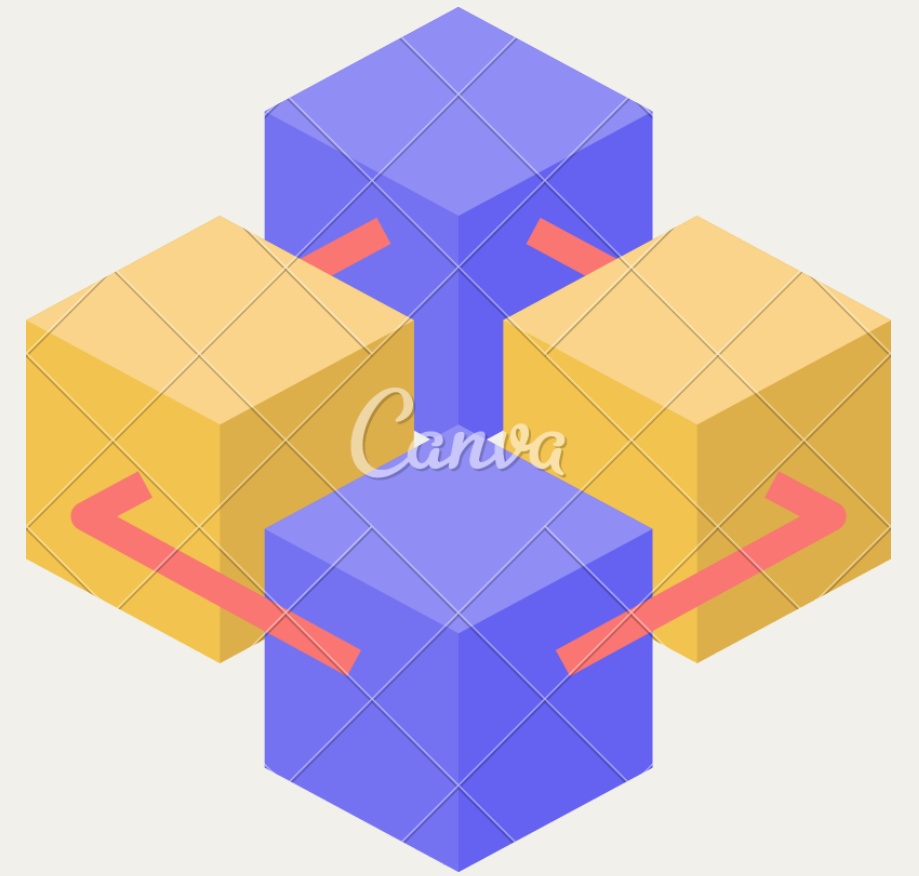


이더리움 블록체인의 기반 SBOM의 무결성 검증 시스템

*SBOM(Software Bill of Materials)



임지현 | 김호석 | 문준호

목차

1. 시스템 소개

2. 기술개발 필요성 및 동향

3. 시스템 설계

4. 설계 수행 결과 및 기대효과

SBOM 이란?

SBOM(Software Bill of Material)은 직역하면 소프트웨어 자재 명세서
최종 고객이 사용하는 소프트웨어 혹은 서비스를 완성하기 위해 활용되는
모든 소프트웨어 정보를 담고 있는 명세서라고 할 수 있다.

1. SBOM 이란?

SBOM 표준 포맷

```
1 SPDXVersion: SPDX-2.2
2 DataLicense: CC0-1.0
3 SPDXID: SPDXRef-DOCUMENT
4 DocumentName: spdx-sbom-generator
5 DocumentNamespace: http://spdx.org/spdxpackages/spdx-sbom-generator--57918521-3212-4369-a8ed-3d681ec1d7a1
6 Creator: Tool: spdx-sbom-generator-XXXXX
7 Created: 2021-05-23 11:25:29.1672276 -0400 -04 m=+0.538283001
8
9 ##### Package representing the Go distribution
10
11 PackageName: go
12 SPDXID: SPDXRef-Package-go
13 PackageVersion: v0.46.3
14 PackageSupplier: NOASSERTION
15 PackageDownloadLocation: pkg:golang/cloud.google.com/go@v0.46.3
16 FilesAnalyzed: false
17 PackageChecksum: TEST: SHA-1 224ffa55932c22cef869e85aa33e2ada43f0fb8d
18 PackageHomePage: pkg:golang/cloud.google.com/go@v0.46.3
19 PackageLicenseConcluded: NOASSERTION
20 PackageLicenseDeclared: NOASSERTION
21 PackageCopyrightText: NOASSERTION
22 PackageLicenseComments: NOASSERTION
23 PackageComment: NOASSERTION
24
25 Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-go
26
```

영양정보

총 내용량 00g
000kcal

총 내용량당	1일 영양성분 기준치에 대한 비율
나트륨 00mg	00%
탄수화물 00g	00%
당류 00g	00%
지방 00g	00%
트랜스지방 00g	
포화지방 00g	00%
콜레스테롤 00mg	00%
단백질 00g	00%

1일 영양성분 기준치에 대한 비율(%)은 2,000kcal
기준이므로 개인의 필요 열량에 따라 다를 수 있습니다.

1. SBOM 이란?



1. SBOM 이란?



Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 / PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Sec. 2. Modernizing Federal Government Cybersecurity.

(a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices, advance toward **Zero Trust Architecture**, and increase its use of cloud services, including but not limited to a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), to ensure and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks, and invest in both technology and personnel to match these modernization goals.

