IOTA ($MIOTA) 분석 보고서

Myles Snider, Kyle Samani, and Tushar Jain

2018년 1월 23일

고지사항: 멀티코인 캐피탈은 IOTA에 대한 매수 혹은 매도 포지션을 가지고 있지 않습니다.

서문

IOTA는 사물인터넷(IoT)의 중추적 역할을 목표로 하는 디지털 화폐 프로젝트이다. 그리고 IOTA 자체적으로는 "포스트 블록체인" 아키텍처를 가지고 있다고 자부하는 프로젝트이기도 하다. 물론 IOTA가 기타 블록체인 프로젝트와 많은 부분에서 공통점을 공유하지만, 실제로 IOTA는 블록이나 단일 체인과 같은 개념을 포함하지 않고 설계되었다. 그 대신, IOTA는 방향성 비순환 그래프(DAG)라 불리는 개념을 중심에 두고 있다. IOTA는 블록체인은 아니지만, DAG를 사용함으로써 비허가성 공개 분산장부라는 사실은 변함이 없다. 이 구조적 특수성이 IOTA에게 현존하는 블록체인과 비교 시 여러 장점을 갖게 하기도 한다.

요약

배경

2014년 처음 개념화되기 시작한 IOTA는 2015년에 David Sønstebø, Sergey Ivancheglo, Dominik Schiener 그리고 Serguei Popov 박사에 의해 설립되었다. 이 프로젝트의 설립자 중 몇몇은 IoT 하드웨어 스타트업에서 근무한 경력이 있다. 그들은 당시 IoT를 위한 결제 옵션의 한계가 있음을 인지하였고, 이러한 문제점들에 대한 해결책으로 IOTA를 세상에 내놓게 되었다.

IOTA의 개발진은 2015년 당시 초도 물량인 2,779,530,283,277,761 IOTA에 대한 토큰 판매를 진행하였고, 이를 통해 1,337 BTC (당시 기준 584,000달러어치) 규모의 자금을 조달하였다. IOTA 공급량은 채굴보상이나 인플레이션이 존재하지 않기 때문에 고정되어 있다. 현재 이 프로젝트는 계속해서 개발이 이루어지고 있고, 베를린에 위치한 비영리 재단인 IOTA 재단에 의해 경영되고 있다.

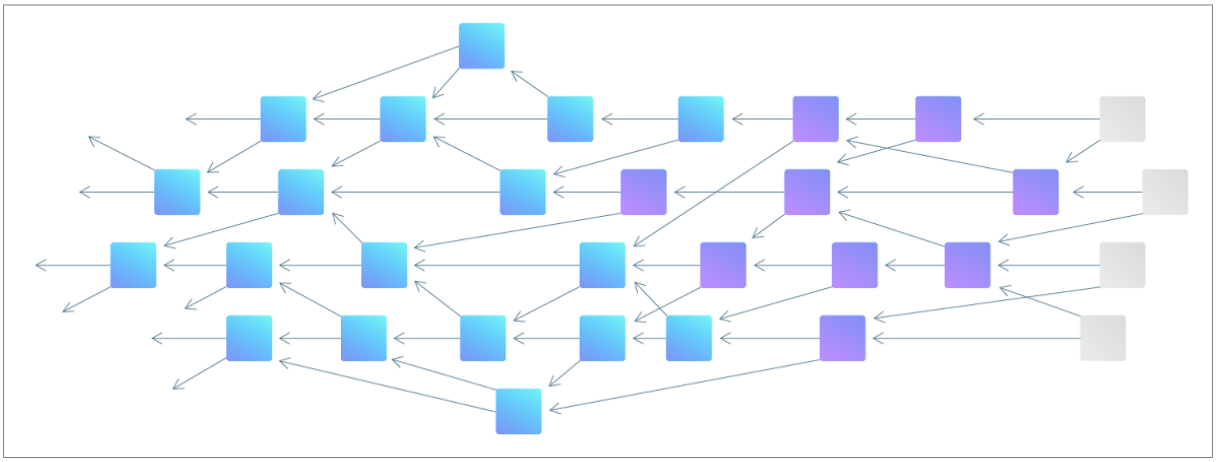
특징

탱글

IOTA가 차용하는 방향성 비사이클 그래프(DAG)를 탱글이라 하며, 자세한 내용은 이하와 같다:

- 탱글 내에서 "그래프"란 상호 연결된 노드들의 네트워크이며, IOTA 내 노드들 간 연결은 각자의 거래를 참조하면서 이루어진다. 그리고 이러한 연결을 "엣지"라 칭한다.
- "비사이클 그래프"란 순환되지 않는 것을 뜻한다. 엣지를 따라 노드 간 이동을 하더라도, 이전에 접촉한 노드로 절대 돌아오지 않는 것이다. 각가의 엣지는 이전의 노드에서 다음 노드로 이동한다.
- 마지막으로 "방향성"은 노드 간 연결이 움직이는 방향이 일방향임을 뜻한다.

이러한 세 가지 속성의 조합은 네트워크가 자체적으로 노드의 구조를 짜고, 이 구조 속에서 관계가 수렴함을 의미한다. 이러한 속성들은 수학적으로 증명될 수 있다. 그리고, 이 속성들을 통해 네트워크가 채굴자나 블록 혹은 단일체인 없이도 거래 순서에 대한 구조화와 이중지불 방지를 가능케 해준다.



