하이퍼레저 패브릭으로 배우는 블록체인

하이퍼레저 패브릭으로 배우는
블록체인

1쇄 발행 2018년 11월 30일

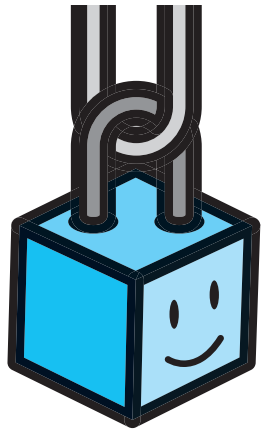
지은이 윤대근
펴낸이 장성두
펴낸곳 주식회사 제이펍

출판신고 2009년 11월 10일 제406-2009-000087호
주소 경기도 파주시 회동길 159 3층 3-B호
전화 070-8201-9010 / **팩스** 02-6280-0405
홈페이지 www.jpub.kr / **원고투고** jeipub@gmail.com
독자문의 readers.jpub@gmail.com / **교재문의** jeipubmarketer@gmail.com

편집부 이종무, 황혜나, 최병찬, 이 슬, 이주원 / **소통·기획팀** 민지환 / **회계팀** 김유미
교정·교열 장성두 / **본문디자인** 북아이 / **표지디자인** 미디어픽스
용지 에스에이치페이퍼 / **인쇄** 한승인쇄 / **제본** 광우제책사

ISBN 979-11-88621-45-3 (93000)
값 24,000원

하이퍼레저 패브릭으로 배우는 블록체인



ETRI 블록체인기술연구센터
윤대근 지음

Jpub 제이펍

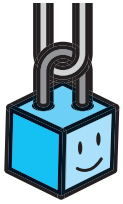
※ 드리는 말씀

- 이 책에 기재된 내용을 기반으로 한 운용 결과에 대해 저자, 소프트웨어 개발자 및 제공자, 제이펍 출판사는 일체의 책임을 지지 않으므로 양해 바랍니다.
- 이 책에 기재한 회사명 및 제품명은 각 회사의 등록 상표(또는 상표)이며, 본문 중에는 ™, ©, ® 등의 기호를 생략하고 있습니다.
- 이 책에서 설명하고 있는 실제 제품 버전은 독자의 학습 시점에 따라 책의 버전과 다를 수 있습니다.
- 책 내용과 관련된 문의사항은 지은이나 출판사로 연락해 주시기 바랍니다.

  – 지은이: ykudfor1@gmail.com

  – 출판사: readers.jpub@gmail.com

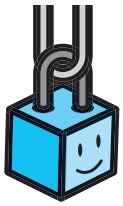
차례



CHAPTER 2 하이퍼레저 패브릭 핵심 분석 _ 13

CHAPTER 3 하이퍼레저 패브릭 실습 _ 77

머리말



블록체인 현황

4차 산업혁명 시대의 흐름에 따라 기존의 중앙화된 세상은 점점 탈중앙화된 세상으로 바뀌고 있습니다. 예를 들어, 방송국의 지위는 유튜브 등에서 활동하는 1인 방송 크리에이터로 인해 점차 하락하고 있으며, 기존 대기업의 사업 영역에 영향을 미칠 만큼 우버, 에어비엔비, 렌딩클럽 등의 공유경제 기업이 성장해 가고 있습니다. 이러한 시대를 맞이하기 위한 가장 중요한 기술 세 가지를 꼽으라면 단연 '빅데이터', '인공지능', '블록체인'이라 할 수 있습니다. 이 세 가지 기술의 공통점은 무엇일까요? 기술의 핵심이 데이터에 있다는 것일 겁니다. 빅데이터는 대량의 데이터를 효율적으로 처리하는 기술이고, 인공지능은 데이터를 이용해 기계를 똑똑하게 만들어 주는 기술이며, 마지막으로 블록체인은 여러 의견이 있겠지만 필자는 중앙 기관이 독점하고 있는 데이터의 주권을 각각의 사용자에게 돌려주는 기술이라고 생각합니다.

이러한 세 가지 기술이 모두 조화를 이루어야만 진정한 4차 산업의 시대가 완성될 수 있다고 생각합니다. 그러나 빅데이터와 인공지능은 오래전부터 많은 관심 속에서 기술의 성숙도가 무르익어 가고 있는 반면, 블록체인 기술은 현재 가지고 있는 잠재력과 장점에 비해 기술의 완성도가 아직까지는 매우 부족한 실정입니다. 대표적으로, 전 세계적으로 가장 활발하게 개발되고 있는 이더리움만 보더라도 실생활에 사용하기까지 아직 수많은 기술적 장벽들이 남아 있습니다.

시중에 블록체인 개론서와 서비스, 코인 관련 서적에 비해 기술을 다루는 책은 극히 일부라는 것을 알고 난 뒤 책을 집필하기로 마음먹었습니다. 하이퍼레저 패브릭 또한 많은 사람의 관심을 받고 있는 블록체인 플랫폼임에도 불구하고 관련 기술 서적이 현재 국내에 단 한 권도 없습니다. 이 책은 시중에 많이 출간되어 있는 블록체인 기술 개론서보다는 한 걸음 더 들어가서 하나의 대표적인 프라이빗 블록체인 플랫폼에 대한 구조를 분석하고 시스템을 직접 운영해 볼 수 있는 내용을 담고 있습니다. 이 책이 여러분이 블록체인 전문가가 될 수 있는 좋은 발판이 되었으면 하고, 더 나아가 블록체인 기술 발전에 조금이나마 이바지할 수 있게 되면 좋겠습니다.

하이퍼레저 패브릭이란?

2015년, 리눅스 재단에서는 기업용 블록체인 개발을 위해 하이퍼레저(Hyperledger) 프로젝트를 만들었는데, 오픈 소스 형태의 프로젝트로서 전 세계 기업과 개발자들이 자발적으로 기술 개발에 참여하는 프로젝트입니다. 하이퍼레저 패브릭은 가장 왕성하게 활동 중인 하이퍼레저 프로젝트로서 초기에 IBM이 제공한 44,000여 줄의 코드를 바탕으로 현재 전 세계 개발자들이 개발에 참여하고 있습니다. 허가형 프라이빗 블록체인(Permissioned and Private Blockchain) 형태로 개발되었으며, 이더리움, 비트코인 등 누구나 참여할 수 있는 퍼블릭 블록체인과는 달리 MSP(Membership Service Provider)라는 인증 관리 시스템에 등록된 사용자만이 하이퍼레저 패브릭 블록체인에 참여할 수 있습니다.

