

공개 SW 기반의 IoT 블록체인

2018. 08. 29

문 승 진
(sjmoon@etri.re.kr)

한국전자통신연구원
블록체인기술연구센터

1. 공개 SW 과제 개발 프로세스 및 추진체계 @ETRI (예시)
2. IoT Blockchain
3. Consortiums/Platforms/Services/Projects
4. Trends
5. Deep Dive : IOTA Tangle

공개 SW 과제 개발 방법(안)

◆ 공개 SW의 목적

- 개발자들과 사용자들의 저변을 확대하여 개발되는 SW의 가치를 극대화하고 글로벌 표준화 협력과 시장 경쟁력을 확보하는 데 있음

◆ 공개 SW 개발 방식

- (방식 1, 개발 쏘단계 오픈 소스화) 개발 초기부터 오픈 소스 외부 개발자들과 오픈 소스 커뮤니티를 구성하여 공동으로 개발하고 개발된 소스를 공유하는 방식
- (방식 2, 개발 완료 후 공개) 최종 SW 개발 완료 후 공개 SW로 공개하는 방식
- (방식 3, 하이브리드 방식) 위 방식의 하이브리드 형태로서 초기 버전 개발 후 공개 SW로 전환하여 완성 버전을 개발하는 방식. 대형 SW의 단계별 개발에 유리

◆ 공개 SW 관리 방식

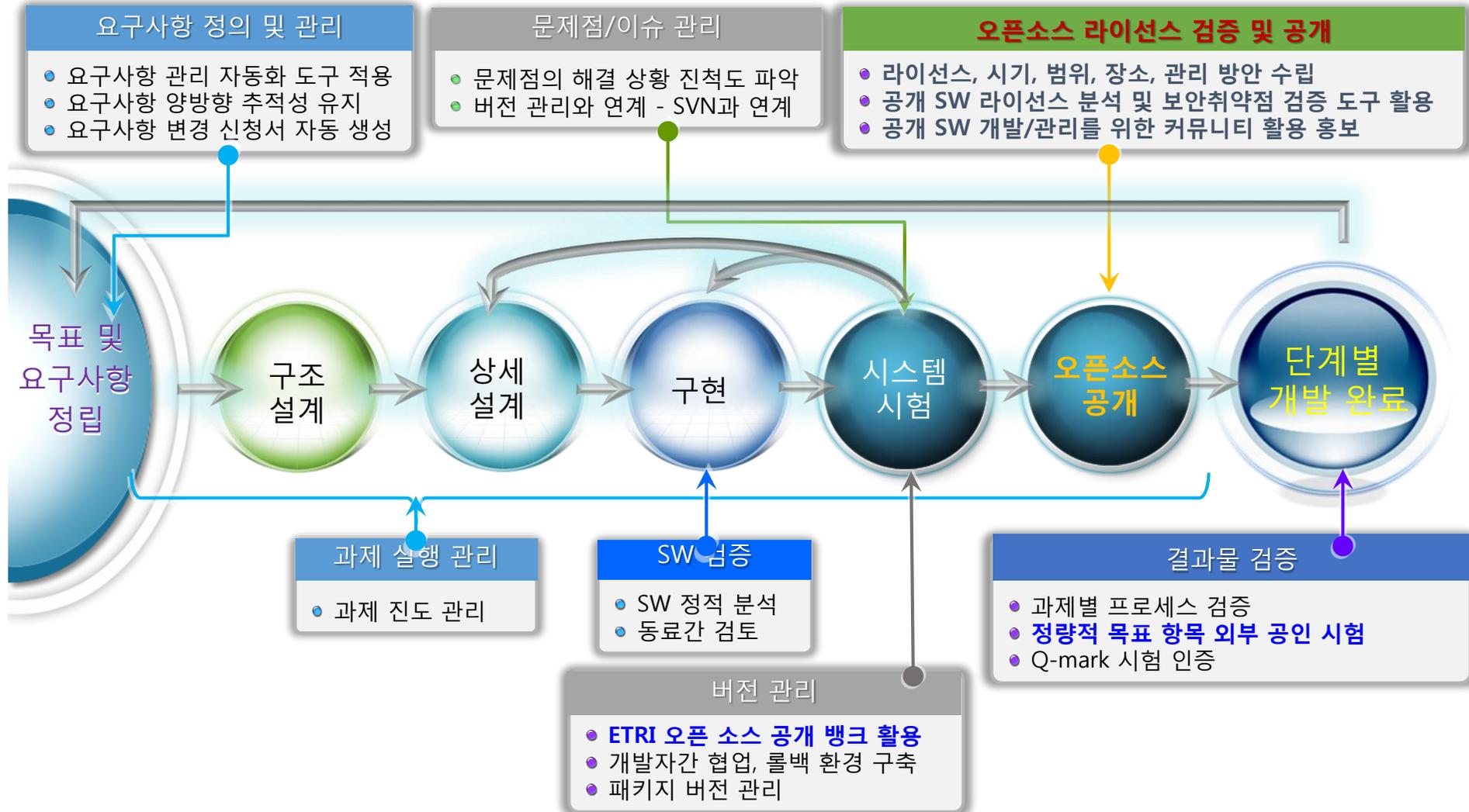
- (개발 단계) 소스 형상관리, 이슈 추적관리, 시험 및 검증 자동화에 의해 관리
- (SW 공개 후) 블록체인 오픈 소스 커뮤니티를 구성하여 이 커뮤니티에서 오픈 소스 관리를 전담
- ※ 오픈 소스 관리 주요 내용 : 오픈 소스 개발 규칙 및 라이선스 결정, 소스 관리 의사 결정, 패키징 및 시험을 통한 배포 등 포함

공개 SW의 Benefit

- ◆ 공개 SW의 경제적 이익 : 라이선스의 종류에 따라 다양한 비즈니스 모델 적용
 - 듀얼 라이선스 모델 : 개발된 SW의 일부(예, 엔터프라이즈용)는 미공개하고 나머지만 공개
 - 독립적 부가제품 모델 : 공개 SW를 기반으로 플러그인 제품 또는 액세서리 형태의 추가기능 제품 판매로 수익 창출
 - 컨설팅 및 시스템 통합 : 개발된 SW를 공개하고 사용자가 필요한 시스템 통합이나 컨설팅으로 수익 창출
 - 공개 SW 전문가 서비스 : 개발된 SW를 공개하고 사용자에게 기술 전문가를 지원하여 수익 창출
 - 공개 SW SaaS(Software as a Service) 모델 : 개발된 SW를 공개하고 사용자에게 SaaS 서비스를 제공해줌으로써 수익 창출
- ※ 출처: “공개 소프트웨어 연구개발 수행 가이드라인”, 2018.6, 과기정통부
- ◆ 특허의 실효성
 - 공개 SW를 제공하는 글로벌 기업들은 특허를 자사 경쟁력 확보의 전략적 수단으로 활용
 - 공개 SW로 외부 SW 개발자와 사용자들을 최대한 확보한 후, 공개 SW에 포함된 특허를 활용하여 다양한 라이선스 정책으로 유리한 비즈니스 창출
- ※ 공개 SW에 포함된 특허는 라이선스에 따라 실시권을 허용하거나, 듀얼 라이선스 정책으로 핵심 특허의 경우는 전략적으로 허용하지 않을 수 있음
- ◆ 공개 SW 과제에서의 주관/참여기관이 민간기업일 때의 이슈
 - SW 공개 시 민간기업의 현실적인 이익은 무엇인가?(과제 참여 이슈, 개발 범위 이슈 등)
 - 특허 출원 후 SW 공개 : 특허 침해 소송 비용, Know-How 이슈

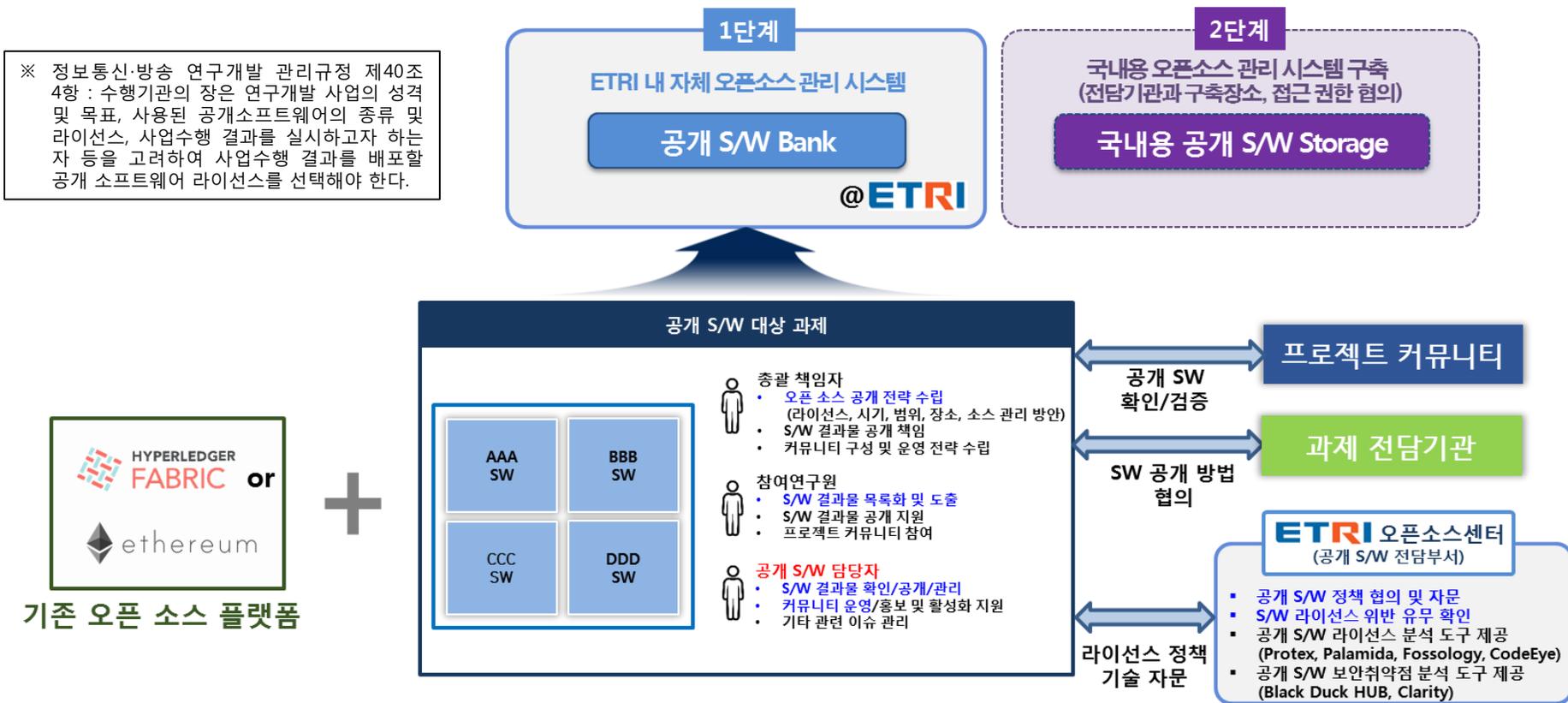
공개 SW 과제 개발 프로세스 @ETRI (예시)