탱글 시각화

IOTA 내에서 노드와 채굴자는 별개의 주체가 아니다. 오히려 거래를 발생시키는 모든 노드는 작업 증명을 통해 해당 거래 이전 두 개의 거래를 컨펌해야만 한다. 결국 사용자와 채굴자가 하나라는 뜻이다. 사용자는 그래프에서의 노드이며, 이전 거래들에 대한 증명이 엣지를 형성한다. IOTA 내 거래는 사용자에게 거래 수수료를 요구하지 않으며, 작업증명은 시빌 공격(Sybil attack)에 대항하는 하나의 메커니즘으로서 자리 잡아 기타 시스템 내의 수수료 역할을 대신 한다.

네트워크 내에서 채굴자와 사용자를 분리하는 것은 위험성을 수반한다. 채굴자들이 경제적 유인을 이유로 사용자들을 검열하거나 선행매매와 같은 행위를 하여 불이익을 가할 수 있기 때문이다. IOTA는 이러한 잠재적 문제점을 제거하기 위해 검증해야하는 거래의 부분 집합을 임의로 선정하고 모든 사용자가 검증인의 역할을 수행하게 한다. 다른 사용자들이 검증을 빠르게 수행하기 대문에 검열 행위나 선행매매가 불가능해진다.

IOTA의 작동방식은 다음과 같다: 사용자가 신규 거래를 생성하고자 하는 경우, 우선 프라이빗 키를 사용하여 거래 인풋값에 서명을 해야한다. 다음 단계로 사용자의 지갑은 Markov Chain Monte Carlo (MCMC) 선택 알고리즘을 사용하여 검증해야 하는 두 개의 "팁"(탱글 내 검증이 미진행된 거래)을 선정한다. 탱글 내 모든 노드가 항상 같은 상태를 공유하는 것은 아니기 때문에, 두 개의 상이한 거래가 하나의 팁을 검증할 수도 있다. MCMC는 프로토콜 단에서 수행되진 않지만, IOTA 팀은 이기적인 팁 선택이 일어나더라도 탱글 내의 균형이 생긴다는 연구결과를 발표했다. 새롭게 생성된 거래가 탱글 내에 반영되기 위해서는 사용자가 작은 규모의 작업증명을 통해 임의로 선택된 두 개의 팁에 대한 검증을 해야한다. 이러한 검증이 이뤄진 후, 사용자의 신규 거래는 탱글에 팁으로 추가가 되며, 기타 거래를 통한 컨펌을 기다리게 된다. 이러한 과정은 무한히 반복된다.

비트코인과 마찬가지로 IOTA 거래는 시간이 흐름에 따라 표준 장부에 포함될 가능성을 갖게 된다. 비트코인 네트워크에서는 대체로 6개로 여겨지는 특정 수의 블록 컨펌을 기다리지만, IOTA에서는 다른 방식을 거치게 된다. 사용자는 MCMC 알고리즘을 통해 자신의 거래의 컨펌 레벨을 정할 수 있다. 만약 알고리즘이 N번 행해질 경우, 거래는 M번 확인되어야 한다는 식이다. N분의 M은 임의로 선정된 팁이 사용자의 거래와 바로 이어져 있을 가능성을 뜻하고, 이는 결국 거래가 전체 네트워크에서 검증받을 확률을 의미한다. IOTA를 지불수단으로 수용하는 주체들은 이를 이용하여 거래가 최종이길 바라는 수준으로 확률을 조정할 수 있다. 네트워크가 커짐에 따라 최종 승인을 받는 데에 걸리는 시간은 점점 더 짧아질 것이다. 왜냐하면 네트워크가 커지면 그만큼 많은 거래들이 생겨나고 그 거래들이 이전의 거래들을 검증하는 수도 증가하기 때문이다. 현재 IOTA 네트워크 내에서는 거래에 대한 컨펌은 수 분 내에 이루어지고 있다.

제로 거래 수수료

본 보고서에서 언급했던 바처럼, IOTA 거래는 수수료를 청구하지 않는다. 물론 거래를 생성하기 위해서 진행하는 작업증명과 이에 수반되는 필요조건이 수수료처럼 보일 수는 있지만, 그 둘 간의 차이를 이해하는 것은 매우 중요하다. IOTA의 주요 목적은 소액결제를 위한 솔루션이기에 거래수수료를 제거하는 것은 IOTA의 핵심이다. 거래수수료는 소액결제를 불가능하게 만들기 때문이다. 많은 이들이 초기 비트코인에 대해 인터넷에 걸맞는 소액결제 솔루션이라 환호하였지만, 예측불가하며 높은 수수료로 인해 오늘날의 비트코인은 소액결제와는 거리가 멀어졌다. 지속적으로 낮은 수수료 혹은 예측가능한 수수료를 구조 안에 녹이는 대신, IOTA는 거래수수료를 없애버렸다. IOTA를 통해 기계 간 1센트 미만의 여러 건의 결제가 수수료없이 가능해진다. 예를 들어, 1 IOTA를 보내면 상대방은 정확하게 1 IOTA를 받게된다.

