Matter Inc. 백서

rev 0.2.1

동기

자산 토큰화는 현재 모든 자산의 토큰화에 대해 경제적, 기술적, 규제 및 인식적 한계가 존재함에도 불구하고 블록체인 커뮤니티에서 뜨거운 주제입니다.
가장 설명하기 쉬운 분야는 경제 부문입니다. 블록체인은 가치나 자산 양도의 맥락에서 기장이나 정해진 규칙을 이행하는데 사용된다면, 거래 당 1 USD 의 주문에 거래 비용을 발생시킵니다(이더리움 트랜잭션 한도인 50,000 단위의 가스, 단위 당 가스 가격 40 GWei 그리고 ETH/USD 교환율 500 USD/ETH). 이는 대규모 거래에 이용되는 자산 뿐만 아니라, 이미 이러한 프로세스를 위해 잘 정립되고 규제된 수단을 보유하고 있는 기관 투자자들 사이에서 발생하는 거래에서 역시 문제가 됩니다.
대규모로 자산 토큰화를 실행하기 위해서 먼저 토큰화 과정에 신뢰를 부여하고 기존의 자산 소유자를 이 시장에 끌어들일 수 있도록 기반 시설과 기술을 완벽히 갖추고 최초로 토큰화 해야하는 자산에 대해 적절한 계획을 구상해야 합니다. 다음 섹션에서 이 부분에 대해 자세하게 설명합니다.

금융 상품과 파생상품 토큰화

전통적인 금융 자산의 토큰화 그리고 관련된 현금 흐름은 기존 세계와 암호 화폐 커뮤니티에 막대한 혜택을 제공합니다. 다른 백서와 대조적으로, 가능한 간단하게 예시를 제시하고자 합니다.
제시된 대규모 대출 포트폴리오의 토큰화 프로세스를 살펴봅시다. 일반적으로, 개별 포트폴리오의 지분은 고정금리를 수수하는 소수(~10)의 대규모 기관 투자자와 그리고 보다 높은 위험을 감수하지만 변동금리를 획득하는 몇 명의 후순위 투자자에게 판매됩니다.

- 예를들어,이러한포트폴리오는격주마다(시간간격은다를수있음)최종대부자가 대금을 회수합니다.
- 회수액은 대출금에 대한 이자와 원금으로 구성됩니다.
- 여기서 원금과 관련된 부분은 생략하고 투명성과 간결함을 위해 배당금에 집중하도록 하겠습니다.
- 배당금은 폭포수 프로세스(waterfall process)로 선순위 투자자와 후순위 투자자에게 분배됩니다.
- 먼저, 고정 수입을 보장하기 위해 배당금 총액을 선순위 투자자에게 분배합니다.
- 배당금이 모든 고정 수입을 보전하는데 필요한 액수를 초과하면, 남은 액수는 ***모두*** 후순위 투자자에게 분배되어, 고정 금리 보다 높은 금리를 획득할 기회를 대가로 감수한 위험을 커버할 수 있습니다.

- 만약 이 금액이 선순위 투자자에게 지급될 이자 금액을 충당할 수 없으면 현금준비금이나 다음 회수액에서 지급됩니다. 이 경우, 후순위 투자자는 동 기간에는 이자를 획득할 수 없습니다. 앞서 제시된 프로세스는 단순화하여 구성했지만, 잠재적 토큰화 자산 개시 프로세스를 스마트 컨트랙트가 포트폴리오의 원본 지분을 기장하고 앞서 언급된 폭포수 프로세스에 대응하여 필요한 모든 계산을 할 수 있고, 이러한 포트폴리오의 파생상품(한 측면에서는 이자의 식별 번호가 있고, 다른 쪽은 신용화폐로 표시된 대금과 은행 계좌에 저장된 금액이 있는 암호 화폐와 동액의 배당금)을 도입할 수 있습니다. 다음은 두가지 개별 사건을 자세하게 다룹니다.

