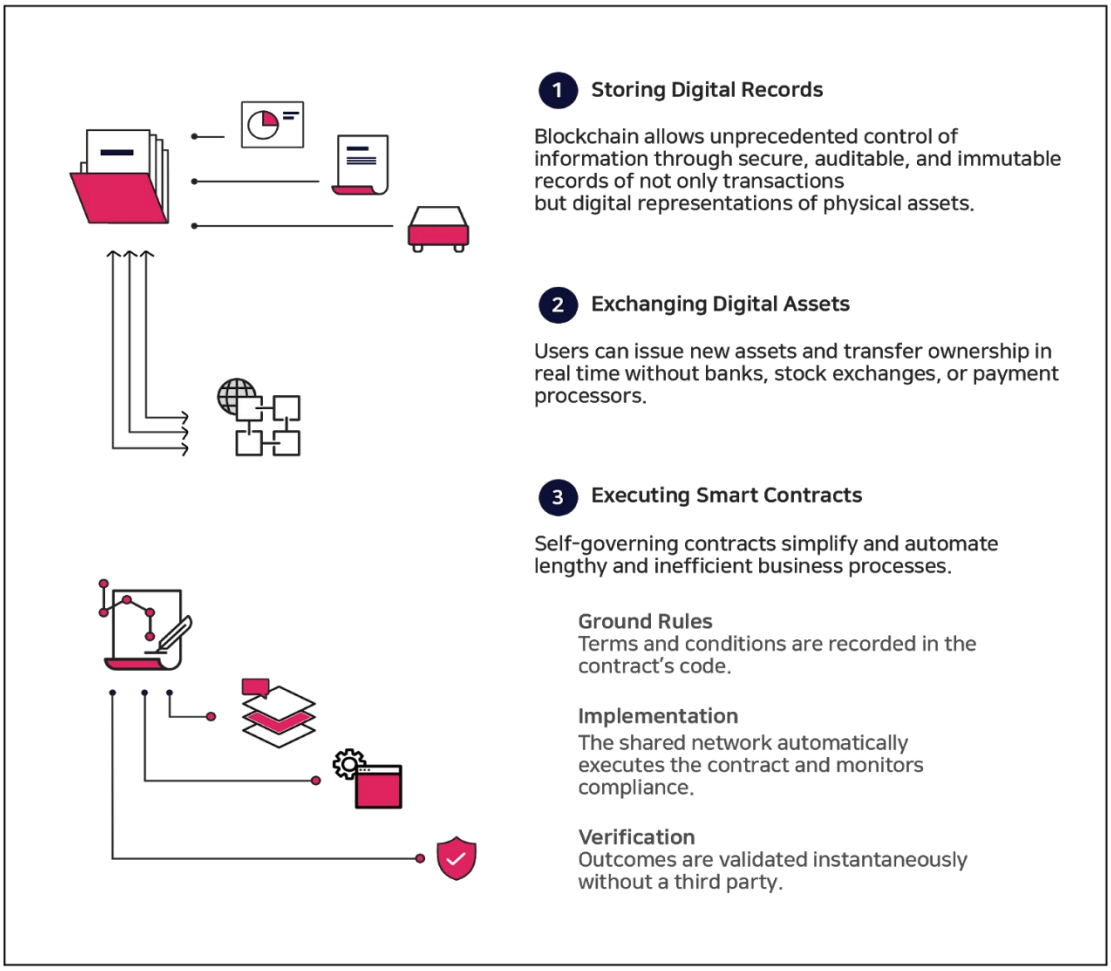


그림 18. 블록체인의 비지니스 기능

두 가지 형태(퍼블릭 및 프라이빗 프로토콜)의 블록체인의 주요 기능에는 각 시스템의 신뢰 및 통제 수준이 포함됩니다. 신뢰 및 통제는 주로 사용되는 블록체인 아키텍처와 소프트웨어 합의 알고리즘의 특성에 따라 결정됩니다. 통제가 증가하면 신뢰 분산이 감소할 수 있고, 신뢰 분산이 감소하면 통제가 증가할 수 있습니다. 확장 배포되면서 처리량 역시 블록체인의 심각한 문제가 되고 있습니다.

퍼블릭 블록체인의 경우 비트코인처럼 참여를 최대화할 수 있는 가능성을 제공하고 참여가 증가하면 네트워크에 컴퓨터 "노드"가 늘어납니다. 블록체인의 합의 알고리즘을 운영하는 대규모의 노드 네트워크의 경우 신뢰도 분산이 커지게 됩니다. 그러나 이 경우, 개별 주체가 이러한 컴퓨터 리소스보다 중요한 지위를 차지하게 되면 그 제어가 어려울 수 있습니다. 현 세대의 프로토콜과 작업 증명(Proof-of-Work) 합의 알고리즘을 운영하는 대규모 블록체인 네트워크들의 경우 매우 비효율적이라고 할 수 있습니다. 이들 네트워크는 노드를 운영하고 신규 거래를 검증하는데 많은 에너지를 소모합니다. 거래의 분산 또한 매우 느리게 이루어집니다.

하이퍼 레저 패브릭(Hyper Ledger Fabric) 등 프라이빗 블록체인에서는 특정 블록체인 네트워크에 속하는 당사자들(노드들)을 훨씬 더 엄격하게 관리합니다. 노드들 간에 효과적으로 설계된 네트워크 인터페이스와

함께 최첨단 컴퓨터, 메모리 및 솔리드 스테이트 디스크를 활용함으로써 처리량을 늘릴 수 있습니다. 그러나 네트워크들의 경우 퍼블릭 프로토콜에 비해 그 규모가 훨씬 작기 때문에 상대적으로 신뢰 분산이 감소하는 경우가 많습니다. 따라서 보다 새롭고 혁신적인 합의 알고리즘이 필요하다고 할 수 있습니다.

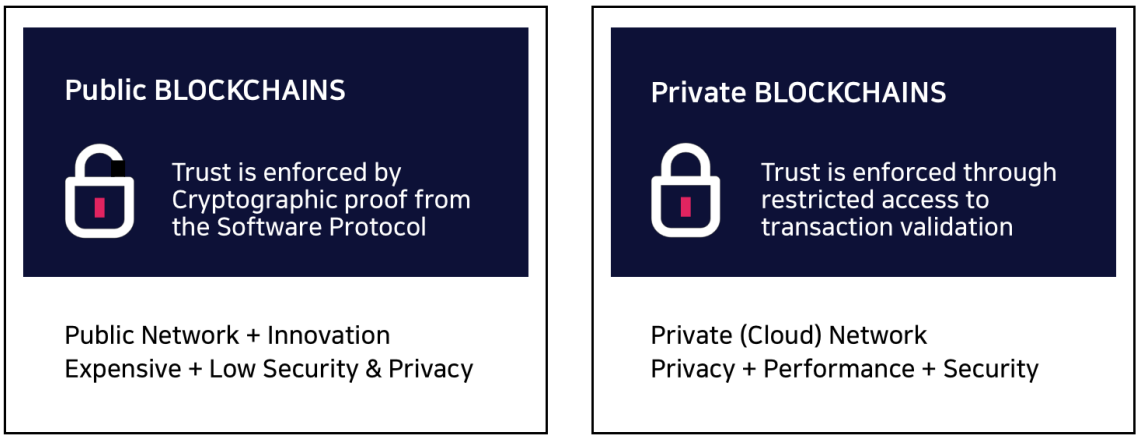


그림 19. 무허가형(퍼블릭) vs. 허가형(프라이빗) 블록체인

기업들이 퍼블릭 블록체인과 프라이빗 블록체인 중 어떤 것을 선택할지의 여부는 몇 가지 주요 고려사항에 따라 결정되게 됩니다.

(i) 거래 관련 신뢰를 극대화해야 할 필요성

(ii) 시스템 제어

(iii) 전반적인 성능 처리량

예를 들어, 신뢰성과 보안 측면이 매우 중요한 은행거래 부문에 있어서 프라이빗 블록체인은 기존 데이터베이스 및 시스템을 대체하기 위해 설계되고 있습니다. 이와 관련해서는 아래 도표에 설명이 나와 있습니다.

