분산 워크플로우 시스템을 위한 블록체인 기반 프로브넌스 지원

Blockchain-Based Provenance Support for Distributed Workflow Systems

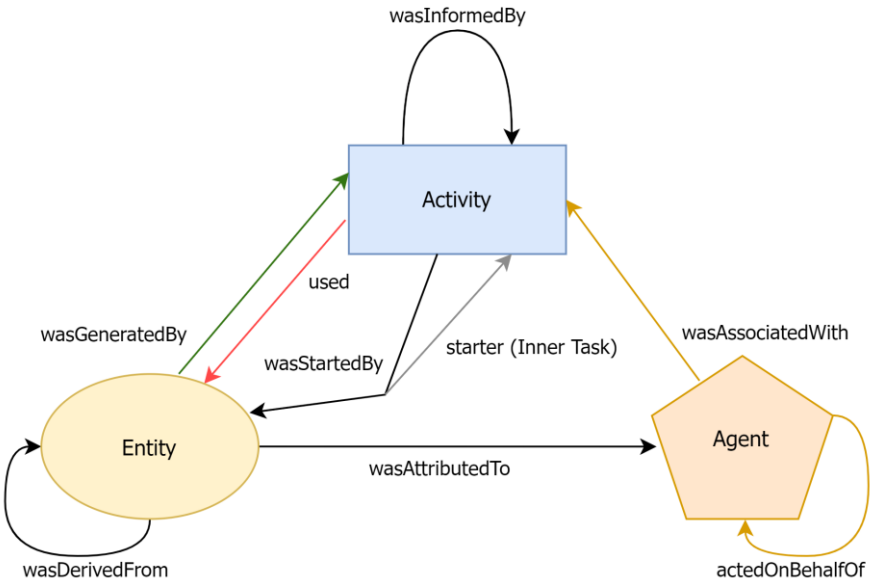
김재하, 다니 메흐턴츠, 이춘화
한양대학교 컴퓨터·소프트웨어학과
{jehakim22oct, dmgpmertens, lee}@hanyang.ac.kr

Jaeha Kim, Dani Mertens, and Choonhwa Lee
Department of Computer and Software, Hanyang University

