

칸톤(Canton)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다.

칸톤 네트워크:

스마트 컨트랙트 애플리케이션을 위한 네트워크의 네트워킹

디지털 애셋(Digital Asset)

2024년 1월 업데이트

초록

현재의 스마트 컨트랙트 네트워크는 전통 금융기관 및 기타 기업들의 실질적인 도입을 크게 제한하는 두 가지 제약을 겪고 있습니다. 첫째, 모든 애플리케이션이 기본 네트워크의 거버넌스 속성과 완전히 투명한 프라이버시 모델을 그대로 상속받아야 합니다. 둘째, 애플리케이션들이 거래 처리량(throughput)을 두고 경쟁해야 합니다.

본 백서에서는 이러한 한계를 극복하기 위해 설계된 칸톤 네트워크를 소개합니다. 칸톤 네트워크는 각 애플리케이션 제공자가 자신들의 애플리케이션에 대한 프라이버시, 확장성, 권한, 거버넌스를 개별적으로 정의할 수 있도록 하면서도, 보다 넓은 탈중앙화된 퍼블릭 퍼미션드 네트워크의 일부로 작동할 수 있게 합니다.

서론

동기

현재 여러 스마트 컨트랙트 블록체인 네트워크가 존재하지만, 이들은 모두 그 위에 구축된 자산과 애플리케이션에 문제적인 제약을 부과합니다. 구체적으로, 이러한 네트워크에서는 다음과 같은 제약이 존재합니다:

1. 모든 자산과 애플리케이션의 데이터가 모든 사용자에게 영구적이고 공개적으로 공유됩니다.
2. 자산 및 애플리케이션과의 상호작용은 ‘전부 아니면 전무(all-or-nothing)’ 방식으로, 애플리케이션 운영자는 서로 다른 사용자가 애플리케이션과 어떻게 상호작용하는지를 쉽게 제어할 수 없습니다.
3. 애플리케이션들이 글로벌 네트워크 자원을 두고 경쟁하므로, 애플리케이션 운영자는 독립적으로 확장하거나 배포할 인프라를 선택할 수 없습니다.

또한 수수료는 상호 연결되어 있고 예측하기 어렵습니다. 한 애플리케이션의 사용량이 증가하면, 모든 사용자의 비용이 상승합니다.

반면, 전 세계 대부분의 자산은 이질적이며, 사용자와 기업이 이를 거래하는 방식에 대해 고유한 규칙이 존재합니다. 이러한 자산과 상호작용하는 애플리케이션 운영자는 애플리케이션의 프라이버시, 확장성, 서비스 가용성, 인프라 비용 등을 통제할 수 있어야 합니다. 따라서 기존 블록체인 네트워크의 제약은 전 세계의 자산과 프로세스를 상호 연결된 네트워크로 온보딩하는 것을 방해하며, 그 결과 퍼블릭 블록체인이 암호화폐 기반 자산을 넘어 실질적인 네트워크 효과를 구축하는 능력을 제한합니다. 이를 설명하기 위해, 기존 퍼블릭 블록체인 네트워크를 가장 성공적인 퍼블릭 네트워크인 인터넷(Internet)과 비교해보겠습니다. 인터넷은 독립적으로 운영되는 애플리케이션들을 호스팅하는 이질적인 네트워크입니다. 예를 들어, 위키피디아(Wikipedia)는 완전히 공개되어 있으며, 같은 퍼블릭 인터넷 위에서 접근 제한이 있는 은행 포털과 함께 공존합니다. 대규모 저가 서비스와 소규모 고가 서비스가 동일한 네트워크에서 함께 운영됩니다. 각 애플리케이션 제공자는 자신의 애플리케이션에 대한 고유한 권한, 수수료, 확장성, 서비스 수준 등을 자율적으로 통제할 수 있습니다. 인터넷은 무제한의 수평 확장성을 지니며, 새로운 애플리케이션이 네트워크에 추가될 때마다 함께 성장합니다. 특정 서비스의 트래픽이 증가하면, 애플리케이션 제공자가 리소스를 추가할 뿐이며, 한 서비스의 성장으로 다른 서비스의 리소스가 줄어들지 않습니다. 인터넷에서 발견되는 애플리케이션의 이질성 덕분에 인터넷은 수십억 명의 사용자에게 도달할 수 있었습니다. 일부 사용자는 위키피디아에 접근하고, 다른 사용자는 은행 포털에 접근하지만, 이들 모두는 동일한 곳—즉, 동일한 인터넷으로 이동합니다.

퍼블릭 블록체인에서 애플리케이션의 이질성을 지원하지 못한 결과, 두 가지 부정적인 현상이 발생했습니다.

첫째, 이러한 네트워크의 프라이버시 한계로 인해 영구적으로 공개 가능한 자산과 데이터만 퍼블릭 블록체인으로 옮겨졌습니다. 그 결과 암호화폐 및 대체 불가능 토큰(NFT)과 같은 실험은 이루어지고 있지만, 기업이나 정부가 전통 자산이나 기록을 퍼블릭 블록체인으로 가져오는 일은 거의 없습니다.

둘째, 공유된 글로벌 자원에 대한 경쟁을 피하기 위해 대부분의 블록체인 애플리케이션 로직이 중앙화된 애플리케이션 제공자 통제하의 “오프체인(off-chain)” 환경에서 구축되고 있습니다. 이는 핵심 기능이 공유 네트워크 밖에서 운영되어, 사용자가 퍼블릭 블록체인에서 기대하는 독립적 검증 가능성을 훼손합니다.

기존 블록체인 네트워크의 한계

구체적으로, 이더리움(Ethereum) 및 유사한 스마트 컨트랙트 네트워크에서는 다음과 같은 문제가 존재합니다:

1. 원장에 접근할 수 있는 누구에게나 모든 데이터가 완전히 투명하게 공개됩니다.
2. 레이어 1에서는 거래 처리 용량에 대한 엄격한 수직적 한계가 존재합니다.
3. 레이어 2, 롤업(rollup), 기타 유사한 확장 채널은 트랜잭션 조합성(transactional composability)이 부족합니다.
4. 자산 발행자는 자산에 대한 통제권을 가명 검증인(pseudonymous validators)의 풀에 넘겨야 합니다.

규제적 관점에서 볼 때, 데이터의 완전한 투명성과 자산에 대한 통제권 상실은 이러한 네트워크가 금융기관이 사용하기에 부적합하게 만듭니다.

스마트 컨트랙트 애플리케이션이 거래 처리 한계에 도달하면, 네트워크와 그 위에서 운영되는 애플리케이션 제공자 모두에게 치명적인 결과를 초래합니다. 예를 들어, 2017년 Axiom Zen은 이더리움 네트워크에서 대성공을 거둔 애플리케이션 크립토키티(CryptoKitties)를 출시했는데, 전체 네트워크 트랜잭션의 12% 이상을 차지하며 대규모 네트워크 혼잡을 유발했습니다. 그 결과, 당시 이더리움 상의 다른 애플리케이션들은 매우 높은 수수료와 지연(latency)을 경험했습니다. 이후 Axiom Zen의 모기업은 새로운 블록체인을 개발 및 상용화하여, 기존 성공의 기반이었던 네트워크를 떠나 시장을 분절화했습니다.