- ◆ 'ETRI R&D 표준 프로세스'에 따른 체계적 관리 및 자동화 환경 구축
- ◆ **과제 특성(공개 SW)**을 고려하여 **오픈소스 공개 프로세스 추가** 수행



공개 SW 과제 개발 추진체계 @ETRI (예시)

- ◆ 1단계: ETRI 내 자체 오픈소스 관리 시스템 구축
- ◆ 2단계: 국내용 오픈소스 관리 시스템 구축 or GitHub (국책과제 결과물의 국외 공개와 관련된 Issue 존재)
 - 구축 장소 및 접근 권한 관리 방법은 과제 전담기관과 협의
- ◆ 운용 방법
 - 전담기관, ETRI 오픈소스센터 및 참여기관과의 협의 하에 공개 SW 라이선스 정책 결정
 - 과제 내 공개 SW 담당자 지정 : SW 결과물 확인/공개/관리 전담
 - 프로젝트 커뮤니티 구축 및 운영 : SW 개발 자문 및 공개 SW 확인/검증



1. 공개 SW 과제 개발 프로세스 및 추진체계 @ETRI (예시)

2. IoT Blockchain

3. Consortiums/Platforms/Services/Projects

4. Trends

5. Deep Dive : IOTA Tangle

IoT + Blockchain : Needs

- 중앙집중식 IoT 플랫폼으로부터 분산형태로의 **시대적 요구**
 - Server가 독식하는 구조가 아닌 **Peer들이 주체 (P2P)**
- 기존 IoT 플랫폼에 블록체인 기술이 접목되면 어떤 장점이 있을까?(거래? 보안? 데이터? Etc.)
 - IoT **디바이스 간의 신뢰(인증) 가능**
 - IoT 디바이스들의 **데이터에 대한 신뢰 문제**(Configuration 또는 FW Update, etc.)
 - IoT 디바이스의 **자율적(사용자 개입 없음) 트랜잭션(거래)의 필요성**
 - 기존 IoT 플랫폼에서는 디바이스(센서 노드 또는 게이트웨이)의 자율 거래 수단이 없어서 서버 및 사용자에게 의존할 수 밖에 없음(지불 방법 부재)
 - 블록체인은 제3의 인증 기관(예, 은행) 없이 거래가 가능한 기술(IoT 플랫폼에 Value-Added Service 가능)
- IoT 플랫폼의 Smart Device가 생산해 내는 데이터를 **M2M(장치 간) 자율적인 계약**을 통해서 거래 가능
 - IoT의 Smart Devices 역할을 Smart Contract가 수행
- IoT 플랫폼의 보안 이슈(사용자/디바이스 인증, 데이터 보안, 암호화 등) 모두 블록체인으로 해결 가능한가?

IoT Blockchain : A few Considerations (1 of 2)

● IoT 블록체인의 정의

- Broad : IoT 플랫폼(센서, GW)으로부터 들어오는 IoT 데이터를 이용하는 블록체인 플랫폼
 - IoT + 블록체인의 단순 연동, 서버가 블록체인 Node
 - Non-IoT 블록체인 서비스와 기술적으로 차별점이 있는가?
- Narrow : IoT 플랫폼 내 센서 노드(or GW)들이 자체적으로(Smart Contract or AI) 판단하여 자율적으로(Autonomous) 처리/거래하는 블록체인 플랫폼 (예, ADEPT)
 - 블록체인은 거래가 가능한(Coin을 주고 받을 수 있는) 플랫폼(IoT 플랫폼에 Value-Added Service 가능)

● IoT 블록체인 노드의 범위

- IoT 데이터를 수집/관리하는 서버?
- WiFi를 지원하는 IoT GW 만?
 - Raspberry Pi 3 사양 : 초경량/저전력 블록체인 필요(한정된 Resource(CPU 용량, Memory, Battery))
- WiFi를 지원하지 않는 단순 Sensor(Zigbee, Bluetooth, etc.)까지 포함?
- Drone, Smart Phone

● 합의 시간/블록 생성 타임/TPS/원장 저장 능력

IoT Blockchain : A few Considerations (2 of 2)

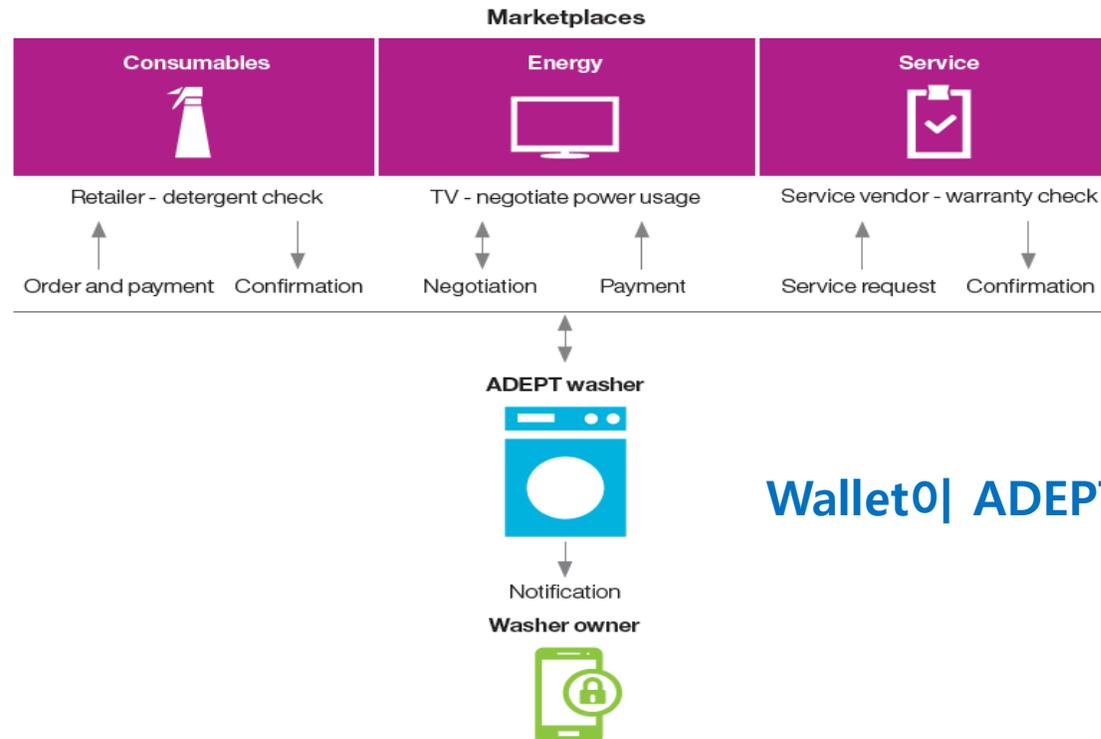
- **Micropayment에서의 거래 수수료 문제**
- **IoT 데이터가 원장에 기록될 만한 가치가 있는 것인가?**
 - Smart Grid(전력 검침 및 거래)
 - FW Update/Patch, Instruction 무결성
 - 기존의 가상통화를 제외한 데이터 전달이 가능한 트랜잭션 구조 필요
- **IoT 데이터의 용량 문제**
 - Smart Grid(수십 GB/day 신규 데이터 생성)
 - Off-Chain으로 실제 데이터를 보내고, 전달 내역(데이터 Hash 값 포함)만 트랜잭션으로 전달
- **Smart Contract 실행 환경(VM, State DB etc.) for IoT**

- ADEPT : Autonomous Decentralized Peer-to-Peer Telemetry

- Ethereum 소스코드 기반의 IoT 플랫폼

- 기존의 IoT 플랫폼에 구상했던 서비스들을 (인간의 개입 없이) 디바이스가 스스로 거래(화폐지불)를 하고 서로 가치를 공유한다는 개념

- ADEPT 기능 내장 세탁기가 세제가 떨어지면 사용자에게 알려서, 세제를 자동적으로 재주문하는 시나리오 제시
- 세제 공급처는 스마트 컨트랙트에 대해 유효성을 확인하고, 지불 받은 후, 주문된 세제를 공급



Wallet이 ADEPT washer 내에 있음

1. 공개 SW 과제 개발 프로세스 및 추진체계 @ETRI (예시)
2. IoT Blockchain
3. Consortiums/Platforms/Services/Projects
4. Trends
5. Deep Dive : IOTA Tangle

Trusted IoT Alliance (<https://www.trusted-iot.org/>)

Tech Giants and start-ups have joined to form a consortium that will look to build a **trusted IoT ecosystem** with enhanced **security and trust protocol**

The screenshot shows the website header with navigation links: For Enterprises, For Developers, About, Events, Contact. The main content features the title "Securing IoT Products With Blockchain" and a sub-headline: "A new open source software foundation is born to support the creation of a secure, scalable, interoperable, and trusted IoT ecosystem." Below this is a large graphic of a blue hexagonal base with various IoT icons (drone, car, shoe, etc.) floating above it. At the bottom, it says "Trust. Innovation. Collaboration." and a short paragraph: "The Trusted IoT Alliance is built by enterprises and developers that are wanting to build the future of the economy through the development of an ecosystem consortium."

