Matter Tunnel

허브 없는 솔루션

한양대학교 정보시스템학과

김동욱, 박기람, 신지수, 정서윤

허브의 가상화

Google을 통해 제어할 수 있는 허브가 필요합니다

Google을 통해 기기를 제어하려면 집에 Matter 지원 허브가 있어야 합니다.

스피커
Google Home, Nest Mini, Nest Audio

디스플레이
Nest Hub(1세대, 2세대), Nest Hub Max

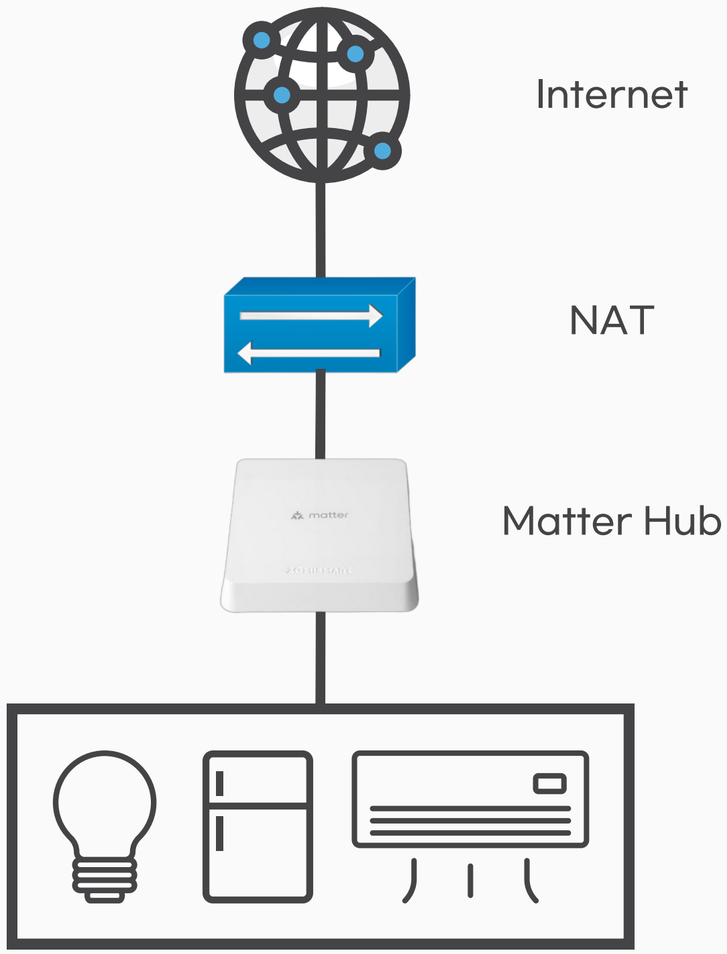
Wi-Fi
Nest Wifi Pro

허브를 구매(제공되는 지역의 경우)하거나 이 기기의 제조업체와 설정 및 제어 옵션을 확인할 수 있습니다.