스마트에셋 개시

앞의 예시에서 첫번째 단계에서 기존의 스마트 컨트랙트 내에 기장 및 효율적이고 합리적인 비용으로 수행될 수 있는 프로세스를 다루는 스마트 컨트랙트 형식으로 포트폴리오를 생성합니다. 이러한 블록체인의 한계 중 하나는 거래 당 최대 계산량이며, 예를 들어 만약 배당금 계산 프로세스가 위에 설명된 것 보다 더 복잡하다면, 계산은 스마트 컨트랙트에서 효율적으로 수행될 수 없습니다. 이러한 문제점은 zkSNARKs/zkSTARKs 의 형식의 현대 암호 방식이나 해당 부분에서 다뤄질 예정인 크립토이코노믹스 접근법 (cryptoeconomical approach)을 이용하여 해결할 수 있습니다. 지금은

- 어떠한 자산의 스마트 컨트랙트를 생성하는 것이 중요하지 않다는 것과 관련 비즈니스 기능 지원은 비싸거나 가능하지 않다는 것
  -자산 토큰화는 시장과 커뮤니티에서 더 실용적이고 흥미로울 수 있는 파생상품으로 이어진다는
  두가지 사실을 설명하기에 충분합니다.

스마트에셋 파생상품

앞의 대출 포트폴리오 토큰화 예시는 신용 화폐에 일대일로 고정된 암호화폐 자산이라는 굉장히 흥미롭고 실질적인 상품을 탄생시킵니다. 이것은 경제적으로 낮은 변동성과 높은 유동성으로 인해 "스테이블코인(stablecoin)"에 해당합니다. 이러한 자산은 실질적인 적용성을 가질 수 있으며 물리적 세계와 암호화 세계를 잇는 다리인 크립토커뮤니티에게 더 흥미로울 수 있습니다. 모든 파생상품 기장은 블록체인에서 수행될 수 있고, 수행되어야

하며, 물리적 세계의 참여자는 변동 위험을 현저히 감소시킨 결제 방식을 기꺼이 수용하게 될 수 있습니다.
한걸음 더 나아가 이 자산의 전체 방출 가치를 보전하는 신용 화폐로 뒷받침되는 캐시 아웃 절차를 도입하고 실질적으로 거래비용을 거의 제거하여 파생상품에 추가적인 혜택을 가져다줍니다. 첫 부분은 해당 섹션에서 서술될 KYC/AML 절차를 요구합니다. 후자는 플라즈마 프로토콜 구현을 다룹니다.
요약하면, 유동성 높은 자산을 생성하는 것은 거시경제학이나 통화정책의 영역과 같은 기반 경제학과 밀접하게 연계되어 있으며, 이 섹션에서 수행될 수 있는 것과 토큰화 과정이 많은 측면에 혜택을 제공하는 방법에 대해 쉽게 설명하도록 하겠습니다.

공개 인증서 표준

블록체인은 직접적인 실제 세계 가치를 지닌 단체와 함께 운영될 때, KYC/AML 분야의 전통적인 금융 규제 당국과 기관의 모든 요구사항을 발생시킵니다. 실질적으로, 암호 화폐 거래 플랫폼과 같은 기업은 등록된 국가의 법률에 따라 절차를 조정합니다. 일반적으로 이 관습은 정당하며 합리적이라고 생각됩니다. 그러나, 이러한 제한은 전통적 자산과 암호화자산 간 거래에는 이행되어야 하는 반면, 암호 화폐와 자산 거래 자체는 제한되지 않아야 합니다. 최근 개인 정보 유출 사건은