확장성

이론상 IOTA 고유의 설계는 IOTA 네트워크가 커질수록 확장 역시 가능하다. 거래가 병렬처리가 가능하고, 각 거래가 이전의 두 개의 거래를 검증하기 때문에 더 많은 사용자가 네트워크에 참가할수록 검증에 소요되는 시간은 줄어든다. IOTA 내에는 블록이라는 개념이 없기 때문에 블록 사이즈가 몇 개의 거래를 담을 수 있는지에 따라 제한을 받지 않기 때문이다. 그러나, 이러한 아키텍처의 확장성은 네트워크 내에 충분한 숫자의 풀 노드를 확보했을 때만 가능하다는 점을 유의해야 한다.

탈중앙화

블록체인과 달리 IOTA 내에는 채굴자 혹은 검증인이라는 개념이 사용자와 별도로 존재하지 않는다. 대신, 각각의 사용자들 모두가 거래를 보낼 때마다 검증인의 역할을 해야한다. 이는 IOTA가 몇 가지 문제점을 해결하기 위해 의도한 것이다. 우선, 사용자와 검증인 사이에 인센티브 차이가 존재하지 않는다는 점이다. 결국 사용자가 검증자이기 때문이다. 사용자가 거래를 보낼 때마다 다른 이들의 거래를 검증해야 한다는 특성과 블록 보상이나 거래 수수료가 없다는 점이 결합되어 검증인 간 경쟁이 불필요해지는 것이다.

탈중앙화의 척도가 "거래의 검증을 몇 개의 주체가 통제하는가"임에 비춰볼 때, 이론상으로는 규모가 커진 IOTA라면 그 어느 블록체인보다도 탈중앙화될 수 있다. 왜냐하면 블록체인의 경우 규모의 경제에 따라 블록 생성이 중앙화되기 대문이다. 하지만, IOTA에 존재하는 한 가지 문제점은 수수료와 블록 보상이 없기 때문에 사용자가 풀노드를 운영할 유인이 없다는 것이다. 대부분의 지갑이 라이트 클라리언트이며 IOTA IRI를 운영하는 풀노드에 연결되어 있고, 이 IOTA IRI가 라이트 클라이언트 사용자들의 MCMC 알고리즘을 수행한다. 이전의 IOTA 네트워크 내에 존재하는 문제들이 부족한 풀노드 숫자에 기인한다는 점을 주목해야 한다. 왜냐하면 더 많은 IoT 기기들이 IOTA 네트워크에 참가하게 된다면 이 문제가 더 심각해질 수 있기 때문이다. IoT 기기들 대부분 기기 자체가 너무 작아 풀노드로서 기능하기 어려울 뿐 아니라 작업증명마저도 힘들 수 있기 때문이다.

악의를 품은 이가 절대 다수의 검증력을 통제하여 시빌 공격을 감행하고 이중지불 공격을 감행할 유인이 충분하다는 점도 존재한다. IOTA가 이러한 공격들에 특히 취약한 이유는 현재 네트워크 규모가 작기 때문이다. 충분한 규모로 네트워크가 커지기 전까지는 이러한 공격을 무효화하는 것이 어렵다. 이로 인해, 현재 IOTA 네트워크는 재단 자체적으로 운영하는 중앙화된 클로즈드 소스 "코디네이터"(Coo)에 의존할 수 밖에 없다. 코디네이터의 구조와 이에 대한 분석은 추후 내용에서 다루도록 한다.

퀀텀 저항성

IOTA의 기능 중 하나는 미래를 대비한 퀀텀 저항성을 가진 해시 기반 서명을 통합했다는 것이다. 이는 블록체인 쪽에서 주로 사용되는 타원 곡선 암호학 대신에 사용되는 것으로, Winternitz 서명이라고 불리운다. 하지만, 이는 IOTA만의 특징이라 할

수는 없다. 왜냐하면 이더리움과 카르다노(Cardano) 커뮤니티 역시 자신들의 프로토콜이 퀀텀 컴퓨팅에 대비한 암호화를 탑재할 수 있는 방향으로 나아가고 있기 때문이다.

사용 사례

IOTA는 IoT 시대에 걸맞는 금융 시스템의 주춧돌이 되고자 하며, 이와 더불어 암호화된 메세징과 데이터 마켓플레이스 등의 기능까지도 통합하였다. 이러한 특징들은 모두 IOTA가 그리는 IoT 시대의 미래 경제를 이루는 요소들이다. 바로 수백만 개의 기계들이 상호간 데이터를 주고받고, 실시간으로 결제를 처리하는 모습이다. 이는 전기차와 전기차 충전소의 충전기 간 결제 시스템부터 전세계에 퍼져있는 센서들이 기후 패턴을 예측하려는 과학자들에게 데이터를 파는 것까지 다양한 기계들에 의해 움직이는 경제라 할 수 있다.