Our 2025 Goals

Create an IoT ecosystem

With security, interoperability, scalability, and performance characteristics that will enable trillions of dollars of assets to ride on top of disparate blockchain systems.

Digitalize systems

Accelerate the digitalization of products, assets, and machines for frictionless M2M and supply chain interactions.

Power a tech revolution

To support the world's automotive, pharma, drone, smart card, postal system, supply chain, industrial IoT, insurance, and emerging machine, and autonomous economies.



Founding Members

BLOCKCHAIN TECHNOLOGY COMPANIES



- BigChain DB : Blockchain Database
- Streamr : Streaming of Live Data in exchange for payment
- IOTA : Tangle

ENTERPRISE MEMBERS



IOT TECHNOLOGY MEMBERS



- Completed PoCs for trusted odometer(차량 주행 기록계), luxury goods identity verification, router firmware verification, trade finance automation, supply chain event logging, smart vehicle charging, data logger provenance

Chain of Things (www.chainofthings.com) (1 of 4)

Chain of Things is developing **Maru - an integrated blockchain and IoT hardware solution** to solve IoT's issues with identity, security, and interoperability

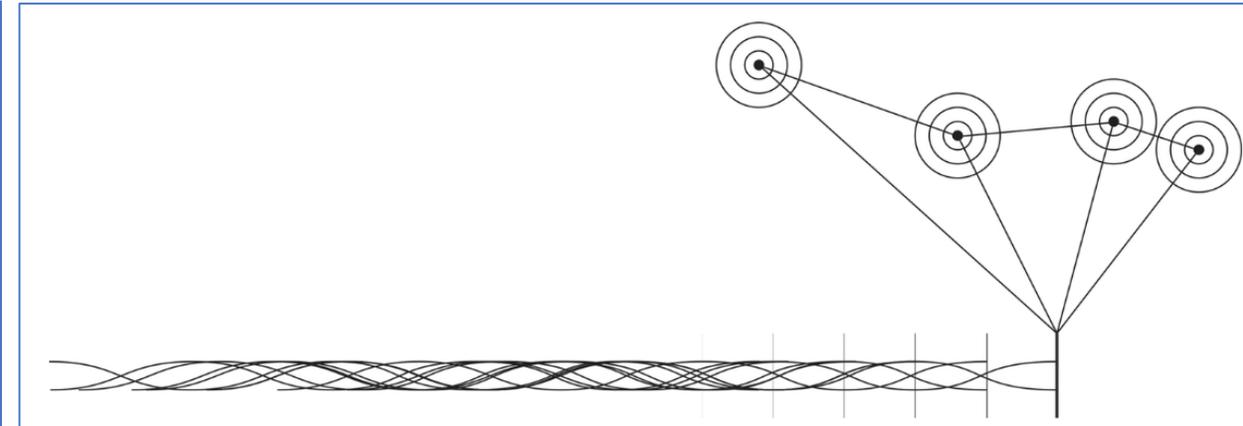


HOME CASE STUDIES RESOURCES ABOUT TELEGRAM



Advancing Innovation in Blockchain & IoT.

Chain of Things is developing **Maru - an integrated blockchain and IoT hardware solution** to solve IoT's issues with identity, security, and interoperability. We are leveraging the nexus between blockchain and IoT to deploy industrial, environmental, and humanitarian related solutions. More information on Maru coming soon.



- Mission 1: Save IoT. CoT will investigate whether the **core technology behind bitcoin, blockchain/ distributed ledger technology**, can provide a more secure and interoperable fabric for the future of IoT.
- Mission 2: Find the best use-cases for blockchain IoT combined. CoT is to investigate the **best possible use-cases where blockchain and IoT combined can offer significant benefits** to industry, governments, individuals..

Chain of Things (www.chainofthings.com) (2 of 4)

Usecase 1. Chain of Security

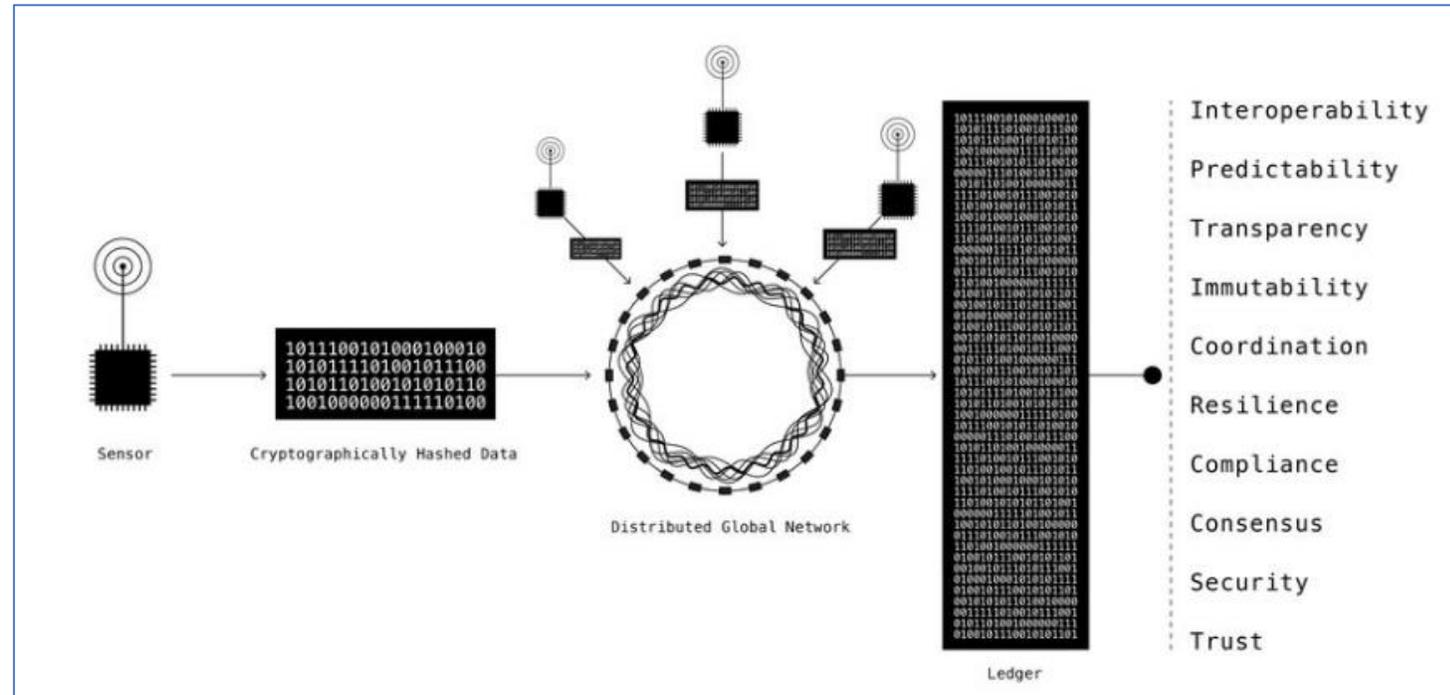
- **Device Firmware Hashing**

Device firmware can be hashed into a Blockchain on a continual basis. If the firmware state changes (by even a single digit) due to malware altering the firmware code, can the hash failure will alert the device owners to foul play.

- **Instruction Authentication**

Information or checking instructions - device hashes information it wants to send to another device and places the hash into a Blockchain...the receiver of the information hashes the same information...if the hash matches the hash on the Blockchain then the information has not changed in transit.