Data Provenance and DID

did:ethr:0xbc0B2F5Dc4dbF08a209091C41592cDfD348c1483

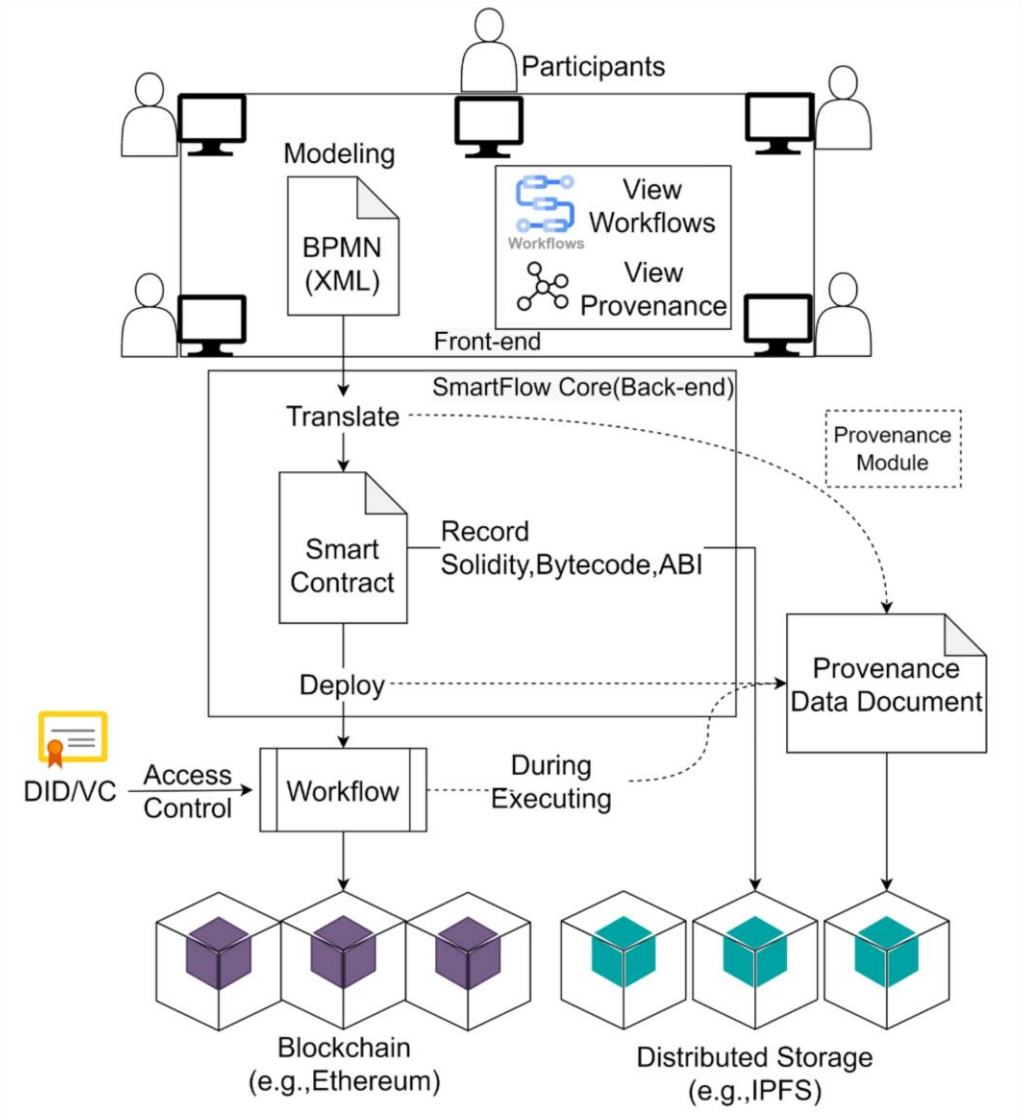
[Scheme]:[DID Method]:[DID Method Specific Identifier]




```
{
 "didDocumentMetadata": {},
 "didResolutionMetadata": {
  "contentType": "application/did+ld+json"
 },
 "didDocument": {
  "@context": [
   "https://www.w3.org/ns/did/v1",
   "https://identity.foundation/EcdsaSecp256k1RecoverySignature2020/lds-ecdsa-secp256k1-recovery2020-0.0.jsonld"
  ],
  "id": "did:ethr:0xbc0B2F5Dc4dbF08a209091C41592cDfD348c1483",
  "verificationMethod": [
   {
    "id": "did:ethr:0xbc0B2F5Dc4dbF08a209091C41592cDfD348c1483#controller",
    "type": "EcdsaSecp256k1RecoveryMethod2020",
    "controller": "did:ethr:0xbc0B2F5Dc4dbF08a209091C41592cDfD348c1483",
    "blockchainAccountId": "0xbc0B2F5Dc4dbF08a209091C41592cDfD348c1483@eip155:1"
   }
  ],
  "authentication": [
   "did:ethr:0xbc0B2F5Dc4dbF08a209091C41592cDfD348c1483#controller"
  ],
  "assertionMethod": [
   "did:ethr:0xbc0B2F5Dc4dbF08a209091C41592cDfD348c1483#controller"
  ]
 }
}
```