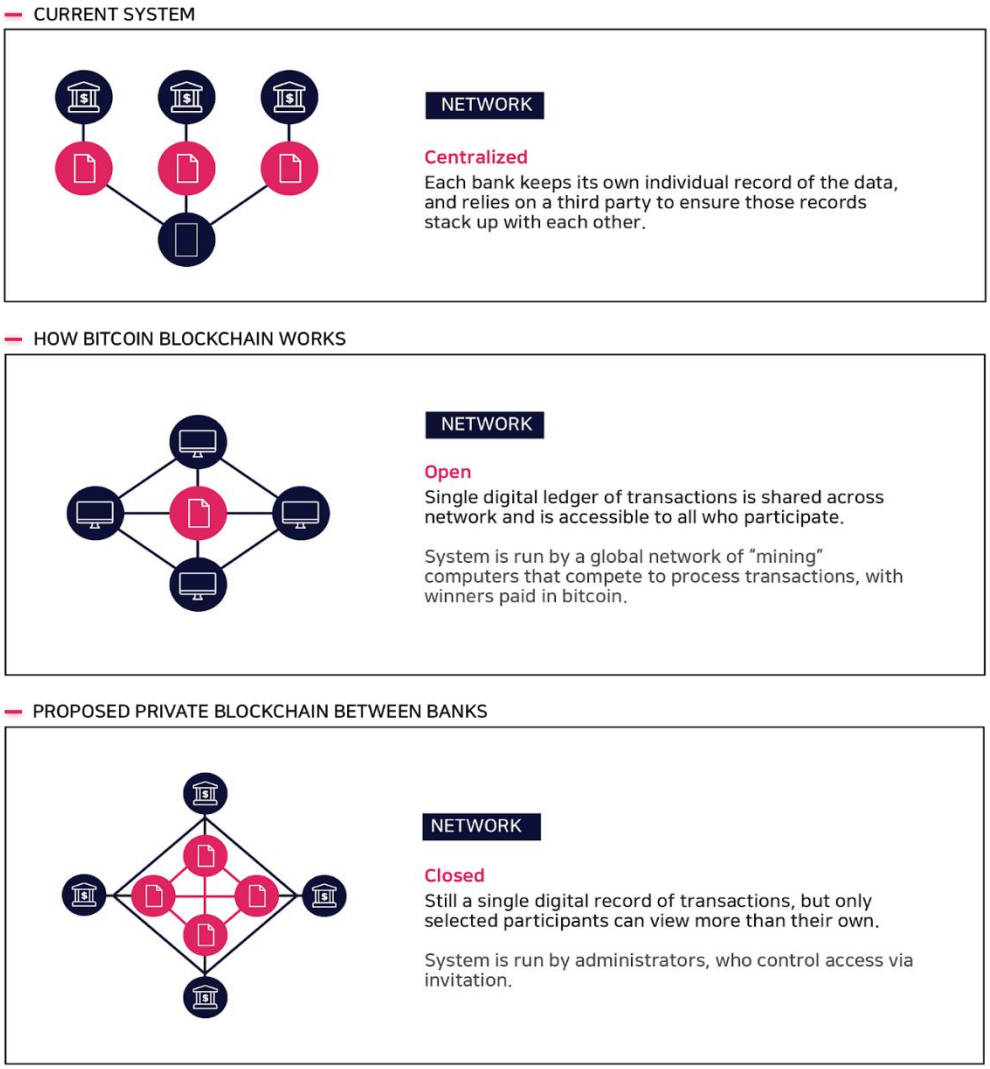


그림 20. 은행 간 블록체인 네트워크 사례

시장 및 고객들은 어떤 방식을 지지해야 할지 혼란스러울 것입니다. 부분적으로는 이러한 이유로 인해 상당한 규모로 생산되고 확장 중인 블록체인 배포 사례가 많지는 않은 상황입니다.

블록체인이 피어투피어(P2P) 구현의 훌륭한 사례이긴 하나, 다음과 같은 이유들로 인해 대량 데이터의 저장이 항상 이상적이지만은 않다고 할 수 있습니다.

(1) 확장성: 블록체인이 느릴 수 있다

(2) 데이터 보호: 특히 데이터가 제대로 보호되지 않고 적합한 관리 액세스 제어를 적용 받지 못하는 경우, 블록체인은 개인정보 보호와 관련해 몇 가지 문제점을 유발할 수 있다(잊혀질 권리 등).

이 부분들은 이와 관련해 현재 블록체인이 상당히 개발되고 있고 향후 수년 뒤에는 적합한 솔루션이 발견될 것으로 예상되는 영역들입니다.

이러한 문제점에도 불구하고 당사는 블록체인이 차세대 인터넷과 분산형 웹의 강력한 추진 요소가 될 것이라고 믿어 의심치 않고 있습니다. 블록체인은 중개자 없이 실제 거래를 가능하게 할 것이며 이것이 최초로 입증된 사례가 바로 비트코인인 것입니다.

동일한 블록체인 기술을 활용해 모든 산업 분야의 기업들이 보다 개방적인 비지니스 생태계에서 새로운 분산 서비스를 구축할 수 있을 것으로 기대됩니다.

공개 플랫폼이 미래입니다

수 년 후에는 이러한 "플랫폼"이 안전한 전자상거래 서비스의 대규모 모바일 채택과 함께 서버리스 유틸리티 컴퓨팅 아키텍처에서 호스팅 되는 블록체인 상에서 운용되는 혁신적인 dApp 를 조합하여 다양한 업계의 환경 및 비지니스 모델을 변화시킬 것으로 전망됩니다.

동아시아 지역에서 상당한 성공을 거둔 위챗(WeChat)[20] 메신저 어플리케이션은 이러한 개방적인 개발자 및 서드파티 친화적 생태계의 대규모 사례에 해당된다고 할 수 있습니다.

위챗은 블록체인 자체와 관련된 참조 모델이라고는 할 수 없으나, 향후 개방형 생태계가 구축 및 운영되는 방식에 대한 참조 모델은 될 수 있습니다. 더욱 중요한 점은 AERGO 를 비롯한 새로운 디지털 플랫폼이 사용자, 개발자, 기업 고객, 서드파티 및 업체들에게 공개될 때 새로운 사업 가치가 어떻게 창출될 수 있는지 보여준다는 것입니다.

2011 년 중국에서 텐센트(Tencent)가 메시징 앱으로 도입한 위챗은 사용자들을 위한 라이프스타일 플랫폼으로 발전했습니다. 매월 10 억 명 이상이 이 서비스를 적극적으로 활용하고 있으며 현재 서구에서 페이스북, 왓츠앱, 메신저, 벤모, 그럽허브, 아마존, 우버, 애플페이 등이 제공하는 모든 서비스를 사용자들에게 제공하고 있습니다.

위챗은 사용자들에게 제공하는 다양한 혜택을 바탕으로 모든 사용자를 통제하는 앱으로 등장했습니다.

모바일을 우선시하는 중국에서 위챗은 사용자들의 다양한 삶의 측면을 다루는 '모바일 라이프스타일'을 구축하고 있으며 현재 사용자들은 하루 평균 10 번 가량 위챗을 열고 매일 같이 약 40 분간 이 앱을 이용하고 있는 것으로 조사되고 있습니다[21]. 2011 년 텐센트(바이두 및 알리바바와 함께 중국 3 대 기술 기업으로 꼽히고 있음)가 단순하게 문자 발송만을 목적으로 하는 메시징 어플리케이션으로서 출시했던 위챗은 단순한 '앱'에서 '플랫폼'으로 발전한 것입니다.

위챗은 모바일을 중시하는 중국 시장에서 직, 간접적으로 매우 강력한 네트워크 효과의 혜택을 입었다고 할 수 있습니다. 플랫폼에 참여하는 사용자들이 늘어나면서 친구 및 가족들과 연락을 하기 위해 가입하는 사용자들이 훨씬 더 많아졌습니다. 처음에는 많은 아시아계 미국인들이 중국의 친척들과 연락하는 수단으로서만 위챗을 이용했습니다.

위챗은 놀랍게도 자체 플랫폼에서 보완 서비스나 완전히 새로운 서비스를 제공하는 서드파티 개발자들에게 플랫폼을 개방했습니다. 규모의 경제가 발생하며 플랫폼 사용자가 늘어날수록 해당 플랫폼에서 서비스를 제공하고자 하는 서드파티 개발자들이 늘어났으며, 다시 플랫폼 사용자들도 늘어나는 선순환이 이어졌습니다.

---

[20] Tech Node.(2017). *WeChat User & Business Ecosystem Report 2017*. Available: https://technode.com/2017/04/24/wechat-user-business-ecosystem-report-2017/

[21] Lily Kuo.(2014). *WeChat is nothing like WhatsApp—and that makes it even more valuable.* Available: https://qz.com/179007/wechat-is-nothing-like-whatsapp-and-that-makes-it-even-more-valuable/

이렇듯 엄청난 네트워크의 효과와 더불어 다양한 어플리케이션이나 서비스에 접속할 필요가 크게 줄어드는 멀티 호밍(Multi-homing) 경우가 늘면서, 위챗은 앱 플랫폼 더 나아가 이들 모두를 통제하는 생태계로 발전하게 되었습니다.

아래에 나와 있는 내용은 위챗이 사용자들뿐만 아니라 해당 생태계에 참여하는 브랜드/기업/서드파티 개발자들에게 제공하는 인센티브들입니다.