기존 블록체인의 확장성 한계는 애플리케이션 데이터 및 상태의 동기화 자체에 내재된 것이 아닙니다. 우리는 이러한 제약을 회피할 수 있는 설계를 제안합니다. 기존 퍼블릭 블록체인은 모든 애플리케이션이 단일 순서화 서비스(single ordering service)를 통해야만 하도록 강제합니다. 그러나 이는 필수적이지 않습니다. 예를 들어, 한 메시징 애플리케이션의 문자 메시지 순서는 다른 애플리케이션의 소셜 피드 순서와 독립적이어야 합니다. 두 애플리케이션은 각각 자체 상태(state)에 대한 독립적인 순서화 메커니즘을 가져야 합니다. 마찬가지로, 스마트 컨트랙트 애플리케이션 네트워크 또한 트랜잭션 순서를 지역화(localization)하여 관리할 수 있어야 합니다. 그러나 이러한 애플리케이션 간에도 필요할 때 상호 운용성을 확보하기 위

해 트랜잭션 순서를 동기화할 수 있어야 합니다. 이를 위해서는 여러 애플리케이션에 걸쳐 구성된 트랜잭션을 동기화하기 위한 공유 프로토콜이 필요합니다. 현재 애플리케이션 간 독립적인 확장성을 제공하면서 동기화를 지원하려는 시도(레이어 2 프로토콜, 롤업, 크로스체인 브리지 등)는 상당한 복잡성과 보안 문제를 초래하고 있으며, 이는 최근 다수의 해킹 사례를 통해 입증되었습니다. 이에 반해 캔톤 네트워크는 레이어 2 프로토콜이나 자산 브리지를 필요로 하지 않고, 여러 서브넷(subnet)에 걸친 애플리케이션들이 네이티브하게 상호 운용할 수 있도록 합니다.

우리의 기여

본 백서에서는 캔톤 네트워크를 소개합니다. 이는 인터넷과 유사한 이질성(heterogeneity)과 확장성(scalability)을 갖춘 스마트 컨트랙트 애플리케이션을 위한 네트워크의 네트워크(network of networks)로, 애플리케이션 제공자가 자신의 애플리케이션을 직접 통제할 수 있도록 합니다.

기존 블록체인 네트워크와 마찬가지로, 캔톤 네트워크는 참가자 간 민감한 데이터를 실시간으로 동기화합니다. 이는 퍼블릭 네트워크 상에서 프라이빗 블록체인의 프라이버시를 유지하며, 캔톤 네트워크의 모든 애플리케이션은 단일 공개 원장(public ledger)을 바라봅니다.

캔톤 네트워크는 Daml이라는 표현력이 높은 스마트 컨트랙트 언어를 사용하며, 모든 자산과 데이터에 프로그래머블 프라이버시(programmable privacy)가 내장되어 있습니다. 캔톤 프로토콜은 각 애플리케이션이 독립적으로 확장할 수 있게 하여 가용성을 높이고 수수료를 낮게 유지합니다.

따라서 캔톤 네트워크는 퍼블릭 원장 영역의 주요 공백을 메웁니다:

- 이더리움, 솔라나, 테조스 등과 유사하게 단일 가상 원장 위에서 스마트 컨트랙트를 지원합니다.
- 비트코인 라이트닝 네트워크(Lightning Network)나 Zcash와 유사하게 선택적 투명성을 갖춘 내장형 프라이버시를 제공합니다.

2023년 초 기준으로, 금융기관들은 하루 500억 달러 이상의 거래를 캔톤 네트워크의 제한된 접근 서브넷에서 처리하고 있습니다.

개요

이 백서의 나머지 부분에서는 캔톤 네트워크의 구현 세부 사항을 높은 수준에서 설명합니다.

1. Daml의 데이터 모델, Daml 스마트 컨트랙트 언어, 그리고 캔톤 프로토콜 등 기반 기술을 설명합니다.
2. 이후, Daml과 캔톤을 사용해 구축된 허가형 서브넷(permissionsed subnets)의 퍼블릭 네트워크인 캔톤 네트워크를 설명합니다.

Daml

Daml은 오픈소스 스마트 컨트랙트 언어이자 프레임워크로, 프라이버시와 데이터 일관성을 유지하면서 멀티 파티 애플리케이션을 쉽게 개발, 운영, 유지보수할 수 있도록 설계되었습니다.

보다 구체적으로,

1. Daml은 실제 비즈니스 거래를 규율하는 규칙을 포착할 수 있는 개념을 제공합니다. 이를 통해 프로그래머는 보안상의 일반적인 함정을 피하면서 비즈니스 로직에만 집중할 수 있습니다.
2. Daml은 스마트 컨트랙트 코드 내에서 접근 및 권한 부여 정책을 명시할 수 있도록 지원합니다. 이를 통해 데이터는 기본적으로 비공개로 유지되며, 접근 정책은 쉽게 정의되어 스마트 컨트랙트 개발자가 이를 이해하고 유지관리하기 용이합니다.
3. Daml은 애플리케이션 상호운용성을 지원합니다. 이는 워크플로우를 더 복잡한 형태로 구성할 수 있게 하며, 이미 서로 다른 네트워크의 다양한 애플리케이션에서 배포된 워크플로우 간에도 조합이 가능합니다. 특정 참여자는 기존 워크플로우를 조합하여 기능을 단독으로 확장할 수 있으며, 이는 원장 사용의 자연스러운 확장을 촉진하고 복잡성을 관리하는 데 도움을 줍니다. Daml은 각 애플리케이션의 프라이버시와 권한 요구사항을 유지하면서, 네트워크 전체에서 워크플로우를 조합할 수 있게 합니다.
4. Daml은 다른 시스템과의 상호운용성을 지원합니다. 일반 프로그래밍 언어에 대한 바인딩 자동 생성, 다른 블록체인으로의 브리지, 공통 표준 및 도메인 특화 라이브러리 등 다양한 통합 도구를 제공합니다.

컨트랙트

Daml에서 컨트랙트(contract)는 네트워크 상의 다수의 참여자 간 워크플로우에 대한 코드화된 합의입니다. 이 컨트랙트에 서명하는 당사자를 컨트랙트 서명자(contract signatories)라고 하며, 컨트랙트를 관찰만 할 수 있는 당사자는 컨트랙트 관찰자(contract observers)라고 합니다. 참여자는 개인(개인 키로 서명)일 수도 있고, 다중 서명 정책(multi-signature policy)을 사용하는 컨소시엄일 수도 있습니다. 따라서 자산은 중앙 기관 또는 컨소시엄에 의해 발행되고 서명될 수 있습니다.

트랜잭션

컨트랙트는 트랜잭션의 일부로 생성되며, 생성 시점에 활성 상태가 됩니다. 이후의 트랜잭션은 해당 컨트랙트를 아카이브하여 비활성화할 수 있습니다. 네트워크 참여자 간의 일관성을 유지하면서 각 컨트랙트의 프라이버시를 보호하기 위해, 트랜잭션은 다음 두 가지 특성을 가져야 합니다:

1. 순서에 대한 합의(Agreement on ordering):
서로 다른 당사자들이 트랜잭션의 순서에 합의할 수 있는 메커니즘이 존재해야 하며, 이를 통해 상이한 상태 인식을 방지합니다.
2. 서브 트랜잭션 프라이버시(Sub-transaction privacy):
특정 컨트랙트의 프라이버시 정의에 따라, 다양한 당사자가 트랜잭션의 서로 다른 부분만 볼 수 있어야 합니다.
트랜잭션은 각 당사자가 자신의 부분적 관점을 검증할 수 있도록 부분 뷰(sub-transaction view)를 제공해야 합니다.

활성 컨트랙트의 상태는 활성 컨트랙트 집합(Active Contract Set, ACS)으로 불리며, 트랜잭션 그래프에서 파생됩니다. 이 그래프의 각 트랜잭션은 컨트랙트를 생성하거나 아카이브하며, 자신이 의존하는 모든 컨트랙트를 참조합니다. 새로운 트랜잭션은 트랜잭션 그래프의 끝을 참조하는 원자적(atomic) 변화로 구성됩니다. 하나의 트랜잭션은 여러 서브 트랜잭션으로 구성될 수 있으며, 서로 다른 당사자는 서로 다른 서브 트랜잭션에 접근합니다. 따라서, 각 당사자는 전역 ACS의 서로 다른 부분집합을 관찰하게 됩니다.