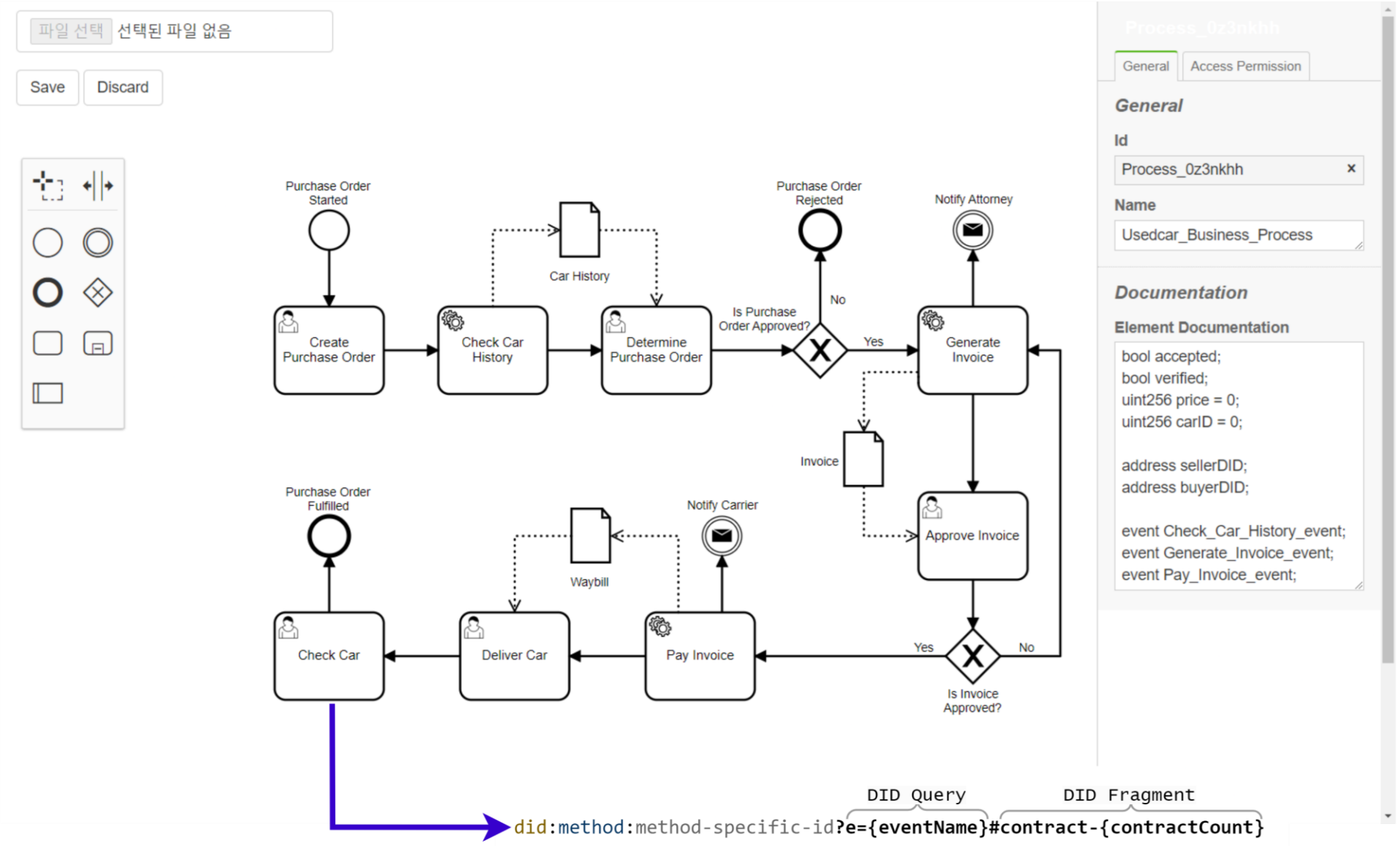

- Provenance(데이터 유래)는 데이터의 생성 및 관련 이력을 나타내는 메타데이터.
- 분산된 워크플로우의 진행 내역에 대해 추적 가능성, 책임성, 투명성을 보장하고 보다 나은 신뢰도를 확보하기 위해 데이터 유래 지원 도입.
- DID는 중앙 집중식 등록 기관이 필요하지 않고 종종 암호화 방식으로 생성 및 등록되는 전역적으로 고유한 영구 식별자. 블록체인 네트워크를 레지스트리로 이용 가능.