(1) Within 60 days of the date of this order, the head of each agency shall: (i) update existing agency plans to include measures for the adoption and use of cloud technology as outlined in relevant OMB guidance;

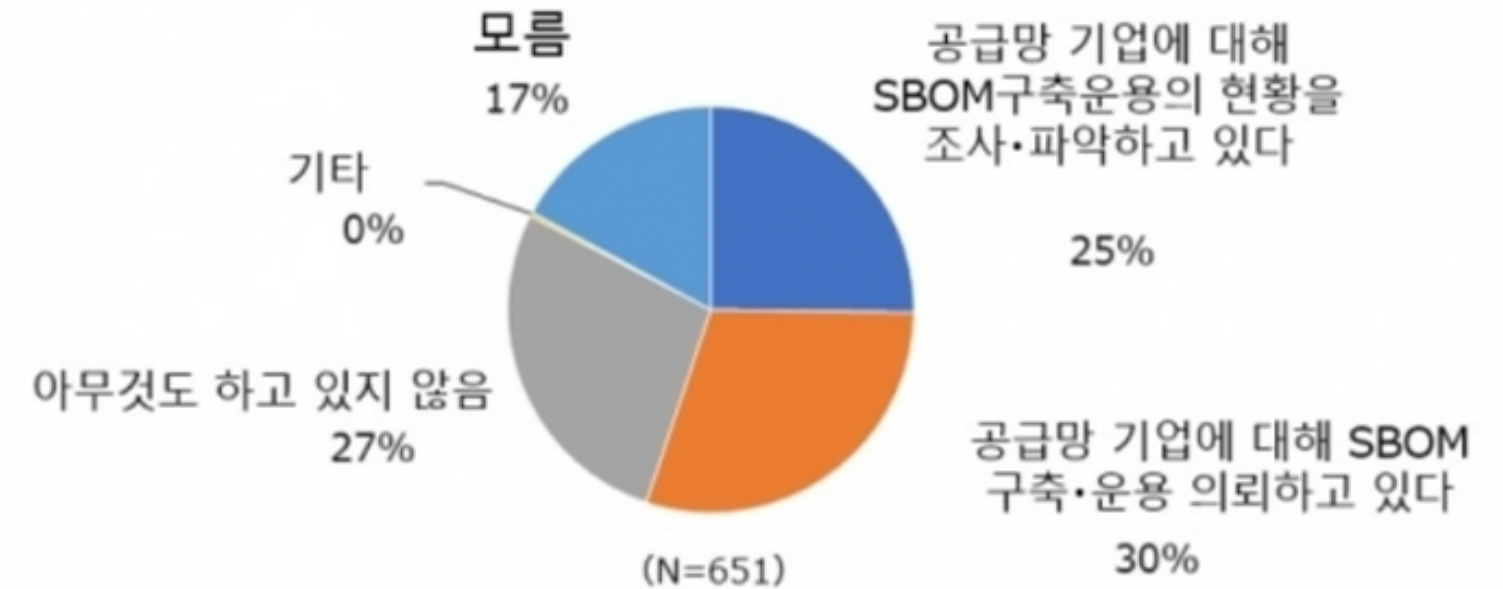
(ii) develop a plan to implement **Zero Trust Architecture**, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that still have the most immediate security impact, and include a schedule to implement them; and

(iii) provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plan required pursuant to subsection (b)(1) and (ii) of this section.

(c) As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that ensures the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt **Zero Trust Architecture**, as practicable. The CISA shall evaluate its current cybersecurity programs, services, and capabilities to identify functional with cloud-enabling environments with **Zero Trust Architecture**. The Secretary of Homeland Security acting through the Director of CISA, in coordination with the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. To facilitate this work:

제로 트러스트

2021. 5. 조 바이든 미 대통령은 연방정부의 사이버 보안 현대화를 위해 '제로 트러스트' 보안 정책을 채택하는 행정명령을 발동했다. 이 행정명령에 '제로 트러스트'는 무려 11번이나 언급된다.



테니엄의 SBOM 관련 일본 설문조사. 공급망의 SBOM 현황을 조사·파악 중인 기업이 25%, 준비 중인 기업이 30%에 달하는 것으로 나타났다.