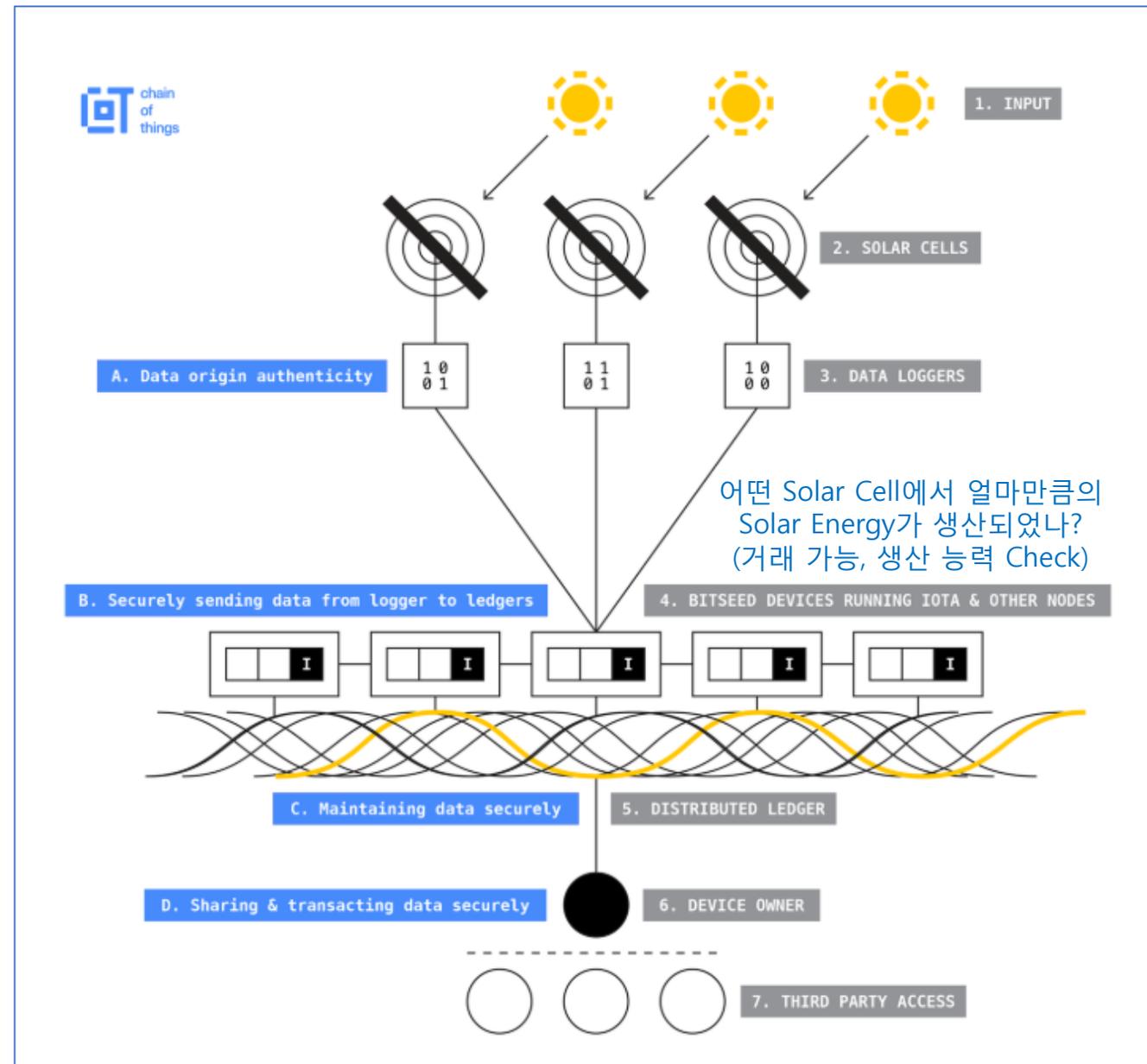
- **Device Identity Protocol**



Chain of Things (www.chainofthings.com) (3 of 4)

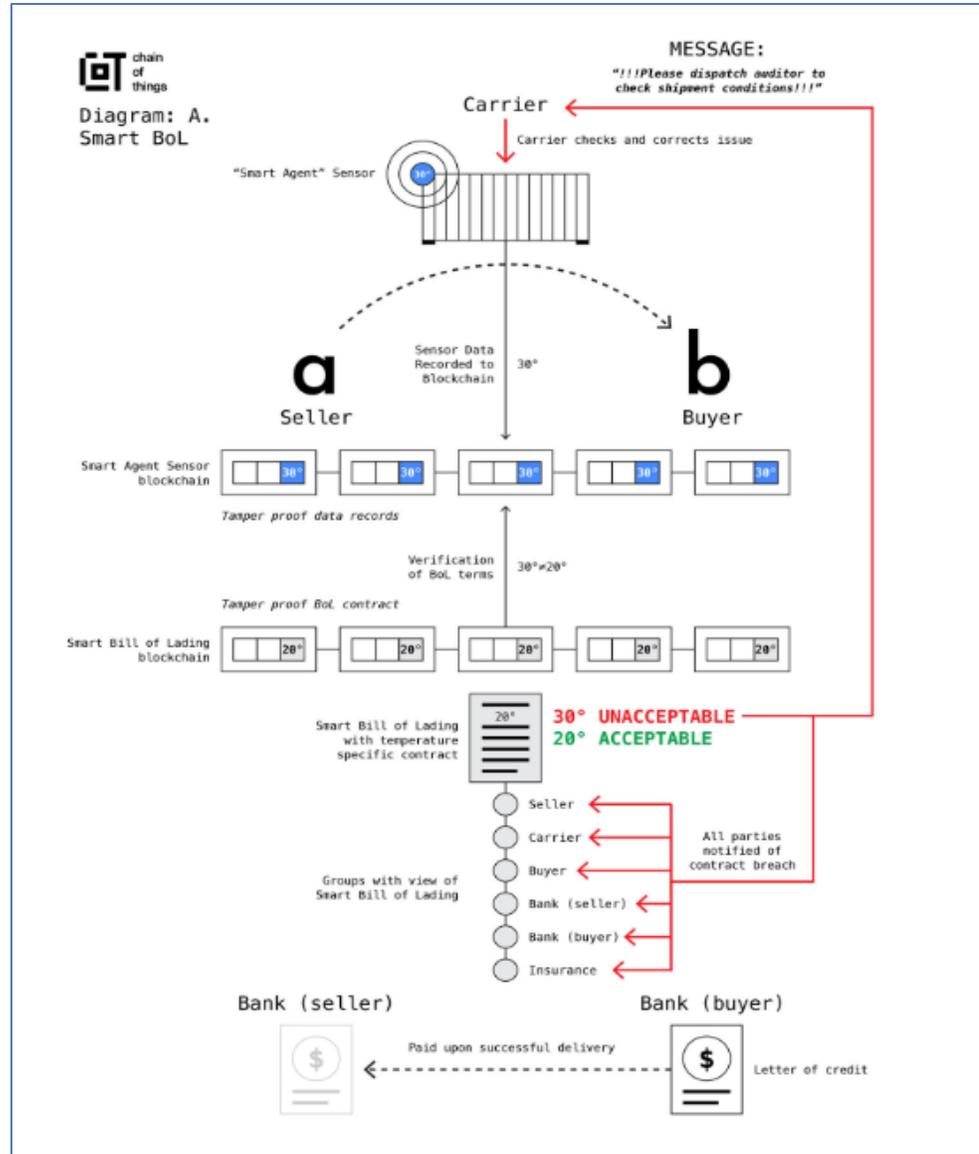
Usecase 2. Chain of Solar (for Energy Trade)

- The **ElectriCChain** is an open science project dedicated to the **intersection of solar energy, IoT and blockchain technology**.
- One of the ElectriCChain's goals is to connect the world's 7 million solar facilities, watching the skies 24/7 and posting live data to one blockchain for scientists, researchers and human progress.
- Initial focus is on **verifying and publishing solar power generation data** publicly in near real time.
- The ElectriCChain project supports the development of open standards and tools to publish and read solar electricity generation data using the **SolarCoin** blockchain and/or other blockchain technologies.



Chain of Things (www.chainofthings.com) (4 of 4)

Usecase 3. Chain of Shipping



- 1) B/L 운송 조건에 대한 정보 전달
- 2) 해당 조건에 따라 화물 운송
- 3) 컨테이너에 부착된 Smart Sensor가 화물 온도 및 품질 정보 감지
- 4) 센서 데이터는 블록체인 Shared Ledger에 기록
- 5) 계약 조건과 화물품질 정보 검증(예 20도 : OK, 30도 : 위반)
- 6) 검증 데이터는 모든 참여자(Seller, Buyer, Carrier, Bank, Insurance)에게 전달
- 7) 조건 충족 시, 인도 후 결제 대금 지급 자동화