Data Provenance based Distributed Workflow System

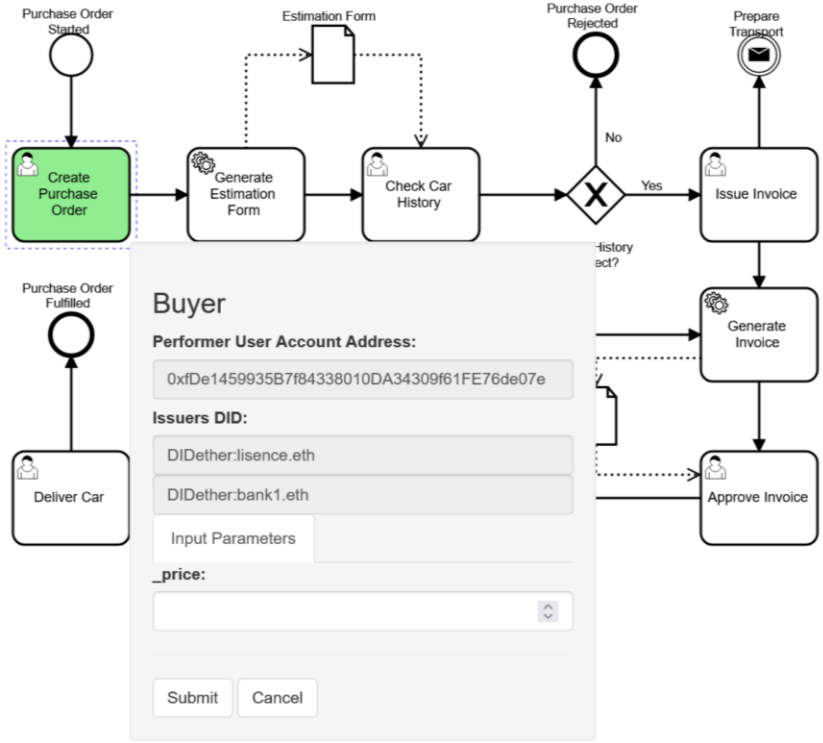


- 프론드엔드 GUI 패널을 통해 워크플로우의 제작(모델링), 배포 및 실행 모니터링 지원.
- 모델링된 BPMN 워크플로우 태스크는 Smart Contract로 변환.
- 배포된 워크플로우 각각의 태스크는 실행 전 DID 및 VC를 이용, SSI 기반으로 검증