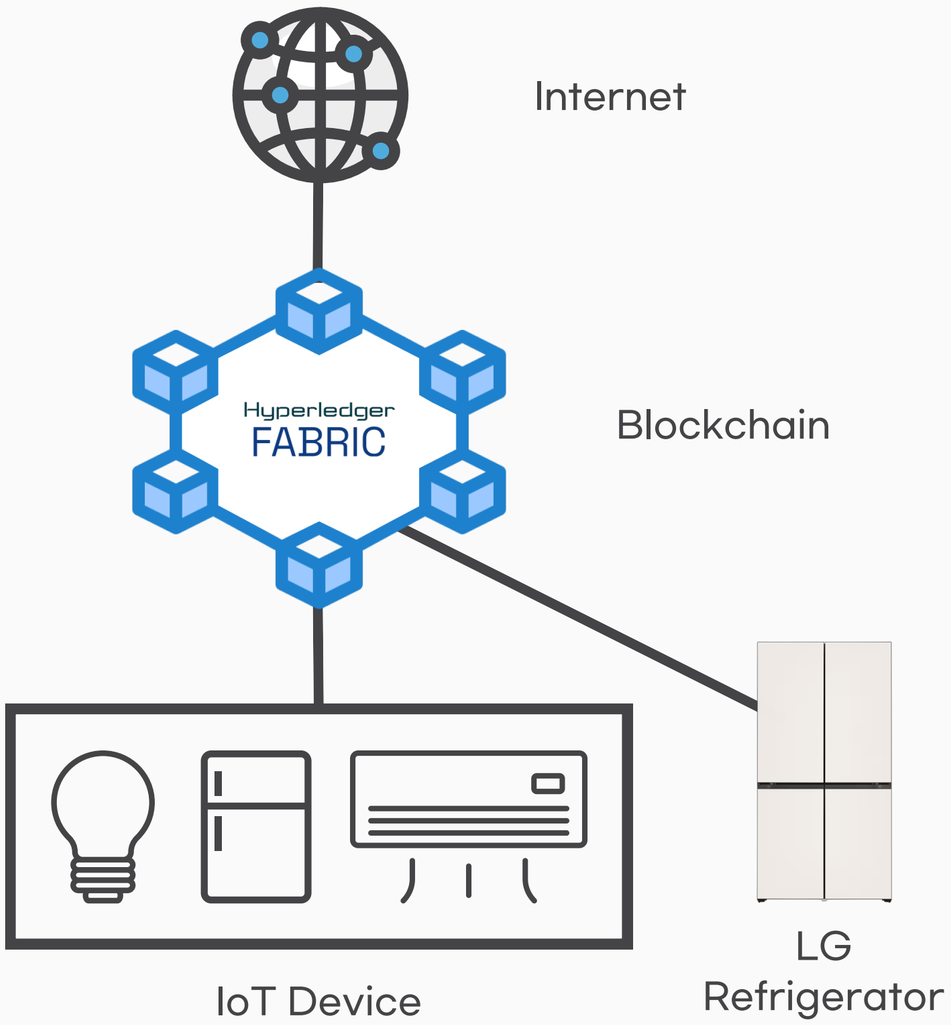
Matter hub

허브의 가상화

Current

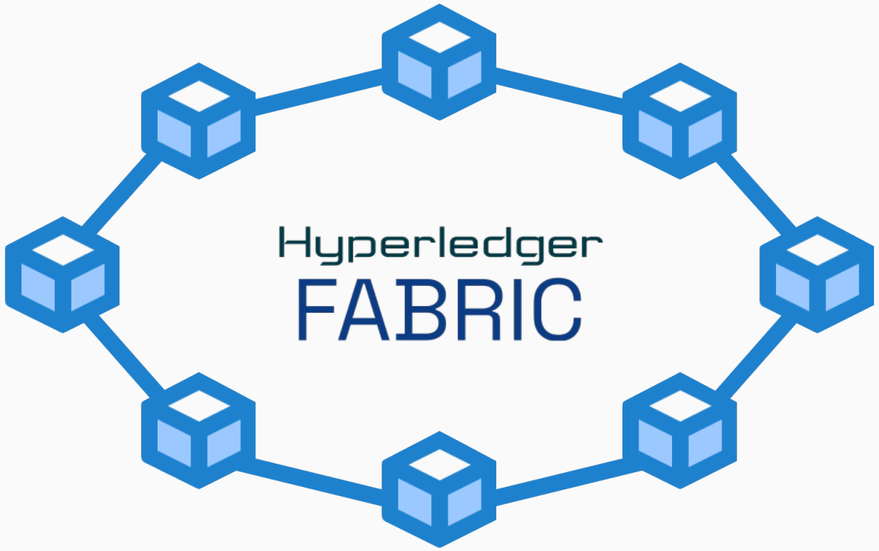


Future



자유성

Blockchain



Matter

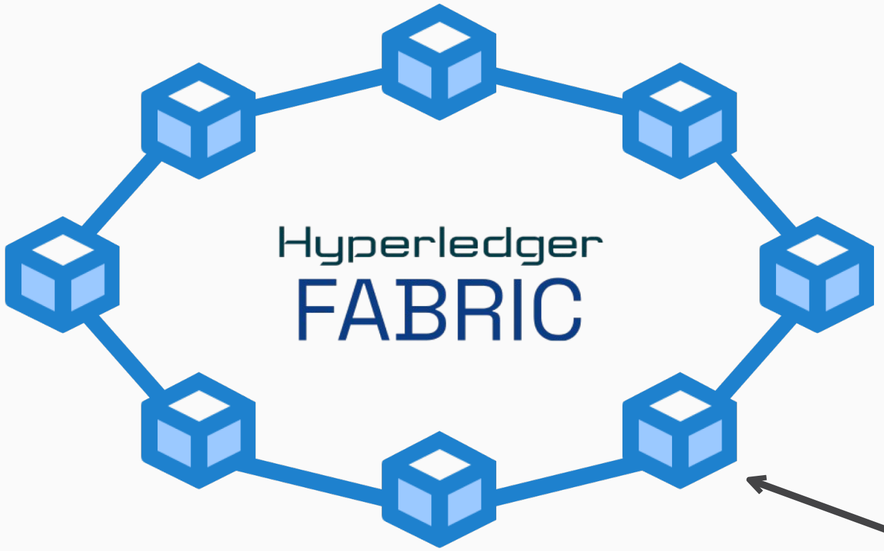
ID : 0x0052	Refrigerator And Temperature Controlled Cabinet Mode
ID : 0x0057	Refrigerator Alarm

Matter Application Cluster Library version 1.4 (MACL)

기기 간 기능을 정의하고 있음 → 기능 제약 존재

자유성

Blockchain



Matter

ID : 0x0052	rigerato emperature ntro abinet Mode
ID : 0x0057	erator Alarm

Matter Application Cl brar 1.4 (MACL)

기기 간 기능을 있음 → 기능 재

Matter Tunnel Protocol 제안

Matter Tunnel QR code

PK (33 bytes)	passcode (16 bytes)	functions (variable length)

name (18 bytes)	types (2 bytes)