Blockchain for Electricity

Payment

- Bank pays

Identity

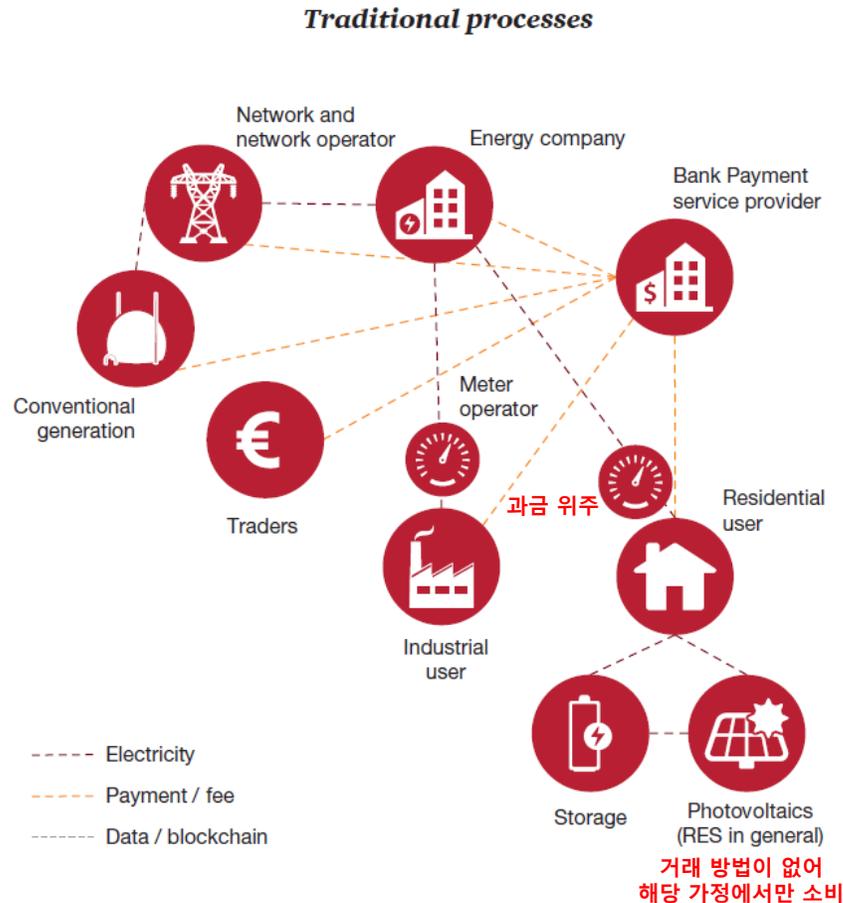
- Managed by bank & energy company

Timing

- Settlement take time

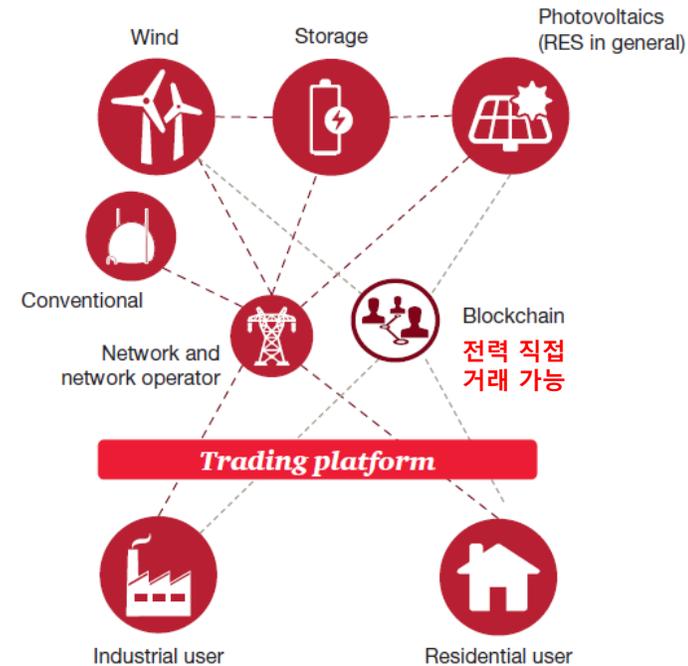
Visibility

- Bank keeps ledger & reconcile needed



- Privacy and security of smart meters
- Peer-to-peer energy transaction and control
- Permanent record of maintenance

Processes in a blockchain-based system



- E-mobility(charging, sharing)
- Clearing and settlement of electricity trading
- Verification of green electricity, CO2 certificates

Payment

- Paid to **digital wallet**

Identity

- Managed by key

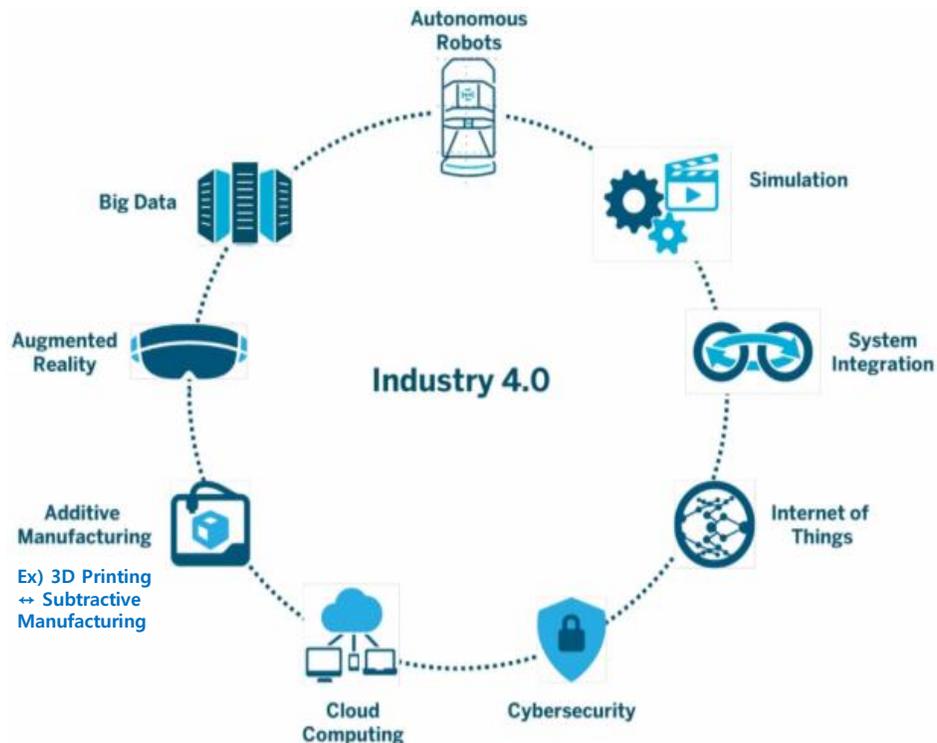
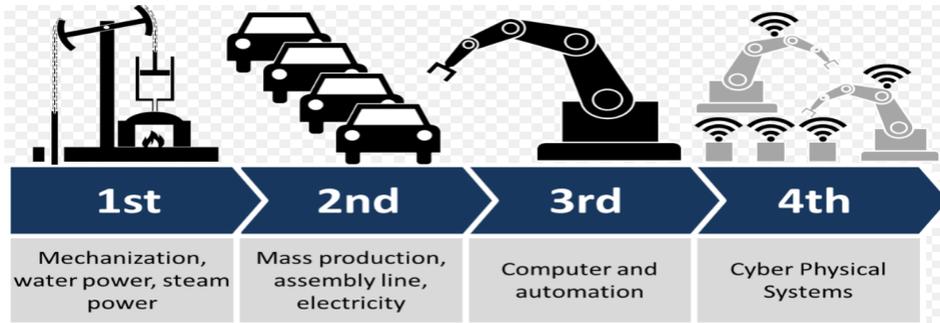
Timing

- **Immediate** fund transfer

Visibility

- **Every stakeholder** keeps ledger & no reconcile

Industry 4.0



- IIoT(Industrial IoT)
- Digital Twin
- Big Data
- AI(Deep Learning)
- Blockchain : 스마트 컨트랙트로 M2M Economy 가능
- 독일 : Industrie 4.0에 IOTA 적용 중.
(www.plattform-i40.de)
 - 폭스바겐과 IOTA 테스트 중

Volkswagen cooperation with the IOTA Foundation

The Tangle (next generation Blockchain)

- Distributed ledger developed for IoT Applications
- Open Source
- Ideal for M2M nano-transactions
- High scalability

Advantages for automotive usage

- Feeless transactions
- Short verification time
- Offline transactions enabled
- Quantum secure

IOTA : ledger-of-things

Blockchain's Limitations

- Scalability
- Storage
- Bandwidth
- Fees
- No Data Privacy
- Expensive Data Storage

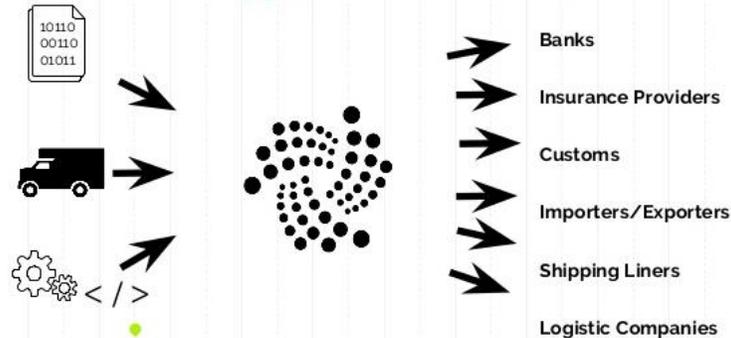
IoT Requirements

- Low Resource Consumption
- Widespread interoperability
- Billions of nano-transactions
- Data Integrity

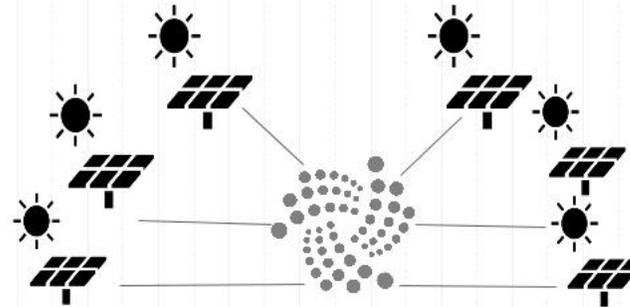
- No Fees
- Scalable
- Quantum Proof
- Modular
- Lightweight
- Offline