이 모델은 비트코인과 기타 퍼블릭 블록체인에서 사용되는 UTXO 트랜잭션 모델과 유사하지만, 두 가지 중요한 차이점이 있습니다:

1. 어느 당사자도 전체 트랜잭션 그래프를 볼 수 없습니다.
각 당사자는 자신의 뷰(view)라고 불리는 그래프의 일부(subgraph)만 볼 수 있습니다. 이는 모든 당사자가 전체 트랜잭션 그래프를 볼 수 있는 비트코인이나 카르다노(Cardano)와 같은 UTXO 블록체인과는 대조적입니다.
2. 트랜잭션이 참조된 컨트랙트를 반드시 아카이브하지는 않습니다.
트랜잭션이 입력 UTXO를 아카이브할지 여부는 애플리케이션 로직에 따라 달라지며, Daml에서는 `consuming` 및 `nonconsuming` 키워드로 정의됩니다. 이는 비트코인 등에서 UTXO를 참조할 때 반드시 소모되는 방식과는 대조적입니다.

트랜잭션은 트리 구조로 구성되며, 이를 통해 워크플로우의 조합이 가능해집니다. 즉, 기존 워크플로우의 트리가 결합된 워크플로우의 서브트리가 되며, 각 당사자는 자신의 서브트리를 검증하고 나머지는 무시할 수 있습니다.

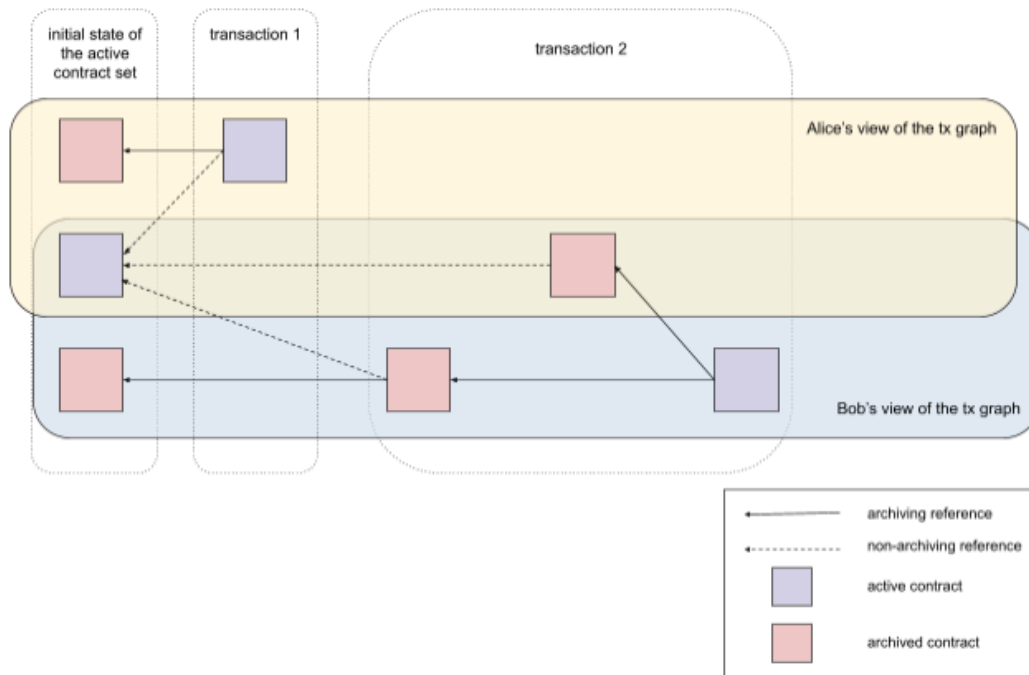


그림 1. 서브 트랜잭션 프라이버시를 갖는 트랜잭션 그래프 예시.

앨리스와 밥은 전체 트랜잭션 그래프의 일부만 볼 수 있습니다. 초기에는 세 개의 활성 컨트랙트가 있으며, 각 당사자는 두 개만 볼 수 있습니다. 앨리스와 밥이 각각 제출한 트랜잭션 1과 2는 활성 컨트랙트 집합(ACS)을 변화시켜, 초기 컨트랙트 두 개를 아카이브하고 두 개의 새로운 활성 컨트랙트를 생성하며, 두 개의 일시적(transitory) 컨트랙트를 생성 후 즉시 아카이브합니다. 두 트랜잭션 이후, 보라색으로 표시된 세 개의 활성 컨트랙트가 존재하며, 각 당사자는 그중 두 개만 접근할 수 있습니다.

다른 말로 하면, 칸톤의 원장 모델과 다른 블록체인 간의 주요 차이점은 칸톤에서는 각 당사자가 전역 ACS의 부분집합 및 전역 트랜잭션 그래프의 서브그래프(즉, 해당 당사자의 뷰)만 본다는 점입니다.

이 당사자별 뷰는 언제나 유효한 원장이며, 각 당사자의 노드에서 로컬로 검증할 수 있습니다. 즉, 검증을 위해 다른 당사자를 신뢰할 필요가 없습니다.

당사자의 노드는 트랜잭션 또는 서브 트랜잭션을 수신할 때 세 가지를 검증합니다:

1. 해당 트랜잭션이 자신의 뷰와 일관되는지,
2. 트랜잭션이 스마트 컨트랙트에 정의된 로직을 따르는지,
3. 트랜잭션이 적절히 승인되었는지.

접근 제어를 관리하는 것 외에도, 이러한 원장 분할 구조는 병렬 처리(parallel processing)를 가능하게 합니다. 트랜잭션은 명시적으로 의존성을 선언하므로, 서로 독립적인 트랜잭션은 개별 인프라에서 병렬로 처리될 수 있습니다. 이로써 칸톤 네트워크는 네트워크 수요 변동에 따라 용량을 추가하여 수평 확장(horizontal scalability)을 달성할 수 있습니다.

이 모델은 두 가지 도전을 제시합니다:

1. 서로 다른 당사자의 글로벌 ACS 뷰 일관성을 보장해야 합니다.
즉, 특정 컨트랙트에 대해 그 컨트랙트를 보는 모든 당사자는 항상 해당 컨트랙트가 활성 상태인지, 아카이브 상태인지에 대해 일치된 인식을 가져야 합니다. 칸톤 프로토콜이 이를 어떻게 달성하는지는 “합의(Consensus)” 섹션에서 설명합니다.
2. 이러한 제한적인 프라이버시 제어 하에서 개발이 용이한 애플리케이션 개발 모델이 필요합니다.
Daml SDK가 이를 어떻게 지원하는지 다음에서 설명합니다.

스마트 컨트랙트 언어

Daml은 정적 타입 시스템(static type system)을 갖춘 현대적인 함수형 언어로, 컴파일 시점에 많은 비의도적 동작이나 정확성 오류를 사전에 방지할 수 있습니다.

개발자는 데이터 스키마, 워크플로우의 의미론(semantics), 트랜잭션 실행 로직을 컨트랙트 템플릿(contract templates) 내에서 정의합니다.

이는 객체지향 프로그래밍(OOP)의 클래스 정의나 SQL 데이터베이스 스키마에 해당합니다.

하나의 템플릿(template)은 다음을 정의합니다:

1. 인자(Arguments) – 컨트랙트가 저장하는 데이터.
2. 선택(Choices) – 컨트랙트에 대해 참여자들이 수행할 수 있는 행위(actions).
선택은 객체지향 언어의 메서드(method) 또는 데이터베이스의 저장 프로시저(stored procedure)에 해당합니다.
3. 권한 부여(Authorization) –
서명자(signatories)는 컨트랙트의 생성 또는 아카이브를 승인해야 하는 당사자이며,
관찰자(observers)는 컨트랙트를 조회할 수 있는 다른 당사자입니다.
통제자(controllers)는 컨트랙트의 선택(choices)을 실행하여 특정 행위를 취할 수 있는 당사자입니다.
한 당사자는 특정 선택에 대한 권한을 다른 당사자에게 위임(delegate)할 수 있으며, 위임된 권한이 사용될 때마다 그 사실을 인지할 수 있습니다.
4. 제약 조건(Constraints) –
템플릿의 모든 컨트랙트에 대해 반드시 충족되어야 하는 조건(predicate)을 `ensure` 키워드로 정의합니다.