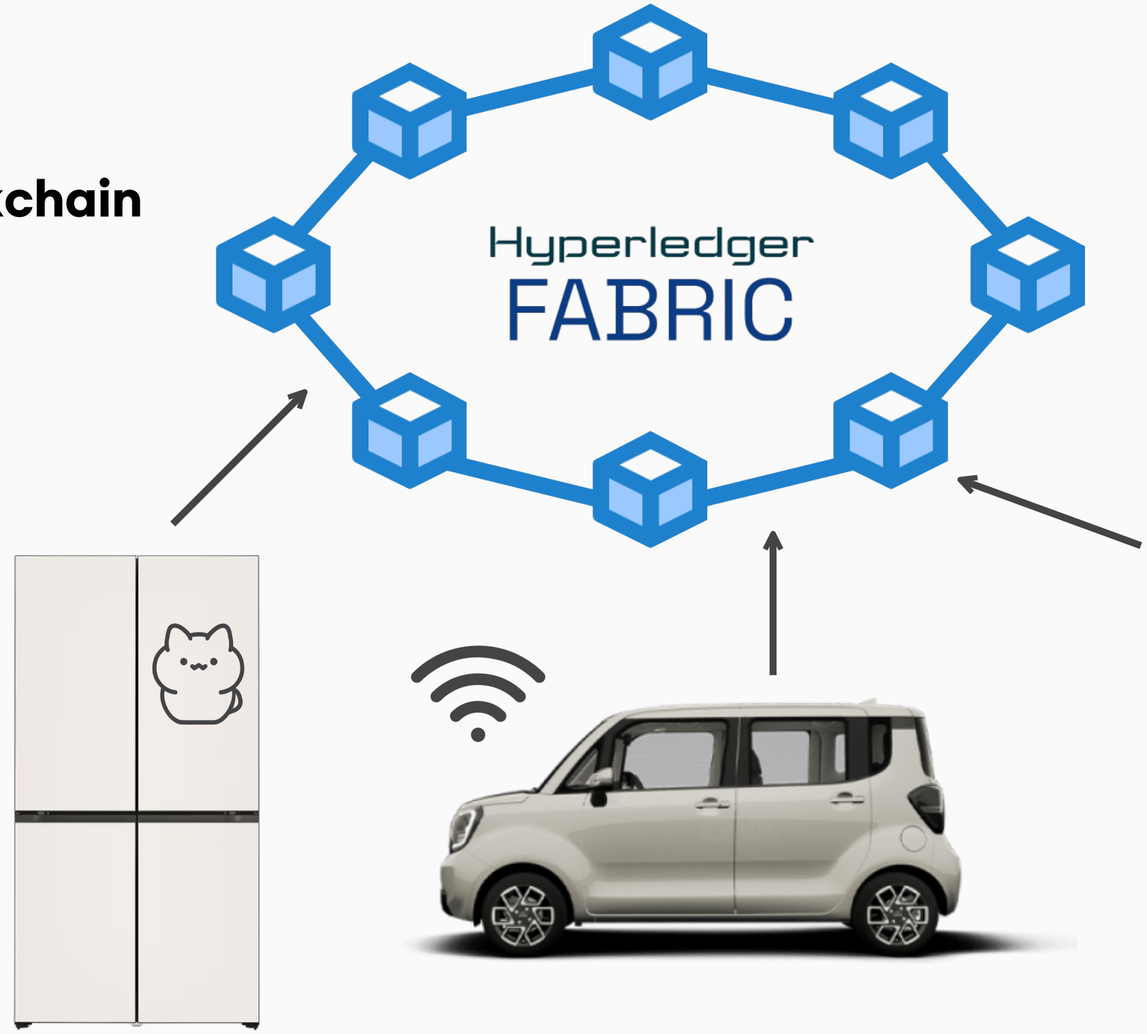
QR code 안에
디바이스 기능을 정의

Matter Tunnel TX Format

TX sign (64 bytes)	function name (18 bytes)	source PK (33 bytes)	time stamp (8 bytes)	encrypted arguments (variable length)

자유성

Blockchain



제조사가 자사 기기에 특화된 기능 정의 가능

Matter Tunnel Protocol 제안

Matter Tunnel QR code

PK (33 bytes)	passcode (16 bytes)	functions (variable length)

name (18 bytes)	types (2 bytes)