위챗은 사용자들에게 아래의 용도들과 관련된 단일의 통합 앱을 제공합니다:

- 가족 및 친구를 상대로 한 문자/음성메시지 발송
- 소셜미디어 공유
- 유명인사 및 브랜드의 팔로우
- 택시 예약
- 음식 배달 주문
- 병원 예약
- 영화 표 구매
- 게임
- 지인에게로의 자금 이체(레드 엔빌로프(red envelopes))
- 청구서 요금 지불 — 공과금, 식당 계산서 등.
- 특정지역 대상 쿠폰 검색
- 잡지 기사 열람
- 낯선 주변 사람들과의 만남

위챗은 상인/브랜드에게 지불, 로케이션, 다이렉트 메시지, 음성, 사용자 ID 등을 제공함으로써 사용자 참여를 유도할 수 있는 개별 통합 앱을 제공합니다.

또한 상인들은 뉴스를 퍼뜨리고 고객별 맞춤 홍보를 가능하게 하는 CRM(고객관계관리) 플랫폼의 용도로 위챗을 활용하고 있습니다. 위챗은 유명인사, 은행, 언론매체, 패션 브랜드부터 병원, 약국, 자동차 제조사, 인터넷 신생기업, 개인 블로그 등여 1 천만 이상의(인증된) 공식 계정을 보유하고 있습니다.

그리고 이 플랫폼은 극히 개발자 - 친화적인 특성을 갖고 있습니다. 개발자들은 위챗의 표준적인 외관과 느낌을 유지할 필요가 없기 때문에 완전히 새로운 차별화 서비스를 개발, 적용할 수 있습니다. 그 결과 사용자들은 위챗 플랫폼 상에서 완벽한 웹 앱 경험을 할 수 있습니다. 2014 년 위챗 관련 연간 라이프스타일 지출 총 규모는 주로 엔터테인먼트 및 공식 계정으로 인해 미화 약 18 억 달러 수준인 것으로 추정된 바 있습니다.

그림 21 에는 위챗 생태계에 대한 내용이 포함되어 있습니다.

아마 가장 중요한 것은 위챗이 플랫폼에 가입하는 사용자에게 요금을 부과하지 않는다는 점일 것입니다. 위챗 서비스는 완전히 무료로 제공되고 있습니다. 이 외에도 플랫폼에서 서비스를 제공하는 모든 상인들에 대한 심사 및 인증 절차를 진행함으로써 생태계의 신뢰도를 보장하려고 노력하고 있습니다.

당사의 경우, 위챗 지원팀이 현재 블록체인을 활용해 훨씬 더 새롭고 안전한 부가가치 서비스를 플랫폼에

구축 내지 추가할 수 있는 방법을 모색 중입니다.

"모멘트(Moments)"(또는 해당 플랫폼의 중국 버전에서 "프렌즈 서클(Friends' Circle)")라고 하는 위챗 모듈에 대한 최근 포스트에서 마화텅 회장(위챗을 개발한 중국 인터넷 대기업 텐센트의 최고경영자이자 회장)은 "*블록체인이 네트워크를 분산시킬 때가 왔다.*"고 선언했습니다. 그는 *"현재 TCP/IP, Packing Switching 이 AT&T 같은 대기업을 제패할 수 있는 것처럼"*[22] 해당 기술은 기존 시스템에 일대 혁신을 가져올 것이라고 강조했습니다.

VC Andreessen Horowitz 는 이렇게 혁신적인 공개 플랫폼 생태계에 대한 기사를 작성했습니다.[23]

그림 21. 위챗 생태계

[22] Sohu.(2018). *Ma Huateng made friends and commented on physicists' views on blockchain*. Available: http://www.sohu.com/a/218207096_117373

[23] Connie Chan.(2015). *When One App Rules Them All: The Case of WeChat and Mobile in China*. Available: https://a16z.com/2015/08/06/wechat-china-mobile-first/

부록-B: 블록체인과 유틸리티 컴퓨팅

가까운 미래에 개발자들은 복잡한 프로그래밍 언어를 이해하고 복잡한 IT 아키텍처를 관리하거나 이를 운영해야 하는 상황으로부터 다른 곳에 관심을 돌릴 수 있게 될 것입니다. 이를 통해 어플리케이션이 최종 사용자들(그리고 향후 몇 년 뒤에는 수십 억 개의 IoT 기기)과 상호 작용하는 프로세스의 프론트엔드에서 어플리케이션 혁신과 가치 창출에만 주력할 수 있을 것입니다.

이러한 "서버리스 아키텍처"에서는 많은 IT 복잡성이 추상화되거나 개발자 및 최종 사용자로부터 간단히 숨겨질 것입니다. 이 개념은 본 백서를 완벽하게 이해하는데 있어서 매우 중요한 사항이며 미래의 AERGO 기반 시스템이 제공할 근본적인 가치 중 하나이기도 합니다.

서버리스 아키텍처는 아마존의 AWS 람다처럼 서드파티 IT 서비스(서비스 형 백엔드, "BaaS") 또는 소위 소프트웨어 컨테이너에서 운영되는 커스텀 노드(서비스로서 기능, "FaaS")에 따라 좌우되는 어플리케이션을 말합니다. 이 아키텍처는 많은 활동을 프로세스 프론트엔드로 이동시킴으로써 IT 운영비를 절감하고 최종 사용자 성능을 개선할 수 있습니다.

"서버리스"라고 해서 어플리케이션이 컴퓨터 서버가 없는 상태로 운용되는 것을 의미하는 것은 아닙니다. 이것은, 시스템 소유자가 서버를 구매하거나 이를 제공할 필요가 없고 백엔드 어플리케이션 코드를 운영하기 위한 가상 기계 또한 필요치 않다는 것을 의미합니다. .

서버리스 아키텍처를 사용하지 않는 전형적인 3 단계 웹 어플리케이션의 간단한 사례를 들어보면 다음과 같습니다(그림 22).

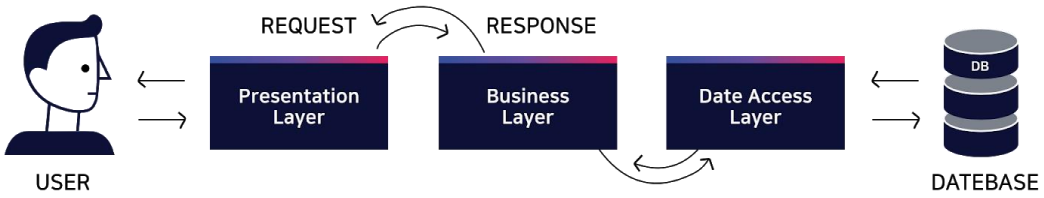


그림 22. "3 단계" 웹 어플리케이션 사례

이 아키텍처는(프론트엔드) 프레젠테이션 계층, 비지니스 계층 및 데이터 액세스 계층(주로 IT 백엔드라고 함)으로 구성됩니다.

최종 사용자가 프레젠테이션 계층에서 어떤 행위를 하는 경우, 비지니스 계층을 호출하여 해당 행위를 처리하도록 합니다(운영 검증 등). 이후 데이터베이스와 상호작용하는 데이터 액세스 계층을 호출합니다. 그 다음, 비지니스 계층에 다시 반응을 돌려보내고 비지니스 계층은 프레젠테이션 계층(즉, 실제 사용자 인터페이스)으로 해당 반응을 전달하게 됩니다.

이러한 사이클은 많은 제 1 세대 3 단계 웹 기반 어플리케이션에서 매우 전형적인 요소입니다. 이 시스템을 설계하기 위해서는, 개발자가 전체 시스템에 관한 세부적인 지식을 확보하고 모든 요소들이 상호작용하고

협력하는 방식을 관리해야 할 필요가 있습니다. 실제로는 여러 요소들이 협력하게끔 만드는데 대부분의 시간을 할애해야 합니다(주로 독점적 인터페이스가 구현됨).

그런데 이것은 보다 현대적인 아마존(AWS)의 서버리스 아키텍처와는 대조적인 모습을 보입니다[24].

아키텍처에도 프레젠테이션, 어플리케이션 및 데이터의 세 가지 계층이 존재합니다. 가장 큰 차이점은 각각의 계층이 표준화된 인터페이스(어플리케이션 프로그램 인터페이스("API"))를 통해 위 아래 계층과 연결된다는 것입니다.

따라서 서버리스 아키텍처를 이해할 수 있는 또 다른(보다 간단한) 방법은 개발자들이 걱정할 필요가 없는 중재적인 서드파티 판매업체의 서버 인프라 상에서 백엔드 IT 비지니스 로직이 작동하는 시스템입니다.

그런데 이것은 백엔드 로직이 작동할 수 있는 서버가 없다는 것이 아니라 서버를 유지할 필요가 없다는 것을 의미합니다. 이러한 서버리스 아키텍처는 아마존, Azure 및 구글과 같은 서드파티 판매업체들의 비지니스입니다. 사실 이러한 결과로 지난 10 년간 클라우드 컴퓨팅이 탄생했다고 할 수 있습니다.

서버리스 아키텍처에는 다음과 같은 두 가지 변종 모델이 있습니다.