예시:

```
template Iou
with
```

```

    issuer : Party
    owner : Party
    currency : Text
    amount : Decimal
  where
    ensure amount > 0.0
    signatory issuer, owner

    choice Transfer : ContractId Iou
    with newOwner : Party
    controller owner, newOwner
    do
      create this with owner = newOwner

```

기본적으로, 선택을 실행하면 해당 컨트랙트는 아카이브 됩니다. 위의 Transfer 선택의 경우, 컨트랙트를 아카이브하는 동시에 새로운 소유자를 가진 새로운 컨트랙트를 생성합니다. 비트코인의 UTXO 모델 및 카르다노(Cardano)의 eUTXO 모델보다 개선된 점은, 개발자가 선택을 `nonconsuming`으로 지정할 수 있다는 것입니다. 비소모 선택은 UTXO를 아카이브하지 않으므로 경쟁을 줄여줍니다.

Daml의 명시적 권한 정의 모델은 컨트랙트 이해관계자가 예기치 않은 상황을 수정하기 위해 수동 개입(manual intervention)을 수행할 수 있도록 합니다. 템플릿은 사전적으로 어떤 종류의 개입이 필요한지 알 필요 없이, 어디서, 어떻게, 누구에 의해 개입이 발생할 수 있는지를 명확히 정의하면서도 어떠한 보안 보장도 완화하지 않습니다.

서명자는 만장일치가 이루어지는 한, 컨트랙트를 아카이브하거나, 업그레이드하거나, 새로운 컨트랙트 인스턴스를 생성하는 데 합의할 수 있습니다. 서명자 중 일부가 컨소시엄인 경우, 해당 당사자의 합의는 그 컨소시엄의 내부 합의 프로토콜(consensus protocol)에 따라 결정됩니다. 예를 들어, 만장일치 대신 $\frac{2}{3}$ 초다수(supermajority)= 동의를 요구할 수도 있습니다.

관찰자는 이러한 변경 사항에 대해 통지받을 권리가 있으며, 이를 독립적으로 검증할 수 있습니다. 단, 그들의 승인은 필요하지 않습니다. 컨트랙트에 대한 모든 행위 — 생성, 아카이브, 선택 호출 — 는 트랜잭션 트리 내 이벤트로 기록되며, 모든 변경 사항에 대한 완전하고 부인 불가능한 감사 로그를 형성합니다. 이러한 적절한 승인 절차 하에서의 사후 변경 기능은 애플리케이션 제공자가 예기치 않은 사건에 대응하여 데이터, 프로세스, 운영 절차를 업그레이드할 수 있도록 합니다. 예를 들어, 규제 당국 또는 사법 결정에 따라 비즈니스 거래의 소급적(retroactive) 수정이 필요한 경우 이를 처리할 수 있습니다.

Daml은 템플릿을 모듈(module)과 패키지(package) 단위로 구성합니다. 패키지는 다른 패키지에 의존할 수 있으며, 이는 서로 다른 네트워크에 배포된 애플리케이션 간에도 가능합니다. 이처럼 서로 다른 칸톤 서버넷의 애플리케이션 간 패키지 의존성이 허용되기 때문에, 참여자들은 워크플로우를 이러한 빌딩 블록으로 결합할 수 있는 개방형 아키텍처가 구현됩니다.

Daml의 설계에 대한 심층적 검토는 Daml 백서를 참고하십시오. Daml 도구에 대한 개요는 <https://docs.daml.com>에서 확인할 수 있습니다.

원장 모델

Daml은 현재 존재하는 기술들 가운데 독특한 방식으로, 참여자들이 스마트 컨트랙트 형태의 가치를 교환할 수 있도록 합니다. 스마트 컨트랙트의 업데이트는 단순히 원장(ledger)의 항목에 대해 승인되고 검증된 업데이트에 불과합니다. 신뢰할 수 있는 중앙 중개자 없이 이러한 업데이트를 수행하려는 근본적인 과제는, 스마트 컨트랙트를 반영하는 원장 항목이 정확하며 제3자에게 증명 가능하도록 하는 것입니다.

이 문제를 해결하기 위한 일반적인 접근법은, 네트워크의 모든 참여자가 전체 원장의 복사본을 보유하고 갱신하도록 하여 원장을 네트워크 참여자 간에 분산시키는 것입니다. 이 경우 합의 메커니즘이 모든 참여자에게 원장을 정확히 복제하기 위해 사용됩니다. 그러나 이러한 접근은 프라이버시가 전혀 없고, 확장성에 절대적 한계가 존재하는 네트워크를 초래합니다.

트랜잭션 섹션에서 논의했듯이, Daml의 원장 데이터 모델은 이러한 프라이버시 및 확장성 문제를 해결하기 위해 전혀 다른 접근 방식을 취합니다. Daml의 원장 모델에서는 원장이 모든 참여자 간에 완전히 복제되지 않습니다. 대신 프라이버시 규칙에 따라 세분화되며, 각 참여자는 자신과 관련된 원장의 일부, 즉 뷰(view) 또는 샤드(shard)만 저장합니다. 따라서 네트워크의 모든 참여자가 공유하는 단일 원장 뷰는 존재하지 않습니다. 대신, 각 참여자는 자신과 관련된 컨트랙트만 포함하는 자체 원장을 보유합니다.

즉, 네트워크의 모든 참여자가 동일한 원장을 복제하는 대신, 각 트랜잭션에 참여한 당사자만 자신의 원장을 업데이트하여 해당 트랜잭션을 반영합니다. 그러나 이 방식에는 문제가 있습니다. 만약 스마트 컨트랙트의 기록이 여러 원장에 분산되어 있고, 각 원장은 특정 참여자만 볼 수 있다면, 네트워크의 어느 누구도 자신이 보유한 스마트 컨트랙트가 정확한지 확인하기 어려워집니다.

Daml은 이 문제를 각 참여자의 뷰가 단일 글로벌 가상 원장(global virtual ledger)의 부분집합(subset)이 되도록 보장함으로써 해결합니다. 즉, 개념적으로 Daml 원장의 모든 참여자는 단일 원장을 인식하지만, 각 참여자는 그 원장 상태 중 자신에게 허용된 부분만 읽을 수 있습니다. 이 글로벌 원장은 특정 데이터 저장소에 존재하지 않기 때문에 가상 원장이라고 부릅니다.

개념적으로 모든 사용자가 동일한 원장을 참조하므로, 공유된 애플리케이션 상태(예: 자산의 소유권)에 대해서는 모든 사용자가 일관된 뷰를 갖습니다.

아래에서 설명할 칸톤 프로토콜은 네트워크 내 모든 정상 작동 노드의 뷰가 단일 유효한 글로벌 가상 원장의 일관된 부분집합이 되도록 보장하는 메커니즘입니다. 이 모든 과정은 해당 당사자가 아닌 제3자는 어떤 정보도 볼 수 없도록 보장하는 방식으로 수행됩니다. 따라서 참여자들은 디지털 자산을 전송할 때, 전송자가 실제로 그 자산을 소유하고 있음을 신뢰할 수 있으며, 명시적으로 허용되지 않는 한 네트워크의 다른 어떤 참여자도 해당 전송 사실을 알 수 없습니다.

다.

Daml의 완전 탈중앙화 및 당사자 중심(Party-centric) 원장 모델은 추가적인 탈중앙화를 가능하게 합니다. 즉, 단일 네트워크 구조로 제한되지 않고, 사용자가 자신만의 서브넷(subnet)을 생성할 수 있습니다. 하나의 참여자는 하나 이상의 서브넷에 연결될 수 있으며, 복수의 서브넷에 연결된 경우 칸톤 프로토콜이 디지털 자산 트랜잭션을 서브넷 간에 동기화할 수 있습니다. 이처럼 Daml 원장 모델은 네트워크의 네트워크(network of networks)를 가능하게 합니다. 이 설계는 탈중앙화 환경에서 프라이버시, 성능, 확장성을 동시에 달성하도록 합니다.