하이퍼레저의 패브릭 참여자들은 비즈니스 목적에 알맞은 형태로 블록체인 플랫폼을 구축하는 것을 목표로 개발되고 있습니다. 예를 들어 금융, 물류, 의료 등 다양한 형태의 비즈니스 데이터를 원장에 기록할 수 있으며, 비즈니스 시스템에 적합한 블록 생성 알고리즘이나 트랜잭션 보증 정책을 선택할 수도 있습니다. 또한, 채널(Channel)이라는 개념을 도입해서 블록체인 참여자들 간의 프라이버시를 강화할 수도 있습니다.

이 책의 구성

이 책은 블록체인에 대한 간략한 설명(1장), 하이퍼레저 패브릭 구조 분석(2장), 하이퍼레저 패브릭 시스템 운영 실습(3장), 프라이빗 트랜잭션(4장)으로 구성되어 있습니다.

- 1장: 블록체인에 대한 전반적인 설명과 함께 하이퍼레저 프로젝트, 하이퍼레저 패브릭을 간략하게 설명합니다.
- 2장: 하이퍼레저 패브릭을 구성하는 각각의 구성요소의 역할과 기능에 대하여 설명합니다. 다음으로, 하이퍼레저 패브릭에서 블록체인 네트워크 구축 과정을 학습한 후 구축된 블록체인 네트워크에서 트랜잭션이 처리되는 흐름에 대해 자세히 알아볼 것입니다.
- 3장: 버추얼박스로 VM을 생성한 후 실제 네트워크 환경과 유사한 멀티호스트 네트워크 환경에서 하이퍼레저 패브릭을 직접 운영해 봅니다. 하이퍼레저 패브릭에서 제공하는 도구인 cryptogen을 이용하여 시스템을 구축하는 방법, Fabric-CA를 이용하여 시스템을 구축하는 방법, 마지막으로 Intermediate CA를 포함하여 시스템을 구축하는 실습 내용을 담고 있습니다.
- 4장: 하이퍼레저 패브릭 1.2 버전에서 추가된 프라이빗 트랜잭션에 대한 설명과 개인 정보 관리 기능에 대해 알아봅니다.

이 책의 대상 독자

다음과 같은 분들이 이 책을 읽는다면 블록체인 기술을 습득하는 데 많은 도움이 되리라 생각합니다.

- 블록체인 기술을 배우고 싶은 IT 전공자
- 블록체인 플랫폼 혹은 서비스를 개발 중인 개발자
- 자신의 회사/기관 등에 블록체인 기술 적용을 고려 중인 관리자
- 그 밖에 블록체인 기술에 관심 있는 IT 업계 종사자

집필 후기 및 감사 인사

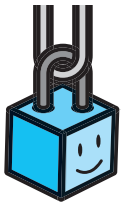
8월의 무더운 여름에 책을 쓰기 시작했는데 쌀쌀한 늦가을이 되어서야 출판이 눈앞에 보이네요. 책을 쓰기로 마음먹고 원고를 탈고하기까지 업무 시간과 약간의 수면 시간을 제외한 대부분의 시간에는 원고만 썼습니다. 이렇게 많은 노력을 기울였음에도 막상 원고를 탈고하고 나니 아쉬움이 많이 남네요. 부족하지만 이 책이 여러분을 블록체인 전문가로 만들 수 있는 좋은 입문 서적이 되면 좋겠습니다. 책의 부족한 부분에 대한 피드백은 언제든지 환영입니다. 제 이메일(myhoneydressing@gmail.com)로 연락해 주시면 빠른 시간 안에 답변드리도록 하겠습니다.

이 책은 많은 사람의 도움으로 탄생했습니다. 먼저, 원고를 멋진 책으로 편집해 주신 제이펍 출판사 관계자분들께 감사드립니다. 편집 과정에서 너무나 잘 도와주셨기 때문에 한층 더 완성도 있는 책을 출판할 수 있었습니다. 제가 ETRI 블록체인기술연구센터에 소속되지 않았다면 이 책은 세상에 나오지 못했을 겁니다. 연구에 집중할 수 있도록 항상 신경 써 주시고 부족한 저를 잘 이끌어 주시는 ETRI 블록체인기술연구센터 연구원들께도 감사드리고, 국가 IT 기술 발전을 위해 항상 노력하는 ETRI 구성원 모두에게도 감사드립니다. 그리고 이렇게 좋은 직장에 입사하여 좋은 동료들을 만나기까지 저에게 물심양면 무한한 도움을 주신 부모님께 감사드립니다.

마지막으로, 뭐든지 할 수 있는 용기를 주고 항상 옆에서 힘이 되어 주는, 서로의 정신적인 버팀목이자 사랑하는 저의 피앙세 최지혜에게도 고맙다는 말을 전합니다. "나도 지혜가 뉴욕에서 힘든 전공의 과정을 무사히 마치고 더 훌륭한 의사가 될 수 있도록 곁에서 힘이 되어 줄게!"