- 개인 정보 처분권은 개인 정보 소유주에게만 귀속되어야 하며
- 개인 정보 접근권은 개인 정보 소유주가 허가한 서비스에 의해 승인되어야 한다는 점을 확인할 필요가 있음을 일깨워 줍니다.
  우리의 야망은 기존의 솔루션을 개선하기 위해 암호 기법과 데이터 구조 분야에서 모범 사례를 찾아내는 것입니다. 다른 프로젝트와 마찬가지로, 인증서 발행은 이미 실제 세계에서 KYC 절차를 착수하도록 허가된 단체에 의해 승인되어야 한다고 생각합니다. 블록체인에서 인증서의 디지털 스냅샷과 이를 저장하는 스마트 컨트랙트가 작동하는 방식에 대한 포맷과 설명을 제공할 예정입니다. 블록체인 기술은 다음과 같은 이유로 적용 가능하며 필수적이라고 생각합니다.
- 무엇보다 권리는 특정인의 의견이 아닌 계산에 의해 승인되어야 합니다.
- 사용자 데이터의 디지털 스냅샷은 변경 불가능한 공개 저장소인 블록체인에 저장되어야 합니다. 이를 통해 검열과 사기를 피할 수 있습니다. 특정 디지털 스냅샷으로 특정인을 위한 서비스 거부는 항상 공개적으로 저항받습니다. 서비스 접근과 개인 정보 관리에 대한 권리는 수학으로 승인되어야 합니다.
- 소유주의 결정에 의해 데이터의 부분적인 공개가 가능하여야 합니다.
- 영지식 증명 덕분에, 모든 사용자의 신원에 대한 지식이 없어도 사용자의 액세스 레벨에 대한 정보 만으로 액세스를 승인할 수 있습니다. 예를 들어, 고객이 충분한 자금이 있는 경우에만 서비스를 제공하고 싶지만 동시에 고객의 계좌에 있는 금액에 대해 물어볼 수 없을 경우 적용가능 합니다.
- 자신의 인증서에 승인되지 않은 접근이 의심되는 경우, 인증서 소유주는 언제든지 어떠한 특정 서비스를 요구하지 않고서도 이를 스스로 취소할 수 있어야 합니다.
- 현대 세계에서 재전송 공격 보호는 필수입니다.
  우리의 솔루션은 소유자가 자신의 데이터를 저장하는 장소, 스스로 데이터를 저장할지 혹은 이를 위임할지 선택할 수 있는 기회를 제공합니다. 일반적으로 개인 정보를 이용하는 사용자 경험은 모든 관련 당사자를 위해 개선될 수 있습니다.
  스마트 컨트랙트가 제시된 KYC 작업 흐름의 중요한 부분이므로, 플라즈마 구현에 이를 통합할 수 있습니다. 송금이나 인출 등 다양한 목적으로 플라즈마 네트워크에서 자금을 인출하여 모블록체인으로 전송하는 KYC 기반 화이트리스트 프로세스가 하나의 예시입니다.

KYC 표준을 구축하는 것이 경제적으로 이익인지 여부는 이 백서의 범위를 벗어납니다. 그럼에도 불구하고, 일반적으로 제시된 시스템과 보다 큰 자산 토큰화 생태계의 필수적인 요소입니다.

플라즈마 프로토콜 구현

플라즈마 프로토콜은 원래 2017 년 8 월 Vitalik Buterin 과 Joseph Poon 이 도입했습니다.
가장 최근의 연구는 해당 웹 페이지 (https://plasma.io (https://plasma.io))에서 찾을 수 있습니다.
플라즈마 프로토콜은 신뢰의 이동을 허용하고 중앙 단체에게 검증가능한 방식으로 블록을 생성할 수 있는 권한을 부여하는데 필요한 요소를 정의하고 아이디어를 도입합니다. 특정 플라즈마 구현 (종종 Minimal Viable 플라즈마, 플라즈마 캐시, 플라즈마, 플라즈마 debit, 플라즈마 XT 등으로 언급됨)을 구축하는데 다양한 방법이 있으며 초 당 10,000 이상의 거래 처리량을 달성할 수 있다는 점은 명백합니다. 거래당 비용을 1 센트 이하로 하락시키는 엄청난 거래 속도와 중앙집중화 정도는 가치(대체 가능한 자산 이전) 및 자산(대체 불가능한 자산 이전) 크립토커뮤니티의 필요성을 완전히 배제합니다. 스마트 컨트랙트가 현 수준에서 플라즈마 내 실현가능하지 않지만 검증가능한 특성은 스마트 컨트랙트 기능에 대한 흥미로운 추측을 허용하지 않음을 이해하여야 합니다.

더 자세한 설명을 위해 플라즈마 프로토콜의 두가지 초석을 언급하고자 합니다.