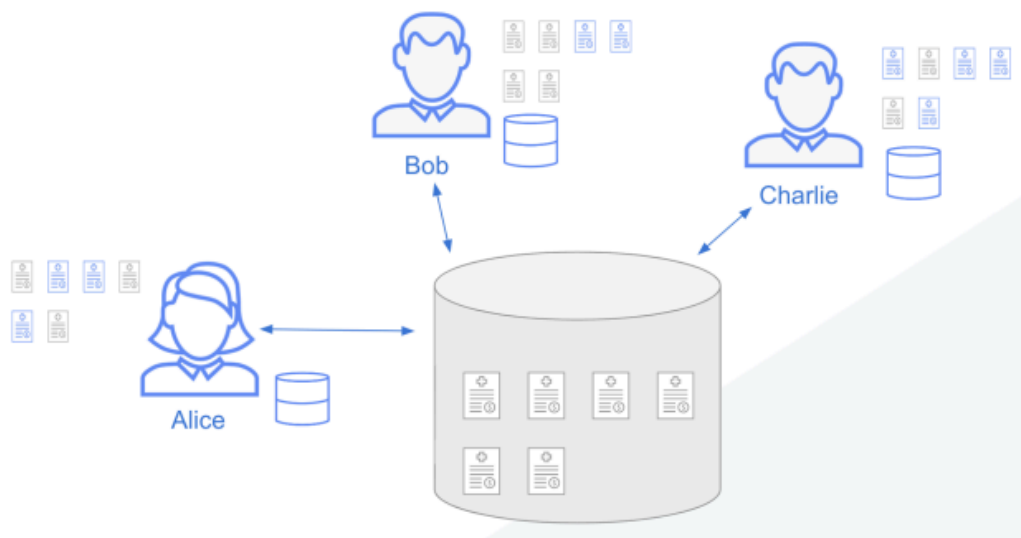


그림 2. 칸톤의 원장 모델

각 참여자는 자체적으로 유효한 원장을 보유하며, 이는 칸톤 프로토콜을 통해 글로벌 원장과 일관성을 유지합니다. 글로벌 원장은 가상(virtual) 원장이므로, 어느 단일 참여자도 이를 전체적으로 저장하지 않습니다. 이 예시에서 활성 컨트랙트 집합(Active Contract Set, ACS)은 총 6개의 컨트랙트로 구성되지만, 각 참여자는 그중 2~4개의 컨트랙트(파란색으로 표시된 부분)에만 접근할 수 있습니다.

Daml의 원장 모델에 대한 심층적인 설명은 [Daml SDK documentation - Daml Ledger Model](#)을 참조하십시오.

칸톤

칸톤은 프라이버시 보호 기능이 포함된 오픈소스 블록체인 프로토콜입니다.

칸톤은 위에서 설명한 Daml의 원장 모델을 구현합니다. 칸톤은 현재 Daml 언어를 지원하지만, 유사한 계층적 서브 트랜잭션 프라이버시 모델을 갖는 다른 언어도 지원할 수 있습니다.

Network topology

캔톤 네트워크의 노드는 참여 노드(participant nodes)라고 불립니다. Daml에서 사용자 또는 회사는 파티(Party)로 표현되며, 하나 이상의 참여 노드를 배포합니다. 이러한 참여 노드들은 해당 파티를 대신하여 작동합니다. 노드 간 데이터를 전송하고 메시지의 순서를 결정하기 위해, 각 참여 노드는 하나 이상의 프라이빗 또는 퍼블릭 캔톤 서비스 제공자(CSP)에 연결됩니다. 이 CSP는 싱크 도메인(“sync domain”)이라 불리는 캔톤 구성 요소를 운영합니다. 따라서 싱크 도메인에 연결하면, 파티는 동일한 싱크 도메인에 연결된 모든 다른 참여자들과 거래할 수 있습니다.

누구나 CSP가 되어 싱크 도메인을 자유롭게 배포할 수 있습니다. 새로운 싱크 도메인을 배포하는 이유로는 처리량 증가, 지연 시간 감소, 특정 국가나 특정 블록체인 네트워크를 통한 데이터 전송 요구, 또는 기타 운영상의 이유가 있을 수 있습니다. 프라이버시와 네트워크 중립성을 촉진하기 위해, 싱크 도메인을 통해 전송되는 데이터는 암호화되어 CSP가 메시지 내용을 접근할 수 없습니다. 싱크 도메인은 참여 노드들 간의고가용성(highly available), 장애 내성(fault-tolerant) 메시징 큐로 볼 수 있으며, 암호화된 메시지를 순서화하고(timestamp), 참여 노드들에 제공합니다. CSP는 단일 기관일 수도 있고, 여러 참여자들이 분산된 싱크 도메인을 운영하는 virtual CSP (vCSP)일 수도 있습니다. 출시 시점에, 캔톤 네트워크는 최소 하나 이상의 공개 가상 CSP (vCSP)를 가지며, 이는 컨소시엄에 의해 운영되고 어떤 참여 노드의 연결 요청도 수락합니다. 애플리케이션 제공자는 이 open vCSP를 사용할 수도 있고, 다른 CSP를 사용할 수도 있습니다. 따라서 캔톤은 신뢰, 접근 제어, 운영 복잡성 간의 다양한 절충점을 가진 Daml 애플리케이션들로 구성된 메쉬 네트워크를 형성합니다.

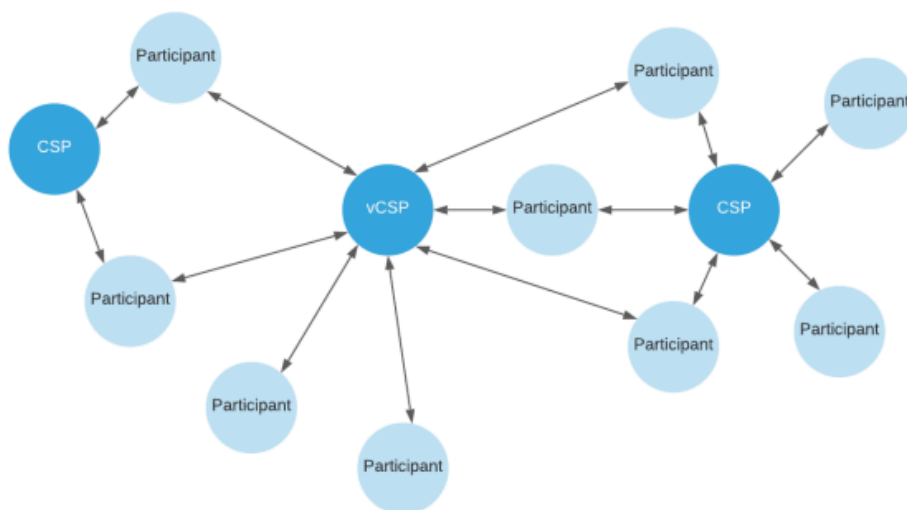


그림 3: 캔톤 네트워크 토폴로지. 참가자들은 캔톤 서비스 제공자(CSP) 또는 컨소시엄 vCSPs를 통해 서로 연결됩니다. 참여 노드가 공통 CSP 또는 vCSP에 연결되어 있다면 거래가 가능합니다. 네트워크의 모든 트랜잭션을 단일 노드가 처리하지 않습니다.

단일 노드는 처리 및 저장의 한계를 가지지만, 캔톤 네트워크는 본질적인 확장성 병목을 가지지 않습니다. 하나의 참여 노드는 자신의 데이터와 워크플로우만 처리하며, 서로 다른 싱크 도메인들은 병렬로 동기화됩니다. 참여자는 싱크 도메인을 운영하는 CSP가 허용하는 한, 원하는 싱크 도메인에 연결할 수 있습니다. Open 싱크 도메인은 형식이 올바른 모든 요청을 수락합니다. 캔톤은 퍼블릭 허가형 네트워크를 가능하게 하며, 누구나 어떤 이유로든 캔톤 싱크 도메인을 배포하여 CSP가 될 수 있습니다. 싱크 도메인은 사일로(silos)가 아닙니다. 하나 이상의 공통 싱크 도메인을 공유하는 참여자들은 더 높은 수준의 워크플로우를 구성할 수 있으며, 여러 애플리케이션에 걸친 원자적 트랜잭션도 가능하며, 이는 애플리케이션이 선택한 싱크 도메인을 통해 처리됩니다. 컨트랙트의 서명자와 관찰자는 어떤 싱크 도메인이 그들의 컨트랙트를 동기화할지를 제어할 수 있으며, 특정 싱크 도메인이 컨트랙트를 순서화하는 역할을 다른 싱크 도메인으로 재할당할 수도 있습니다. 이를 통해 싱크 도메인 종속이나 검열을 방지할 수 있습니다. 아래 다이어그램은 싱크 도메인 1에서 싱크 도메인 2로 컨트랙트의 동기화 책임을 재할당하는 과정을 보여줍니다.