윤대근

추천사



박세열 _ IBM 블록체인 기술총괄(상무), 이화여자대학교 컴퓨터공학 겸임교수

IBM은 2014년 말부터 2015년 초에 블록체인 기술을 광범위하게 탐구하기 시작했습니다. 사용 가능한 모든 플랫폼, 특히 오픈소스로 제공되는 플랫폼들을 시험해 보았으며, 기업들의 블록체인 솔루션에 대한 요구사항을 더 잘 이해하기 위해 많은 기업 고객들과 개념 검증(Proof of Concept) 프로젝트를 수행하였습니다. 그 결과, 기존 플랫폼 중 어느 것도 기업들의 요구사항을 실제로 충족시키지 못한다는 결론에 이르게 됩니다. 이에 IBM은 기업들만을 대상으로 한 기업용 블록체인 기술을 개발하게 되었습니다. 또한, 블록체인 기술이 시장에서 성공하기 위해서는 이를 오픈소스로 공개해야만 한다는 것을 인지하고 있었습니다. 그래서 IBM은 리눅스 재단과 협력하여 2015년 12월에 하이퍼레저 프로젝트 조직 참여를 사전에 발표하고, 오픈 거버넌스 모델하의 프로젝트 조직 구성을 돕기 위한 예비 스폰서들을 초청했습니다. 드디어 2016년 2월에 IBM을 비롯한 30명의 초기 회원 및 11명의 프리미어 회원이 공식적으로 창립되었습니다. 이에 IBM은 2015년부터 개발해 온 자산인 44,000여 줄에 해당하는 '오픈 블록체인(Open Blockchain)' 코드를 기부하였는데, 이것이 하이퍼레저 패브릭 프로젝트의 기원이 됩니다.

이 패브릭은 퍼블릭 블록체인의 한계를 넘어 멤버십, 성능, 거버넌스, 프라이버시, 결제의 완결성 등 기업들이 활용하는 허가형 블록체인 솔루션으로 모든 산업에 적용 가능한 산업의 표준으로 자리매김할 것입니다. 또한, 글로벌 기업들의 구축 사례 대부분은 하이퍼레저 패브릭을 기반으로 적용되어 있습니다. 이제 하이퍼레저 패브릭은 가상화폐를 뛰어넘어 금융산업, 에너지산업, 식품산업, 의료산업, 제조산업 등 산업 전반에 활용되어 새로운 미래의 청사진을 제시할 것입니다.

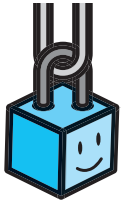
이 책을 통해 독자들은 하이퍼레저 패브릭의 구조와 시스템 운영에 대한 개념을 쉽고 빠르게 접할 수 있을 것입니다. 또한, 풍부한 그림과 예제를 통해 하이퍼레저 쉽게 이해할 수 있을 것입니다. 복잡한 시스템 운영 방식이 친절한 설명과 함께 제시되어 있어 실제 다양한 상황에 적용해 보기에도 쉽습니다. 특히, 패브릭을 활용한 비즈니스 및 시스템 기획, 애플리케이션 개발, 시스템 구축 및 운용에 종사하는 사람들에게 많은 도움이 될 뿐 아니라, 패브릭에 대한 관심을 높이는 계기가 되리라 생각합니다.

인 호 _ (사)한국블록체인학회 초대 학회장, 고려대 컴퓨터학과 교수

인류 역사에 있어서 분산원장을 기반으로 한 최초의 디지털 머니인 비트코인, 이 비트코인이 중앙집권식 금융산업에서 탈중앙화된 금융산업으로 바꾸고 있습니다. 이것이 1세대 블록체인 혁명입니다. 스마트 컨트랙트를 기반으로 한 이더리움이 제3자 신뢰 방식 계약에서 탈중앙화된 계약 방식으로 다시 한번 세상을 바꾸고 있습니다. 이것이 2세대 블록체인 혁명입니다. 하지만 모든 장부를 모두가 볼 수 있는 공개형 블록체인(Public Blockchain) 기술은 영업비밀이 많은 기업에 그대로 적용할 수 없습니다. 또한, 트랜잭션에 필요한 성능을 만족시킬 수 없습니다. 따라서 이제는 프라이빗 블록체인 기술이 각광을 받기 시작했습니다. 현재 가장 앞서가고 있는 프라이빗 블록체인 기술은 IBM을 필두로 개발 중인 오픈소스 프로젝트인 하이퍼레저 패브릭입니다. 이 책은 글로벌 대표적인 프라이빗 블록체인 중 하나인 하이퍼레저 패브릭에 대해 자세히 기술되어 있습니다.

만약 독자가 하이퍼레저 패브릭이나 프라이빗 블록체인에 관심이 있다면 이 책은 큰 도움이 될 것입니다. 하이퍼레저 패브릭은 다른 블록체인 플랫폼과는 달리 시스템 구조와 사용법이 복잡하기 때문에 진입장벽이 높고, 블록체인에 해박한 지식이 없다면 이해하고 사용하는 데 많은 시간이 소요될 수 있습니다. 이 책은 하이퍼레저 패브릭에 대한 구조를 풍부한 예시와 그림으로 이해하기 쉽게 설명하고 있고, 어려운 시스템 사용법을 IT 기초 지식만 있으면 누구나 따라 하고 이해할 수 있도록 실습 예제를 담고 있습니다. 또한, 블록체인을 처음 배우려는 독자들에게도 좋은 입문서가 될 것입니다. 이 책을 통해 한국에서 더 많은 개발자, 연구자가 블록체인에 기술적 관심을 두는 계기가 되어 한국의 블록체인 기술 영향력을 확대하는 데 많은 도움이 되기를 바랍니다.

베타리더 후기



김용현(마이크로소프트MVP)

이 책은 블록체인 기술의 한 축인 하이퍼레저 패브릭에 대한 개념과 실습 환경을 친절한 설명과 예제를 통해 제공해 줍니다. 하이퍼레저 패브릭을 처음 접하거나 블록체인 기술에 대한 개념을 쉽고 간략하게 실습을 통해 익히고 싶은 분들에게 추천합니다. 깔끔한 내용과 쉬운 설명, 그리고 간결하면서 확실한 환경 설명, 모나지 않고 반드시 실행되는 실습이 매우 인상 깊었습니다. 개인적으로 조금만 더 깊은 내용을 다루거나, 아니면 응용 사례와 같은 내용이 있으면 더 좋았을 것 같기도 하지만, 초심자를 대상으로 하는 도서인 만큼 기획 의도에 충분히 부합하는 책인 것 같습니다.