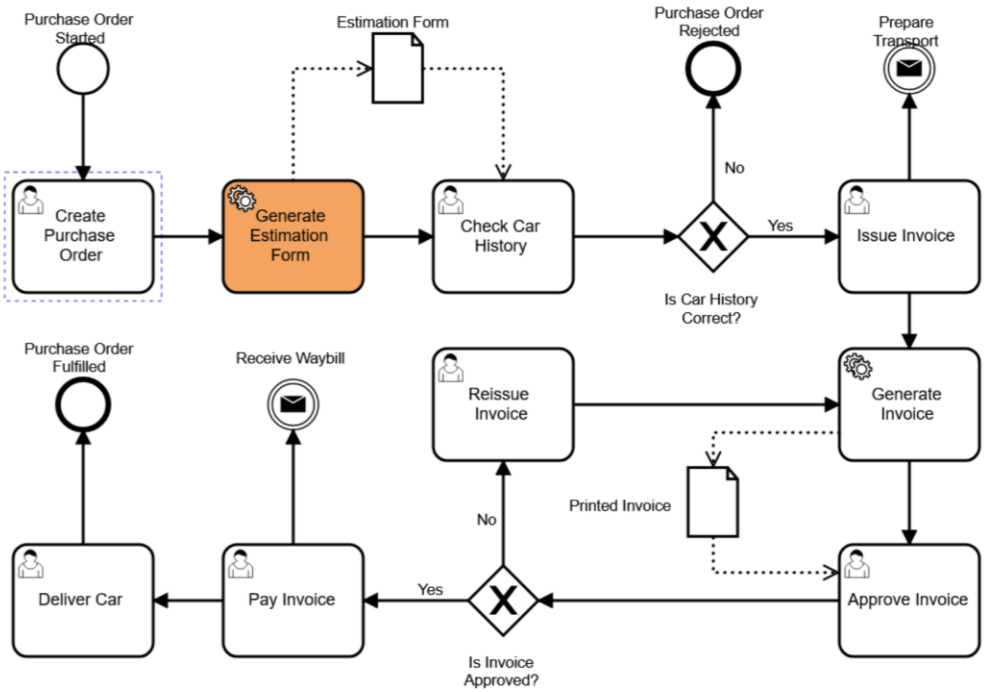
Implementation



Modeling Workflow in BPMN

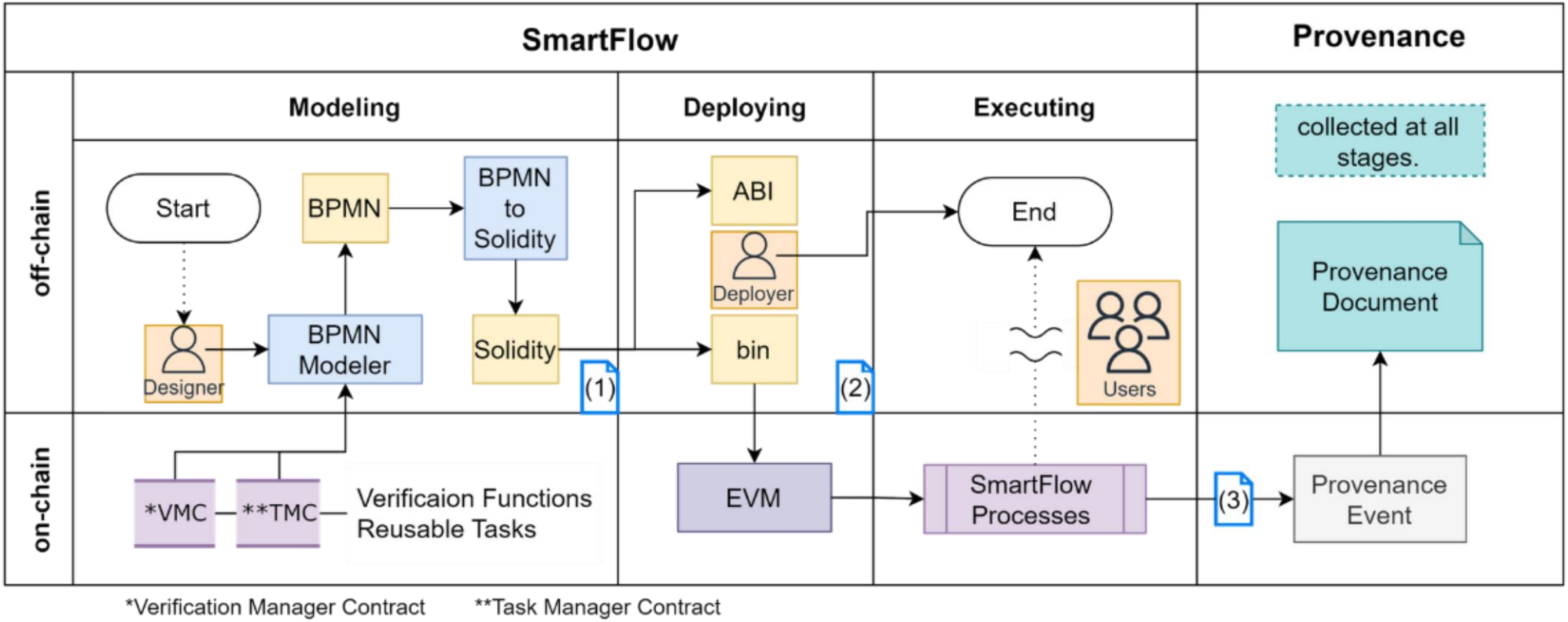


Generate_Estimation_Form: https://ipfs.io/ipfs/zdj7WW1Zmi7M4VFD9cBee6yELzXxUHY8



Executing Workflow