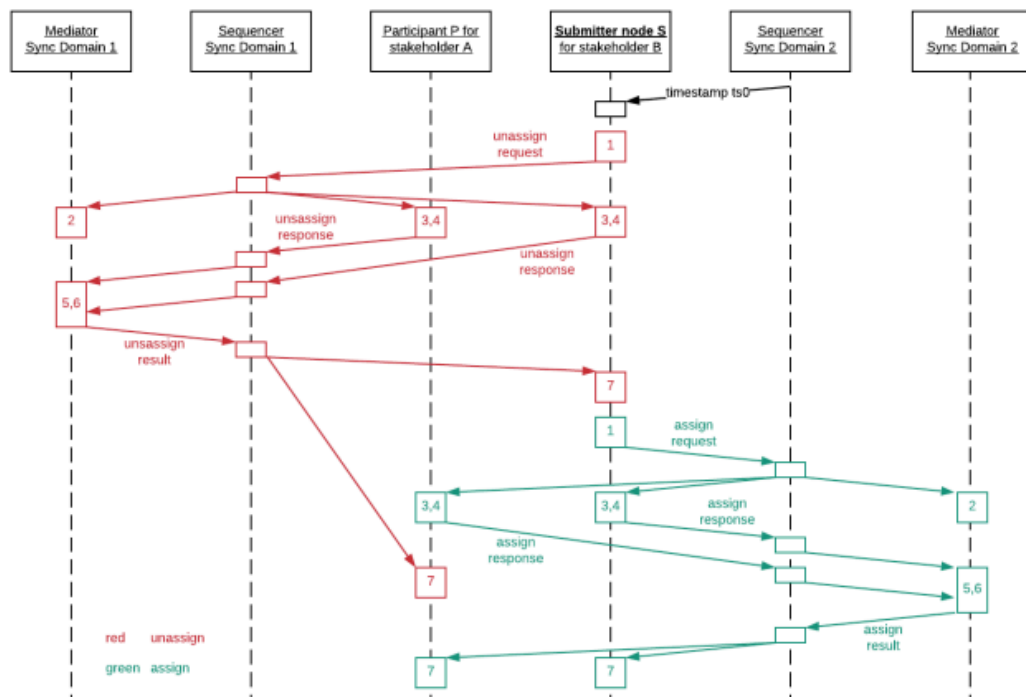


그림 4: 싱크 도메인 재할당 시퀀스 다이어그램. 컨트랙트의 signatories는 합의하여 컨트랙트의 동기화 역할을 한 싱크 도메인(CSP)을 다른 싱크 도메인으로 재할당할 수 있습니다.

캔톤 네트워크는 단일 중앙화된 거버넌스나 접근 및 사용에 대한 정책을 가지고 있지 않습니다. 각 구성 노드나 서브넷이 자체 정책을 설정합니다.

데이터 프루닝(Data pruning)

캔톤은 로그에 대한 이력 프루닝 및 수정 기능을 제공합니다. 참여자 및 싱크 도메인 운영자는 노드가 과거의 암호화 데이터를 저장할지 혹은 삭제할지를 설정할 수 있으며, 이를 통해 감사 가능성과 유럽연합 일반개인정보보호법(GDPR)과 같은 ‘잊힐 권리(right-to-forget)’ 규정 준수를 위한 컨트랙트 삭제 가능성 사이에서 균형을 조정할 수 있습니다.

이전 데이터를 오프라인 스토리지로 이동하면, 변경 불가능한 완전한 감사 로그를 유지하면서도 데이터 저장 비용을 절감하고 운영 환경의 지속 가능성을 향상시킬 수 있습니다. 캔톤 노드는 공유된 상태에 대한 암호화된 커밋을 지속적으로 교환하므로, 설령 과거 데이터를 프루닝 하도록 설정하더라도 악의적이거나 오작동하는 상대방에 의한 부인 시도로부터 보안을 유지합니다.

따라서, 개별 노드 운영자는 완전하고 변경 불가능한 이력 감사 가능성 유지와 그 외의 운영적 및 규제 준수 요구사항 사이에서 선택할 수 있습니다.

지분 증명 기반 합의(Proof-of-Stakeholder: Consensus with privacy)

캔톤의 주요 목표는 참여자 간 데이터 일관성을 제공하는 것입니다. 즉, 캔톤은 여러 참여자들이 공동으로 이해관계를 가진 활성 컨트랙트에 대해 합의에 도달하고, 해당 상태로 이어진 트랜잭션의 유효성을 검증하도록 합니다.

일반적인 합의 접근 방식은 상태 머신 복제(state machine replication)로, 모든 참여자가 동일한 전역 상태를 복제하는 것입니다. 그러나 전체 전역 상태를 복제하는 것은 프라이버시와 확장성 측면에서 바람직하지 않습니다.

이에 캔톤의 proof-of-stakeholder 합의 프로토콜은 두 개의 합의 계층(consensus layers)으로 분리되어 있습니다. 프라이버시를 유지하면서 일관성을 확보하기 위해, 첫 번째 합의 계층은 2단계 커밋(two-phase commit) 프로토콜로, 각 컨트랙트를 해당 컨트랙트의 이해관계자(stakeholders)에게 복제하는 동시에 각 이해관계자가 트랜잭션을 검증할 수 있도록 합니다. 개념적으로 이는 모든 참여자 부분집합(subset)에 대해 상태 머신을 복제하는 것과 같습니다.

첫 번째 계층이 트랜잭션을 일관되게 커밋하려면, 노드들이 충돌하는 트랜잭션 요청이 원장에 적용되는 순서에 대해 합의해야 합니다. 따라서 두 번째 합의 계층은 시퀀싱 프로토콜(sequencing protocol)로, 암호화된 트랜잭션을 수신하고 각 트랜잭션에 타임스탬프를 부여합니다.

이 시퀀싱 계층은 중앙 CSP에서 실행될 수 있으며, 또는 가상 CSP의 분산 싱크 도메인에 연결된 경우, 비잔틴 장애 허용(BFT, Byzantine Fault Tolerant) 합의 알고리즘으로 보호되는 복제 상태 머신으로 작동합니다.

따라서 가상 CSP는 싱크 도메인 내 트랜잭션 요청에 대한 총 순서(total order)를 결정하며, 트랜잭션 처리는 결정적(deterministic)으로 이루어집니다.