김종욱(네이버)

하이퍼레저 패브릭이 무엇인지 한눈에 파악할 수 있도록 잘 정리된 책입니다. 본 도서를 통해 하이퍼레저의 개념과 용도 그리고 기존의 블록체인 방식과 무엇이 다른지를 손쉽게 파악할 수 있었습니다. 다만, 책의 수준은 어디까지나 처음 입문하는 사람의 눈높이에 맞추었기 때문에 하이퍼레저 패브릭을 어느 정도 아시는 분이라면 보다 심화된 내용을 다루는 책을 찾아 읽기를 권합니다.

박재유(LG전자)

올해의 IT 기술 트렌드는 단연 블록체인일 것입니다. 많은 사람들이 비트코인과 블록체인을 혼동하지만, 사실 블록체인이라는 기술 자체는 금융뿐만 아니라 다른 산업에도 광범위하게 응용이 가능한, 암호학 기술의 결정체라 할 수 있습니다. 하이퍼레저 패브릭은 리눅스 재단의 주도로 만들어진 오픈소스 블록체인 프로젝트입니다. 퍼블릭 혹은 프라이빗 형태로도 운영이 가능하므로, 관련 사업을 새롭게 추진하려는 분들에게 이 책이 좋은 지침서가 될 것 같습니다.

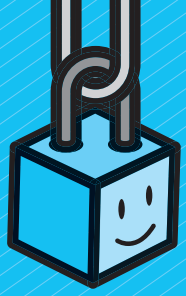
손승하(삼성전자)

리눅스 파운데이션에 의해 시작된 하이퍼레저 패브릭은 엔터프라이즈 콘텍스트에서 사용하도록 설계된 오픈소스 프로젝트입니다. 이 도서는 많은 개발자가 참여하여 빠르게 성장하고 있는 프로젝트를 쉽게 명확하게 설명하고 있습니다. 전체 구조와 동작 원리를 쉽고 빠르게 접하길 원하시는 분들에게 이 책을 추천합니다.

장성만(incowiz)

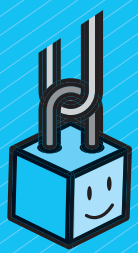
프라이빗 블록체인 플랫폼이자 다양한 산업군에 범용적으로 도입 가능한 하이퍼레저 패브릭에 대한 개념을 빠르게 잡기에 좋은 책입니다. IBM이 깃허브를 통해 제공하는 예제보다 실제 운영 구축에 필요한 사항이 세세하게 정리되어 있는 것이 이 책의 큰 장점입니다. 실제 구축 환경이 자세히 설명되어 있어서 아주 만족스러웠습니다.

제이펍은 책에 대한 애정과 기술에 대한 열정이 뜨거운 베타리더들로 하여금
출간되는 모든 서적에 사전 검증을 시행하고 있습니다.



CHAPTER

1 블록체인 이해하기



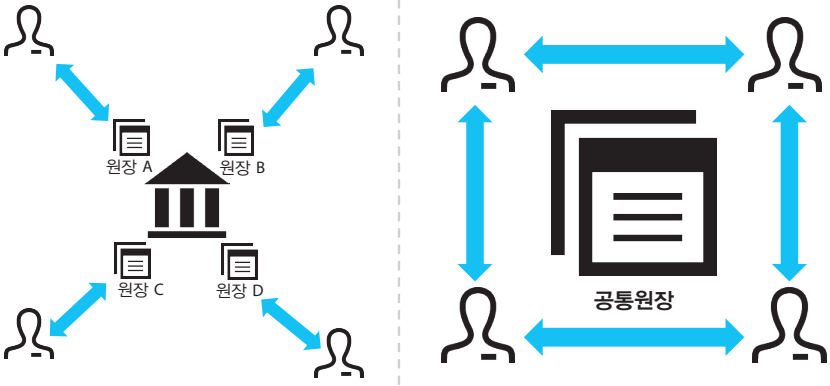
1.1 블록체인이란?

하이퍼레저 패브릭(Hyperledger Fabric)을 소개하기에 앞서 블록체인(Blockchain)을 처음 접하시는 분들을 위해 블록체인의 주요 개념을 간단하게 짚고 넘어가겠습니다. 1장에서는 블록체인의 동작 방식과 핵심 구성요소인 분산원장, 스마트 컨트랙트, 합의를 간략하게 설명한 후 하이퍼레저 패브릭이 기존의 블록체인과 비교해서 어떠한 특징이 있는지 설명하겠습니다.

1.1.1 분산원장

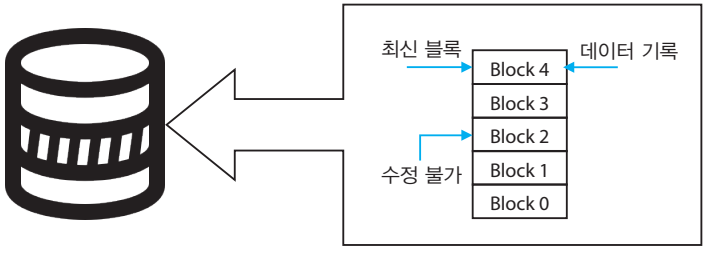
분산원장(Distributed Ledger)은 블록체인을 구성하는 가장 중요한 요소 중 하나입니다. 또한, 블록체인을 탈중앙화된 시스템으로 만들어 주는 핵심 기술입니다. 거래 기록 등의 데이터를 저장하는 데이터베이스(원장)를 중앙화된 서버가 소유하는 것이 아니라, 블록체인에 참여하는 모든 사람이 동일한 원장을 소유하고 관리하는 기술을 일컫습니다. 기존의 시스템에서는 동일한 비즈니스 네트워크에서도 사용자마다 서로 다른 원장에 비즈니스 정보를 기록하는 것과는 달리 블록체인에서는 블록체인 사용자 모두 동일한 원장에 비즈니스 정보를 기록하고 관리합니다. 예를 들어, A 은행을 이용하는 고객들은 각각의 서로 다른 고유한

계좌(원장)를 가지고 금융 정보를 기록하는 반면, 다들 잘 알고 있는 비트코인, 이더리움 등과 같은 블록체인 플랫폼의 경우 모든 사용자에 대한 거래 기록이 하나의 비트코인 원장에 모두 기록됩니다. 하지만 이러한 구조에서는 프라이버시 문제가 발생할 수 있는데, 하이퍼레저 패브릭에서는 **채널(Channel)** 개념을 도입하여 프라이버시 문제를 해결하였습니다. 채널에 대해서는 2장에서 좀 더 자세히 다루겠습니다.