- BaaS 또는 MBaaS(M 은 모바일을 의미)
- FaaS

서드파티 제공자는 BaaS 또는 MBaaS 를 통해 백엔드 IT 로직을 운영하게 됩니다. 어플리케이션 개발자는 이러한 백엔드 서비스를 운영하는 서버 또는 인프라를 제공하거나 이를 유지할 필요가 없습니다. 대부분, 이러한 백엔드 서비스들의 경우 일단 시작되면 연속적으로 운영됩니다. 어플리케이션 개발자들은 호스팅 업체에게 이용료(또는 향후 "IT 토큰")만 지불하면 됩니다. 대부분의 경우, 이용료는 몇 주, 몇개월 치를 지불하거나 년 단위로 지불할 수도 있습니다. BaaS 의 또 한 가지 중요한 점은 공유된 컴퓨터 인프라에서 운영되며 다수의 다양한 어플리케이션이 동일한 백엔드 서비스를 사용한다는 점입니다.

두 번째 변종인 FaaS 은 요즘 들어 훨씬 더 각광을 받고 있는 모델이라고 할 수 있습니다. AWS 람다 및 마이크로소프트 아주르 기능, 구글 클라우드 기능 같은(현 세대의) 선두 기술 대부분이 이 카테고리에 해당합니다. 어플리케이션 개발자들은 FaaS 플랫폼을 통해 자체적인 백엔드 로직을 구현하고 서버리스 프레임워크 내에서 이들을 운영할 수 있습니다. 서버 내에서 이러한 기능은 바로 서버리스 "프레임워크"가 처리하게 됩니다. 그리고 이 프레임워크가 확장성, 신뢰성 및 보안성 업무를 담당하게 됩니다. 다른 업체들은 자바 및 C#과 같은 인기 프로그래밍 언어로 이러한 기능을 구현할 수 있는 다양한 옵션을 제공합니다.

어플리케이션을 운영하는 개발자 또는 업체의 경우(아마존 API 게이트웨이 및 AWS 람다 같은) 서드파티 공급자 서비스를 활용할 수 있습니다. 개발자들은 이를 통해 인증, 검색, 업데이트 및 기본 데이터베이스 계층 탐색 등 주요 기능의 복잡성에 대해 걱정할 필요 없이 안전하고 확장 가능한 고가용성 서버리스 생산 어플리케이션을 구축할 수 있습니다.

FaaS 는 BaaS 와 몇 가지 차이점이 있습니다

- 비용은 실제 사용되는 리소스의 수량과만 연관된다(예.분당 단계적 요금 부과)
- FaaS 는 이용량 변동성이 상당히 높은 경우에 이상적이다

[24] Serverless Computing and Applications. Available: https://aws.amazon.com/serverless/?nc1=h_ls

- FaaS 기능은 단기간에 운영된다(대개 몇 분 간)

개발자는 어플리케이션의 작동, 수행 및 확장 방식에 대한 극히 정밀한 제어가 필요할 경우 BaaS 가 아니라 FaaS 를 사용해야 합니다.

이 혁신적인 어플리케이션은 더욱 축소된 상태에서 이동성을 보유하면서도 기타 이와 유사한 어플리케이션들과 연결을 통해 상호 작용하게 됩니다. 이것이 이른 바 "마이크로 서비스" 모델의 본질입니다.

현재 업계 선두권의 디지털 업체들에서 근무하는 고급 개발자들이 이 기술들을 활용하고 있습니다(예. B2B 및 B2C 모바일 전자상거래나 소셜 미디어, 게이밍 및 커뮤니케이션 등 대량 소비자 어플리케이션). 향후 몇 년 안에, 페이스북, 아마존, 구글, 애플 및 알리바바 같은 최첨단 기업들뿐만 아니라 모든 유형의 개발자 및 기업들에 걸쳐서 이러한 기술이 일반화될 것입니다.

서버리스 아키텍처는 다양한 유형의 분산형 마이크로 서비스 기반 dApp 을 처리하는 데 소요되는 비용 및 그 성능이라는 측면에서 중요한 이익을 제공하면서 향후 백엔드 IT 시스템의 정비를 단순화하는 데 기여하게 될 것입니다.

요약하자면, 개발자들은 더 이상 스스로를 "IT 배관공"이라고 생각하지 않으면서, 창조적인 부가 가치 어플리케이션에 주력하고 싶어하는 것입니다.

그러나, 이러한 형태의 서버리스 아키텍처의 이점은 상당히 많기는 하지만, 이를 운용할 경우 다음과 같은 몇 가지 측면들에 대해 신중하게 고려해야 할 것입니다.

- 판매업체에 대한 종속은 문제점을 야기할 수 있다(예. 빈번하게 이루어지는 의무적 API 변경, 가격 구조 및 기타 미래 기술 변경)
- 네트워크 전반적으로 속도 문제가 발생할 수 있고 다수 사용자의 동시 이용에 따라 엔터프라이즈 서비스 수준 협약("SLAs") 준수에 지장이 초래될 수도 있다
- 서버 인스턴스가 나타났다 사라졌다 하기 때문에 이러한 유형의 프레임워크에서 어플리케이션의 상태를 유지하는 것이 실질적으로 어려울 수 있다
- 이 기능들의 경우 정해진 시간이 경과하면 종료되는 관계로 장기 운영 비지니스 프로세스에는 적합하지 않을 수 있다
- 메모리 접속 속도, 네트워크 속도, 안정성 및 네트워크 반응시간(지연속도) 등 네트워크 내에서 상호 연결되어 있는 IT 서비스들의 속도 및 주로 사용되는 프로토콜로 인해 초당 최대 처리 건수("TPS")가 제한되는 등의 중요한 한계가 존재한다
- 이러한 역동적인 기능들이 스핀업하거나 필요 시 나타났다 사라지기 때문에 단대 단 테스트나 통합 테스트를 실시하기가 어렵다
- 생산 시스템 및 시스템 행동과 관련해 개발자가 그 성능에 대해 전적으로 신뢰할 수 있을 정도의 적절한 모니터링 및 디버깅 역량이 부족하다

그러나 이러한 한계에도 불구하고 가까운 미래에 AERGO 기반 블록체인(서버리스 인프라 배포 모델)에서 운영되는 마이크로 서비스 기반 dApp 은 새롭게 등장하는 분산 유틸리티 컴퓨팅 세계에서 여러 신규 서비스의 주요 배포 모델 중 하나가 될 것입니다.

요약하자면, 서버리스 아키텍처가 가진 장점들은 향후 수 년 간 블록체인의 진화에 있어 매우 중요한 역할을 하게 될 것이라고 말할 수 있습니다.

서버리스 아키텍처는 다음과 같은 기능을 제공합니다.

1. 개발비 절감을 위해 여러 비지니스 어플리케이션을 서비스로서 사용할 수 있는 기능
2. 개발자가 인프라 및 유지 비용을 고려할 필요가 없기 때문에 운영비를 절감할 수 있는 기능
3. (필요 시) 자원을 빠르게 확장하고, 완벽한 수준으로 탄력적이면서 자동적으로 어플리케이션을 수평 확장할 수 있는 기능
4. 모든 물리적 IT 개입을 서드파티 제공자가 관리함에 따라 이러한 업무를 수행하는데 자원과 시간을 쏟아 부을 필요가 없어지게 되어 IT 자원을 훨씬 더 손쉽게 관리, 운영할 수 있는 기능
5. 서버리스 dApp 어플리케이션의 기본적인 가용성과 오류 허용 한계를 제공할 수 있는 기능

새로운 서버리스 어플리케이션으로의 이전은 이미 시작되었다고 할 수 있습니다.