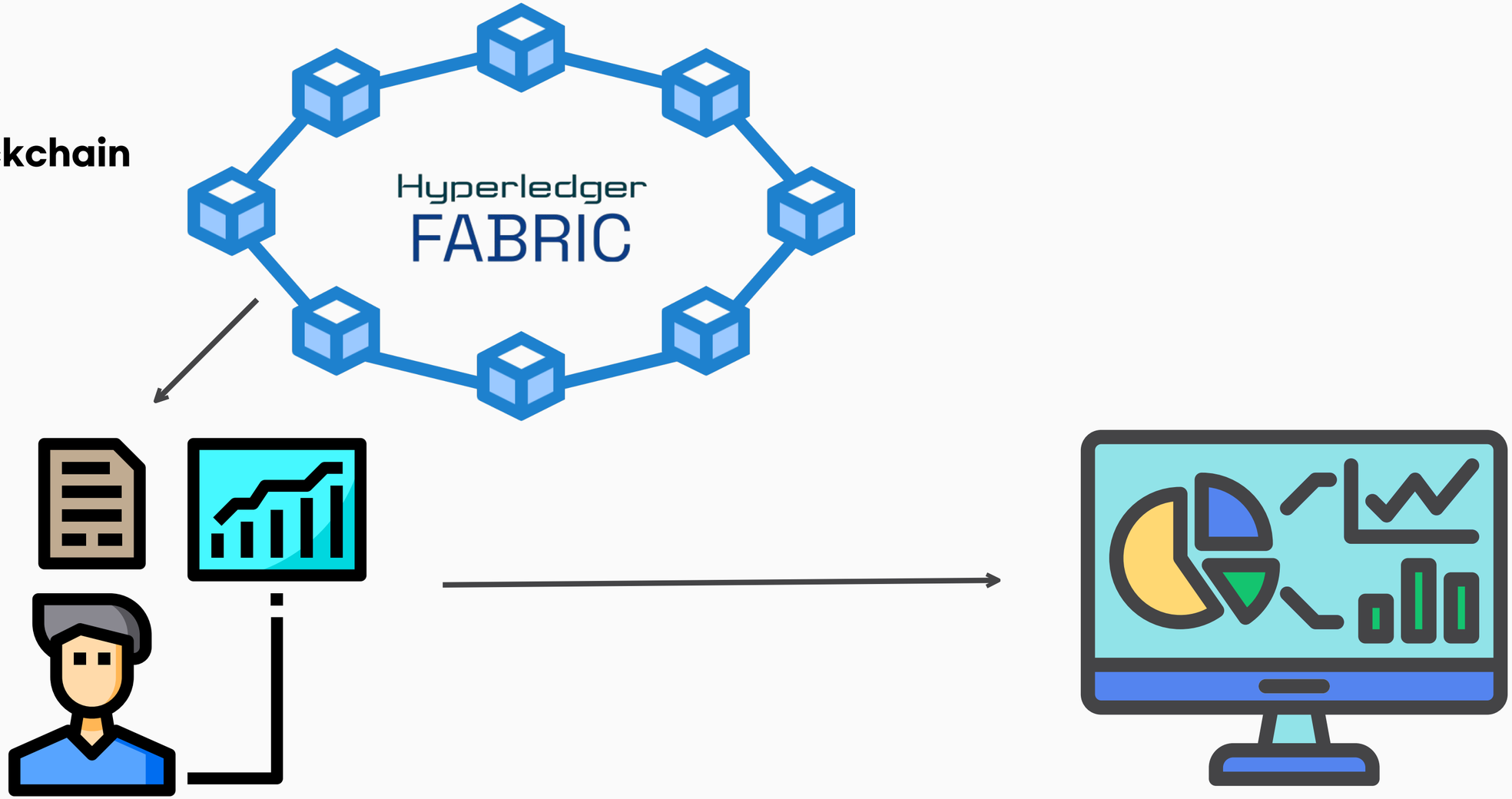
QR code 안에
디바이스 기능을 정의

Matter Tunnel TX Format

TX sign (64 bytes)	function name (18 bytes)	source PK (33 bytes)	time stamp (8 bytes)	encrypted arguments (variable length)