- 검증가능성: 블록을 생성할 권한이 없는 외부 관찰자는 무효한 블록 생산에 대해 중앙 운영자를 처벌할 수 있어야 합니다. 운영자가 이중 지출을 허용한다면 외부 관찰자는 필요한 증거를 제공하여 운영자를 처벌할 수 있어야 합니다. 이러한 목적으로 분쟁을 자동적으로 해결하기 위한 스마트 컨트랙트가 존재하며 운영자는 특정 형태의 보증금을 요구합니다.
- 활성화: 의심스러운 행동을 감시하기 위해 체인을 항상 모니터링하는 자가 있습니다. 전체 체인을 모니터링하는 외부 관찰자 일 수도(초 당 10,000 트랜잭션을 잊지마세요), 자신의 트랜잭션과 체인의 불특정 일부를 모니터링 하는 소규모 사용자일 수 있습니다.
  요약하자면, 프로토콜 수준의 정확성 외에도 특정 구현은 대형 참가자와 개별 사용자들을 체인 모니터링에 참여시키는 인센티브 매커니즘을 제공하여야 합니다. 이러한 매커니즘에 대한 토론은 이 백서의 범위를 넘어서지만, 가장 쉬운 것은 플라즈마와 스마트 컨트랙트가 위치하는 모 블록체인간 트랜잭션에 대한 유동성 공급 매커니즘입니다.
  플라즈마 프로토콜 구현은 토큰화 자산 거래에 대한 경제적으로 효율적인 매커니즘을 제공하며, 더 중요한 사실은 파생 상품의 양도입니다. 우리의 제안은, 특정 플라즈마 구현은 거래 비용을 낮춰줄 뿐만 아니라 다음 섹션에서 설명할 매커니즘 또한 제공합니다.

탈중앙 거래소 (DEX, Decentralized exchange)

플라즈마의 분명한 적용은 효율적은 거래소를 설립하는 것입니다. 플라즈마 프로토콜을 사용한 탈중앙 거래소 구현은 최소한 초기 단계에서는 교환 거래를 요구합니다. 블록체인 상의 모든 거래는 소유주의 서명(거래에 대한 명시적인 동의)를 요구하며 동시에 해당 거래가 올바른지 여부(올바르지 않은 경우 운영자를 처벌하기 위함)를 확인할 수 있는 간단하고 효율적인 증명이 존재하여야 합니다. 불행하게도, 기존의 거래소가 사용했던 매칭 매커니즘에 적합한 효율적인 증명을 제공하기

란 쉬운 일이 아니였고 사용자는 해당 거래의 수량과 가격에 명시적으로 동의를 하여야 했습니다. 그럼에도 불구하고, 탈중앙 거래소들은 이미 이더리움 네트워크에서 이러한 매커니즘을 사용하였고 거래 당 가격 인하는 탈중앙화 솔루션으로 더 많은 사용자들을 끌어들였습니다.

감시 스마트 컨트랙트와의 결합

모든 플라즈마 구현은 정확성과 자동적인 분쟁 해결을 보장하기 위하여 복잡한 스마트 컨트랙트를 요구합니다. 특정 사용자 집단만 특정 자산 거래에 접근할 수 있도록 제한하는

것과 유사하게 이 스마트 컨트랙트에 추가적인 제한을 부과할 수 있습니다. 이러한 매커니즘의 필요성에 대해서는 아래에서 논의할 것이며, 우선 이 매커니즘이 실행되는 방식에 대한 예시를 제시하고자 합니다.