IOTA의 주요 특징 중 사물인터넷과 잘 맞아떨어지는 부분은 결제수수료가 없다는 점이다. 이론상으로는 결제수수료가 없는 이러한 시스템을 활용하는 사례가 많을 거 같지만, **IOTA는 아직까지 프로덕트 마켓 핏(PMF)을 찾지 못하였다.** 그래서 IOTA의 "실사용 사례" 관련 문서들 역시 찾기 어려울 뿐 아니라 내용 역시 구체적이지 않다. 이에 대해 IOTA 측은 "중점을 두는 분야는 당연히 사물인터넷이며, 스마트 시티, 인프라와 스마트 그리드, 공급사슬, 모빌리티와 교통/수송 분야이다"라고 밝히고 있지만, 아직 위와 같은 분야에서 실시간 결제가 필요한 지 여부는 불분명하다. 왜냐하면 아직까지 주로 선결제를 하거나 주기적으로 금액이 축적된 후에 결제하는 후불 방법이 사용되고 있기 때문이다.

거래 당사자들이 만약 서로를 신뢰하지 않는다면 선불 혹은 후불을 원하지 않는 경우도 있을 수 있다. 이런 경우, 건당 결제를 채택하면 어느 당사자나 많은 금전적 손해 없이 손쉽게 거래를 중단할 수 있다는 장점을 가진다. 그러나 소규모 거래 중 건당 결제로 처리해야 하는 시장의 크기는 현재 미미하며 사용자들이 결제 체계에 대한 전환 비용을 감당하면서까지 건당 결제로 바꿔야 할 유인 역시 적다.

물론 인터넷에 연결된 센서들이 늘어나서 데이터 판매가 더 많아지거나 메시 네트워크와 결합된 소액결제와 같은 신규 비지니스 모델들이 사람들의 관심을 더 받기 시작하면 시장의 크기는 바뀔 수 있을 것이다. 그러나 만약 그러한 미래가 도래하더라도 IOTA는 여전히 블록체인 레이어-2 솔루션들인 라이트닝 네트워크과 Raiden, 그리고 확률론적 소액결제 체계들, 그 외에도 제로 수수료 블록체인인 EOS와 같은 프로토콜과의 경쟁을 계속 해야한다.

도전과제

물론 IOTA와 같은 DAG 유형 장부의 근간을 이루는 핵심 수학 논리가 타당해보이는 것은 사실이지만, IOTA 측이 내건 약속들은 기술적으로 굉장히 어려운 문제들이 해결된 미래가 도래해야만 지켜질 수 있다. 대부분의 암호화폐 관련 프로젝트들 역시 실험적인 성격을 띠지만, IOTA의 현재 진척도와 기능들이 큰 차이점이라 할 수 있다.

지나치게 중앙화된 코디네이터

IOTA는 현재 재단에서 운영하는 중앙화된 코디네이터(Coo)의 사용에 의존하고 있고, 재단 내 멤버들의 다중서명을 통해 코디네이터를 관리하고 있다. 이러한 코디네이터의 코드는 오픈소스가 아니다. 이러한 코디네이터는 네트워크가 충분히 커져서 계산상 공격이 불가능하다고 판단된 이후 제거될 것이기 때문에 IOTA 네트워크의 "보조바퀴"라고도 불린다.

Coo는 거래가 매 분마다 가능토록 해주는 노드이다. 이러한 거래들은 "마일스톤"이라고 불리며, 네트워크 내에서 다른 노드들이

유효한 참고 포인트로 사용할 수 있는 기능을 지닌다. 즉, 이러한 마일스톤들은 네트워크의 상태에 대한 스냅샷을 제공하여 유효성 여부를 신뢰할 수 있게 해준다. 어떤 거래가 Coo 거래에 의해 직접적으로 혹은 간접적으로 이어진다면 그 거래는 유효하다는 뜻이다. 물론 이러한 코디네이터가 만능이여서 IOTA를 무에서 창조해낸다거나 한다는 뜻은 아니며, 오히려 네트워크 차원에서 보면 단일 실패점이다. **뿐만 아니라, 거래가 유효하다는 판단을 받기 위해서는 Coo의 검증을 거쳐야 한다는 점은 현재 IOTA가 검열저항성을 가진 네트워크라고 부르거나 탈중앙화된 네트워크라고 부르기에는 무리가 있다는 뜻이기도 하다.**

Coo가 존재하는 이유는 네트워크가 공격을 방지할 수 있을만큼 크지 않기 때문이다. 악의를 가진 주체가 네트워크 전체의 34%에 대한 통제권을 가지는 것이 상대적으로 쉽고, 이러한 통제권을 갖게 된다면 유효하지 않은 거래들을 만들어 낼 수 있기 때문이다. 만약 이러한 사태가 벌어지게 된다면, 공격을 감행하는 주체는 일정 시간 동안 네트워크 전체 거래의 3분의 1에 육박하는 거래를 생성해내고 이를 소위 검증해버리면 된다. IOTA 내에는 거래수수료가 없기 때문에, 네트워크를 공격하는데 드는 비용은 충분한 연산력을 위한 컴퓨터 관련 비용 밖에 없다.

Coo와 관련된 추가적으로 심각한 문제점은 IOTA 팀이 언제 코디네이터를 작동 중지할 지에 대해서 뚜렷한 지침을 보여준 적이 없다는 것이다. 또, 네트워크가 얼마나 커져야 코디네이터 없이 자체적으로도 작동가능한지에 대해서도 다룬 바가 없다. IOTA 측에서 잠정적으로 2017년도 여름 코디네이터를 작동 중지하겠다고 밝힌 바 있지만, 현재도 Coo는 운영되고 있다.