무결성

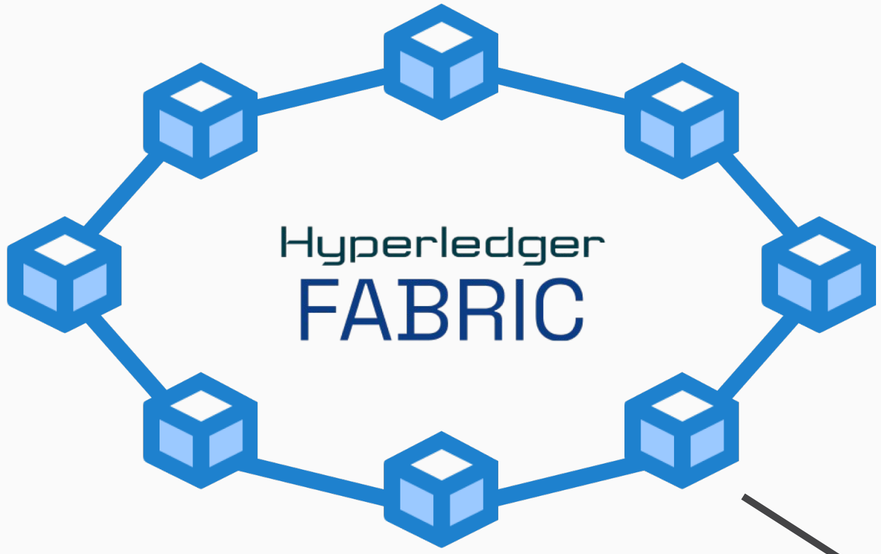
Blockchain

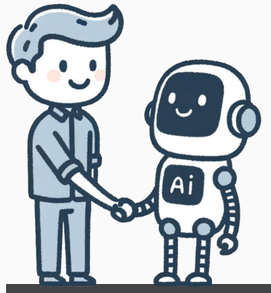


기존의 데이터 분석 시스템 : 데이터를 처리하는 중간 계층 필요

무결성

Blockchain





익명성

사용자의 프라이버시를 보장하면서
실행 함수, 타임스탬프 등 데이터 활용 가능

무결성

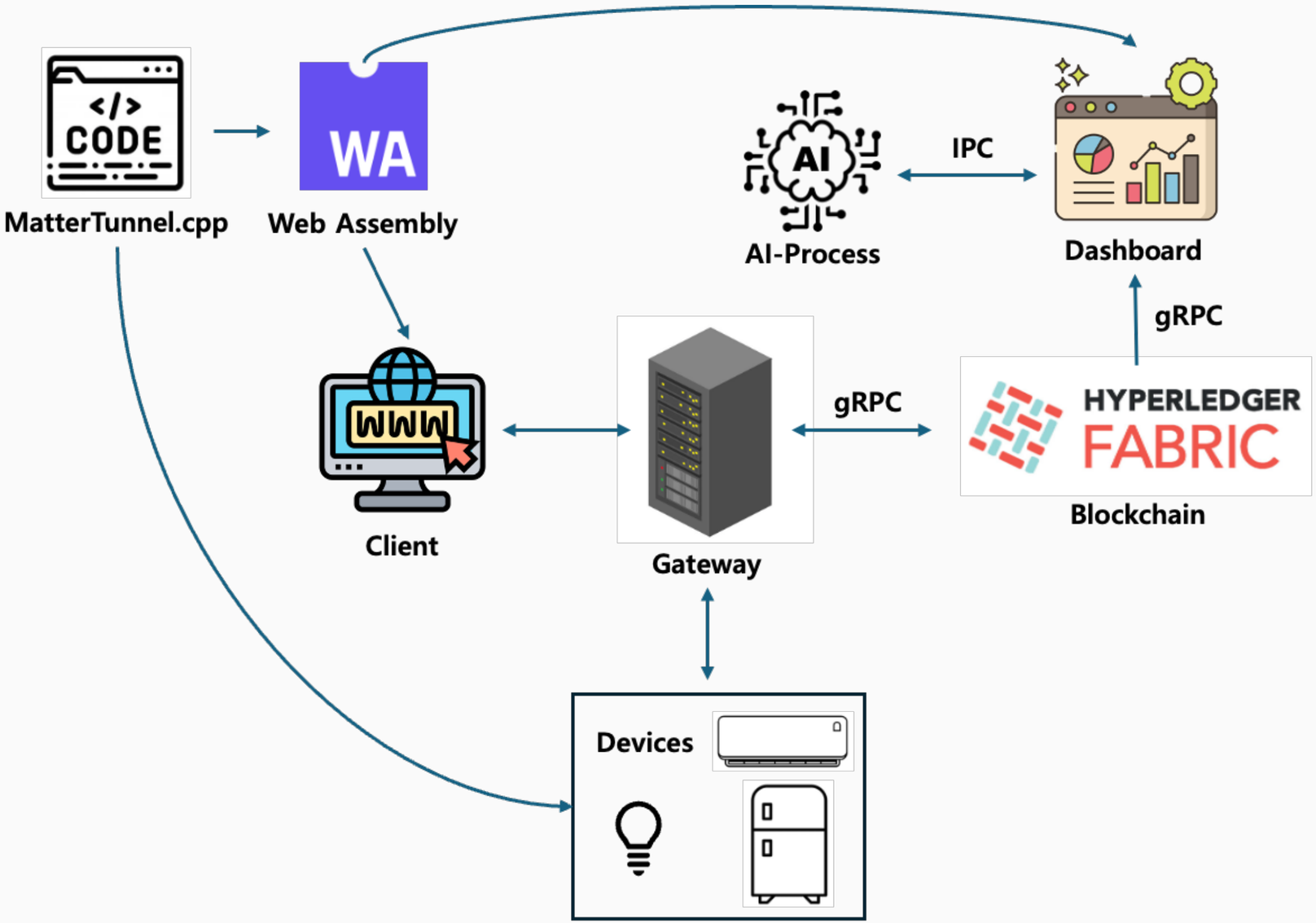
데이터 변조를 원천적으로 차단하여
정확한 의사결정 지원 가능

Matter Tunnel 데이터 분석 시스템

데이터를 처리하는 중간 계층 제거

시연 영상

전체 구조


MatterTunnel.cpp
Web Assembly
AI-Process
IPC
Dashboard
gRPC
Client
Gateway
gRPC
HYPERLEDGER
FABRIC
Blockchain
Devices

블록체인 구현 방식

Container CPU usage
1.95% / 1100% (11 CPUs available)