- 플라즈마 체인을 모니터링하는 관찰자가 있습니다.
- 모든 이더리움 주소(설명을 덧붙이자면 이더리움 네트워크를 플라즈마 구현을 위한 모 체인으로 사용합니다) 그리고 해당 권한에 대한 액세스 레지스트리를 보유한 스마트 컨트랙트가 있습니다. 이는 자발적 KYC 형식으로 볼 수 있습니다.
- 중앙집중 플라즈마 운영자가 당시에 필요한 권한이 없는 사용자로부터 제한된 자산에 거래를 추가하면, 관찰자는 이러한 사실을 증명할 트랜잭션을 전송하고 스마트 컨트랙트는 자동적으로 운영자의 보증금에서 삭감하고 플라즈마 체인을 중단할 가능성이 있습니다.
  플라즈마 구현에 대한 철학은 사용자의 자유의지와 완벽한 자유에 기반하고 있습니다. 물리적 세계에 등가물이 없으며 쉽게 현금화 할 수 없는 (KYC/AML 형식의 절차 없이) 모든 자산은 제한없이 플라즈마에서 양도되어야 하며, 따라서 크립토커뮤니티의 사용자들이 낮은 수수료로 자유롭게 거래할 수 있어야 합니다. 한편으로는, 신용화폐로 쉽게 전환할 수 있는 모든 자산은 자발적으로 KYC 절차를 거친 사용자들 만이 거래할 수 있어야 합니다. 이 요구사항은 규제로 보일 수 있지만, 우리는 자금 세탁과 불법 거래를 방지하기 위한 도덕적 해결책이라고 생각합니다.
  이 규제의 명백한 혜택은 대형 기관 참여자와 규제 당국의 이목을 끌 수 있다는 점입니다. 이러한 단체 모두 완전한 체인 관찰자가 될 수 있으며 다른 사용자를 위해 정확성과 체인 유효성 및 활성화 상태를 보장할 수 있습니다. 동시에 완전히 고정된 토큰화 파생 상품이 시장에 등장하고 높은 유동성을 자랑하여 일상생활에서 결제 수단으로 사용될 수 있다면, 물리적 세계와의 차이를 메울 수 있을 것입니다.

플라즈마 구현의 개선

앞에서 플라즈마 프로토콜 구현을 구축하는 다양한 방법과 사용자에게 접근성이 높은 기능에 대해 설명했습니다. 여기서는 두가지, 장기 및 단기 개발 계획에 대해 설명하고자 합니다.

- 단기적으로, 플라즈마에 "비밀 거래"를 실행할 수 있습니다. 이 기능은 사용자가 정확한 거래 금액을 감출 수 있지만, 여전히 가치가 없는 것이 아님을 증명함으로써 거래의 정확성을 증명해야하는 프로토콜 구현입니다. 다양한 특이 구현은 이러한 기능을 위해 존재하며, 예를 들어 Monero, zCash 블록체인이 있습니다. 우리의 구현은 Greg

Maxwell 의 오리지널 "비밀 거래" 프로토콜에 기반을 둡니다. 이러한 기능은 거래 비용이 매우 높음에도 불구하고 (한 거래 당 수 백만 가스가 필요합니다. 정상적인 거래는 21,000 가스가 필요합니다) 이미 이더리움 네트워크에 실현되었을 수 있습니다.

- 장기적으로, 블록의 완벽한 유효성을 증명하고 사용자의 체인 모니터링 부담을 줄이기 위해 zkSNARKs/zkSTARKs 와 같이 현대 암호학적 진보의 결과물을 사용하려고 시도할 수 있습니다. 비록, 이는 상당히 실험적이고 궁극적인 목표를 달성하기 위해 더 많은 연구가 필요합니다. zkSNARKs/zkSTARKs 에 대한 간략한 설명은 해당 섹션에서 찾을 수 있습니다.

크립토이코노믹스(Cryptoeconomics)

이 섹션에서, 크립토이코노믹스가 무엇인지, 그리고 사고 모델에서 특정 패러다임 변화를 어떻게 필요로 하는지 설명합니다.
스마트 컨트랙트가 블록체인(대부분 주요 이더리움 네트워크를 의미)에 구현되었을 때, 전통적인 거래 로직을 이 컨트랙트로 이전하고자 하는 다양한 시도가 있었습니다. 가장 좋은 예는 임의로 표시된 대체 가능한 자산에 대해 원장을 정의하는 ERC20 토큰 표준입니다. 불행하게도, 계산 비용이 높을 수 있거나 너무 높을 수 있는(거래 당 최대 가능 한도 이상) 거래가 존재합니다. 이 절차를 블록체인에 구현하기 위해 모든 사용자가 효율적인 공간에서 낮은 계산 비용으로 입력과 출력 데이터 관계의 정확성을 검증할 수 있고 검증가능한 (그리고 효율적으로 검증가능한) 계산 구현으로 전환할 수 있거나 크립토이코노믹스 절차를 도입할 수 있습니다.
크립토이코노믹스 절차 사용자들은 입력 및 출력 데이터의 정확성을 입증할 필요가 없으며, 단지 데이터가 정확함을 진술하고 상호적이거나 비상호적인 도전 절차에 대한 시간 제한과 담보를 제공하기만 하면 됩니다. 크립토이코노믹스 패러다임이 생태계의 모든 사용자에게 혜택을 제공하는 것은 분명하지만 모든 절차가 이 패러다임으로 변화할 수 없다는 것을 이해해야 합니다. 다음은 간단한 예시입니다.