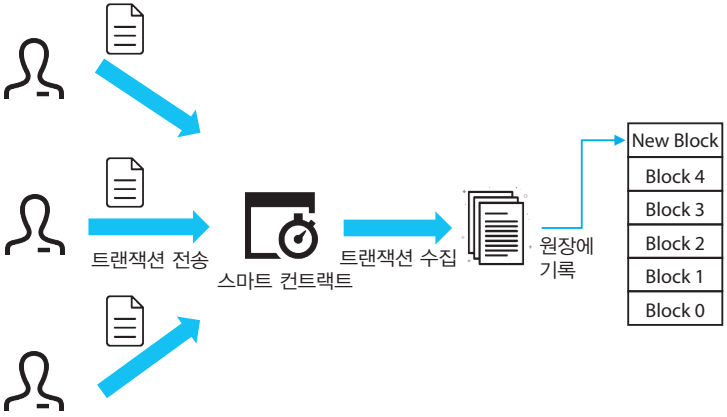
● **오늘날 비즈니스 네트워크 VS 블록체인 비즈니스 네트워크**

블록체인 분산원장의 또 다른 특징은 모든 정보가 해시화되어 Append-only 방식으로만 원장에 저장되기 때문에 한번 원장에 기록된 정보들은 절대 수정할 수 없습니다. 이와 같은 **불가변성(immutability)**의 특성은 블록체인 데이터에 대한 악의적인 변조를 불가능하게 만들어 데이터에 대한 신뢰도를 향상시켜 주는 역할을 하게 됩니다.



● **블록체인의 Append-only 저장 방식**

1.1.2 스마트 컨트랙트



● **스마트 컨트랙트를 통한 분산원장 접근 예시**

블록체인 참여자는 **스마트 컨트랙트(Samat Contract, 스마트 계약)**를 통해서 분산원장에 정보를 기록하거나 불러올 수 있습니다. 또한, 스마트 컨트랙트를 이용하여 단순히 거래 정보를 읽고 쓰는 것뿐만 아니라 프로그래밍을 통해 거래 자동화 등의 다양한 응용프로그램을 만들 수도 있습니다. 예를 들어, 그룹 공동 명의의 계좌를 만들어서 특정 인원 수 이상의 서명이 있어야 잔액을 출금할 수 있는 기능이나, 특정 날짜에 월급이 입력되는 기능 등을 스마트 컨트랙트를 통해 구현할 수 있습니다. 또한, 스마트 컨트랙트를 좀 더 편리하게 사용하기 위해 개발되는 프로그램을 **분산 애플리케이션(Decentralized Application, DApp)**이라고 하는데, 하이퍼레저 패브릭에서 스마트 컨트랙트와 분산 애플리케이션이 어떻게 동작하는지는 2장에서 좀 더 자세히 살펴보겠습니다.

1.1.3 합의

앞 절에서 블록체인에 참여하는 모든 사람이 동일한 원장을 소유해야 한다고 설명했습니다. 이러한 조건을 만족시키기 위해 비트코인과 이더리움에서는 블록체인에 참여한 모든 노드 중 암호화된 퍼즐의 답을 가장 먼저 찾아내는 노드의 블록을 최신

블록으로 업데이트하는 PoW(Proof of Work) 방식이 있습니다. EOS는 블록체인 참여자가 21명의 블록 생성자를 선출하여 선출된 블록 생성자가 최신 블록을 생성하는 DPoS(Delegated Proof of Stake) 방식을 사용합니다. 이 밖에도 대부분의 블록체인 플랫폼에서 PoW와 PoS 알고리즘을 기반으로 PBFT(Practical Byzantine Fault Tolerance), Casper PoS, RPCA(Ripple Protocol Consensus Algorithm) 등으로 변형하여 합의 과정에 사용하고 있습니다.

하이퍼레저 패브릭에서는 조금 다른 관점으로 합의 알고리즘을 정의합니다. 하이퍼레저 패브릭의 합의 과정은 PoW, PoS 혹은 BFT와 같이 합의 과정을 특정 알고리즘에 국한시키지 않고 아래 세 가지 일련의 과정을 통틀어 합의 과정이라고 말합니다.

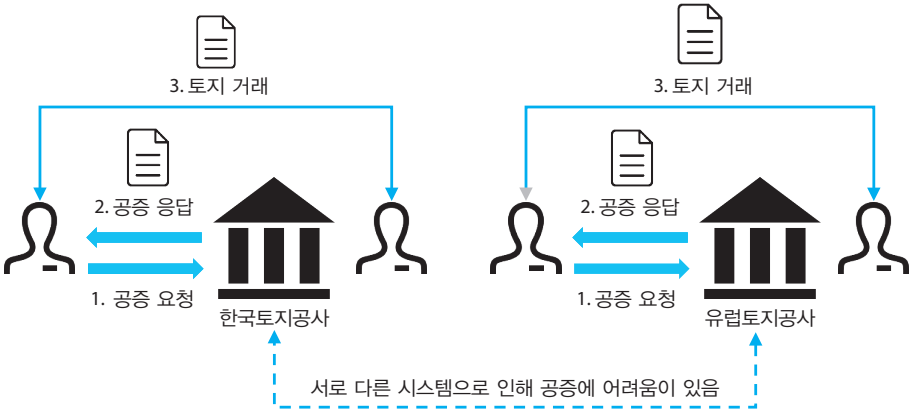
- 보증 정책 확인
- 트랜잭션을 정해진 순서에 맞춰 정렬
- 정렬된 트랜잭션의 유효성 검증 후 최신 블록 업데이트

각 항목별로 자세한 합의 과정은 2장에서 설명할 예정입니다.

1.2 블록체인은 어떻게 사용될 수 있을까?