Coo의 기능에 대한 구체적인 정보를 IOTA 공식 문서에서는 찾기 어렵다. 개발진은 레딧, 슬렉(Slack), 트위터(Twitter) 등의 채널을 통해 여러 번 현 상태에서도 네트워크에 대한 공격을 불가능하다는 내용을 게시하였다. 이에 대한 근거로 스팸 공격이나 네트워크의 절대다수 지분을 차지하기 위해 취하는 행동들이 결국은 컨펌 숫자를 증가시켜 네트워크 공격이 아닌 네트워크를 향상시킨다고 밝혔다. 뿐만 아니라, 34% 공격을 하기 위해서는 충분한 연산력 외에도 더 많은 요소들이 필요하다고 하였다. 이러한 IOTA측의 주장은 코디네이터가 그럼 애초에 왜 필요하였는지에 대한 의구심을 낳는다. 그리고, 만약 스팸 거래가 네트워크를 돕는 행위라면 거래를 위해 최소한의 작업증명이 왜 필요한지에 대해서도 설명하기 힘들다. IOTA측은 코디네이터의 존재에도 불구하고 100% 탈중앙화가 가능하다고 주장하고 있다. 이는 결국 Coo가 왜 필요한지를 설명하지 못하며, 미래에 왜 Coo가 제거되어야 하는지에 대한 부분에 대해서도 명쾌한 해설을 주지 못한다.

IOTA측의 주장에도 불구하고 몇몇 잠재적인 공격 가능성이 식별되었다:

- 공격 주체가 네트워크를 두개의 하위 탱글로 나누고, 과반 이상의 해시 파워를 사용해 유효하지 않은 하위 탱글에 더 힘을 실어 행하는 이중지불 공격.
- 코디네이터 자체에 의한 이중지불 공격.
- 과반수 이상의 해시 파워를 장악하여 행하는 이중지불 공격.
- 이기적인 네트워크 사용과 네트워크 수렴에 대한 해당 토의.
- IOTA의 자체 네트워크가 커지더라도 이를 이루는 IoT 기기들의 해싱 파워가 너무 작기 때문에 공격 주체의 엄청난 연산력을 버텨내지 못할 수 있다는 가능성.

그리고 IOTA 네트워크 내 코디네이터가 공격 혹은 버그로 인해 일시적으로 작동을 중지한 적도 있다. 지난 10월 코디네이터의 작동 중지로 인해 Coo가 검증한 거래들만 수용하는 IOTA 공식 지갑이 며칠 간 거래를 검증하지 못했었다. 비트코인과 이더리움과 같은 프로토콜들이 수년 간 거의 100%로 작동된 것과 비교해보면 이러한 작동 중지는 굉장히 우려되는 부분이다. 암호화 네트워크는 탈중앙화를 통해 절대로 다운되지 않도록 설계된다.

IOTA 측은 이러한 문제점을 해결하는 동안 거래소들로 하여금 입출금을 중지토록 하였다. 네트워크 자체가 멈추지 않았고 공식

지갑만 아니라면 사용자들이 여전히 거래를 진행할 수 있다는 주장도 펼쳤지만, 이는 입증하기 어려운 주장이다. 왜냐하면 거의 모든 사용자가 공식 지갑을 사용하기 때문이다. 당시 공격으로 인해 IOTA 사용자들의 잔액이 위험하다는 판단 하에 IOTA측은 위험에 노출된 사용자들의 잔액을 직접 관리하고 추후에 사용자들로 하여금 잔액을 되찾아가게 하였다. 이로 인해 IOTA 재단의 신뢰성마저도 추락한 사건이었다.

버그로부터 자유로울 수는 없겠지만 IOTA 팀은 이번 사고가 버그 때문인지 혹은 공격 때문인지 명확히 밝히지 않았다. 뿐만 아니라, 사용자들의 잔액에 대한 통제를 함에 있어서 Coo가 어떤 역할을 했는지도 밝히지 않았다. 일련의 사태들이 실제로 일어났다는 그 자체만으로도 위험하다 할 수 있으며, IOTA가 탈중앙화 네트워크가 아니라는 점을 재확인했다 할 수 있다.

필수 하드웨어 요건

IOTA가 목표하는 바를 이루기 위해서는 IOTA 네트워크에 참가하는 IoT 기기들의 특정 하드웨어 변경이 필수적이다. IOTA 팀에 따르면 Curl hahser라는 하드웨어 장치가 있어야만 IOTA 거래를 생성하기 위해 필요한 작업증명을 수행할 수 있다고 한다. IOTA 측은 이러한 부분에 대해서 "사소한 문제"라고 입장을 밝혔고, IoT 기기가 점점 탈중앙화된 장부와의 연결성을 필요로 하면서 하등웨어 스택의 표준으로 자리잡을 것이라 하였다. 그러나 이는 주객을 전도한 논리일 수도 있다. 닭이 먼저냐, 달걀이 먼저냐의 문제일 수도 있지만, IOTA는 이러한 하드웨어 변경이 없이는 목표하는 바를 모두 이룰 수 없다. 동시에 하드웨어 회사들은 IOTA가 IoT 생태계 내에서 결제 표준 및 데이터 공유의 표준이 되지 않는 이상 하드웨어 수정을 해야할 유인이 없다. IOTA의 go-to-market 전략은 결국 IOTA의 자체적인 성공이며, 플랜 B는 존재하지 않는 것이다.