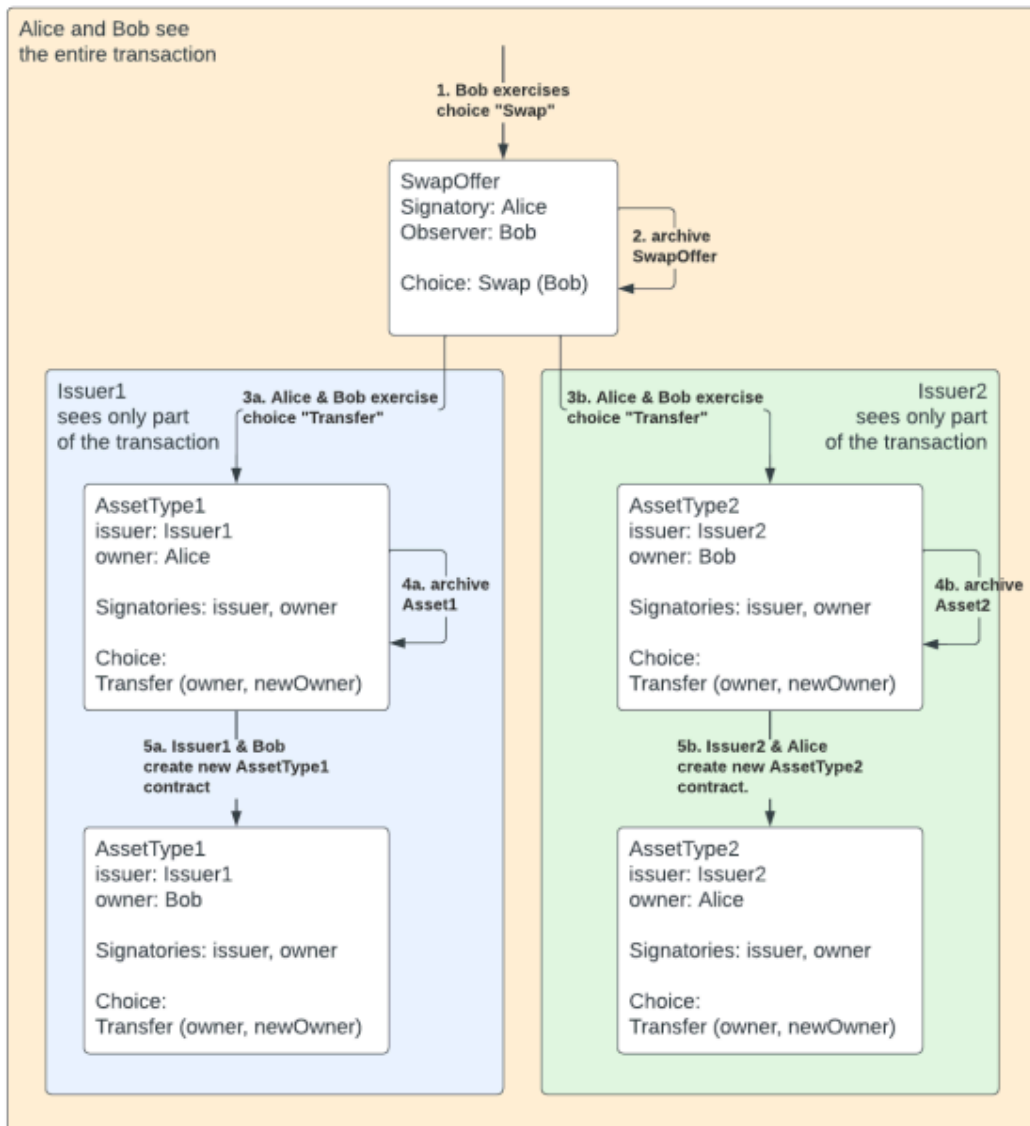


그림 5: 원자적 자산 교환 트랜잭션(Atomic asset swap transaction).

서명자들이 두 서브 트랜잭션 모두에 동의해야만 자산 교환이 성공합니다. 그렇지 않으면 교환이 거부되고 자산은 전송되지 않습니다. 앨리스와 밥은 전체 트랜잭션을 볼 수 있으며, 발행자 1(Issuer1)과 발행자 2(Issuer2)는 각자 자신과 관련된 부분만 볼 수 있습니다.

위 그림의 예시 트랜잭션을 살펴보면, 트랜잭션이 원장에 적용되기 전에는 세 개의 컨트랙트가 활성 상태입니다: (AssetType1) 앨리스가 발행자 1이 발행한 자산을 소유하고, (AssetType2) 밥이 발행자 2가 발행한 자산을 소유하며, (SwapOffer) 앨리스가 밥에게 자산 교환 제안을 합니다. 밥이 교환 제안을 수락하면, 세 개의 컨트랙트가 모두 아카이브되고 두 개의 새로운 컨트랙트가 생성됩니다: (AssetType1) 밥이 발행자 1의 자산을 소유하고, (AssetType2) 앨리스가 발행자 2의 자산을 소유합니다.

컨트랙트에 인코딩된 일부 규칙(예: 자산 금액 보존 등)은 간략화를 위해 생략되었습니다. 이 트랜잭션에서 밥은 “Swap” 선택을 실행하며, 이는 SwapOffer를 아카이브합니다. 각 선택(choice)은 호출에 필요한 권한을 정의하며(위 다이어그램의 괄호 안에 표시됨), 앨리스는 “Swap” 선택을 오직 밥의 권한만으로 실행할 수 있도록 제안을 생성했습니다. 앨리스가 SwapOffer의 서명자이기 때문에, “Swap” 선택은 밥의 권한과 함께 앨리스의 권한을 사용하여 두 자산에 대한 “Transfer” 선택을 호출할 수 있습니다. 이로써 자산 컨트랙트는 아카이브되고 소유자가 바뀐 두 개의 새로운 자산 컨트랙트가 생성됩니다. 발행자들이 자산의 서명자였기 때문에, 그들의 권한은 해당 자산의 “Transfer” 선택 호출에도 사용됩니다.

트랜잭션에 참여한 모든 당사자가 트랜잭션의 유효성을 확인할 수 있는 것은 아니지만, 각 당사자는 자신이 볼 수 있는 서브 트랜잭션의 유효성을 검증할 수 있습니다. 예를 들어, 발행자 2(Issuer2)는 자신이 발행한 자산만 볼 수 있으며, 발행자 1(Issuer1)이 발행한 자산이나 앨리스와 밥 간의 교환 컨트랙트는 볼 수 없습니다. 또한, 발행자 1은 앨리스가 전송을 승인했다는 확신이 있어야만 트랜잭션을 수락해야 합니다.

악의적인 참여자에 대한 내성을 확보하기 위해, 칸톤은 트랜잭션을 두 단계로 처리하여 합의의 달성을 합니다. 먼저, 제출자는 각 서명자에게 확인 요청을 전송하며, 그 서명자가 볼 수 있는 트랜잭션 부분만 암호화하여 첨부합니다. 각 서명자는 자신의 서브 트랜잭션을 복호화하고 요청의 유효성을 검증한 후, 서명된 확인 응답을 반환합니다.

이 검증 과정은 두 가지를 보장합니다: 첫째, Daml 권한 부여 모델이 준수되며, 올바른 당사자들이 트랜잭션에 대해 통지받음을 확인합니다. 이를 통해 제출자의 악의적인 행위를 차단합니다. 둘째, 이중 지불을 방지합니다. 이중 지불 시도는 악의적인 행위자가 아닐 수도 있으며, 상충하는 동시 워크플로우에서 발생할 수 있습니다.

싱크 도메인의 총 순서화와 Daml의 결정성은 모든 참여자가 동일한 방식으로 충돌을 해결할 수 있게 합니다. 결과적으로, 트랜잭션은 모든 서명자에게 원자적으로 적용되거나 거부되며, 각 당사자가 서로 다른 원장 뷰를 가지고 있더라도 합의는 유지됩니다.

애플리케이션 구성 가능성(Application composability)

칸톤에서는 서로 다른 싱크 도메인을 통해 동기화되더라도 두 개 이상의 애플리케이션이 원자적 트랜잭션을 기반으로 상호 구성될 수 있습니다. 예를 들어, 두 중앙은행이 각각 자국의 CSP를 이용해 자국 통화 거래를 동기화하더라도, 해당 통화의 보유자들은 여전히 크로스도메인 트랜잭션을 통해 원자적으로 자산을 교환할 수 있습니다.