2. 필요성 및 차별성

근거 1. 현재 과기부 SBOM 자동생성 및 무결성 검증 기술 개발중

과기부 'SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발(2022-2025)' 연구과제 참여

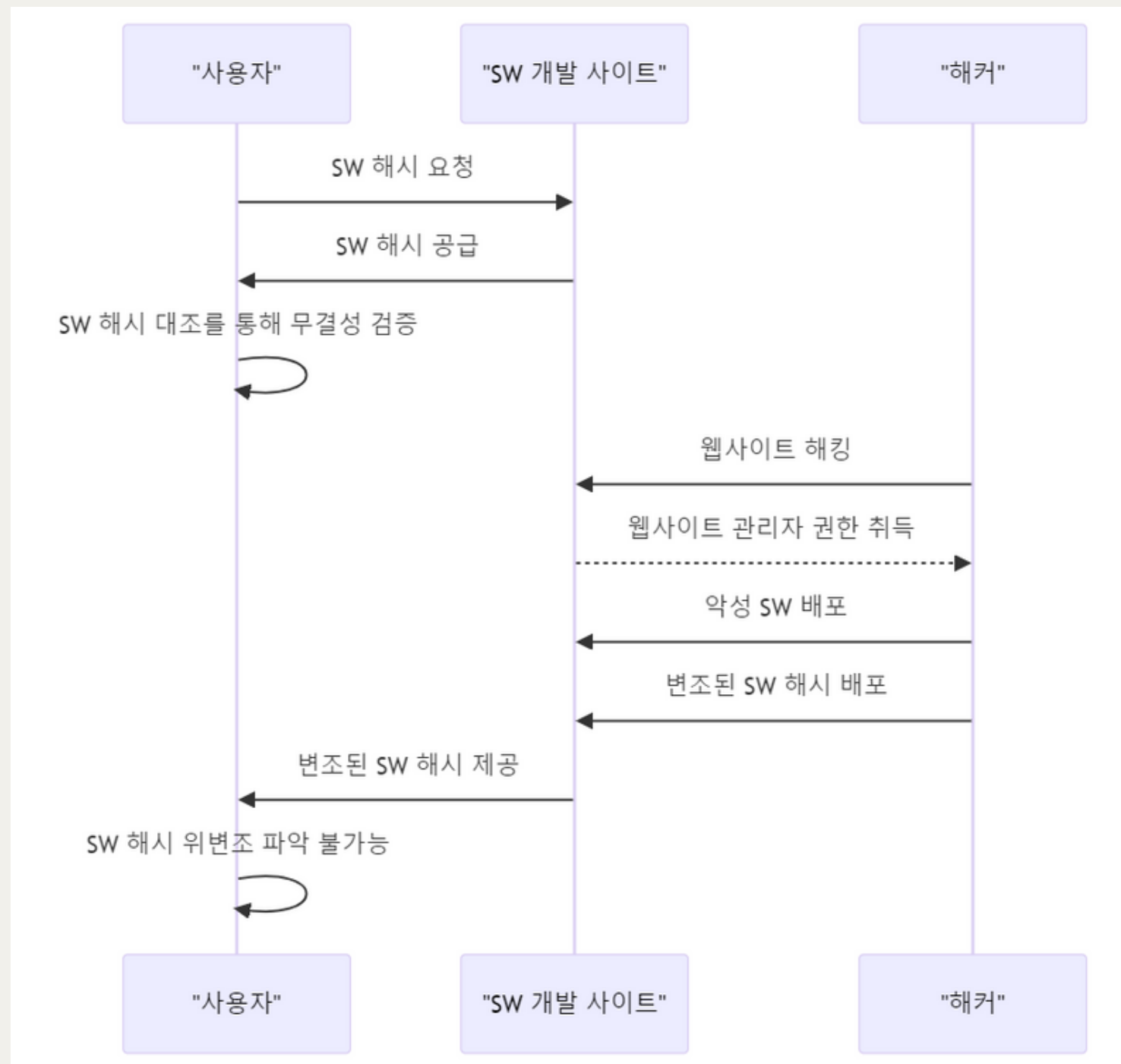
근거 2. SBOM 작성을 하지 않으면 SW 수출이 어려워짐

2023년 8월 기사

"SW(소프트웨어) 공급망 보안이 새로운 무역장벽이 되고 있다. 우리 기업의 재화·서비스의 수출에 제동이 걸릴 수도 있다."

美 "한국 SW에 SBOM 있나요?"...국내 제도화 언제쯤?

3. 기존 시스템 현황



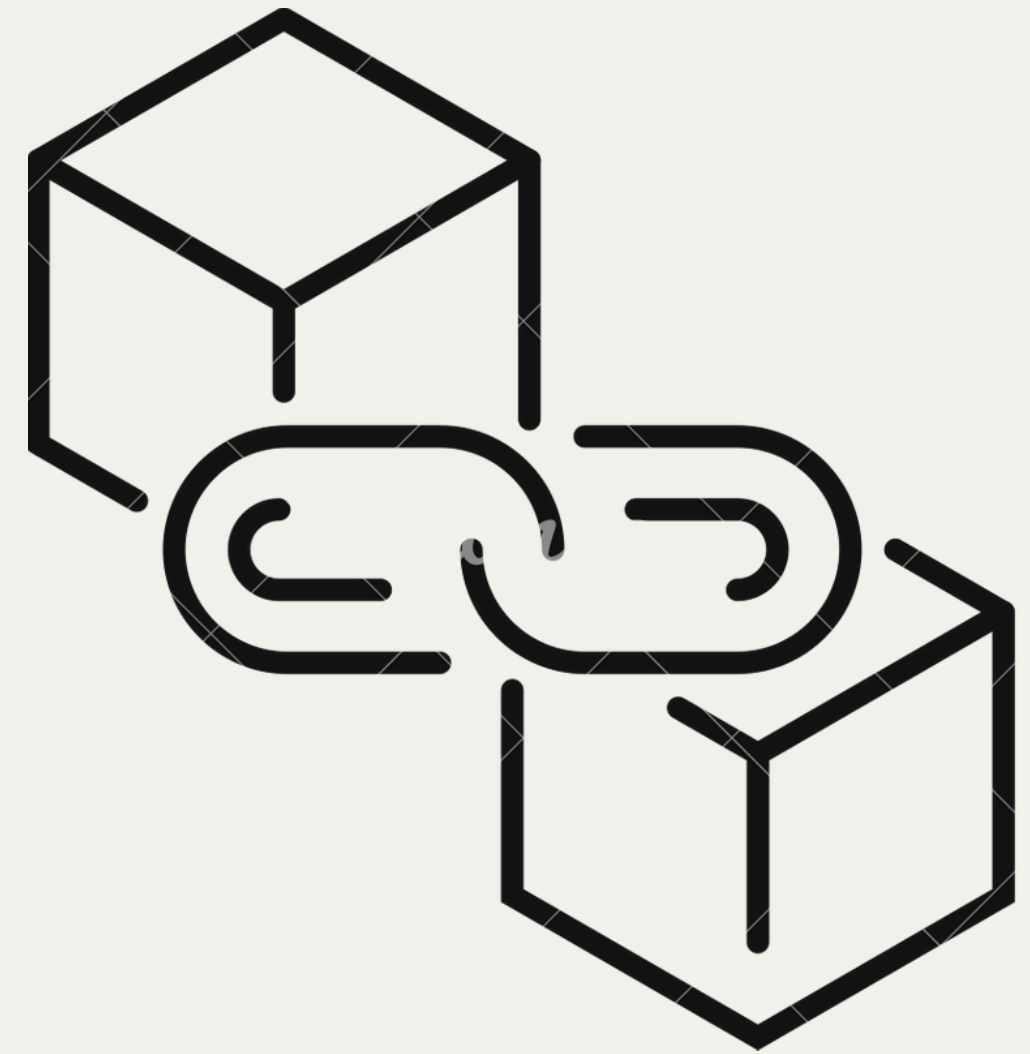
현재 SBOM 무결성 검증 방식의 문제점(컴포넌트 해시)

-> 공격자의 서버 해킹으로 인해 SW개발사에서 제공하는 SBOM의 정보가 위·변조되어 컴포넌트 해시 또한 위·변조될 수 있는 문제가 발생할 수 있다.