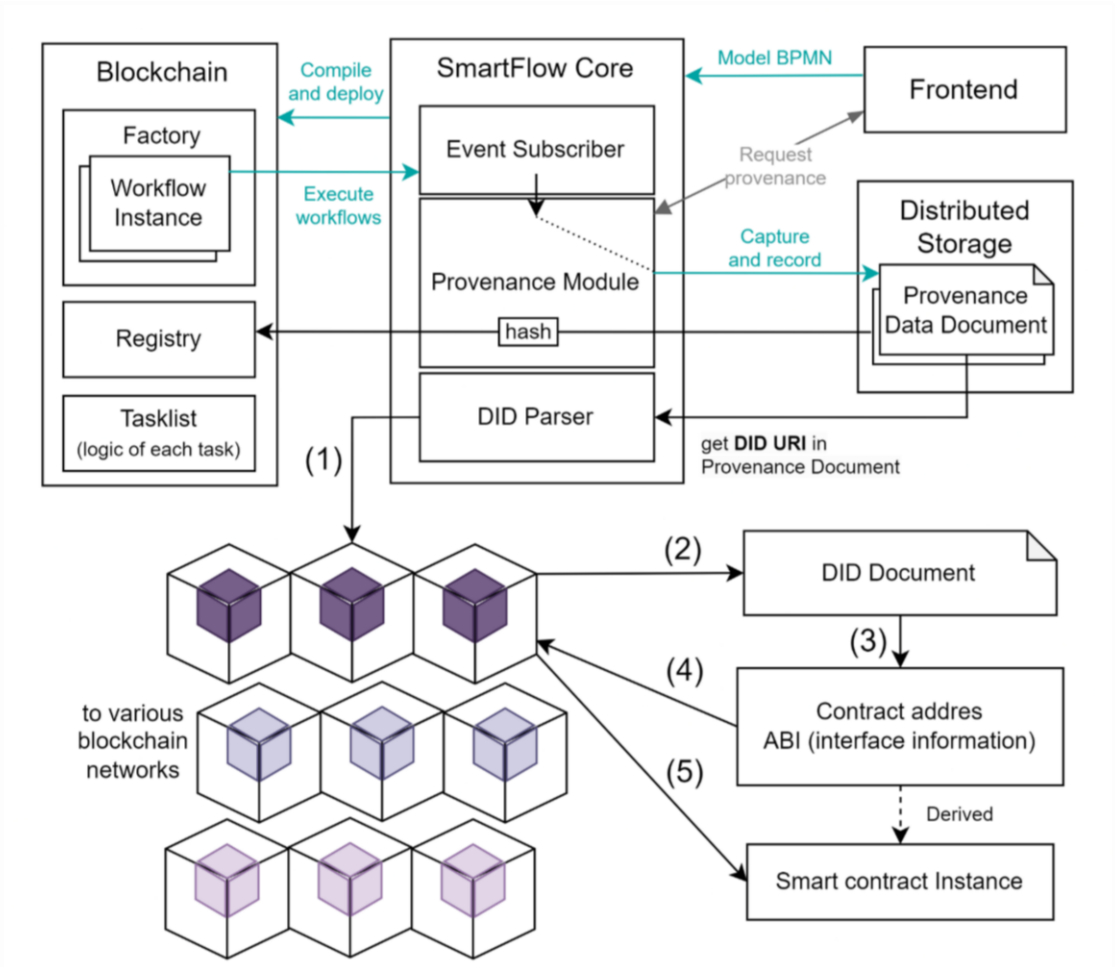
Capturing Provenance sequence



Provenance with DID

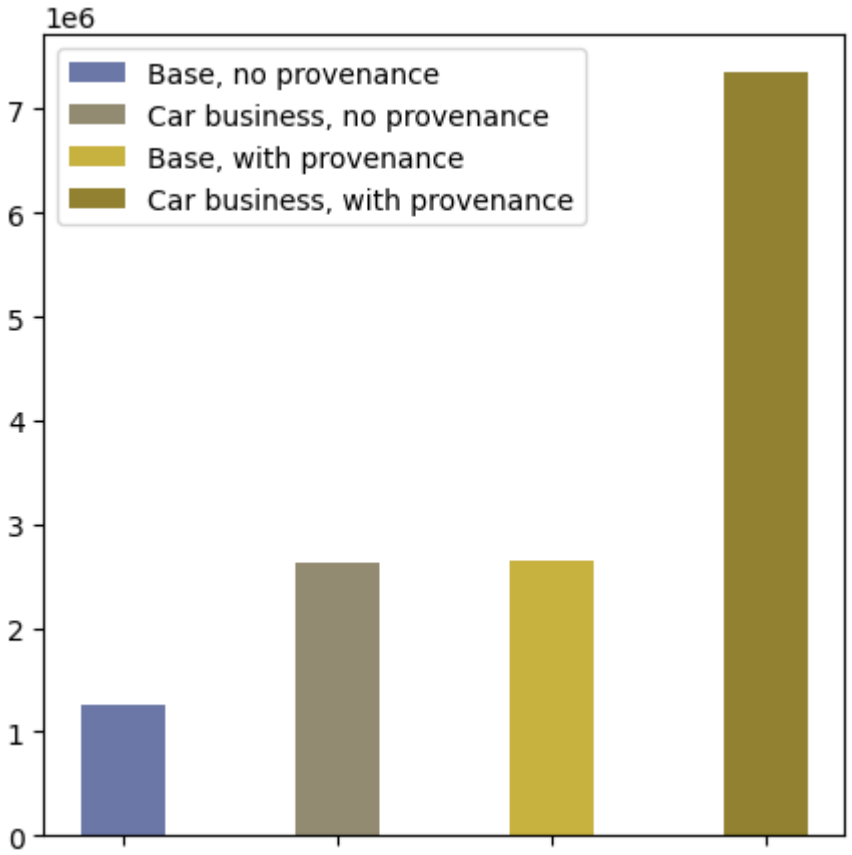
DID Query　　DID Fragment

```
did:method:method-specific-id?e={eventName}#contract-{contractCount}
```