< IOTA's Background & Features >

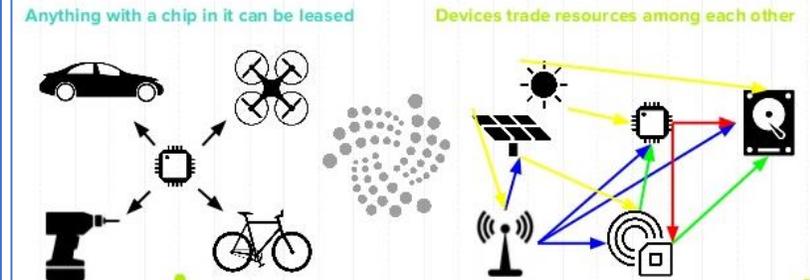
Supply Chain Visibility



Smart-Grid



Sharing Economy 2.0



< IOTA's Usecases and Vision >

1. 공개 SW 과제 개발 프로세스 및 추진체계 @ETRI (예시)
2. IoT Blockchain
3. Consortiums/Platforms/Services/Projects
4. Trends
5. Deep Dive : IOTA Tangle

Current Blockchain Vs. IoT Blockchain

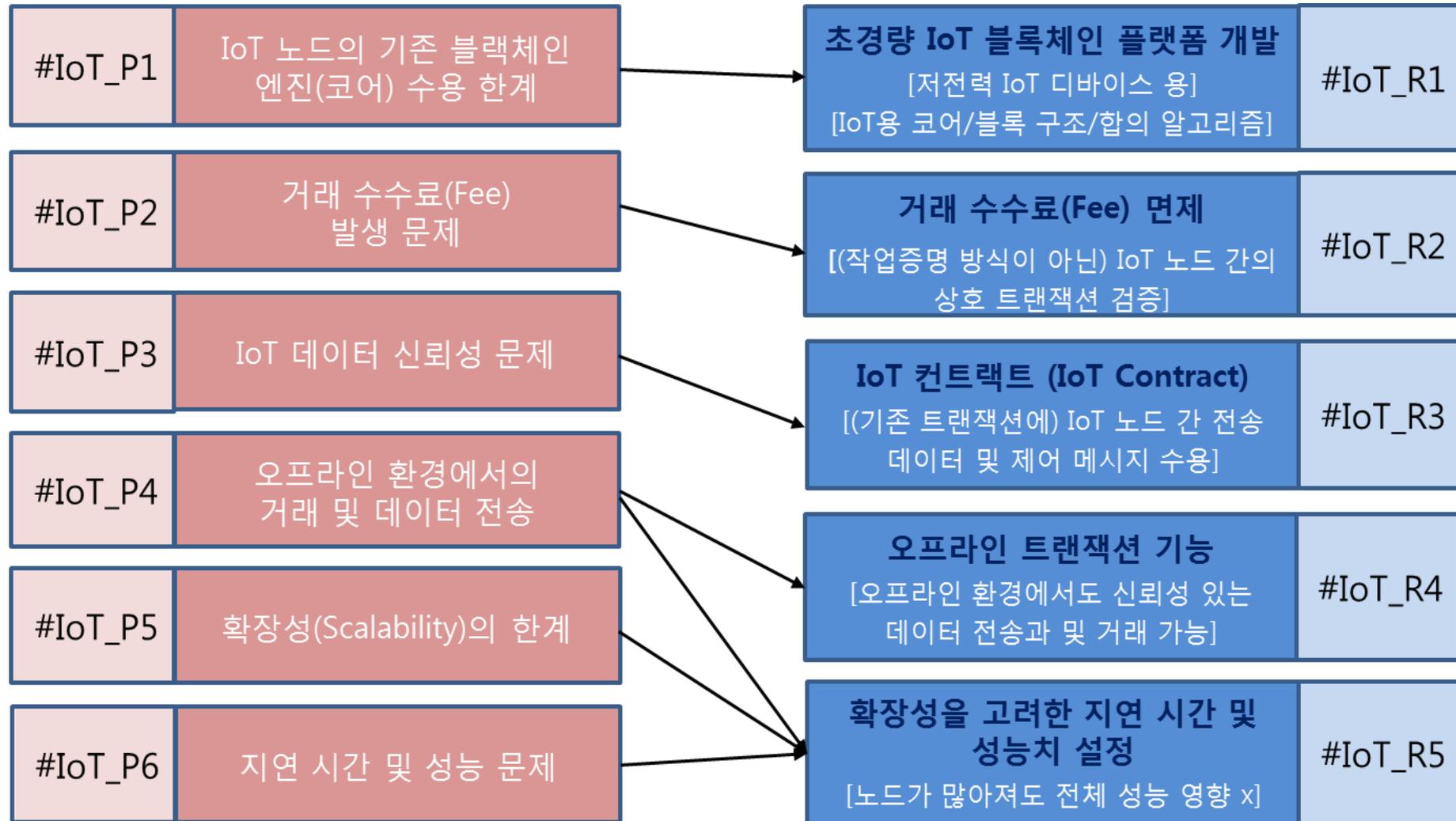
● 기존 블록체인 기술로부터 IoT 블록체인 개발 시 고려해야 할 문제점

#IoT_P1	<p>IoT 노드의 기존 블록체인 엔진(코어) 수용 한계 (Tangle의 Light Node는 Full Node와, ADEPT의 Light Peer는 Standard Peer와의 협력으로 트랜잭션을 발생 가능. 저전력 IoT 노드(Drone/Smart Phone/IoT GW etc.)를 Full Node/Standard Peer 형태로 구축할 수 없다면 메인 네트워크와 단절되는 환경에서는 트랜잭션 처리가 불가능)</p> <ul style="list-style-type: none"> - 저전력 기반 IoT 디바이스에서 JVM, Middleware, Docker 등 탑재 불가 - PoW 작업 부담(Load)
#IoT_P2	<p>거래 수수료(Fee) 발생 문제</p> <ul style="list-style-type: none"> - 기존 블록체인 플랫폼은 사용자와 채굴자가 분리된 구조로 거래 수수료가 발생(Bitcoin Fee Rate, Ethereum Gas Rate 계속 상승 중)하여 IoT 환경의 소액결제에 부적합
#IoT_P3	<p>IoT 데이터의 신뢰성 문제</p> <ul style="list-style-type: none"> - 사용자와 IoT 노드 간, 또는 IoT 노드 간의 Configuration, 전송 데이터 및 제어 메시지가 제3자에 의해 위변조 가능성
#IoT_P4	<p>오프라인 환경에서의 거래 및 데이터 전송</p> <ul style="list-style-type: none"> - 비동기적인 IoT 환경에서는 네트워크에 지속적 연결이 용이하지 않을 수 있음 - 오프라인 환경(메인 네트워크와 연결이 되지 않은 상태)에서도 안전한 데이터 전송과 거래 보장
#IoT_P5	<p>확장성(Scalability)의 한계</p> <ul style="list-style-type: none"> - 기존 블록체인 플랫폼은 참여 노드 수가 많아지면 시스템 성능이 현저히 저하
#IoT_P6	<p>지연 시간 및 성능(Latency & Performance)</p> <ul style="list-style-type: none"> - 많은 노드들이 참여하는 IoT 플랫폼에서 지연 시간 및 성능(TPS)는 매우 중요 - IoT 데이터 및 제어 메시지 포함하는 IoT Contract 적용 시, 실시간성 강화 필요

JVM: Java Virtual Machine



Future R&D Trends of IoT Blockchain



1. 공개 SW 과제 개발 프로세스 및 추진체계 @ETRI (예시)
2. IoT Blockchain
3. Consortiums/Platforms/Services/Projects
4. Trends
5. Deep Dive : IOTA Tangle



IOTA

- IOTA : 블록체인 기술을 IoT 플랫폼에 적용하여 실제 운영하고 있는 재단
 - founded by 4 individuals: David Sønstebø, Sergey Ivancheglo, **Dr. Serguei Popov** (Whitepaper(2016.04.03) 저자) and Dominik Schiener in 2015.
- MIOTA
 - IOTA 재단의 코인(암호화폐)
 - 2015년 10월 21일 런칭
 - ICO(Initial Coin Offering)를 통해 약 27억개 코인 발행 및 유통



IOTA Ranking

출처: <https://coinmarketcap.com/>
(2018년 8월 15일 현재)

Top 100 Cryptocurrencies By Market Capitalization

Cryptocurrencies ▾ Exchanges ▾ Watchlist USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	\$109,532,919,984	\$6,364.06	\$4,435,034,137	17,211,175 BTC	4.02%	...
2	Ethereum	\$28,832,038,485	\$284.50	\$1,824,638,549	101,341,269 ETH	8.39%	...
3	XRP	\$11,285,520,139	\$0.286635	\$290,274,935	39,372,399,467 XRP *	8.73%	...
4	Bitcoin Cash	\$8,974,542,770	\$518.93	\$373,376,003	17,294,188 BCH	5.39%	...
5	EOS	\$4,171,639,405	\$4.60	\$624,883,076	906,245,118 EOS *	5.27%	...
6	Stellar	\$4,160,568,935	\$0.221640	\$84,291,869	18,771,748,950 XLM *	3.33%	...
7	Litecoin	\$3,211,725,267	\$55.51	\$267,207,541	57,856,459 LTC	5.62%	...
8	Cardano	\$2,465,534,032	\$0.095095	\$81,175,639	25,927,070,538 ADA *	2.57%	...
9	Tether	\$2,408,468,082	\$1.00	\$2,939,384,482	2,407,140,346 USDT *	-0.27%	...
10	Monero	\$1,458,678,866	\$89.38	\$24,269,422	16,319,260 XMR	8.48%	...
11	IOTA	\$1,321,370,836	\$0.475394	\$39,427,976	2,779,530,283 MIOTA *	12.17%	...
12	TRON	\$1,288,363,042	\$0.019595	\$110,563,422	65,748,111,645 TRX *	9.39%	...