- 앨리스는입력데이터I와출력데이터O를기반으로밥과거래를하려고합니다.
- 출력데이터O는입력데이터I에올바른값이라는것을결정적으로증명할수있는 상호적이거나 비상호적인 절차가 존재합니다.
- 앨리스는로컬에서(가정용PC나모바일기기를사용하여)I에서O를계산하고다음을 명시하는 스마트 컨트랙트에 트랜잭션을 전송합니다.
- 앨리스는 입력 데이터 I 에 대한 계산을 기본으로 합니다. - 앨리스는 출력 데이터 O 를 계산합니다.
- 앨리스는 O 가 I 에 대해 유효한 출력 데이터라고 ***진술합니다***. - 앨리스는 담보 X 를 사용하여 자신의 진술을 지지하고자 합니다.
- X 의 값은 위에 언급된 절차를 제공하는 비용보다 높습니다.
- X 는 즉시 컨트랙트에 이전되고 Y 시간 후 앨리스의 소유가 됩니다.

- Y시간동안,모든관찰자(밥)은O는I에대해유효한출력데이터라고입증할수있으며 만약 불일치를 발견하게 되면 앨리스와 분쟁 절차로 들어가게 되고, 만약 불일치가 밥이 담보 X 를 가져야 한다고 증명되면 앨리스의 트랜잭션은 무효로 간주됩니다.
  크립토이코노믹스의 효과성을 보장하기 위해 네트워크의 높은 "활성화"가 요구되어 가능한 많은 사용자들이 가능한 많은 트랜잭션을 모니터링하여 분쟁을 시작할 수 있도록 하여야 합니다.
  여기서 Matter 토큰이 등장합니다. Matter 토큰이 담보로 사용되면, 추가 제한을 도입할 수 있습니다.

- 사용자 밥이 성공적으로 앨리스의 트랜잭션에 대해 반박하면 그는 해당 담보를 수령합니다.

- *Matter*는 누구도 네트워크를 감시하지 않더라도 무효한 트랜잭션에 대해 이의를 제기할 책임이 있습니다.

- 허용된 시간 내 앨리스의 트랜잭션에 대해 어떠한 이의를 제기하지 않았고 이후 앨리스의 트랜잭션이 여전이 무효한 것으로 증명되었을 때, 이 사실을 입증한 자는 예외적인 상황이므로 *Matter*의 보증금에서 삭감합니다.
  추가적인 부담을 감수하고 경제 매커니즘으로 네트워크를 활성화합니다. "우리가 놓친 트랜잭션을 우리가 직접 입증한다"는 형식의 부정을 예방하고 보증금을 다시 회수하기 위해 절반만이 입증한 자에게 지급되며 나머지 절반은 소멸됩니다.

Matter Inc. 토큰의 직접적인 적용

특정 절차에 대해 다음과 같이 토큰 적용을 제안하지만, 우리 생태계에 있는 모든 제품에 대한 차별적인 접근에 대해 강경한 입장을 취하고 있습니다.

- 플라즈마송금및이전시수수료결제수단으로토큰을사용합니다.만약변동성이큰 다수의 자산이 플라즈마 구현에 포함되어 있다면, 양도된 자산(예를 들면, ERC20 토큰)의 기본 금액에서 지불해야할 수수료를 제공하는 정교한 모니터링 시스템을 구현하거나 수수료 징수를 위해 우리 토큰을 사용해야 합니다.