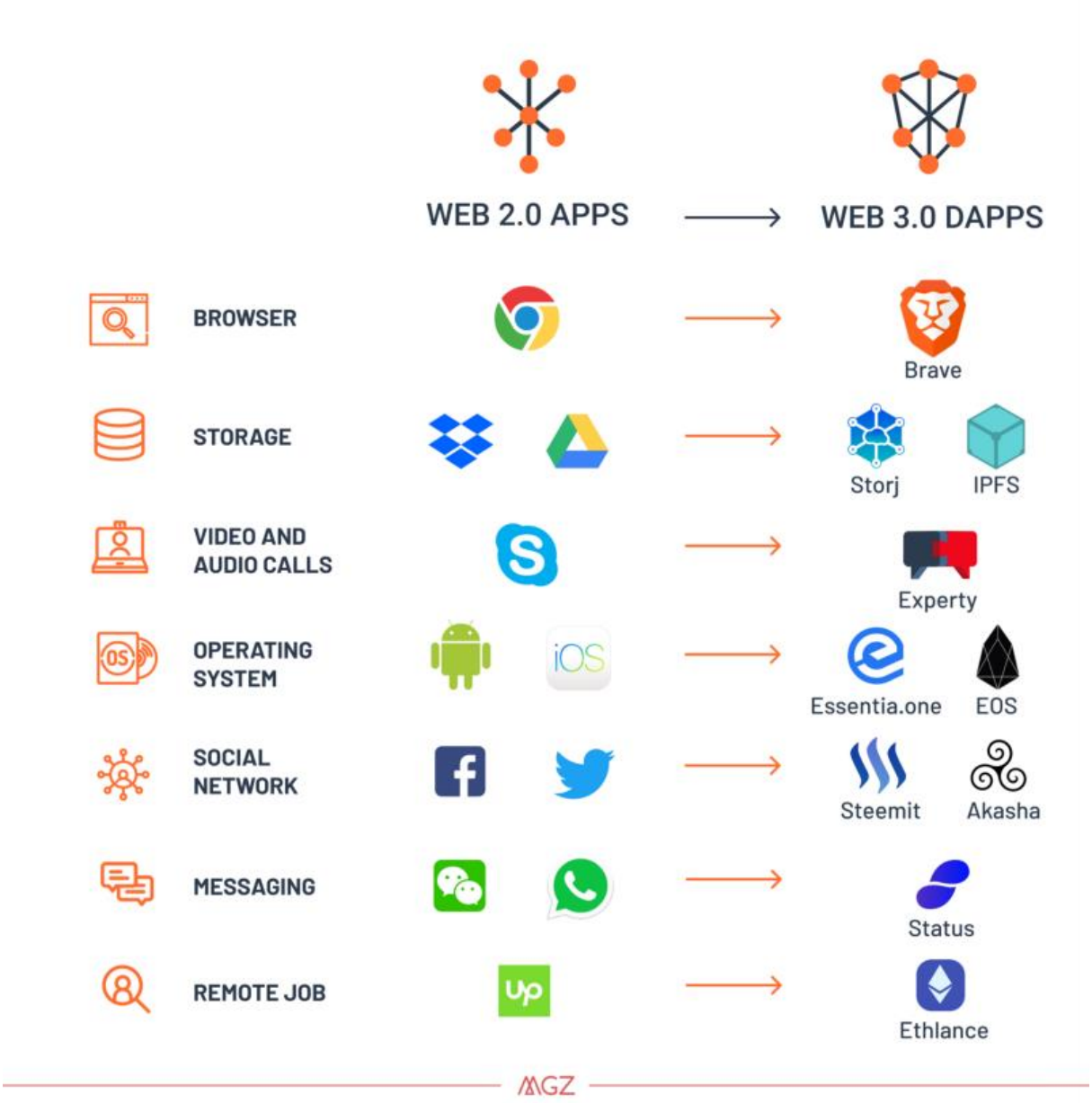


그림 24. 웹 2.0 에서 웹 3.0[25]으로의 발전

서버리스 dApp 의 채택은 이미 상당히 많이 진행되고 있으며, 이것은 업체들이 안전한 분산형 클라우드 기반 서비스를 통해 신규 서비스를 전달하는 방식을 주도하게 것으로 예상됩니다.

일부 보안 역량과 생태계 툴들은 여전히 성숙해야 할 필요가 있기 때문에 현재 업무상 중요하고 확장 가능한 일부 비지니스 어플리케이션의 경우에는 이러한 방식의 즉각적인 타깃이 아닐 수도 있습니다. 그러나, 서버리스 컴퓨팅의 수많은 잠재적 활용 사례들을 통해 향후 모든 기업들이 해당 기능을 이용할 가능성이

[25] Matteo Gianpietro Zago.(2018). *Why the Web 3.0 Matters and you should know about it.* Available: https://medium.com/@matteozago/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949

점차적으로 늘어나고 있음을 가늠할 수 있습니다. 실제로 이것은 여러 가지 측면에서 클라우드 컴퓨팅이 다양한 산업에서 이미 채택되어 온 방식과 유사할 것입니다.

이러한 아키텍처 방식이 발전하면서, 디지털 자산과 보안 데이터 교환을 다루는 거의 모든 산업 부문에서 다양한 신규 비지니스 프로젝트들에 이 방식이 점차적으로 도입될 것으로 보입니다. 예를 들어, 에베레스트 그룹의 경우, 은행거래 산업에서 향후 몇 년 내에 블록체인의 채택이 가속화될 것으로 예측하기도 했습니다.

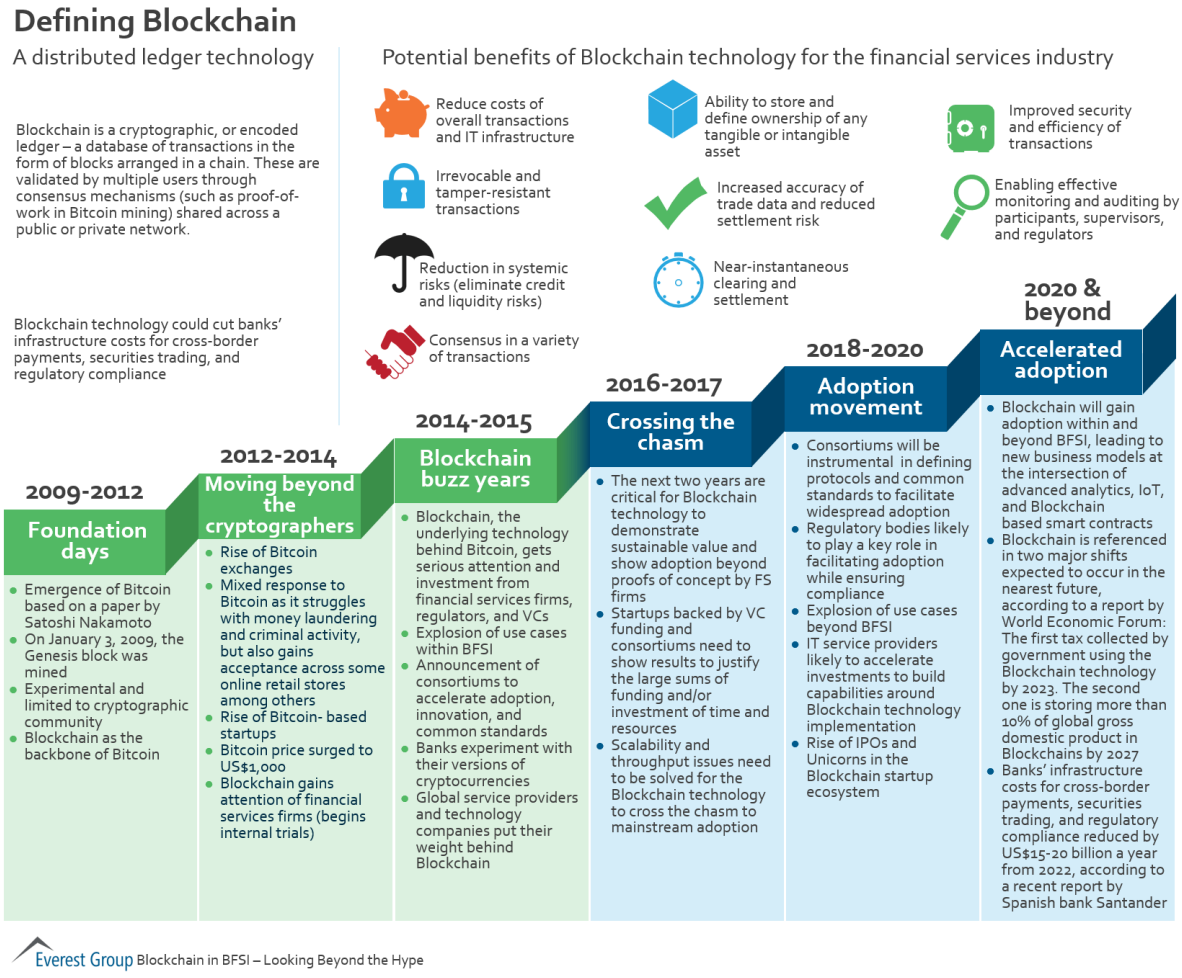


그림 25. 은행거래 부문의 블록체인 채택 현황[26]

현재, 특정(아마도 미성숙한) 버티컬 블록체인 솔루션 구현을 활용하는 많은 기업들이 다양한 dApp 을 구축하고 있습니다. 그러나 미래의 추가적인 구현으로 이어지는 표준화가 존재하지 않는 관계로, 다양한 비지니스 및 제품 군 전반에 걸쳐 블록체인을 활용하고자 하는 기업들에게는 원치 않는 비용, 복잡성 및 리스크가 발생할 수도 있습니다. 많은 기업들이 블록체인 솔루션 지원이 매우 어렵다고 인식하면서 난관에 봉착했습니다.

[26] Everest Group.(2016). *Defining Blockchain*. Available: https://www.everestgrp.com/2016-05-blockchain-technology-bfsi-benefits-market-insights-20805.html/

현재 발견되고 있는 단편화(fragmentation) 및 복잡성 수준이 아래 도표에 나와 있습니다.