프로젝트 목표

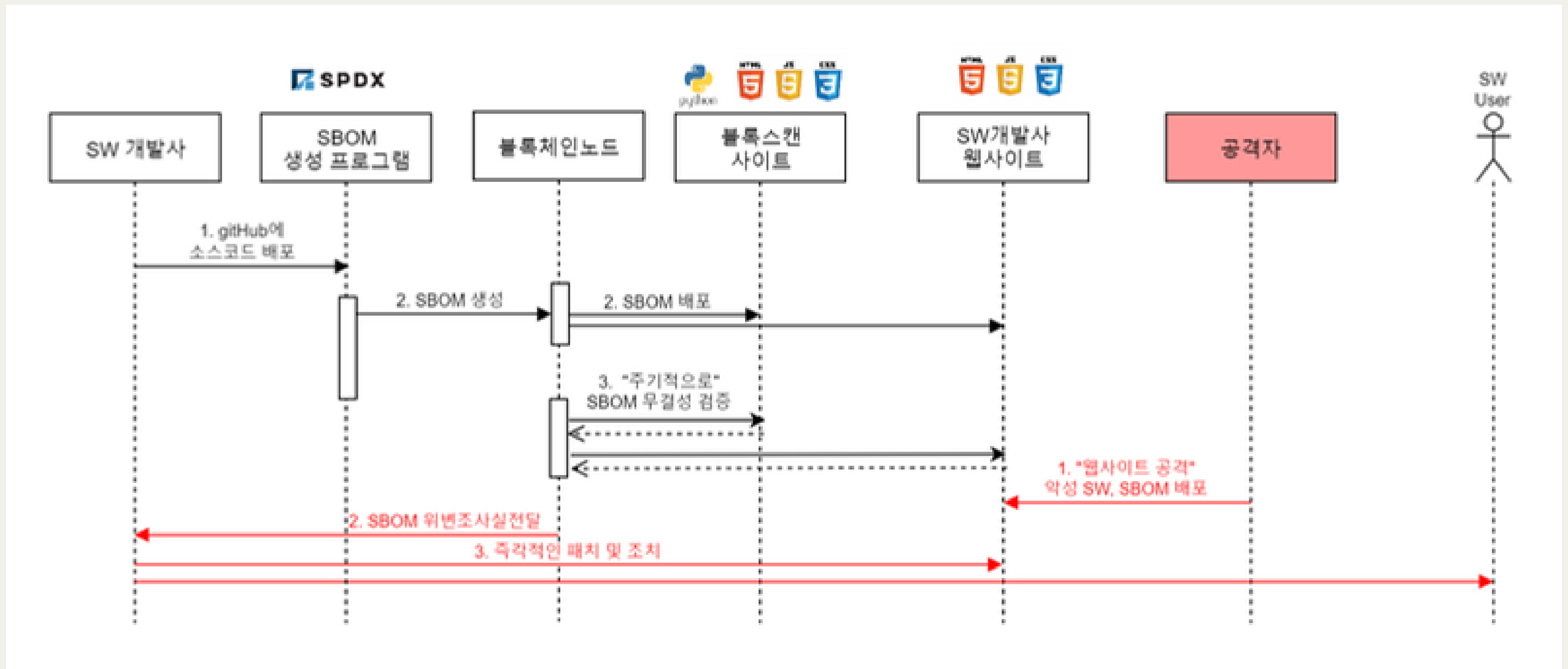
SBOM 무결성 검증기술

“블록체인”