- KYC 인증서 발행은 하나의 (혹은 하나 이상의) 사법권의 제공자와 교류해야 하고 절차에 대한 결제는 다양한 방법으로 이루어 집니다.

- 몇 파생상품에 대해 캐시 아웃 절차가 시작죄면, 특정 수수료는 *Matter Inc.* 토큰이나 자산의 표시 단위로 지급하여야 합니다.

zkSNARKs/zkSTARKs 에 대한 개요

zkSNARKs 와 익명 거래 목적의 zCash 블록체인을 통한 실질 사용사례에 대해 익숙할 수 있습니다. 이는 *영지식 간결한 비대화식 지식 논증(zero-knowledge succinct non-interactive argument of knowledge)*의 앞글자를 딴 것이지만, 다음과 같이 대화형식(앨리스와 밥이 재등장 합니다)으로 설명해보려고 합니다.

- 앨리스는 자신이 정확하게 계산을 수행하였음을 증명하려고 합니다.
- 앨리스는 높은 확률(천문학적으로 1 에 가까움)로 밥을 설득하려고 합니다.
- 앨리스가수행한계산금액은상당히클수있으며,그녀는계산프로세스와관련된모든 결과 중 소액만을 제공합니다(전체 집합은 일반적으로 "증인"으로 불리며, 앨리스는 "공개" 매개 변수만을 공개합니다).
- 앨리스와 밥은 계산의 특성에 대해 동의합니다. (마지막 사인까지!)
- 목표를 달성하기 위해 앨리스는 zkSNARK 프로토콜에 기반한 증명을 준비하고 제공합니다.
- 보너스로,밥은앨리스의중간계산결과에대해어떤정보도얻을수없습니다.우리의 목적과는 상관이 없으나 어떤 경우에는 편리할 수 있습니다.
- 앨리스의 증거 크기는 항상 일정하고 미리 공개되어 있으며 검증 비용은 항상 일정하고 미리 공개되어 있습니다.
  zkSNARKs의 활용도는 동일한 크기의 증거와 일정한 검증 비용에 대해 언급한 마지막 문장으로 인해 효율적입니다. 이러한 절차는 트랜잭션 동안 단순히 입력 데이터I에 대한 출력값O를 계산하는 것 보다 높은 증명 준비 비용으로 복잡한 계산 시 크립토이코노믹 접근법 대신 사용될 수 있습니다. 트랜잭션 동안 크립토이코노믹스와 혼합되어 해당 증명은 확인될 뿐만 아니라 추가적인 분쟁 해결 목적으로 기록됩니다!