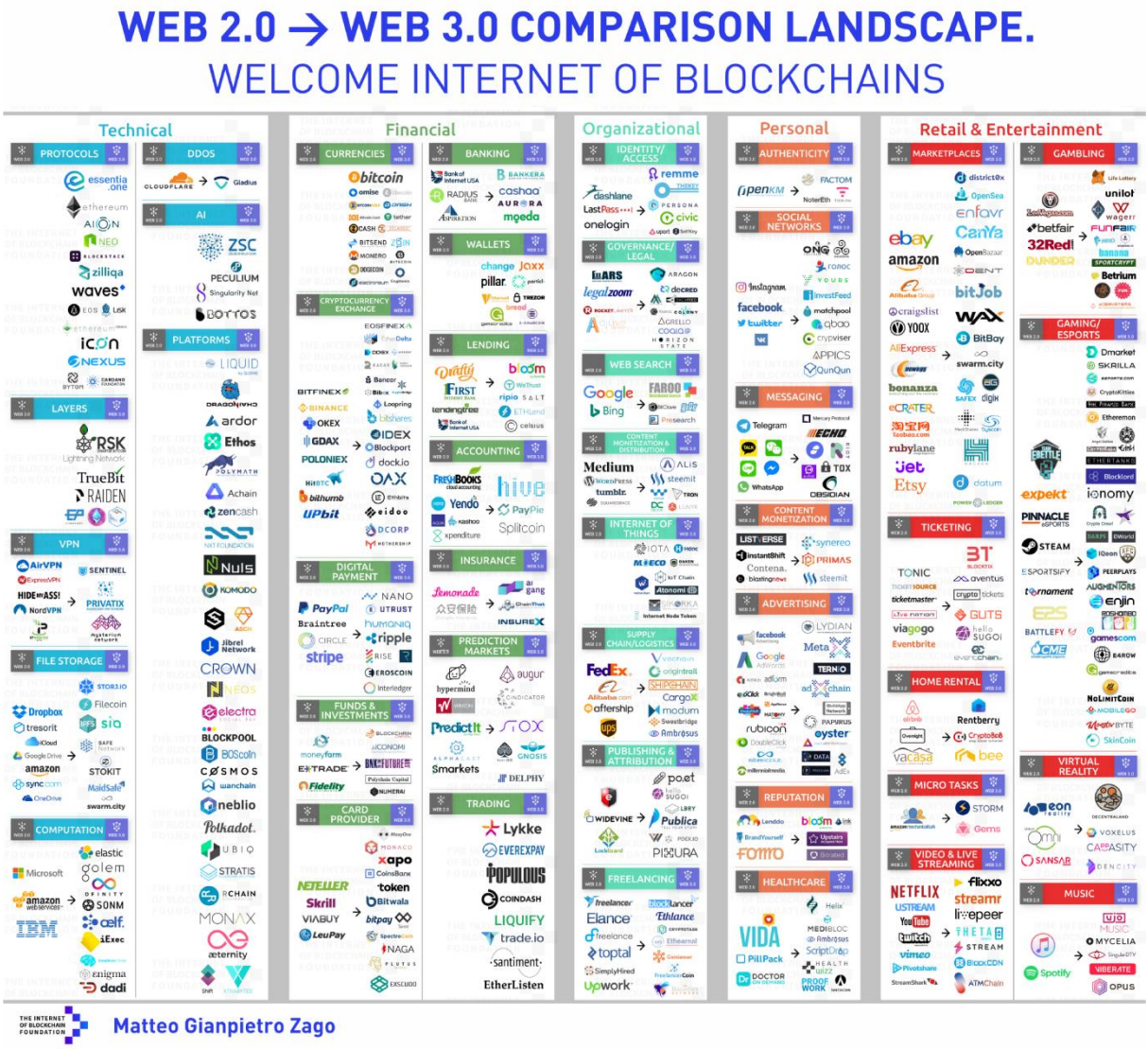


그림 26. 블록체인 솔루션의 복잡한 조망(현재)[27]

[27] Matteo Gianpietro Zago.(2018). *Why the net giants are worried about the Web 3.0.* Available: https://medium.com/@matteozago/why-the-net-giants-are-worried-about-the-web-3-0-44b2d3620da5

부록-C: 프라이빗 vs 퍼블릭 엔터프라이즈 블록체인

퍼블릭 및 프라이빗 블록체인 프로토콜은 다음과 같은 많은 유사점을 갖고 있습니다.

- 분산 피어투피어(P2P) 네트워크로서 각 참여자들이 디지털 서명 거래로 공유되는 첨부 전용 분산 원장의 복제본을 유지한다
- 블록체인 프로토콜이 데이터 무결성 및 비가역성을 제공한다(즉, 블록체인에 포함된 데이터 및 특히 그 기록 상태는 일단 생성되면 네트워크에서 일부 참여자들에게 결함이 있거나 악성인 경우에도 그 수정이 불가능).
- 합의라고 알려진 프로토콜을 통해 복제본들을 동시에 관리한다.
- 일부 참여자들에게 결함이 있거나 악의를 가진(즉 신용이 필요 없는 네트워크 환경에서 작업)에도 분산 원장의 비가역성을 보장한다.

퍼블릭 블록체인

퍼블릭 및 프라이빗 블록체인의 중요한 개념적 차이는 네트워크 참여자, *합의(consensus)* 프로토콜 집행자, 공유되는 분산 원장 관리자 역할을 누가 담당할 것인 지와 관련됩니다. 퍼블릭 블록체인 네트워크는 완벽하게 공개되어 있는 관계로 누구나 네트워크에 가입하고 참여할 수 있습니다. 네트워크에는 일반적으로 참여자들을 늘리기 위한 인센티브 메커니즘이 존재합니다. 비트코인은 현재 최대 규모의 퍼블릭 블록체인 네트워크 중 하나하고 할 수 있습니다.

기존 퍼블릭 블록체인의 한 가지의 결함은 대규모로 분산된 분산 원장을 유지하는데 필요한 연산 권한이 너무 많다는 점입니다. 보다 구체적으로 합의를 도출하려면 네트워크의 각 노드가 복잡한 자원집약적 암호화 문제를 해결함으로써 모든 노드를 동기화하고 신뢰를 유지해야 할 필요가 있습니다.

그런데 이 프로세스가 매우 복잡하기 때문에 엄청난 시간과 에너지(전기)가 소모됩니다.

특정 사용자들과 관련된 또 한 가지 단점은 기존의 여러 퍼블릭 블록체인들의 개방성입니다. 즉, 거래와 관련된 개인정보를 거의 또는 전혀 제공하지 않습니다(익명성에 입각). 또한 모든 네트워크 참여자들에게 공개되어 있기 때문에 전반적인 시스템 수준 관리의 취약한 부분만을 지원합니다.

이러한 요인들은 기업들이 향후 블록체인을 활용하고자 할 때 중요한 고려 사항이 됩니다.

그러나, 이러한 설명에도 불구하고 퍼블릭 블록체인에서는 그 어떤 개인, 그룹 또는 조직도 블록체인 상의 정보나 프로토콜 자체를 뒷받침하는 일련의 규칙을 제어하지 않으며, 그 어떤 멤버도 일방적으로 블록체인의 프로토콜과 포함된 정보를 변경할 수 없습니다. 사용자는 퍼블릭 블록체인을 전적으로 신뢰함으로써 동일한 블록체인을 이용하는 제삼자를 전적으로 신뢰할 수 있어야 합니다.

요약하자면, 퍼블릭 블록체인은 신뢰성을 극대화할 수 있지만 운영 속도가 느리고 비용도 많이 든다고 할 수 있습니다. 또한 다양한(심지어 경쟁적인) 이해관계를 가진 다수의 참여자가 속한 집단의 합의가 필요한 관계로 업그레이드 과정이 매우 어려울 수도 있습니다. 더불어 채굴자들의 프론트 러닝(front-running) 등의 악의적 활동, 담합 행위(즉, 채굴 권한이 소수 참여자에게 집중되는 경우), 또는 동시에 수많은 관할구역에서

거래가 기록되거나 검증되면서 발생하는 법률 관련 복잡성 등 다양한 요인들로 인해 신뢰성이 훼손될 수도 있습니다.

프라이빗 블록체인

프라이빗 블록체인 네트워크의 경우 초청이 필요하며 네트워크 스타터 또는 네트워크 스타터가 정한 규칙에 의한 검증이 필요합니다. 프라이빗 블록체인을 구축하는 업체들은 일반적으로 *퍼미션* 네트워크를 구축하게 됩니다. 이것은 누가 네트워크 참여자가 될 지, 어떤 거래에 참여하게 될 지의 문제를 제한합니다. 참여자는 가입 초청 또는 *허가*를 받아야 합니다. 액세스 제어 메커니즘은 다양할 수 있습니다. 예를 들어, 기존 참여자들이 향후 진입자를 결정하거나, 규제당국이 참여 라이선스를 발행하거나, 컨소시엄이 대신 관련 결정을 내릴 수도 있습니다. 특정 주체가 네트워크에 가입하게 되면, 분산된 방식으로 블록체인을 유지하는데 일조하게 될 것입니다.