차별성 : 블록체인을 통한 SBOM 무결성 검증

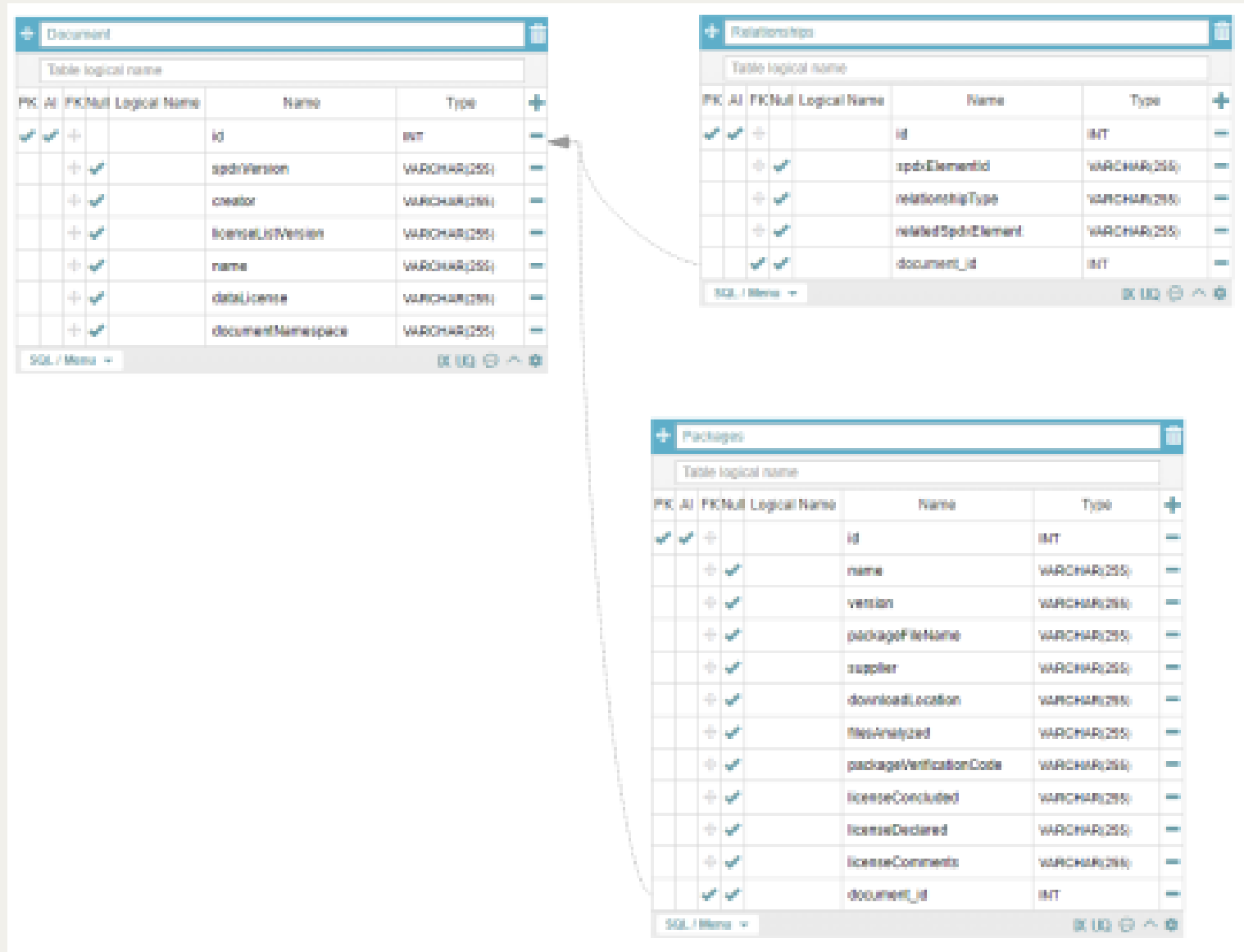
3. 시스템 흐름도



3. 기능명세

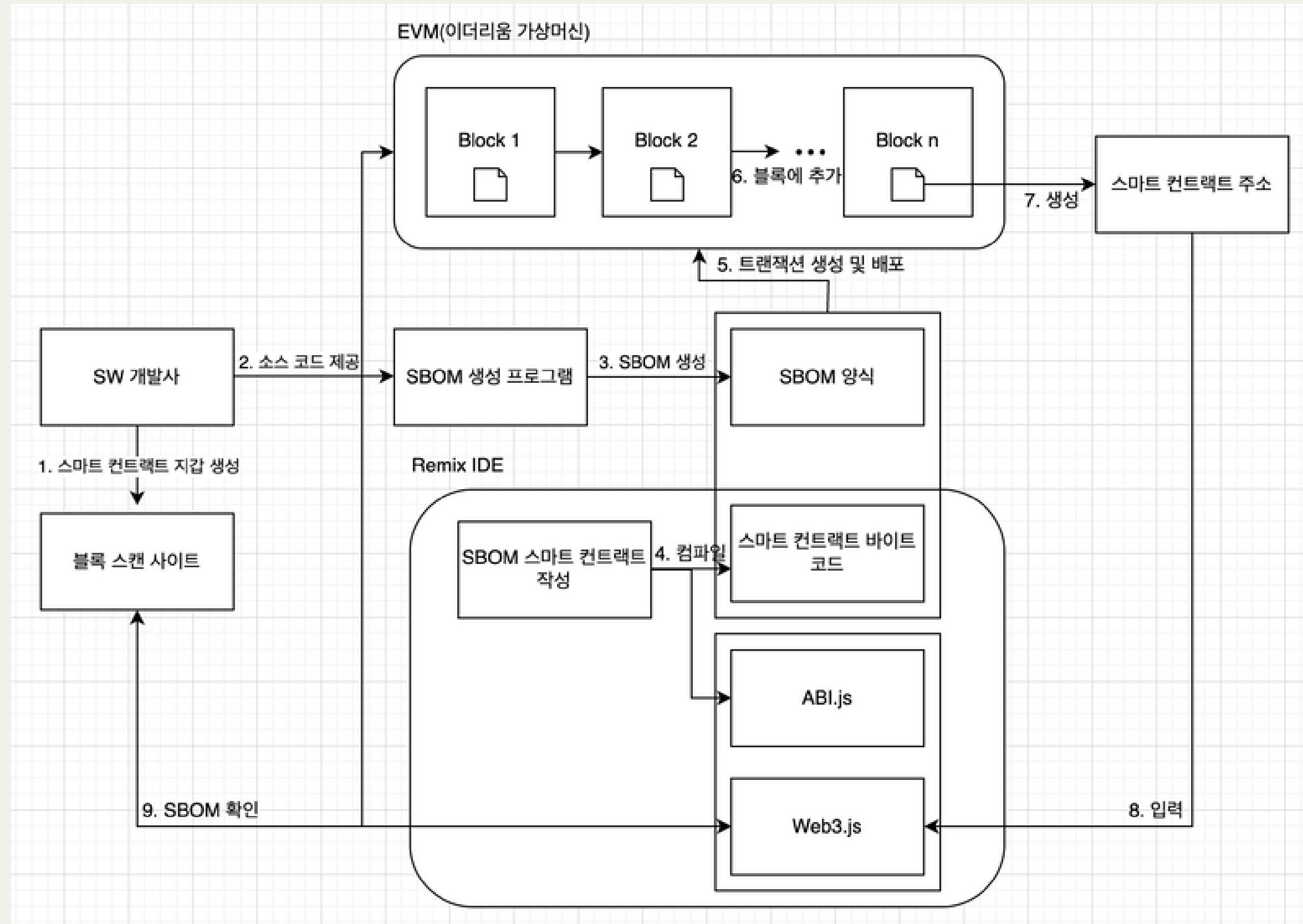
모듈	기능	도구/기술	작업 내용	결과물
SBOM 프로그램	소스 코드 분석	SBOM 생성 프로그램	소스 코드에서 구성 요소 추출	SBOM 데이터
	SBOM 데이터 변환	SBOM 생성 프로그램	데이터를 JSON 형식으로 변환	SBOM 파일
블록체인 노드	스마트 계약 개발	Remix IDE	SBOM 데이터 처리 계약 개발	스마트 계약 코드
	스마트 계약 배포	Remix IDE, EVM	스마트 계약을 이더리움에 배포	블록체인 상의 스마트 계약
	트랜잭션 생성 및 처리	스마트 계약, EVM	SBOM 데이터를 블록체인에 등록	블록체인 트랜잭션
	트랜잭션 검증 및 승인	블록체인 노드	트랜잭션의 자동 검증 및 승인	승인된 트랜잭션
블록체인 스캔사이트	블록체인 데이터 추가	EVM(이더리움 가상 머신)	승인된 트랜잭션을 블록에 추가	블록체인의 새로운 블록
	데이터 조회	Web3.js	블록체인 데이터 조회	조회 가능한 SBOM 데이터
	라이브러리 활용	ABI.js, Web3.js	스마트 계약과 상호작용	스마트 컨트랙트코드