1.2.1 오늘날의 비즈니스 모델

오늘날 대부분의 비즈니스 모델에서는 신뢰성 있는 거래를 위해 중개자(intermediary)가 꼭 필요하게 됩니다. 현금 보유량을 증명하려면 은행이 현금 보유량에 대한 증명을 대신 해 줘야 하고, 토지 소유에 대한 증명은 부동산이 토지에 대한 증명을 대신 해 줘야만 합니다. 이렇게 중개자를 거치는 거래 방식은 높은 수수료를 유발함과 동시에 자산 증명에 많은 시간이 소요됩니다. 또한, 각각의 중개자마다 데이터를 기록하는 시스템이 모두 다르기 때문에 중개자들 간에 자산을 증명하는 작업에도 상당한 시간과 비용이 소모되고 있습니다.

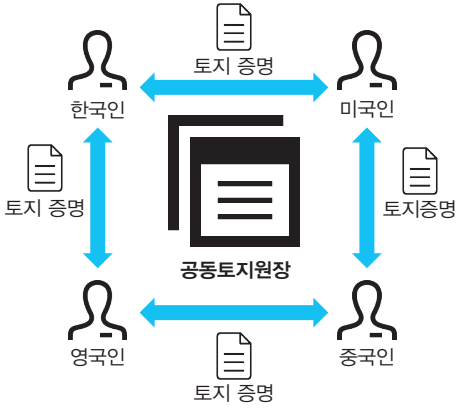


• **오늘날의 비즈니스 네트워크**

예를 들어, 한국 부동산에 등록된 토지 재산을 유럽에서 증명해야 한다고 가정해 봅시다. 먼저, 한국에서 부동산(복덕방) 등을 통해 토지에 대한 공증을 받은 후 유럽으로 관련 서류를 보내야겠죠. 한국으로부터 토지 증명 서류를 수신한 유럽에서는 다른 언어 혹은 다른 양식으로 기록된 해당 공증에 대한 확인에 큰 비용과 시간이 소요될 것입니다.

1.2.2 블록체인 비즈니스 모델

블록체인 비즈니스 모델에서는 현금 보유량이나 토지 증명 등을 중개자 없이 거래 참여자들 간에 수행할 수 있습니다. 거래 당사자들 간에 직접 수행하는 합의 알고리즘(Consensus Algorithm)을 통해 중개자 없이도 신뢰성 있는 거래가 가능하게 되는 것입니다. 또한, 원장에 한번 기록된 정보는 수정이나 변경이 불가능하여 거래 기록에 대한 신뢰성이 제공됩니다. 이러한 블록체인 비즈니스 모델에서는 중개자가 없기 때문에 중개 수수료를 절감함과 동시에 하나의 일관된 시스템에서 거래가 발생하므로 자산 증명에 대한 시간과 비용을 절약할 수 있습니다.



• **블록체인 비즈니스 네트워크**

1.3 하이퍼레저 패브릭 소개

1.3.1 하이퍼레저 프로젝트 소개

2015년, 리눅스 재단에서는 기업용 블록체인 개발을 위해 **하이퍼레저(Hyperledger)** 프로젝트를 만들었는데, 오픈 소스 형태의 프로젝트로서 전 세계 기업과 개발자들이 자발적으로 기술 개발에 참여하는 프로젝트입니다. IBM, Cisco, American Express, 화웨이 등 외국계 기업뿐만 아니라 카카오페이, 삼성SDS 등 국내 기업도 함께 참여하고 있습니다(2018년 기준). 하이퍼레저 프로젝트는 다음과 같이 크게 두 가지로 나뉩니다.

- 하이퍼레저 프레임워크(Hyperledger Frameworks)
- 하이퍼레저 툴(Hyperledger Tools)

하이퍼레저 프레임워크

하이퍼레저 프레임워크(Hyperledger Frameworks)는 분산원장, 스마트 컨트랙트, 합의 알고리즘 등 블록체인에 대한 원천적인 기술을 개발하는 프로젝트입니다. 대표적으로, 다음과 같은 하이퍼레저 프레임워크가 있습니다.

- **하이퍼레저 프레임워크 프로젝트 소개**

프로젝트 이름	특징
HYPERLEDGER FABRIC	가장 활발하게 활동 중인 하이퍼레저 프로젝트로서 IBM이 제공한 44,000줄의 코드를 기반으로 개발되고 있습니다. MSP(Membership Service Provider) 기반의 접근 제어 기능을 제공하고, 트랜잭션을 블록에 정렬한 후 합의하는 방법으로는 현재 Solo, Kafka, SBFT(향후 개발 예정)가 있습니다.
HYPERLEDGER SAWTOOTH	Intel의 Intel Distributed Ledger를 바탕으로 개발되었으며, SGX(Secure Guard Extension)를 이용해 구현한 PoET(Proof of Elapsed Time) 합의 알고리즘을 사용합니다. 하이퍼레저 패브릭과 마찬가지로 동시 처리를 지원하고 높은 확장성과 모듈화를 추구하는 블록체인 플랫폼입니다.
HYPERLEDGER IROHA	블록 해시에 대한 투표로 합의를 수행하는 YAC(Yet Another Consensus) 합의 알고리즘 기반의 블록체인 플랫폼입니다. iOS, Android, JavaScript 등 모바일과 웹을 위한 인프라를 제공하기 때문에 블록체인 참여자들에게 간편한 거래 환경을 제공할 수 있는 것이 특징입니다.
HYPERLEDGER INDY	Sovrin foundation 주도로 개발되고 있는 블록체인 플랫폼입니다. 인터넷 환경에서 중개자 없이 신원을 제공하는 것을 목표로 개발 중인 블록체인 플랫폼입니다.
HYPERLEDGER BURROW	BFT(Byzantine Fault Tolerance) 합의 알고리즘 기반의 블록체인 플랫폼입니다. 대표적인 특징으로는 이더리움의 DApp을 Hyperledger Burrow 플랫폼에서 작동시킬 수 있습니다.

하이퍼레저 툴

하이퍼레저 툴(Hyperledger tools)은 블록체인 시스템의 성능 측정, 운영, 개발을 쉽게 할 수 있도록 도와주는 툴을 개발하는 프로젝트입니다. 대표적으로, 다음과 같은 하이퍼레저 툴이 있습니다.