프라이빗 블록체인은 시스템 수준의 정교한 IT 설계를 통해 거래 처리량 측면에서 확장성을 개선합니다.

간단히 말해, 프라이빗 블록체인의 경우 개인정보보호 실무를 개선하고 처리량을 극대화하며 운영비가 상대적으로 저렴하다는 장점을 갖고 있지만, 보다 광범위하게 배포된 퍼블릭 블록체인에 비해 신뢰 수준 및 네트워크 효과는 부족하다고 할 수 있습니다.

현재 다양한 기업들이 자체 프라이빗 블록체인 구축과 관련된 테스트를 진행하고 있습니다. 이러한 수많은 이니셔티브들(및 관련 컨소시엄)은 실 세계 생산 시스템에서 프라이빗 블록체인을 확보하기가 어렵다는 문제점에 직면해 있습니다.

여기에는 아래에 나와 있는 원인을 포함해 다양한 이유가 존재합니다:

1. 사설 프라이빗 블록체인 시스템 구축 시에는 극히 소수의 기업들만 소유하고 있는 전문 IT, 클라우드 및 개발자 기술과 노하우가 필요하다

2. 이들을 보다 장기적으로 사용하고 개선하며 유지,관리하기 위해 오픈소스 모델을 활용해 구축하는 것은 상당히 어렵다(또한 소프트웨어 개발 및 유지보수는 대개 이러한 업체들의 핵심 역량이 아니다)

3. 상기 두 가지 요인들로 인해 해당 시스템의 운영과 관련된 장기적 비용이 상당히 증가할 수 있다.

따라서, 비지니스 프로세스에 블록체인 기술을 통합하고자 하는 기업들의 경우(i) 신뢰성과 상호운용성 관계(퍼블릭),(ii) 성능과 개인정보보호 관계(프라이빗) 요건을 신중히 고려해야 할 것입니다.

이것은 통합된 퍼블릭 및 프라이빗 블록체인 처리 시 근본적인 패러독스라고 할 수 있습니다.

엔터프라이즈 PoC 와 관련된 노력의 대부분이 프라이빗 블록체인 네트워크에서 구현되었으며,이들 중 단 3 분의 1 만이 실제로 퍼블릭 네트워크에 배포된 것으로 확인되었습니다.

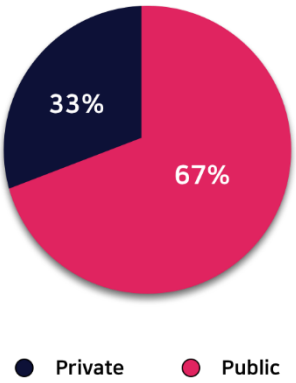


그림 27. 은행 주도 PoC 에서 사용된 블록체인 형태[28]

대기업들의 경우 엄격한 보안 및 준수 요건으로 인해 주로 프라이빗 컴퓨터 아키텍처에서 자신들의 IT 시스템을 구현해 왔습니다(프라이빗 인터넷 클라우드 등). 같은 이유로, 이 중 다수가 프라이빗 블록체인으로 실험을 하고 퍼블릭 프로토콜은 일체 사용하지 않고 있습니다.

수많은 산업계 컨소시엄들에서(R3 및 하이퍼 레저 등) 한 가지 유형의 블록체인 아키텍처만 고려함으로써 잠재적인 장기적 가치 및 유용성을 제한할 가능성도 존재합니다.

사실, 블록체인과 관련된 많은 혁신이 퍼블릭 프로토콜 스페이스에서 이루어지고 있습니다. 이는(주로 암호화폐 기반의) 다양한 대규모 블록체인 프로젝트들에서 확인된 완전히 새로운 아이디어, 프로젝트 및 서비스들에 의해 입증되고 있습니다. 이들 프로젝트 대부분이 직접적인 dApp 개발에 집중하고 있지만, 이들을 운영하는 내재된(주로 퍼블릭) 블록체인의 혁신도 촉진하고 있습니다.

블록체인에 하이브리드 방식을 사용할 경우 실제로 변화를 창출할 수 있는 경제적 이점을 확보할 수 있을 것입니다. 이러한 방식은 통합된 퍼블릭 및 프라이빗 블록체인 아키텍처의 이점을 극대화하는데(그리고 결함을 줄이는데) 일조하게 될 것입니다. 데이터 및 가치(자산) 거래와 관련해 규제준수 기록 및 개인정보보호를 활성화하고 필요한 엔터프라이즈 수준 성능을 위해 구성 및 최적화된 프라이빗 블록체인과 더불어 엔터프라이즈 무결성 및 비가역성의 신용이 필요 없는(trustless) 네트워크 환경을 제공하기 위해 퍼블릭 블록체인을 사용하는 비지니스 아키텍처를 구축함으로써 이익을 얻을 수 있을 것입니다.

현재 이와 유사한 한 가지 형태의 하이브리드 방식이 클라우드 컴퓨팅과 함께 이미 활용되고 있습니다. 엔터프라이즈 기업들은 비지니스 어플리케이션 자동 확장 및 성능 처리량을 위해 극히 정보 중심적인 프라이빗 클라우드 데이터 센터를 보다 저렴하고 안전한 퍼블릭 클라우드와 통합하고 있습니다.

[28] Nivedita Bhattacharjee.(2017). *Blockchain is becoming more than a buzzword, and now there's tangible proof*. Available: https://www.techinasia.com/bankers-like-blockchain

부록-D: AERGO 팀 구성 및 자문 패널

AERGO 는 현재 진행 중에 있는 복잡하고 포괄적인 프로젝트입니다. AERGO 의 개발 및 성공적인 배포를 위해서는 블록체인 기술, 클라우드 컴퓨팅 및 오픈소스 노하우 등 모든 관련된 분야의 통합이 필요합니다.

AERGO 는 이러한 분야에서 탁월한 경력과 전문지식을 보유한 팀을 구성했습니다.

AERGO 이사진

Phil Zamani

- Global VP Sales & Biz Dev. Internet Embedded Linux Appliances for Redhat Inc.
- Global Head of Big Data & Cloud Biz Models at Santander
- Senior VP of Cloud Biz Unit at Deutsche Telekom

Hun Young Park

- Expertise in Machine Learning solution development
- 12 years of experience in Relational DBMS and distributed solutions
- KAIST, Computer Science. MS

Roderik van der Graaf

- Founder of Lemniscap, an investment and advisory firm in the blockchain space
- 7 years of PE/VC at Caldera Pacific and KCP Capital
- 13 years of equity derivatives trading at Deutsche Bank, HSBC, Rabobank, Bear Stearns, LIM Advisors and All Options
- Queen Mary, Univ. of London, Information Technology. MSc

이사회 대표

Won Kim
Technology Committee Head

- 9 years of experience in Relational DBMS
- 6 years of research & development of distributed systems
- Boston Univ. Computer Science

Jane Lee
Finance Committee Head

- 7 years of experience in Strategy Consulting at Accenture
- Expertise in digital transformation, and technology commercialization
- Cornell Univ. Hotel Administration

Alison Shim
Ecosystem Committee Head

- 5 years of experience in Strategy Consulting at Accenture
- Expertise in go-to-market, and business development
- New York Univ. Economics and Communication studies

기술팀

Yun Woo Park

- 7 years of experience in relational DBMS
- Principal software researcher in database R&D
- Korea Univ. Computer Engineering

Sung Jae Woo

- 11 years of experience in Relational DBMS buffer cache and IO subsystem development
- Expertise in Computational Physics
- Korea Univ. Physics. PhD

Pierre-Alain Ouvrard

- Python, Solidity developer
- Offchain scaling and plasma researcher
- INSA Lyon. Electrical Engineering

Kyung Tae Lee

- 12 years of experience in Relational DBMS and Query engine development
- Expertise in Graph database
- Kangwon Univ. Computer and Communication Engineering

Bernardino Ramos

- 19 years of experience on software development
- Expertise on SQLite database replication
- Creator of Binn, LiteReplica and LiteSync

+25 more

Blocko Team

사업팀

Mason Park

- 7 years of experience in Advertising and Marketing
- Innovator and expertise in branding, marketing strategy & execution
- Univ. of Wisconsin-Madison, Biochemistry

Han Kim

- 5 years of experience in Public Relations development
- Excellence in cryptocurrency dynamics and ecosystem
- HUFS, Social Science

Seona Kim

- 3 years of experience in IT Consulting & Cloud management service
- Strategy project manager and researcher for blockchain market
- HUFS, English-Korea Interpretation & Translation

Camron Miraftab

- 4 years of experience in innovation strategy and venture capital
- 3 years of experience in blockchain research and due diligence of blockchain businesses
- Newcastle Univ. International Economics and Finance MSc

AERGO 자문

Eddie Alleyn

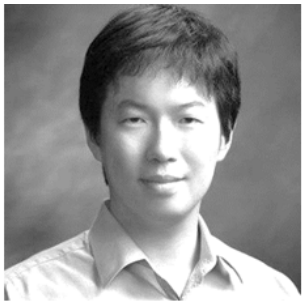
Eddie Alleyn is a technology entrepreneur and expert in security and secure communications. He spent thirty five years leading special projects for the UK Government, in the Ministry of Defence and the Foreign and Commonwealth Office. From 2011-2016 he was Chair and CEO of HMGCC, an agency of the FCO, involved in the design, manufacture and integration of secure communications and cyber systems for the UK Government. He is now an Exec and Non-Executive Director to innovative tech start-ups in the security and cyber security fields, and an Adviser to SANS Institute. Eddie knows how to get the best out of innovative technology and engineering teams to deliver ground-breaking security solutions.