3. DB 설계

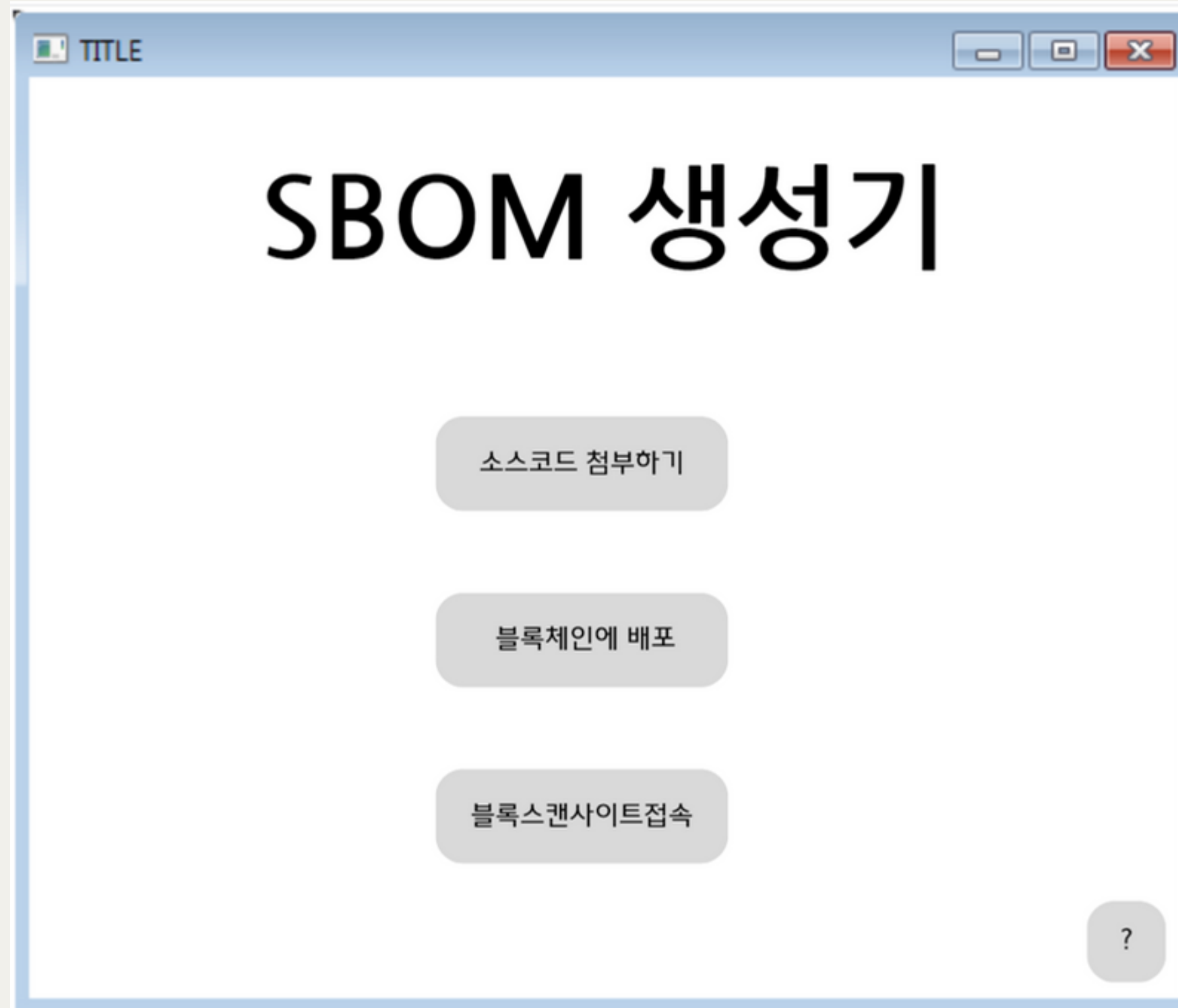


구분	속성 이름	데이터 타입
공급자명	Supplier_Name	VARCHAR(255)
저작권자명	Author_Name	VARCHAR(255)
고유 식별자	Unique_Identifier	VARCHAR(255)
컴포넌트명	Component_Name	VARCHAR(255)
컴포넌트 버전	Component_Version	VARCHAR(255)
컴포넌트 해쉬	Component_Hash	VARCHAR(255)
관계성	Relationship	VARCHAR(255)
릴리즈 날짜	Release_Date	VARCHAR(255)
보안취약점 DB	VulnerabilityDB_Name	VARCHAR(255)
CWE	CWE_Number	VARCHAR(255)
CVE ID	CVE_Year_SerialNumber	VARCHAR(255)
CVSS Base Score	CVSS_Base_Score	INT(255)
CVSS Severity	CVSS_Severity	VARCHAR(255)