Container memory usage
447.68MB / 7.47GB

Show charts

Search

Only show running containers

Name	Container ID	Image	Port(s)	CPU (%)	Last started	Actions
dev-peer0.org2.example.	a9fd3a5390c4	dev-peer0.org2.example.		0%	2 minutes ago	
dev-peer0.org1.example.	3b2bff0741e1	dev-peer0.org1.example.		0%	2 minutes ago	
compose	-	-	-	1.95%	2 minutes ago	
ca_orderer	912caca86e6f	hyperledger/fabric-ca:lat	19054:19054 Show all ports (2)	0%	2 minutes ago	
ca_org2	bf2c1f84f27d	hyperledger/fabric-ca:lat	18054:18054 Show all ports (2)	0%	2 minutes ago	
ca_org1	e73cdb431480	hyperledger/fabric-ca:lat	17054:17054 Show all ports (2)	0%	2 minutes ago	
orderer.example.com	9f2f37663ea5	hyperledger/fabric-order	7050:7050 Show all ports (3)	0.04%	2 minutes ago	
peer0.org2.example.c	da77db03ab47	hyperledger/fabric-peer:l	9051:9051 Show all ports (2)	0.72%	2 minutes ago	
peer0.org1.example.c	3fb75ebb09e9	hyperledger/fabric-peer:l	7051:7051 Show all ports (2)	1.19%	2 minutes ago	

Docker Container

Hyperledger Fabric 기반의 블록체인 네트워크를 Docker 컨테이너로 구현한 것

결론 및 토의

1. Matter Tunnel : IoT 관리의 새로운 패러다임

- 허브의 가상화로 공간 제약 제거
- 기능적 다양성
- 익명성, 무결성 보장

결론 및 토의

2. 향후 계획

- 동적 링크 파일로 빌드하여 다양한 플랫폼에서의 호환성을 강화하고, 더 많은 IoT 기기와 사용 사례를 지원
- 다양한 파인튜닝 접근 방식을 활용하여 자연어 처리 시스템이 다양한 쿼리 패턴을 더 효과적으로 처리할 수 있도록 AI 대시보드 기능을 개선

감사합니다 !

노션

유튜브

깃허브

Appendix

Appendix

Hyperledger Fabric

- 높은 TPS 지원
  2,000~20,000 TPS의 처리 성능으로 실시간 디바이스 제어 지원

- 호환성 높은 보안 구조
  secp256r1 암호화와 CA 기반 인증 체계 적용으로 Matter와 동일한 보안 체계 구현

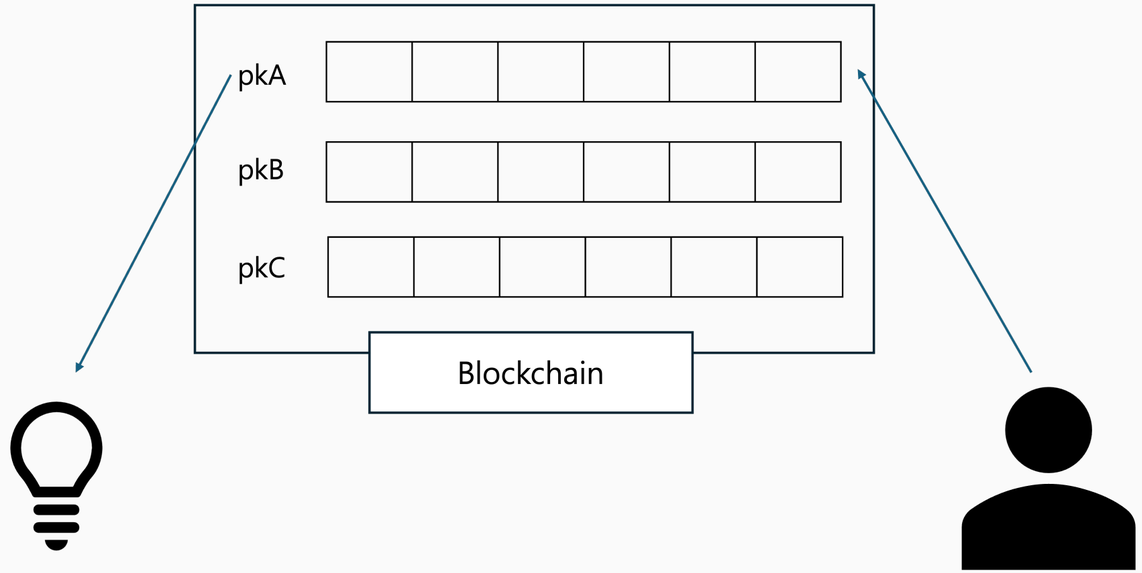
TABLE II
HYPERLEDGER FABRIC BENCHMARK RESULT