결론

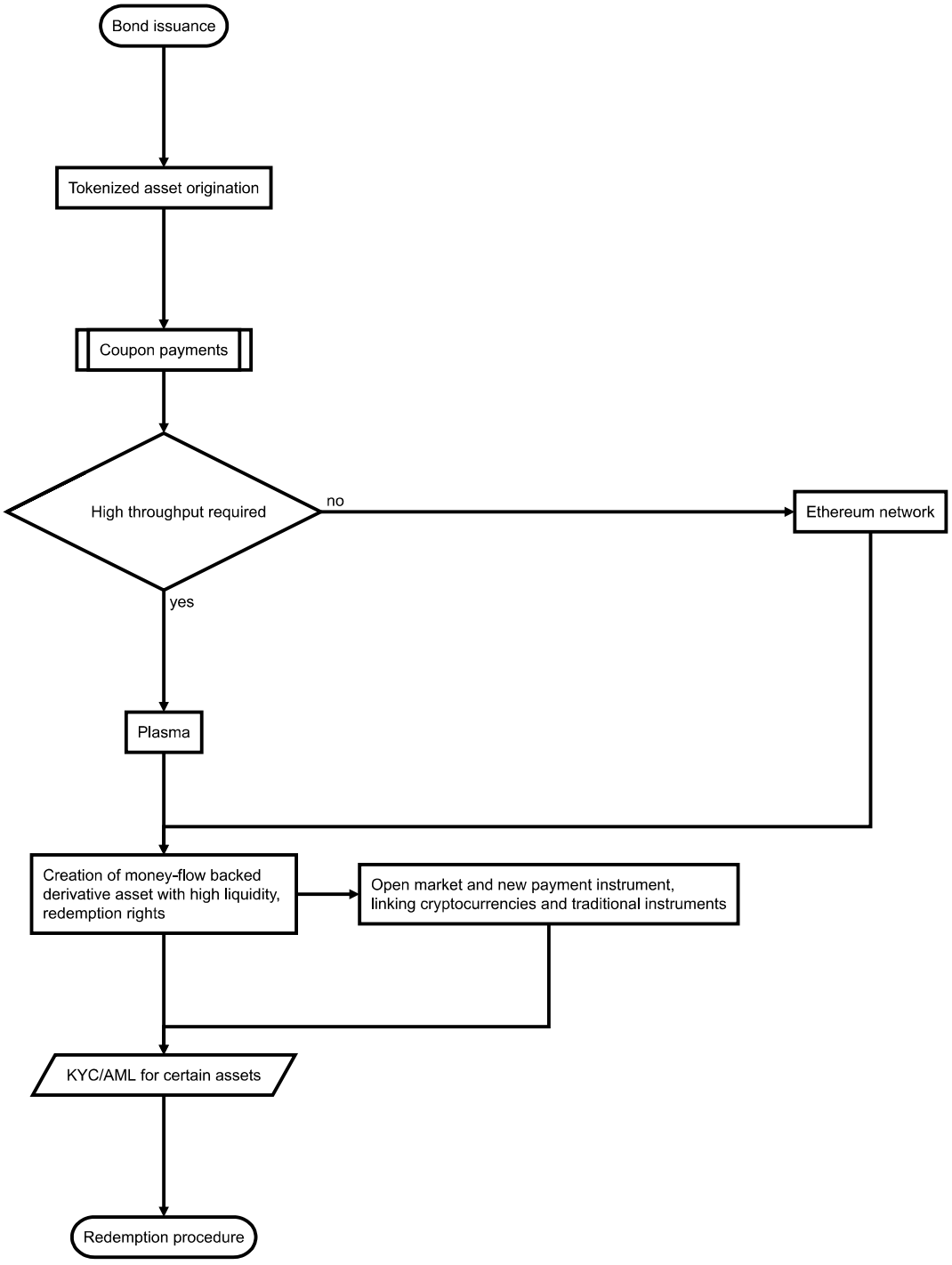
장황한 결론이나 "우리 토큰을 구매하세요"라는 말 대신 우리의 목표를 설명하고자 합니다.

*Matter*는 주로 엔지니어로 팀이 구성되어 있으며 우리는 시스템(크립토이코노믹스 역시 마찬가지로)은 일관성이 있고, 가격면에서 합리적이며, 실용적이고 뛰어난 UX 를 보유하고 있어야 한다고 생각합니다. 많은 기업들은 자산 토큰화 혹은 빠른 블록체인 구현에 몰두하지만, 우리는 더 겸손하게 시스템을 구축하려고 하는데 이 시스템은 막대한 처리량을 가진 플라즈마가 이 능력을 사용할 수많은 트랜잭션으로 채워질 수 있으며 우리는 우선 어떤 분류의 자산을 토큰화할 것입니다. 이 분류는 토큰화 프로세스에 모범 사례와 신뢰를 가져오며 투명한 가격 책정, 높은 유동성과 적절한 캐시 아웃 매커니즘의 작동하는 실제 세계와 분명히 연계되어 있는 "스테이블코인"의 새로운 시대를 열 것으로 기대합니다. 이를 통해 이 간결한(300 페이지 아님) 백서에 우리의 아이디어를 설명하고, 가능한 간결하고 쉽게 설명하려고 하였으며 실용적인 측면에서 플라즈마 구현과 포트폴리오 토큰화 파일럿에 대한 경험을 제공하였기를 바랍니다(그렇지 않으면 당신에게 빠르게 설명할 수 없습니다).

Alex Vlasov, Artem Vorobev

Appendix

Example of proposed bond tokenization flow chart



Matter Inc. Plasma implementation structure