The Tangle

A Blockchain **without the Blocks** and the **Chain**



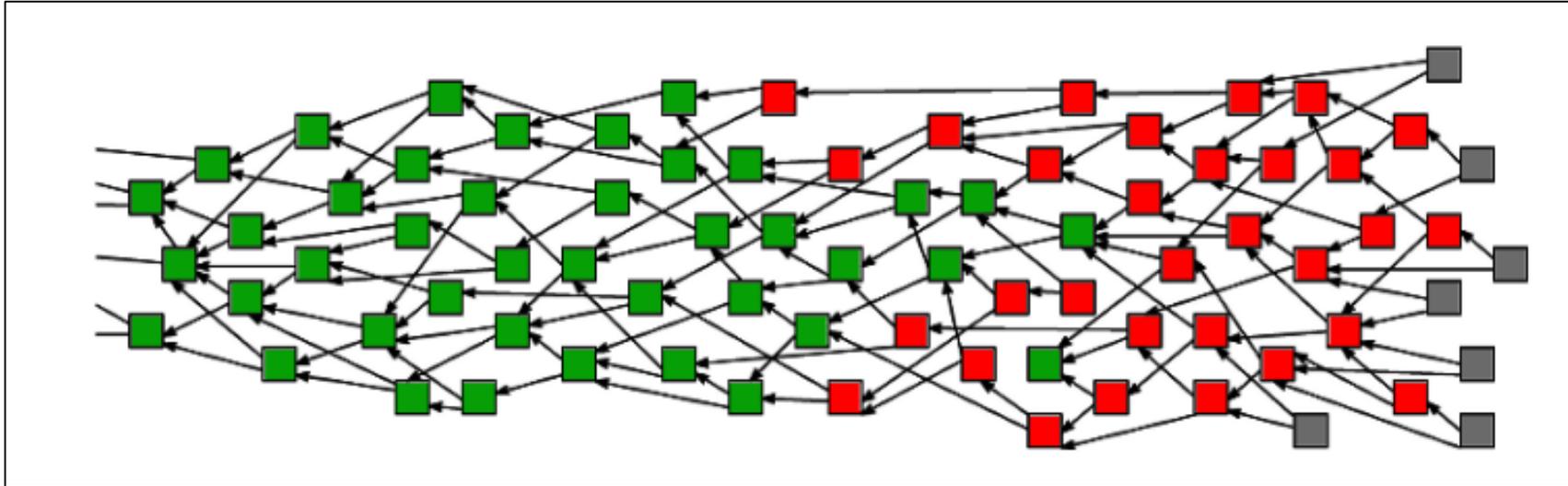
⚠ IOTA IS CURRENTLY IN BETA

It should be noted that IOTA is currently still in Beta. This means that the current Java implementation is an **reference implementation**. Major improvements to performance, features as well as ease of use will be made over the coming months.



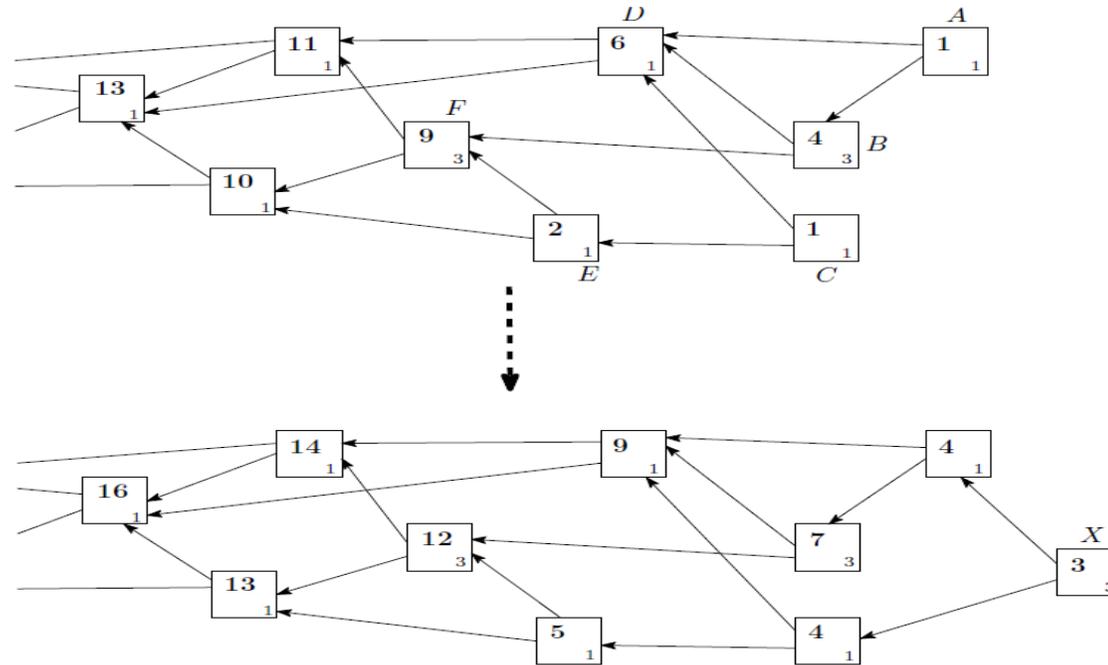
- Tangle 이라고 불리는 새로운 형태의 분산 원장 사용
 - 기존 블록체인의 사용자 및 채굴자 구분 구조 탈피
 - 사용자가 직접 검증(Transaction 승인)에 참여(PoW 방식)
 - 신규 Transaction 1개 발생을 위해 기존 Transaction 2개 검증 필수
 - 기존 Transaction (= Tip) 선택하는 알고리즘: MCMC (Markov Chain Monte Carlo)
 - 블록 형성을 위한 별도 과정이 존재하지 않아 거래 수수료 및 고성능 하드웨어 자원 불필요
- IoT 환경에서 마이크로 payment를 활성화를 목적으로 전송 수수료 면제(No Fee) 개념 도입
- 방향성 비-사이클 그래프(Directed Acyclic Graph, DAG) 알고리즘을 이용한 검증(approve) 기법 적용
- 근본적으로 블록체인과 동일한 분산 데이터베이스 및 P2P 네트워크를 이루고 합의와 확인(consensus and validation) 메커니즘 보유





- 초록 : 합의가 이미 이루어진 거래
- 빨강 : 아직 100% 승인이 이루어지지 않은 불확실한 거래
- 회색 : 팁/미확인된 거래

- Tangle에서 Transaction(거래)이 진행/검증되는 4 단계
 1. 서명하기: 개인 키로 거래 인풋(Tx Hash)을 서명
 2. 팁 선발: 한 거래를 통해 다른 두 개의 팁(미확인된 거래들)을 선택하기 위해 Markov Chain Monte Carlo(MCMC) 알고리즘 사용
 3. 작업 증명: Hashcash
 4. 신규 Transaction(거래)가 네트워크에 브로드캐스트 됨 → "팁"



- cumulative weight of a transaction: the own weight of this transaction plus the sum of own weights of all transactions that approve our transaction directly or indirectly.
- The small numbers in the SE corner stand for the own weights of the transactions, while the (bigger) bold numbers are the cumulative weights
- For example, the transaction F is approved, directly or indirectly, by the transactions A;B;C;E. The cumulative weight of F is $9 = 3 + 1 + 3 + 1 + 1$, the sum of the weight of F and the weights of A;B;C;E.
- On the top picture, the only unapproved transactions (the tips) are A and C.
- When the new transaction X comes and approves A and C, it becomes the only tip; the cumulative weight of all other transactions increases by 3 (which is the weight of X).

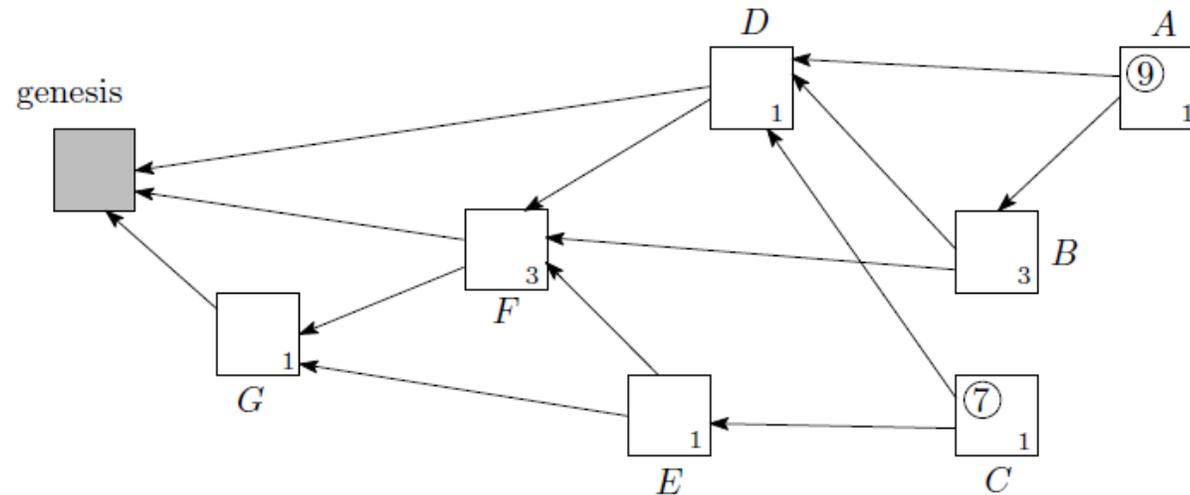


Figure 2: On the calculation of scores (circled)

- For the discussion of approval algorithms, we need also to introduce some other variables.
 - *height*, as the length of the longest oriented path to the genesis;
 - *depth*, as the length of the longest reverse-oriented path to some tip.
- For example, on Figure 2, G has height 1 and depth 3 (because of the reverse path F;B;A), while D has height 2 and depth 2.
- By definition, the score of a transaction is sum of own weights of all transactions approved by this transaction plus the own weight of the transaction See Figure 2.
- Again, the only tips are A and C. Transaction A approves (directly or indirectly) transactions B;D; F;G, so the score of A is $1 + 3 + 1 + 3 + 1 = 9$. Analogously, the score of C is $1 + 1 + 1 + 3 + 1 = 7$.