3. 상세 설계



3. GUI 설계- SBOM 생성기



3. GUI 설계 - 블록스캔 사이트



검색

Transaction Details

Transaction ID: 123456789

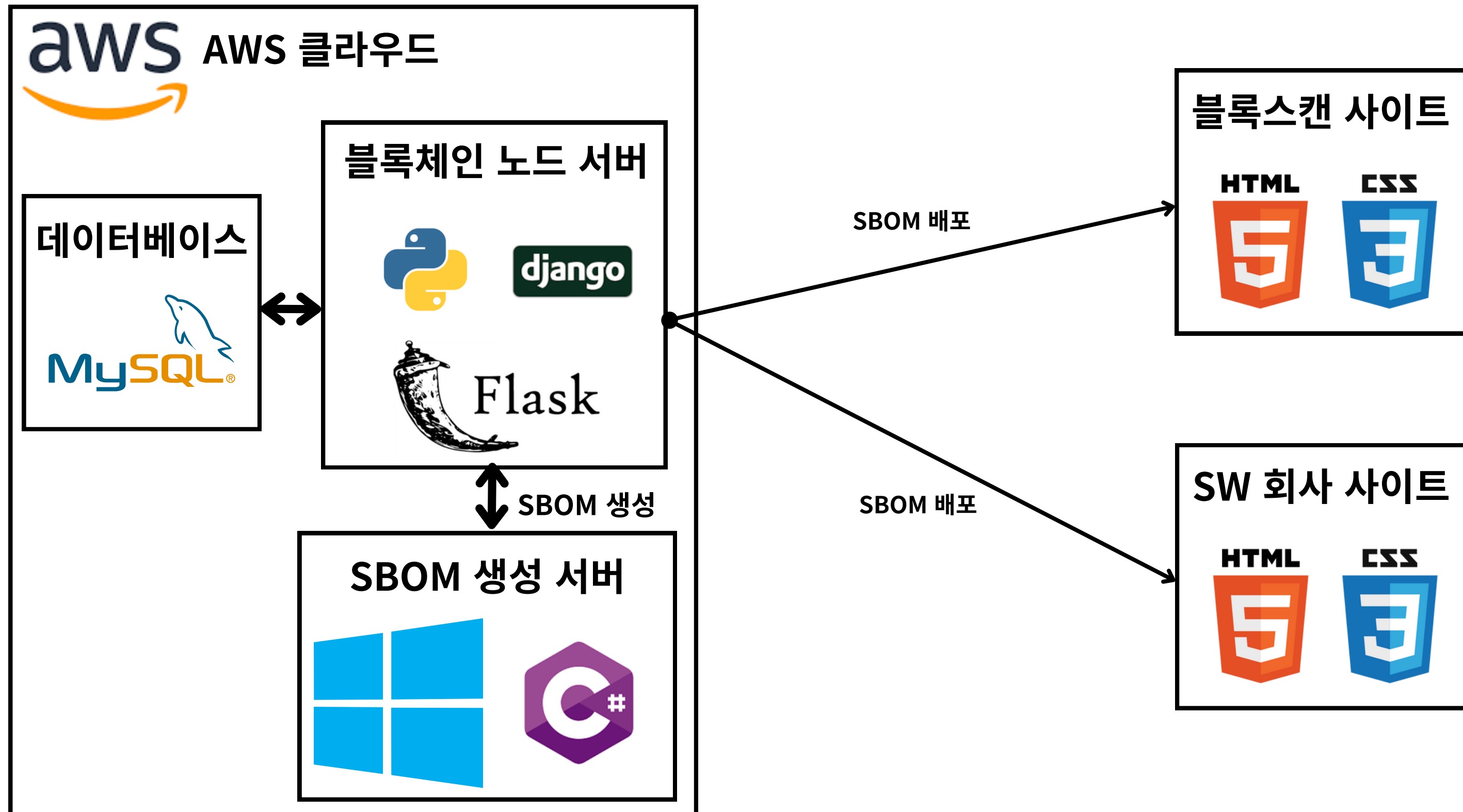
Block: 987654321

Timestamp: 2023-12-17 12:34:56

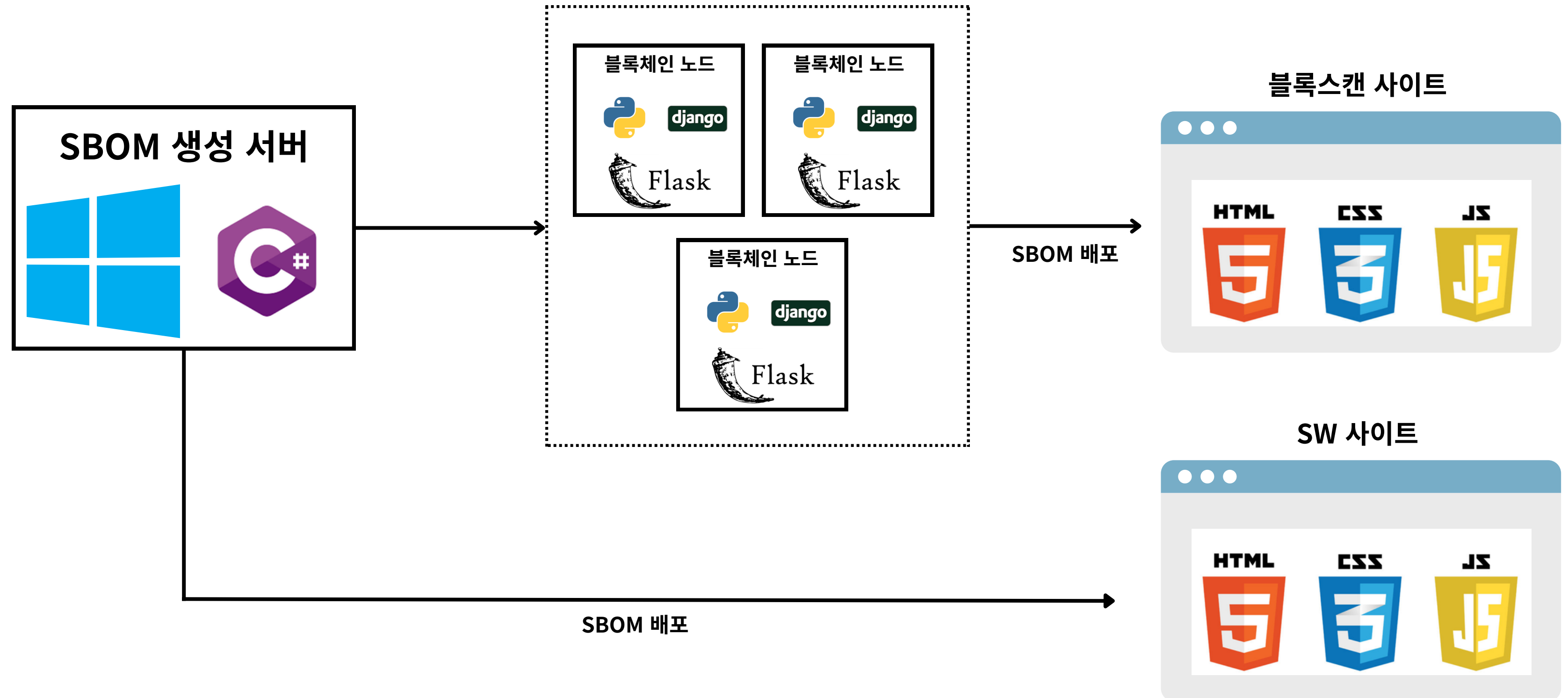
Block	Transactions	Miner	Timestamp
123456	50	0x1a2b3c	2023-12-17 11:34:56

© 2023 Blockchain Scanner. All Rights Reserved.

3. 기존 개발 환경



3. 개선된 개발 환경



3. 역할 분담



김호석

블록체인 노드 개발

이더리움 네트워크 구성

스마트 컨트랙트 개발



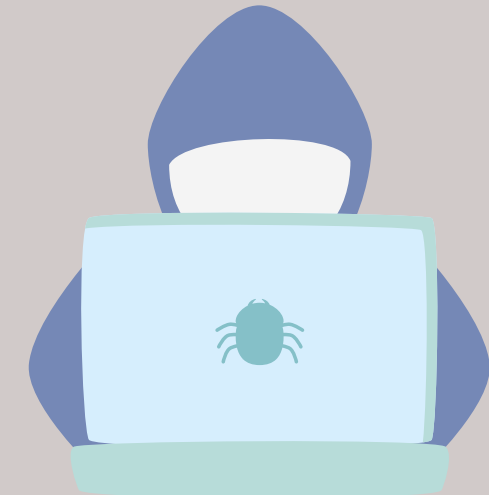
임지현

웹사이트 구축

- 블록체인 스캔사이트

SBOM 프로그램 기능

- 웹 크롤링
- Snyk 취약점 분석



문준호

SBOM 생성 툴 개발

API 서버 구축

데이터베이스 구축

3. 추진 일정(WBS)

[illegible]

4. 현재까지 결과물

The screenshot displays the 'Car Auction Dapp' interface. On the left, a 'Car Details' section is highlighted with a red box, showing 'Brand: MOKPOUNIVERSITY', 'Registration Number: 1234', and a 'Bid value' input field with '10' entered. Below this is an 'Auction Details' section listing: 'Auction End: 1702970042', 'Auction Highest Bid: 0', 'My Bid: 0', 'Auction Highest Bider: 0x00', and 'Auction Status: 1'. On the right, a table of recent blocks is highlighted with a red box, showing blocks 2, 1, and 0 with their respective mined times and gas used.

BLOCK	MINED ON	GAS USED
2	2023-12-19 15:14:02	1104849
1	2023-12-19 15:06:23	352930
0	2023-12-19 15:05:18	0

4. 기대 효과

경제적 기대효과

- 소프트웨어 개발 및 유지보수 비용 절감
- 효율적인 개발 및 유지보수 가능
- 보안 문제 신속 파악 및 해결 비용 및 시간 절감

사회적 기대효과

- 더 안전한 소프트웨어 환경 경험 가능
- SW에 대한 신뢰성 높아짐
- 정보 보호 인식 증진

산업적 기대효과

- 소프트웨어 산업 표준화 촉진
- 산업 전반의 품질 향상 및 혁신 도모
- 소프트웨어 구성 요소 투명성 보안 강화, 라이선스 준수 등을 통해 산업 건전성 증진

THANK YOU

감사합니다