● **하이퍼레저 툴 프로젝트 소개**

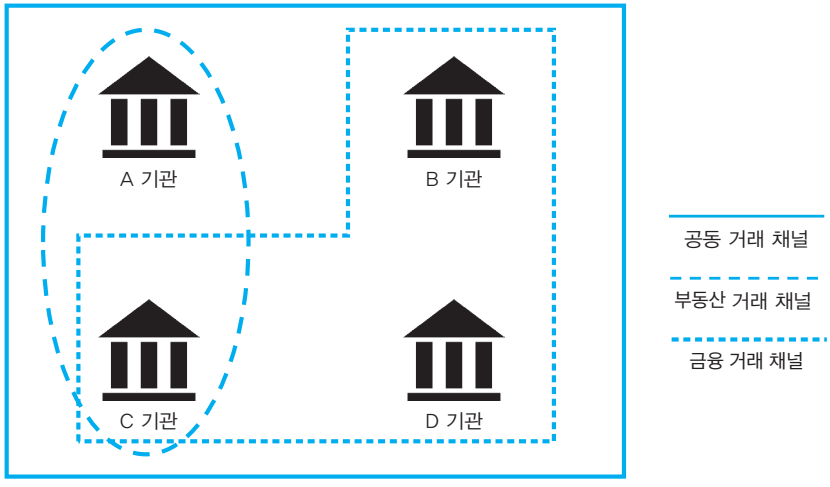
프로젝트 이름	특징
HYPERLEDGER CALIPER	블록체인 성능 측정을 위한 프로젝트입니다. 현재 Hyperledger Fabric v1.0+, Sawtooth 1.0+ Iroha 플랫폼 성능 측정을 지원하며, TPS(Transaction Per Second), Latency, Resource utilisation 등에 대한 성능을 측정할 수 있습니다.
HYPERLEDGER CELLO	블록체인의 운영 및 관리를 위한 프로젝트로서 블록체인 플랫폼의 생명주기를 관리하고 대시보드를 통한 시스템 상태 확인과 자원 확장 등의 기능을 제공합니다. 현재는 Hyperledger Fabric v1.0까지 지원합니다.
HYPERLEDGER COMPOSER	하이퍼레저 패브릭의 애플리케이션 개발과 기존 비즈니스 시스템, 블록체인 시스템의 통합에 편의성을 제공해 주는 프로젝트입니다. Github를 통해 소스 코드를 다운로드하여 사용할 수 있고, IBM의 Bluemix 클라우드에서 서비스를 제공하기도 합니다.
HYPERLEDGER EXPLORER	IBM과 DTCC의 주도로 개발 중인 블록체인 모니터링 툴입니다. 현재는 하이퍼레저 패브릭 v1.0에 대한 모니터링을 지원하고 노드, 채널, 블록, 트랜잭션 등에 대한 모니터링을 할 수 있습니다.
HYPERLEDGER QUILT	서로 다른 원장 간 연동 프로토콜을 개발하는 프로젝트로서 Ripple과 NTT Data에서 처음 프로젝트를 시작하였습니다. 현재는 분산원장과 일반원장 사이의 지급 시스템 연동을 목표로 개발되고 있습니다.

1.3.2 하이퍼레저 패브릭 개요

이번 절에서는 본격적으로 하이퍼레저 패브릭의 구조를 공부하기 앞서 간략하게 몇 가지 특징을 설명하겠습니다.

하이퍼레저 패브릭은 가장 왕성하게 활동 중인 하이퍼레저 프로젝트로서, 초기에 IBM이 제공한 44,000여 줄의 코드를 바탕으로 현재 약 30여 개의 조직에서 개발에 참여하고 있습니다. **허가형 프라이빗 블록체인(Permissioned and Private Blockchain)** 형태로 개발되었으며, 이더리움, 비트코인 등 누구나 참여할 수 있는 퍼블릭 블록체인과는 달리 **MSP(Membership Service Provider)**라는 인증 관리 시스템에 등록된 사용자만이 하이퍼레저 패브릭 블록체인에 참여할 수 있습니다. MSP와 관련해서는 2.1.9 'Identity' 절과 2.1.10 'MSP' 절에서 자세히 설명하겠습니다.

하이퍼레저의 패브릭 참여자들은 비즈니스 목적에 알맞은 형태로 블록체인 플랫폼을 구축할 수 있습니다. 예를 들어 금융, 물류, 의료 등 다양한 형태의 비즈니스 데이터를 원장에 기록할 수 있으며, 비즈니스 시스템에 적합한 블록 생성 알고리즘이나 트랜잭션 보증 정책을 선택할 수도 있습니다. 또한, **채널(Channel)**이라는 개념을 도입해서 블록체인 참여자들 간의 프라이버시를 강화할 수 있습니다.



● **채널 개념 예시**

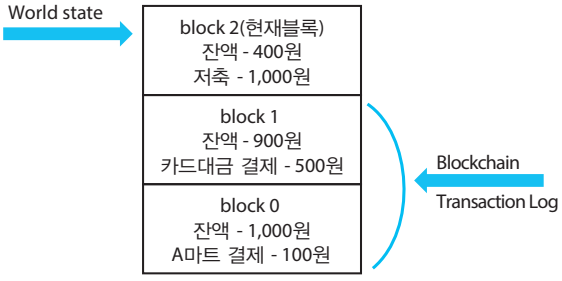
모든 사용자가 동일한 원장을 가지고 모든 정보를 공유할 수 있을 뿐만 아니라, 비즈니스에 민감한 내용을 공유하고 싶은 참여자들 간에만 채널을 통해서 별도의 원장을 생성하여 정보를 공유할 수도 있습니다. 위 그림에서 보는 바와 같이 모든 조직이 거래하는 공동 거래 채널이 존재할 수 있고, 또한 A-C 기관과 B-C-D 기관만이 거래 내용을 공유할 수 있는 부동산/금융 채널도 생성할 수 있습니다.