Djamel Souici

Djamel Souici is a legal expert on open source technology, Licensing and business models. He is also a leading advisor and practitioner in Data Privacy and Regulation (such as GDPR). Djamel, a member of the German Legal Barr Association, has spent the past 19 years as General and Legal Counsel for a number of innovative software firms, leading their representations in respect of open source, data privacy and compliance. He has also developed a number of strategic partnerships with many Fortune 100 firms in diverse sectors such as Telecoms, Financial Services, Government, Automotive, Manufacturing, Petrochemicals, Logistics, Retail and Healthcare. Djamel is also a renowned negotiator and expert in international mergers and acquisitions.

Vincent Zhou

Vincent is the founding partner of FBG Capital. He has extensive experience in digital assets trading and investment. His professional experience has seen him work at leading technology companies including the likes IBM and Oracle. With an aptitude towards distributed ledger technology, Vincent has become an early investor in a broad spectrum of blockchain companies and projects.
His successes in the blockchain arena has led him to being considered as one of the most well-connected and visionary crypto hedge fund managers in Asia.



Joon-Hong Jake Kim

Jake Kim has a deep understanding of capital markets, strategic business development, as well as hands-on experience in system engineering and back-end computing. He is currently a venture capital and cryptocurrency fund manager based in Seoul where he specializes in corporate venturing, M&A, company building and (selective) Angel investments. He is a seasoned startup investor, adviser and enterprenuer with over 20 years of combined experience in capital markets, consultancy and large-scale back-end and middleware systems development. Jake currently manages Innobase, the corporate venture capital arm of Kolon group. He holds an MBA in Strategy and Corporate Governance from IE Business School.

Riad Hartani

Riad is a seasoned technology specialist and strategist with over 20 years contributing to the development of Internet, Mobile and AI technologies. He co-founded and led multiple high-tech startups (Caspian, Anagran, Wichorus and more) with some seeing very successful exits. He has advised over 10 leading technology corporations, numerous private equity houses and several governments and regulators. He also co-founded Xona Partners, a boutique technology and investment advisory firm and ivalley.co, a Fintech co-creation studio. Riad holds a Ph.D in in Artificial Intelligence. He is frequently invited as a lecturer, speaker and panelist at leading industry fora and academic institutions

Sinhae Lee

Sinhae Lee is a Partner at GBIC, leading blockchain investments and accelerating robust projects. Prior to joining GBIC, she has been deeply involved in the FinTech/blockchain industry in Silicon Valley. She led business development and operations at a payment start-up, Coin, which was acquired by FitBit in 2016 and later worked at NerdWallet, a FinTech start-up in San Francisco. She started her career as a management consultant at McKinsey & Company. She brings her Silicon Valley and consulting experience to the blockchain/crypto industry. Sinhae holds an MBA from Stanford University and a B.A. in Business from Korea University.

Pierre F. Suhrcke

Pierre Suhrcke is a leading Fintech expert and investor in Europe, having been active in this sector since 1999. Pierre spent more than 17 years in various senior executive management positions in Investment Banking at Deutsche Bank in London and Frankfurt (Equities, Risk Management and Head of Capital Venture Partners). Pierre is currently a Venture Partner at Tempocap, a European technology investment firm, and a board member of Acorus Capital, a Hong Kong based Private Equity firm. He is an angel investor, mentor and advisor to companies - having worked with and sat on the board of - over 20 successful private companies (US & Europe). He is frequently invited as an expert fintech panel member at leading conferences.

부록-E: 용어정리

브랜칭(Branching): 두 브랜치(branches)에서 수정이 가능하도록 수정 제어 하에 객체를 복제하는 행위(소스 코드 파일이나 디렉터리 트리 등).

병행 제어(Concurrency control): 멀티 유저 시스템으로 인해 발생할 수 있는 데이터 관련 동시 접속 또는 변경으로 인한 충돌을 처리하는데 사용되는 데이터베이스 관리 시스템 개념.

컨텐츠 전송 네트워크(Content Delivery Network): 프록시 서버와 데이터 센터의 지리적으로 분산된 네트워크. 그 목표는 서비스를 최종 사용자에 비례하여 공간적으로 분산시킴으로써 고가용성 및 고성능을 제공하는 데 있다.

분산형 어플리케이션(Decentralized Application, dApp): dApp 은 분산된 피어투피어(P2P) 네트워크에서 운영되는 백엔드 소프트웨어 코드를 갖고 있다. 이와 달리 전형적인 앱에서는 중앙집중 서버에서 벡엔드 코드가 운영된다.

서비스 거부(Denial-of-service attack, DoS) 공격: 일시적으로나 무제한적으로 인터넷에 연결된 호스트 서비스를 와해시킴으로써 목표로 하는 사용자들이 기계 또는 네트워크 리소스를 사용할 수 없도록 하려고 하는 범죄자의 사이버 공격.

하드포크(Hard-fork): 이전에는 무효였던 블록/거래를 유효화하는 프로토콜의 급진적 변경(또는 이전에 유효했던 블록/거래를 무효화하는 프로토콜의 급진적 변경).

JIT 컴파일(JIT compilation): 실행 이전 보다는 프로그램 실행 즉, 운영 시 편집과 관련된 컴퓨터 코드 실행 방법.

LLVM: 컴파일러 프론트엔드와 백엔드를 개발하는데 사용되는 모듈식의 재사용 가능 컴파일러와 툴 체인 기술 모음인 컴파일러 인프라 프로젝트.

머징(Merging): 파일이나 폴더 상의 다양한 버전의 통합 또는 변경.

마이크로서비스: 느슨하게 결합된 서비스 모음으로서 어플리케이션을 구조화하는 서비스 지향 아키텍처(SOA) 스타일의 변종인 소프트웨어 개발 기술.

통합(orchestration): 제어 이론의 요소들을 배포하는 자동화 또는 시스템 효과.

병렬화(PARALLELISM): 다수의 계산 또는 프로세스 실행이 동시에 수행되는 계산.

프라이빗 체인: 신규 노드가 네트워크에 가입하기 위해서는 특정한 규칙에 따른 승인이 필요하고 퍼블릭 체인에 비해 개방 및 분산 정도가 제한적인 블록체인 네트워크.

지분증명(PoS): 소지한 코인의 개수에 따라 블록 거래를 채굴하거나 검증할 수 있음을 명시하는 개념.

작업증명(PoW): 서비스 요청자에게 일부 작업을 요구함으로써 네트워크 상의 스팸 등 서비스 거부 공격 및 기타 서비스 악용을 막기 위한 경제적 조치로 대개 컴퓨터의 처리 시간을 의미한다.

퍼블릭 체인: 참여자들이 관련 프로토콜을 준수할 경우 네트워크 가입이 가능하며 전적으로 개방된 분산형 블록체인 네트워크.

직렬화(Serialization):(파일이나 메모리 버퍼 등에) 저장되거나 전송되어(네트워크 연결 링크 전반에 걸치는 방식 등으로) 추후(다른 컴퓨터 환경에서) 재구성 될 수 있는 형식으로 데이터 구조나 객체 상태를 변환하는 프로세스.

서버리스 컴퓨팅: 클라우드 제공자가 극적으로 기계 리소스 할당을 관리하는 클라우드 컴퓨팅 실행 모델.

스마트 컨트랙트: 계약 관련 협상이나 성능을 디지털 방식으로 촉진, 확인 또는 집행하기 위한 컴퓨터 프로토콜.

스마트 오라클: 실시간 발생을 발견, 검증하여 스마트 컨트랙트를 통해 사용 예정인 블록체인에 제출하는 외부 에이전트 또는 프로그램. 외부 데이터를 제공하고 스마트 컨트랙트를 “유발”한다. 실제로 스마트 오라클은 서드파티 “데이터 피드”이며 해당 정보를 안전하고 신뢰할 수 있는 방식으로 공급한다.

소프트웨어 저장소: 소프트웨어 패키지가 컴퓨터 상에서 검색되고 설치될 수 있는 저장 위치.