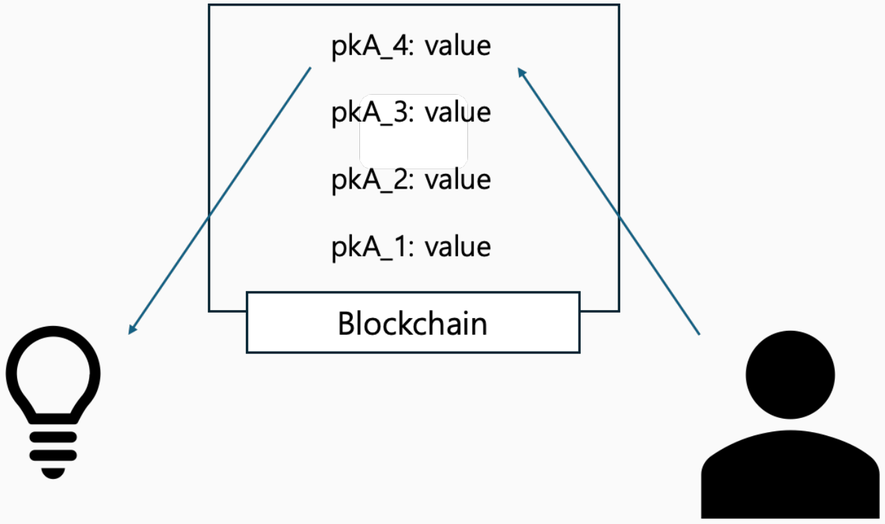
Name	Max Latency	Average Latency	Throughput
create asset 100	2.13	0.33	2946.7
create asset 1000	3.21	1.52	2938.9
read write assets previously read 100	0.21	0.06	2544.3
read write assets previously read 1000	0.26	0.11	1527.0

출처 : Benchmark testing by Hyperledger Caliper maintainer

Appendix

Queue Optimization





Blockchain Queue

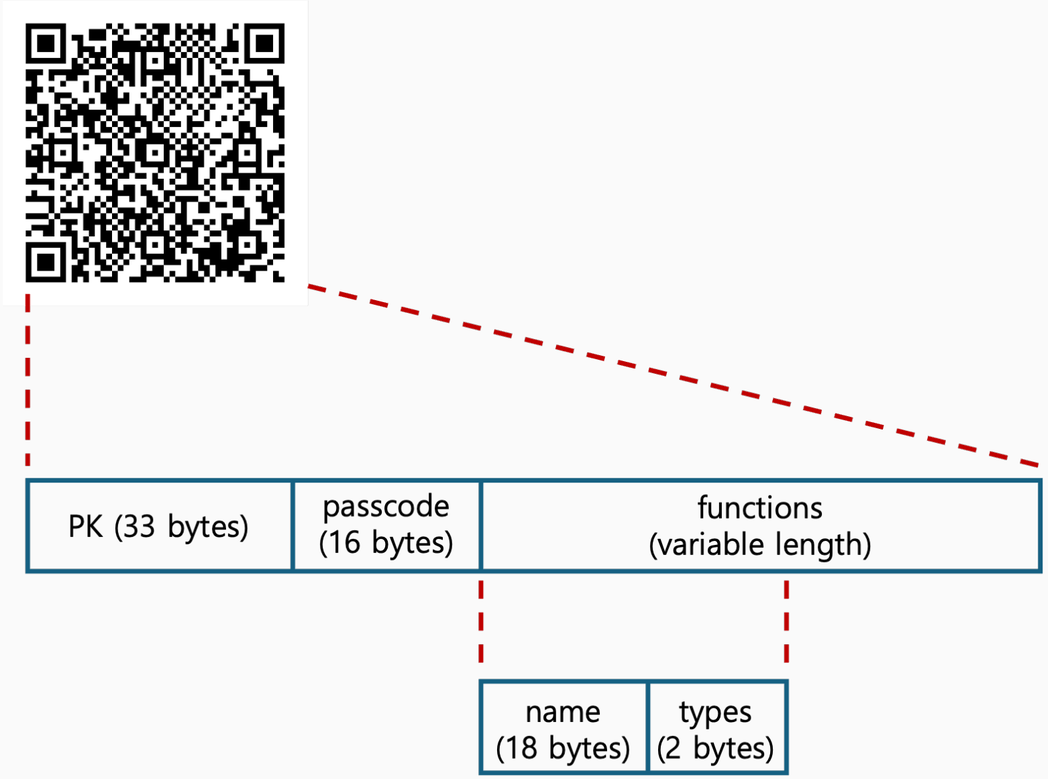
전통적인 블록체인 큐 구조에서는
메시지를 추가할 때마다 전체 배열을 읽어야 하는
비효율성이 존재함

Key-Value based Blockchain Queue

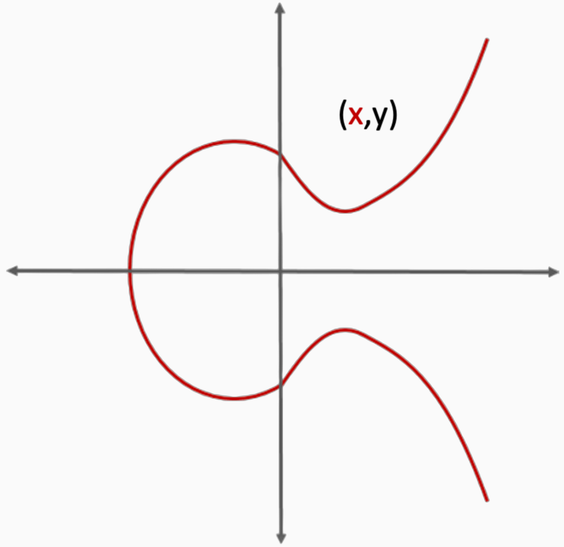
키-값 기반 블록체인 큐에서는
디바이스의 공개키와 인덱스를 조합하여 메시지를 저장함
메시지 추가 시 인덱스의 값만 읽으면 되므로 효율적임