NOTE

위 예제에서 C 기관은 부동산 거래 채널과 금융 거래 채널의 데이터를 모두 사용할 수 있지만, 서로 다른 채널 간의 분산원장 전달은 불가능합니다. 예를 들어, A 기관으로부터 받은 원장을 B와 D 기관으로 전달할 수 없고 반대의 경우도 마찬가지입니다.

하이퍼레저 패브릭의 **원장(Shared Ledger)**은 다음과 같이 두 가지 구성요소로 이루어져 있습니다.

- 월드 스테이트(World state)
- 블록체인(Blockchain)



● **원장 구조 예시**

월드 스테이트(World state)는 원장의 현재 상태를 말합니다. 은행 잔고를 예로 들면, 현재 가지고 있는 금액이 바로 World state입니다. **블록체인(Blockchain)**은 원장의 전체 기록을 일컫습니다. 마찬가지로 은행을 예로 들면, 계좌를 만든 후부터 현재까지 결제한 모든 기록이 바로 블록체인입니다. 은행과 블록체인의 다른 점은 은행은 본인 계좌의 현재 상태와 거래 기록밖에 확인할 수 없지만, 블록체인은 모든 참여자 계좌의 현재 상태와 결제 기록을 확인할 수 있다는 점입니다(블록체인의 이러한 특성 때문에 하이퍼레저 패브릭은 채널 개념을 도입하여 채널에 참여한 사용자의 정보만을 확인할 수 있도록 프라이버시를 강화하였습니다.)

하이퍼레저 패브릭에서 스마트 컨트랙트는 **체인코드(Chaincode)**에 쓰여집니다. 체인코드는 기존의 스마트 컨트랙트와 같이 원장에 데이터를 읽고 쓰기 위해 사용될 수 있습니다. 다만, 스마트 컨트랙트와의 차이점은 **시스템 체인코드(System chaincode)**라는 특수한 체인코드를 이용하여 블록체인 시스템 설정이 가능하다는 특징이 있습니다. 체인코드에 대한 내용은 2장에서 좀 더 자세하게 다루겠습니다. 참고로, 체인코드는 현재 Go와 Node.js 언어를 지원하고 있습니다.

블록체인의 합의 알고리즘은 IT 관련 학계에서 활발하게 연구가 이루어지고 있습니다. PBFT(Practical Byzantine Fault Tolerance) 알고리즘은 블록체인 네트워크의 전체 노드가 n개라고 가정했을 때 악의적인 노드가 (n-1)/3개 이하면 정상적인 합의를 이끌어 낼 수 있는 알고리즘입니다. 비트코인과 이더리움 등은 블록체인 네트워크의 모든 노드가 동시에 암호화된 수학 퍼즐을 푸는 작업을 수행하여 가장 빠른 시간 안에 답을 찾아낸 노드가 자신의 원장을 새로운 공동 원장이라고 전파하여 합의를 진행하는 알고리즘입니다. 하이퍼레저 패브릭의 합의 알고리즘은 PBFT나 비트코인의 PoW(Proof of Work) 등의 합의 방식과는 달리, 트랜잭션의 생성부터 새로운 블록 생성까지 모든 과정을 통칭해서 합의 과정이라고 말합니다. 하이퍼레저 패브릭의 합의 방식도 2장에서 좀 더 자세히 설명하겠습니다.

1.3.3 하이퍼레저 패브릭 특징

하이퍼레저 패브릭의 대표적인 특징은 다음과 같습니다.

- 프라이버시와 기밀성
- 작업 구간별 병렬 처리
- 체인코드
- 모듈화된 디자인

하이퍼레저 패브릭은 블록체인 참여 조직 간에 채널 개념을 도입하여 **프라이버시**와 **기밀성**을 제공합니다. 예를 들어, 블록체인 참여 기업 중 특정 정보를 특정 회사에만 공유하고 싶은 경우를 가정해 봅시다. 해당 기업들은 정보를 공유하고 싶은 회사와 협정을 맺은 후 채널을 생성하여 정보를 공유할 수 있습니다. 같은 블록체인 네트워크에 있다고 하더라도 채널에 소속되지 않은 조직은 채널의 거래 내용을 확인할 수 없습니다.

● **하이퍼레저 패브릭의 3단계 데이터 처리 과정**

하이퍼레저 패브릭에서는 트랜잭션의 생성부터 합의하는 과정까지 단계별로 분리하여 처리할 수 있습니다. 첫 번째 **실행(Execute)** 단계에서는 트랜잭션을 실행하고 결괏값을 검증하는 작업을 수행합니다. 두 번째 단계인 **정렬(Order)** 단계에서는 실행 단계에서 검증이 끝난 트랜잭션을 취합하여 순서에 맞게 정렬한 후 블록을 생성하는 작업을 수행합니다. 마지막으로, **검증(Validation)** 과정에서는 블록에 포함된 모든 트랜잭션에 대한 결괏값 검증을 수행하고, 각종 디지털 인증서 등을 확인한 후 이상이 없을 시 최신 블록을 업데이트하게 됩니다. 이처럼 작업을 분리하여 처리하게 되면 트랜잭션을 실행하고 검증하는 노드와 트랜잭션을 정렬하는 노드의 부하를 줄일 수 있고, 동시에 두 가지 이상의 작업을 수행하는 병렬 처리가 가능하기 때문에 시스템의 성능 또한 향상하게 됩니다.

체인코드는 기존 블록체인의 스마트 컨트랙트와 동일한 기능을 가지고 있으며, Go와 Node.js를 이용해서 다양한 형태의 응용프로그램으로 개발될 수 있습니다. 또한, **시스템 체인코드**는 트랜잭션의 보증, 블록 검증, 채널 설정 등 시스템 레벨에서의 설정이 필요할 때 사용되는 체인코드입니다.

마지막으로, 하이퍼레저 패브릭은 시스템 구축 시 인증, 합의 알고리즘, 암호화 등의 기능을 참여자들이 원하는 형태로 선택해서 블록체인을 운영할 수 있도록 모듈화된 디자인을 지원합니다. 이와 같이 모듈화된 디자인은 하이퍼레저 패브릭 블록체인을 다양한 비즈니스 모델에 맞추어 개발할 수 있는 유연성을 제공합니다.