주요 우려사항

네트워크 사용가능 여부

여러차례 지속적으로 네트워크 작동 중단이 일어났다는 점은 IOTA 관련 문제 중 하나로 지적된 부분이다. 실제로 멀티코인 측에서 IOTA 기능성 시험을 위해 구매했을 당시에도 거래소 출금이 네트워크 문제로 인해 불가했다. 물론 비트코인이나 이더리움의 경우에도 거래소 출금이 중단되는 경우가 있긴 하지만, IOTA의 경우 이 문제는 계속해서 발생하고 있다. 실제로 깃헙의 IOTA 관련 이슈 게시판에서도 거래가 검증이 안되거나, 잔액이 사라지는 등의 문제가 지속적으로 일어나고 있다. 뿐만 아니라, 재단이 보관하고 있는 금액에 대한 청구가 안되는 부분 역시 지적되고 있다.

보고서에서 이미 언급했듯, 코디네이터의 일시적인 작동 중단으로 인해 네트워크가 사용 불가했었다. 레딧과 깃헙 사용자들에 따르면 IOTA 네트워크는 이미 여러차례 스팸 공격에 의해 멈춘 적이 있다고 한다. 이 공격 중 한 차례는 부족한 풀노드 숫자가 주 원인으로 꼽히기도 했다. 이에 대해 IOTA 팀 인원들은 네트워크는 아무 문제 없이 작동하고 있었다며 레딧 사용자들의 의견을 반박하였다 (다음 아티클의 코멘트를 참조).

12월 초에 발생한 다른 공격은 사용자들이 거래를 검증할 수 없게 하였고, 모든 네트워크 활동을 멈춘 것으로 추측된다:

- 레딧 내 스팸공격에 대한 토의
- 커뮤니티 인원들의 스팸 공격 감행자들에 대한 공격 중지 요청
- IOTA 개발진의 스팸 공격이 발생하고 있음에 대한 공식 의견
- 12월 초 공격 당시 미검증 거래에 대한 깃헙 이슈 게시판

대다수의 탈중앙화 장부가 때로는 제한된 네트워크 사용성을 보였던 것은 사실이다. 몇몇 ICO가 진행될 당시나 Cryptokitties 프로젝트의 인기가 절정일 당시에 이더리움 네트워크 역시 겪었던 바이다. 하지만, 네트워크 사용성 관련 문제가 IOTA 에서 훨씬 더 자주 일어나고 있는 것으로 보인다. 뿐만 아니라 지갑 잔액 불일치 문제도 훨씬 빈도가 높다. 그리고 네트워크 사용 불가가 공격에 의한 것인지 버그에 의한 것인지를 판단하는 것이 불가능한 부분도 지적되는 바이다. IOTA에 있어서 네트워크 사용 불가를 야기하는 원인이 버그인지 공격인지는 중요한 문제이다. IOTA 팀은 과거의 스팸 공격이 거래 처리량을 늘리기 때문에 네트워크를 더 강화한다고 주장해왔다. 하지만 상기 링크들에서도 알 수 있듯 IOTA 팀은 상반된 주장을 함으로써 자가당착에 빠지고 있다. 스팸공격이 야기한 지금까지의 문제들을 살펴볼 때, 미래에 거래처리량이 늘어나면 어떻게 IOTA 네트워크가 이 문제점들에 대처할지가 불분명하다.

IOTA의 주요 문제점 중 하나로 꼽히는 사용자 경험 역시 짚고 넘어가야 한다. 왜냐하면 이 문제로 인해 사용자들이 자금을 잃었기 때문이다. 예를 들어, 최근 사용자들 중 악성 온라인 시드 생성기를 사용한 이들이 수백만 달러 어치의 IOTA 토큰을 탈취당했다. 시드 기반 지갑의 경우, 임의 생성이야말로 가장 중요한 부분이라 할 수 있다. 그런데 그런 시드 기반 지갑을 사용하는 IOTA가 공식 지갑 내 빌트인 소프트웨어가 아닌 제3자에게 이 부분을 맡긴다는 것 자체가 잘못된 결정이라고 판단된다. 실제로 한 때는 공식 IOTA 지갑 안에 시드 생성기가 있었지만, 사전 예고 없이 개발진에 의해서 삭제되었다.

암호학 및 소프트웨어 취약점

IOTA 개발과 관련하여 가장 큰 우려를 자아내는 것은 MIT 미디어랩의 디지털 화폐 이니셔티브 담당 디렉터인 Neha Narula가 발행한 보고서이다. 이 보고서는 IOTA가 사용하는 해시 함수의 치명적인 결함을 담고 있다. Narula 디렉터는 이 개념에 대해 친절히 설명하였다:

> 암호화된 해시 함수의 경우 임의의 입력값을 기반으로 고정되어 있지만 예측 불가한 출력값을 생성한다. 해시 함수에 있어서 중요한 점은 출력값을 통해 어떤 입력값이 이 출력값으로 귀결되었는지를 알아내는 것이 매우 어려워야 한다는 점이다. 또한 입력값과 출력값을 안다 하더라도 기타 입력값이 동일한 출력값으로 이어지는지를 알아내는 것이 매우 어려워야 한다. 만약 동일한 두 개의 입력값이 동일한 출력값을 가진다면 이를 충돌이라고 부른다. 충돌을 야기하는 입력값을 쉽게 알아낼 수 있다면 그 암호화 해시 함수는 실질적으로 쓸모가 없다.
>
> 암호화 해시 함수가 암호화폐에 있어 중요한 이유는 대부분의 거래가 서명 이전에 해싱되기 때문이다. 즉, 누군가가 해시 함수를 쉽게 해독할 수 있다는 사실은 서명 역시도 쉽게 깨질 가능성을 내포한다. 거래가 유효한지 그리고 암호화폐 사용을 승인하는 그 메커니즘 자체가 결함이 있다는 뜻이다. 암호화폐의 근간을 이루는 수학적 무결성은 이 해시 함수가 안전하다는 것을 가정으로 하고 있다.

Narula와 MIT 미디어랩 팀은 IOTA의 Curl 해시 함수 내에서 충돌 지점을 쉽게 찾아낼 수 있었다. 해당 Curl 해시 함수는 IOTA 팀에 의해 직접 만들어졌는데, 이렇게 직접 개발해야 했던 이유는 이진법 대신 IOTA가 삼진법을 사용하기 때문이다. 암호화폐계에서 황금률이라 할 수 있는 "자신이 직접 암호화하지 말 것"을 어긴 것이라 할 수 있다. 프로젝트들은 암호학 관련 라이브러리에서 이미 수차례 시험을 거쳤고 제3자 검토를 거친 암호학만을 써야한다. 물론 불가피하게 연구원들이 신규 암호학에 대한 가능성을 탐구해야 하는 상황이 있음을 인지하지만, IOTA의 함수에서 발견된 취약점들은 황금률을 지켰어야 함을 보여준다. 해당 취약점이 알려진 뒤, IOTA는 Curl 해시 함수에서 Keccak-384 (SHA-3)으로 암호화 서명 방식을 교체하였다.

잘못된 결정은 누구나 할 수 있다. 하지만 역경에 처했을 때 어떻게 팀이 대응하는지는 통제할 수 있는 부분이다. 이러한 곤란한 상황에 IOTA 팀이 대응한 방식은 끔찍했다.

IOTA 팀은 레딧, 미디엄, 개인 블로그 등을 통해 해시 함수의 결함 관련 해명을 수차례 게재하였다. 심지어 이 해명들은

상충하는 부분마저 존재했다. 그리고 문제 지적이 있은 후 6개월 가까이 지나서야 팀의 공식 입장이 나왔다. 이 링크는 관련 입장 게시물 시리즈 중 4번째에 해당한다. 이 게시물에서 IOTA 팀은 충돌 가능성이 실제로는 IOTA 소프트웨어가 악의를 가진 이들에 의해 사용되는 것을 방지하고자 의도적으로 설계된 것이라 주장하였다. 클로즈드 소스 기반의 중앙화된 코디네이터의 사용을 통해 해당 취약점이 IOTA 거래에 영향을 주는 것을 방지하였고, 이미 IOTA 측에서는 이 취약점의 존재 사실에 대해서 인지하고 있다는 내용이었다. IOTA의 소스코드를 사용하려는 이들 중 선의를 가진 오픈소스 프로젝트라면 이 취약점을 발견 한 후 해시 함수를 변경하겠지만, 악의적인 주체들은 부주의로 인해 이런 변경을 하지 않을 것이라는 주장을 하였다.

IOTA 팀의 주장은 이러한 취약점이 의도된 것이며, 사용자들이 돈을 잃거나 악의적 프로젝트들에 의해 사기당하지 않도록 하기 위함이란 것인데, 이는 터무니없는 주장이다. 만약 그 주장이 사실이라 하더라도, 우선 이는 오픈소스 커뮤니티의 정신에 완전하게 위반되는 행위이다. 뿐만 아니라, 다른 프로젝트가 취약점에 대해 미처 파악하지 못한 채 IOTA의 소스코드를 사용하였을 때 IOTA 팀이 어떻게 대응했을지 의문을 자아낸다. 취약점을 인지한 채 그대로 내버려두어 사용자들이 돈을 잃게 만들 가능성을 열어둔다는 것 그 자체가 이미 용납할 수 없는 주장이다.

멀티코인은 IOTA 팀이 해당 상황에 대해 펼치는 논리를 받아들일 수 없다. 개인 투자자들이 IOTA 팀의 행위와 윤리적인 부분에 대해 평가를 내리는 것은 자유이지만, 멀티코인은 이러한 행위가 용납불가하다고 판단하였다. 그렇기 때문에 IOTA에 대한 자사의 기조는 투자 불가한 상품이라는 평가이다. 그리고 레딧에 Sergey Ivancheglo가 게시한 취약점에 대한 해명글은 IOTA 소프트웨어 내에 추가적인 결함이 있을 수 있다는 사실을 인정하길 거부하였다. 이를 인정하는 대신 오히려 그는 "결함"이라는 단어가 갖는 의미에 대해 반론을 펼치면서 공개적으로 그 결함을 밝히는 것이 되려 사기꾼들에게 IOTA 팀이 속수무책으로 당하게 할 것이라는 의견을 개진하였다. 이러한 주장은 수십억 달러 가치를 가진 네트워크로서는 낯뜨거운 모습이다. IOTA 팀은 네트워크를 통제할 수 있는 행위들에 대한 접근권은 가지고 있지만, 그 어떠한 책임감도 없는 것이다.