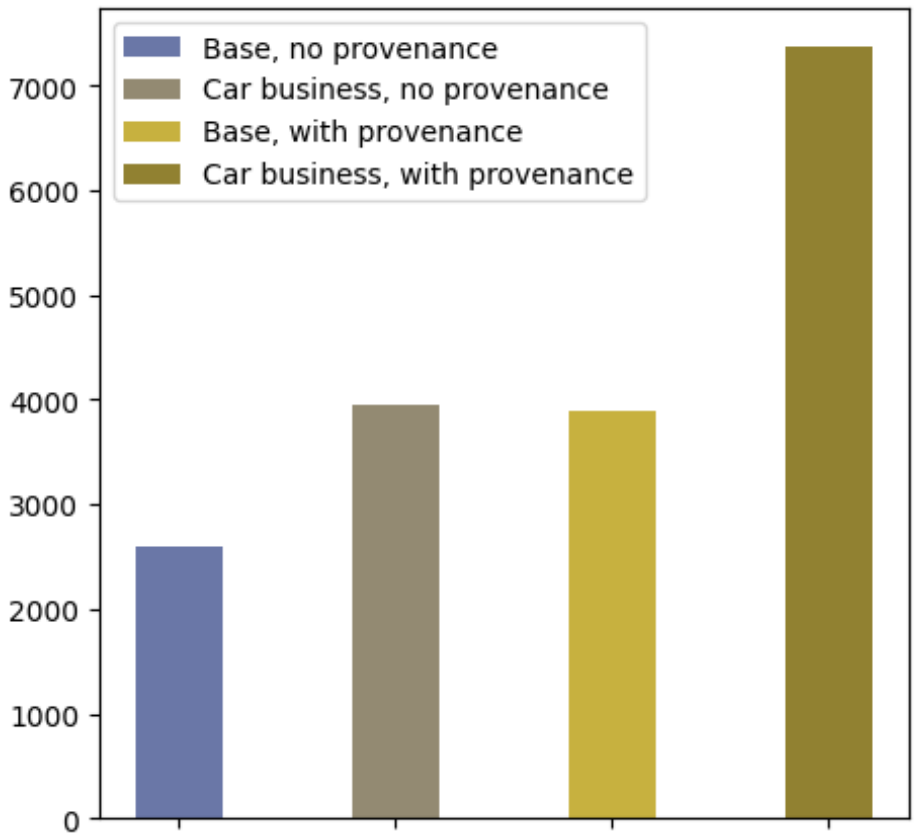


- 수집된 유래 데이터의 각 노드들은 DID로 표현.
- 기존 ethr-did 라이브러리를 수정한 자체 DID parser를 이용, 출력된 DID 문서에서 스마트 컨트랙트 인스턴스에 액세스 하기 위한 메타데이터 추출. 이를테면 EVM 네트워크에서는 contract address와 ABI.

Evaluation



Gas for pre-deploy



Time for pre-deploy

- 데이터 유래 기능 추가로 전 과정에서 대략 2배 가량의 gas 추가 소모.
- 소요 시간은 상대적인 비율은 크지만 실제 체감상 유의미한 차이를 느끼지 못함.

Conclusion

- 이 연구의 주된 기여는 시스템의 확장성 및 안전성을 보강하는 기술로서 DID와 결합된 데이터 유래 기술의 잠재력을 탐구하는 것임.
- 투명한 기록 확인을 통해 책임 추적이 보다 쉬워졌고 사후 감사 시 근거 기반 결정에 유용한 데이터로서 참조 가능. 나아가 전체적인 워크플로우의 개선 근거로도 이어질 수도 있음.
- DID를 사용하여 독립적인 네트워크에 속한 워크플로우끼리 제한적인 용처를 갖는 한계를 넘어 폭넓게 상호 작용이 가능한 범용성을 가짐.