Appendix

Protocol Flexibility and QR Code Innovation



Matter Tunnel QR code



PK 압축

- 타원곡선의 특성을 활용하여 공개 키를 33바이트로 압축
- QR 코드 용량을 최적화하면서도 암호화 시스템의 보안성은 유지

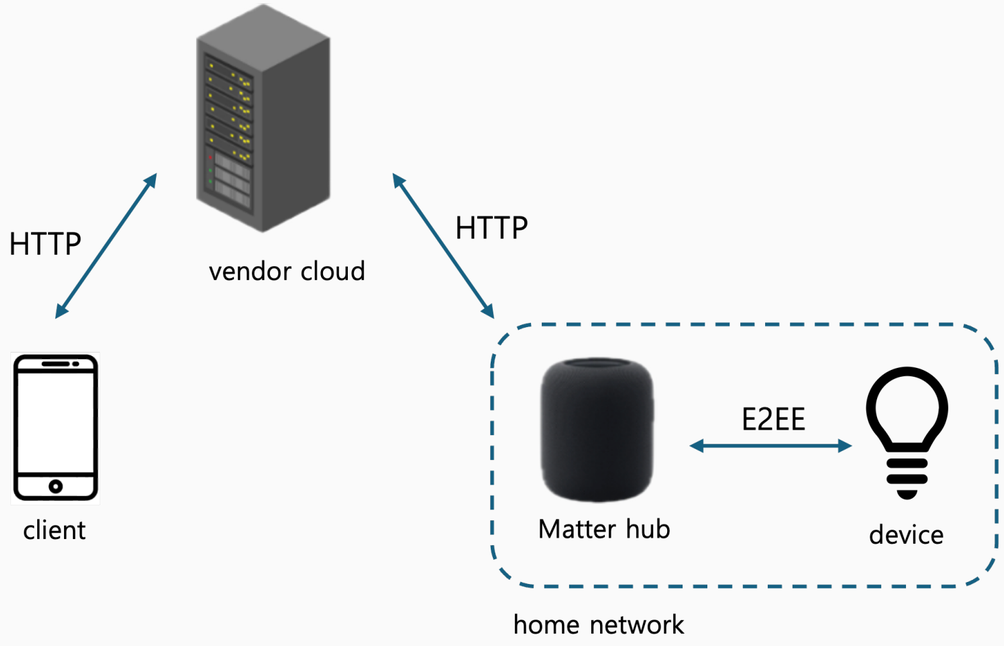
Constant	Value (bit)
void	00
String	01
number	10
boolean	11

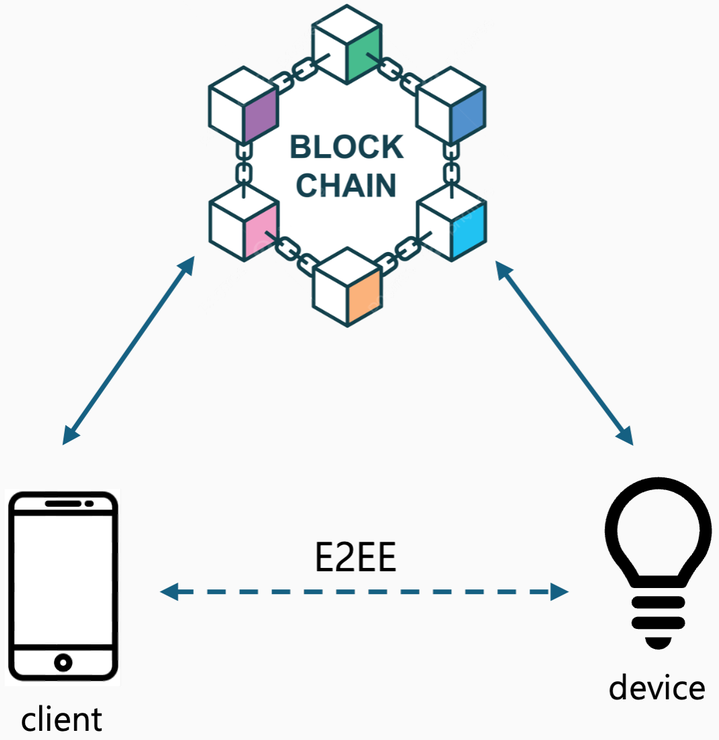
Matter Tunnel 프로토콜 type 인코딩 구조

- 4가지 기본 타입 (void, string, number, boolean)
- 2바이트 타입 정의 내 7개 파라미터와 1개 리턴값 지원
- Latin-1 인코딩을 통한 바이트 최적화

Appendix

Enhanced Security and Privacy Protection





Traditional Matter

- 기존 Matter 구조에서는 클라이언트와 디바이스 간 통신이 벤더 클라우드와 Matter 허브를 거쳐야 함
- Matter 허브는 홈 네트워크 내에서 E2EE로 디바이스와 통신함
- 중간 경유 구조는 보안과 프라이버시 측면에서 취약점 존재

Matter Tunnel E2EE

- 클라이언트와 디바이스가 블록체인을 통해 직접 E2EE 통신을 수행함
- 보안성 향상