다른 블록체인과 유사하게, 단일 글로벌 칸톤 싱크 도메인을 통해 임의의 워크플로우를 원자적으로 구성할 수도 있습니다. 그러나 다수의 싱크 도메인을 보유하는 것은 여러 가지 이점이 있습니다. 예를 들어, 기업이나 개인은 네트워크 자원에 대해 더 많은 통제권을 원할 수 있습니다. 단일 글로벌 싱크 도메인은 일부 또는 모든 참여자에게 동일한 트랜잭션 지연을 의미하게 됩니다. 반면 다중 싱크 도메인은 서로 독립적으로 완전 병렬 처리되어 처리량을 증가시킬 수 있습니다. 또한 운영상의 이유로, 예를 들어 중요 워크플로우의 경우 접근이 제한된 새로운 싱

크 도메인을 사용할 수도 있습니다. 마지막으로 싱크 도메인 운영자들은 각자의 서비스에 대해서도 다른 요금을 부과할 수 있습니다. 위 예시에서 각 지역 통화의 트랜잭션은 해당 중앙은행 관할 내에서 완전히 처리됩니다.

그러나 다수의 싱크 도메인을 사용하는 것은 서로 다른 도메인 간 워크플로우를 어떻게 결합할 지라는 새로운 과제를 야기합니다. Daml에서 워크플로우 구성이란, 서로 다른 싱크 도메인에서 동기화된 컨트랙트들을 단일 트랜잭션 내에서 사용할 수 있음을 의미합니다. 이러한 기능이 없다면 실제로 구성 가능성 문제를 해결하지 못하게 되며, 이는 상호운용 가능한 단일 네트워크의 서브넷들이 아닌, 각각 고립된(싱크 도메인 단위의) 다수의 네트워크를 생성하게 됩니다.

캔톤은 크로스서브넷 트랜잭션의 원자성을 보장합니다. 서로 다른 싱크 도메인은 각자 처리하는 서브 트랜잭션들 간의 순서에 대한 공통 개념이 없기 때문에, 원자성과 내결함성을 동시에 유지하기가 어렵습니다. 이를 해결하기 위해, 캔톤은 모든 트랜잭션 참여자가 최소 하나의 공통 싱크 도메인에 연결되어 있는 경우에만 크로스서브넷 트랜잭션을 허용합니다. 크로스서브넷 트랜잭션으로 인해 발생하는 컨트랙트 변경은 이 공통 싱크 도메인을 통해 동기화됩니다. 또한 캔톤은 컨트랙트에 대한 동기화 서비스를 제공하는 싱크 도메인을 변경할 수 있도록 합니다. 이러한 동기화 재할당은 주어진 컨트랙트의 작업 순서를 관리하는 새로운 권한 도메인을 지정하는 것을 의미합니다.

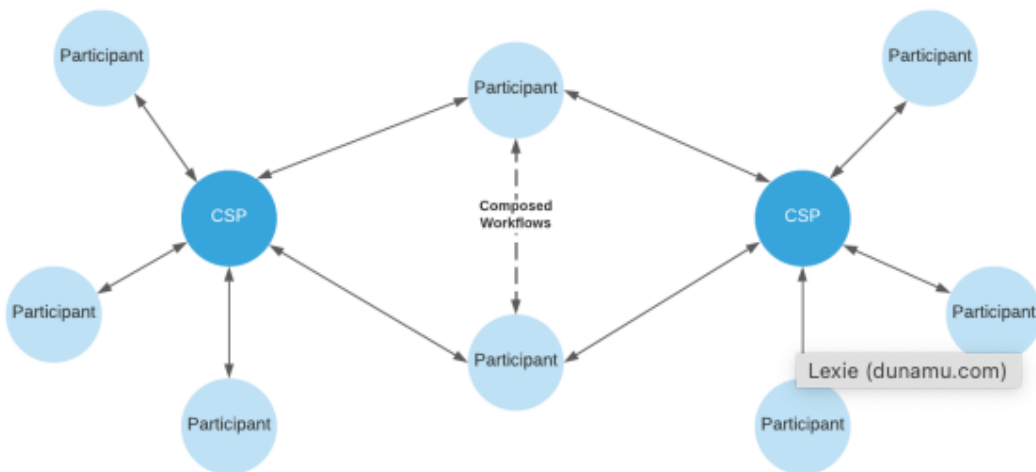


그림 6: 네트워크 토폴로지 예시. 둘 이상의 싱크 도메인에 연결된 참여자는 원자적 크로스서브넷 트랜잭션을 구성할 수 있으며, 이를 통해 여러 애플리케이션과 네트워크 전반에 걸친 트랜잭션 워크플로우를 구축할 수 있습니다.

캔톤 프로토콜의 설계에 대한 심층적 검토는 [캔톤 프로토콜 백서](#)를 참고하십시오.

캔톤 네트워크

칸톤 네트워크는 모든 싱크 도메인과 그에 연결된 참여 노드들로 구성된 네트워크의 네트워크(network of networks)입니다. 이는 전 세계적으로 상호 연결된 참여 노드, 싱크 도메인 node, 그리고 그 위에 배포된 프라이빗, 세미프라이빗, 퍼블릭 스마트 컨트랙트 애플리케이션으로 이루어진 시스템입니다.

칸톤 네트워크의 사용자는 세 가지 주요 역할을 수행합니다.

1. 애플리케이션 제공자 – 스마트 컨트랙트 애플리케이션을 구축하고 유지합니다. 이들은 하나 이상의 참여 노드, 애플리케이션 백엔드 인프라, 프론트엔드 웹 인터페이스를 운영합니다. 애플리케이션 제공자는 필요에 따라 자신들의 애플리케이션을 위한 CSP 역할을 수행하거나, 다른 CSP의 서비스를 이용할 수 있습니다.
2. 애플리케이션 사용자 – 대부분의 사용자는 API 및 웹 UI를 통해 애플리케이션과 상호 작용합니다. 사용자는 참여 노드를 보유해야 하며, 직접 운영할 수도 있고 타인이 관리하는 호스팅된 노드를 사용할 수도 있습니다.
3. 칸톤 서비스 제공자(CSP) – 일반적으로 애플리케이션 제공자이기도 한 인프라 제공자로, 칸톤 싱크 도메인을 운영하여 참여 노드들을 연결합니다.

칸톤 네트워크는 다수의 서브넷으로 구성됩니다. 칸톤 서브넷은 하나 이상의 싱크 도메인 노드를 통해 서로 트랜잭션을 수행할 수 있는 하나 이상의 참여 노드 집합을 의미합니다.

네트워크는 vCSP가 운영하는 퍼블릭 싱크 도메인의 출시와 함께 공개적으로 사용 가능해질 예정이며, 이는 모든 참여 노드의 연결 요청을 수락합니다. 이 퍼블릭 싱크 도메인은 Super Validator Collective(SVC)라 불리는 독립 기업들의 컨소시엄이 운영합니다.

SVC는 네트워크 대역폭 사용량에 따라 수수료를 부과하며, 수수료는 대역폭 단위당 고정되어 있고 미 달러(USD)로 표시됩니다. 따라서 네트워크 사용자는 예측 가능한 네트워크 비용 구조를 갖게 됩니다. SVC는 필요 시 수수료를 조정할 수 있습니다. SVC 퍼블릭 싱크 도메인의 사용은 선택 사항이며, 네트워크 참여자는 서로 다른 결제 메커니즘과 수수료 구조를 가진 추가 퍼블릭 또는 프라이빗 싱크 도메인을 자유롭게 개설할 수 있습니다.

결론(Conclusion)

본 백서에서는 새로운 형태의 스마트 컨트랙트 네트워크인 칸톤 네트워크를 소개했습니다. 기존 퍼블릭 블록체인의 제약, 즉 전역 복제 상태로 인한 프라이버시 부족과 확장성 한계를 출발점으로 삼아, 칸톤이 이러한 한계 없이 글로벌 네트워크를 구축하는 방법을 제시했습니다.

또한 Super Validator Collective(SVC)가 운영하는 가상 칸톤 서비스 제공자(vCSP)의 출시에 따라 칸톤 네트워크가 퍼블릭 사용을 위해 개방될 예정임을 논의했습니다. 현재 운영 중인 퍼미션드 칸톤 네트워크들은 퍼블릭 칸톤 네트워크의 서브넷으로 통합되며, 칸톤 네트워크는 기관 자산을 위한 최초의 퍼블릭 퍼미션드 블록체인이 될 것입니다.