결론

방향성 비사이클 그래프(DAG) 아키텍처 자체는 흥미롭고 새로운 방식으로 분산 장부를 만드는 메커니즘이다. 그러나 멀티코인 캐피탈은 DAG가 블록체인을 대체할 수 있다 생각하지 않는다. 특정 종류의 탈중앙화 앱을 위해서 DAG가 제공하는 기능이 더 알맞을 수는 있다. 현재 대다수의 분산 장부 기술과 마찬가지로 DAG 역시 태아기에 해당하는 기술이며, 시험되지 않았다. 이 분야에 대한 추후의 연구가 계속되길 기대한다.

- Coo 사용과 수반되는 노골적인 중앙화와 불확실한 탈중앙화 시점
- 수차례의 네트워크 작동 중단
- 팀이 책임감이나 거버넌스 없이 사용자의 자금에 대한 통제 실행
- 코드 내에 취약점에 대해 인지하면서도 이를 그대로 포함하는 결정
- 해당 취약점들에 대한 핵심 IOTA 팀의 상충되는 해명
- 불분명한 사용 사례. 확률론적 소액결제나 스테이트 채널로는 감당이 불가능하기 때문에 M2M(머신투머신) 소액결제를 필요로 하는 사용 사례가 많다고 판단하지 않는다.

멀티코인은 IOTA 팀에 행운을 빌며, IoT 시대에 걸맞는 경제로 한발짝 더 다가설 수 있도록 비전을 실현하길 기원한다. 그러나 현재 IOTA 네트워크의 상태와 심각한 수준의 기술적 리스크, 그리고 프로토콜 내 자명한 결함 관련 압도적인 양의 증거를 감안하면 IOTA의 현재 가격은 과대평가 되어있다. 본 보고서가 쓰이는 시점에서 IOTA의 시가총액은 6,807,664,212 달러이며, 암호화폐 시장 전체에서 시가총액 기준 11위로 책정되어 있다.

고지사항

본 보고서 발간 시점에 멀티코인 캐피털 매니지먼트 LLC 및 멀티코인 소속 직원들(이하 멀티코인), 본 보고서의 리서치에 기여하고 결과물을 공유받은 이들(이하 투자자) 모두 리포트 내에서 언급된 토큰을 매매하고자 하거나 이와 관련된 옵션을 보유하고 있을 수 있으며, 토큰 시세의 상승하락에 맞추어 이익을 실현하려는 입장을 취합니다. 본 보고서 발간 이후 투자자들은 다뤄졌던 프로젝트의 암호자산을 거래할 수 있습니다. 멀티코인은 본 보고서 내의 모든 정보를 정확하고 믿을만하다고 판단 정보원으로부터 확보합니다. 하지만 모든 정보는 있는 그대로 제시되어 어떤 형식으로도 - 직접적으로 혹은 암시적으로 - 보장될 수 없습니다.

본 문서의 유일한 목적은 정보 제공이며, 특정 거래에 대해 공식적으로 확인하지 않습니다. 모든 시장 가격, 시장 데이터 및 기타 정보에 대한 완벽성과 정확성은 보증되지 않으며, 선별된 공개시장 정보를 기반으로 합니다. 해당 정보는 현 시점까지의 멀티코인의 관점을 반영하며, 별도의 통보 없이 변경될 수 있습니다. 멀티코인은 본 보고서에서 다루는 프로젝트에 대해 지속적으로 리포트를 발간할 의무를 갖지 않습니다. 본 리포트는 명시된 일자를 기준으로 작성되었으며, 이후 시장 혹은 경제 상황의 변화로 인해 그 신뢰성이 저하될 수 있습니다.

모든 투자는 가격 변동성, 불충분한 유동성, 원금의 완전한 손실 가능성 등의 상당한 리스크를 내포합니다. 본 보고서에서 멀티코인이 평가한 기초가치는 특정 토큰의 잠재적 기초가치에 대한 최선의 예측만을 반영하며 투자자를 위한 토큰 품질평가, 실적 요약, 투자전략 등을 의미하거나 시사하지 않습니다.

본 문서는 해당 토큰의 매수매도와 관련된 청약 혹은 청약 권유를 포함하지 않습니다.

본 문서에 담겨진 정보는 향후 가능성을 예측하는 내용을 포함하고 있을 수 있으며 역사적인 사실을 다루는 것이 아님을 밝힙니다. 이와 같은 내용은 추후 잘못된 것으로 밝혀질 수 있으며, 부정확한 전제, 알려진 혹은 알려지지 않은 리스크, 불확실성 등을 포함하여 멀티코인이 통제할 수 없는 요인의 영향을 받을 수 있습니다. 투자자들은 본 문서에서 다루어지는 모든 암호자산에 대해서 금융, 법률 및 조세 전문가 등의 도움을 받아 독립적인 자가 실사를 수행해야 하며, 그 어떠한 투자 결정을 내리기 전에 앞서 관련 시장에 대한 독립적인 판단을 해야합니다.