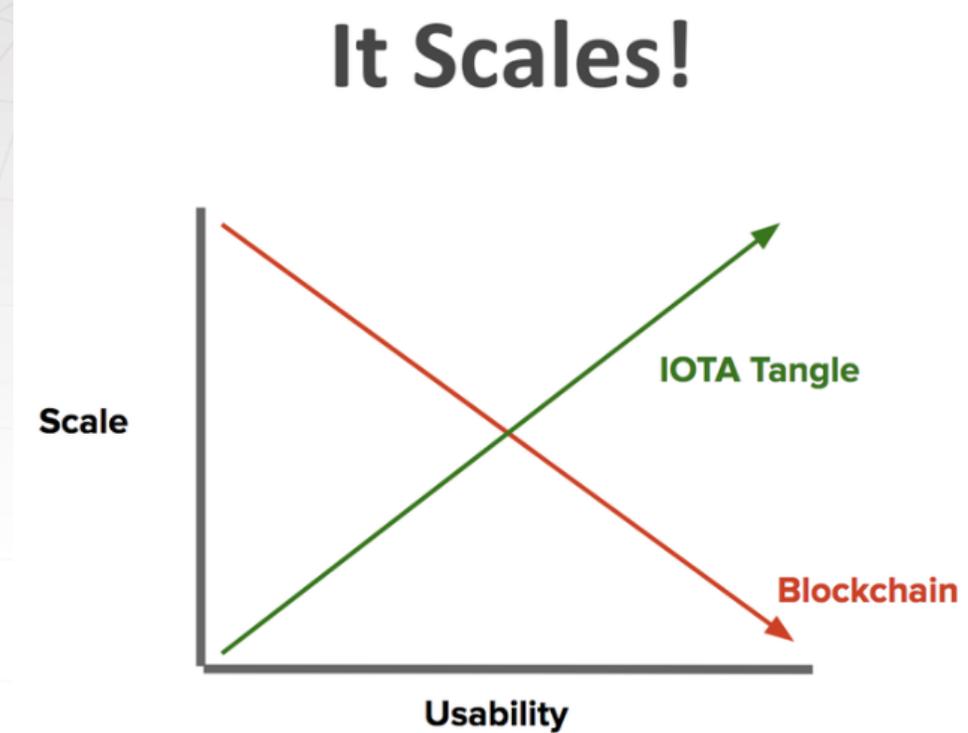
- (In Progress) weight, score 정보를 참조하여 tip을 선택하는데, 아직까지 취약점이 많아서 계속 수정 중
- (We also notice that the approval strategy may be further modified)
- Nevertheless, it is still worth considering the simplest tip selection strategy ("**approve two random tips**"), since it is the easiest to analyze, and therefore may give some insight about the qualitative and quantitative behavior of the system.
- In fact, the author's feeling is that **the tip approval strategy is the most important ingredient for constructing a tangle-based cryptocurrency**. It is there that many attack vectors are hiding. Also, since there is usually no way to enforce a particular tip approval strategy, it must be such that the nodes would voluntarily choose to follow it.



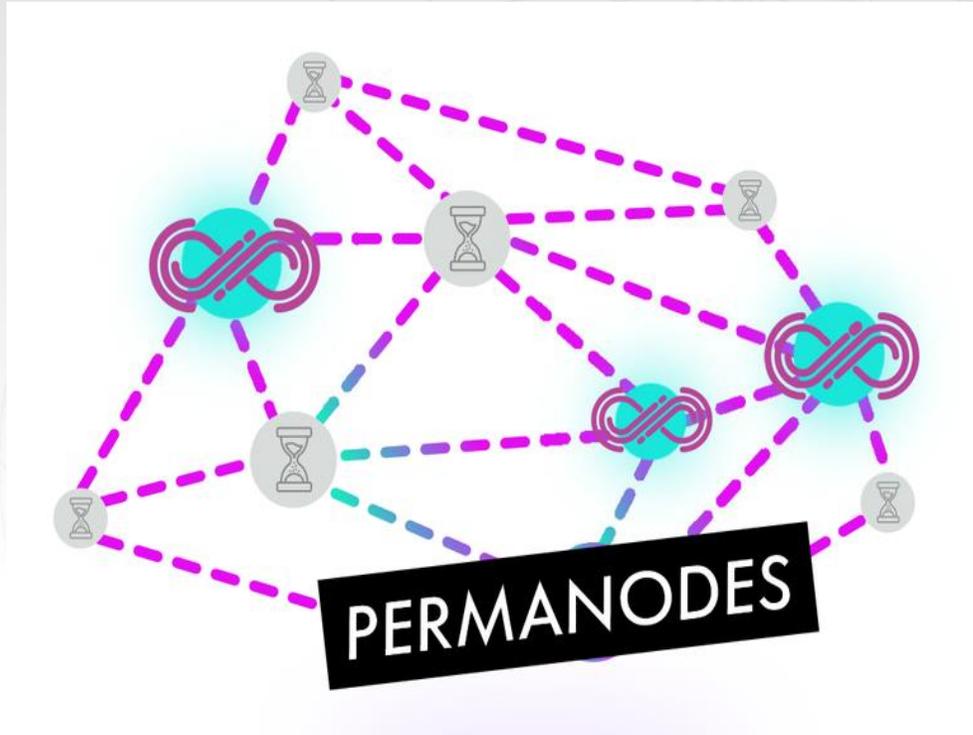
No Transaction Fees



- 채굴자 없이 거래의 유효성 합의를 얻어낸다는 특징
- 아이오타는 10원보다 더 적은 가치의 P2P를 송금인 혹은 수령인에게서 수수료를 청구하지 않고도 보낼 수 있는 첫 번째 거래 지불 프로토콜
- 현재 및 미래의 마이크로 페이먼트뿐만 아니라 나노 페이먼트 사용 사례의 근간



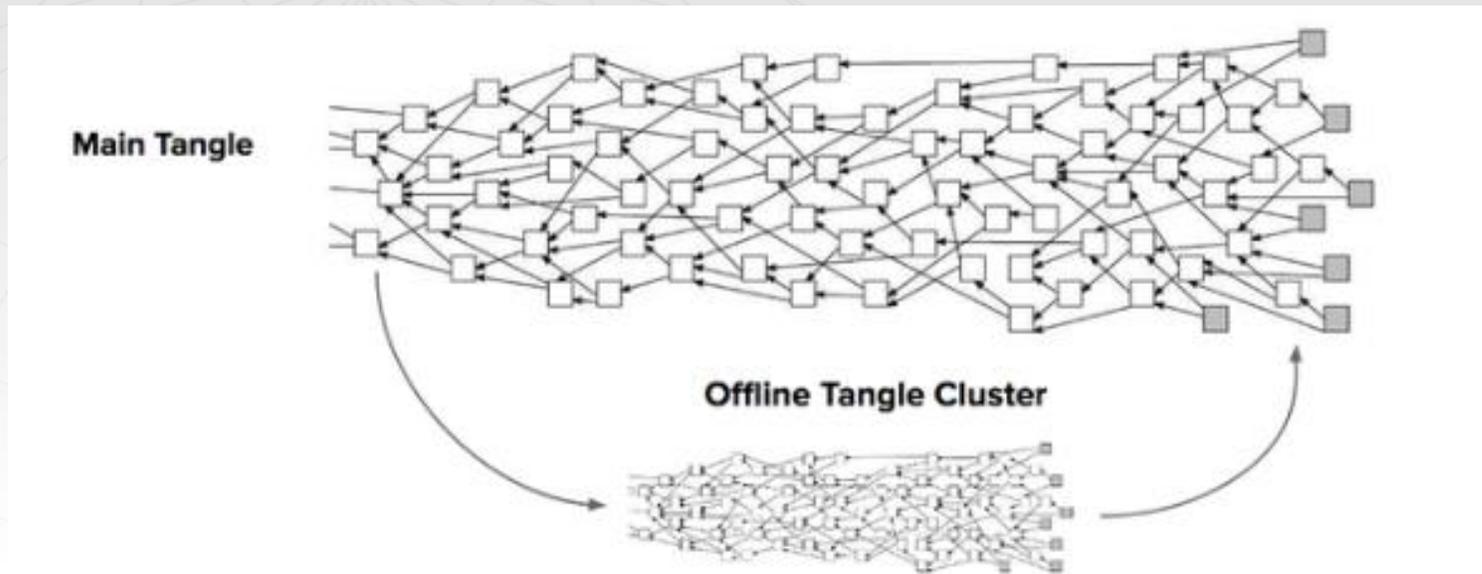
- 기존 블록체인의 거래들이 순차적인 간격을 두고 처리되지 않고 평행적으로 이루어지는 덕분에 많은 거래가 이루어져도 아이오타는 문제없이 확장 혹은 증가 가능
- 더 많은 거래가 이루어지면 그만큼 탱글 또한 더 효율적이고 안전



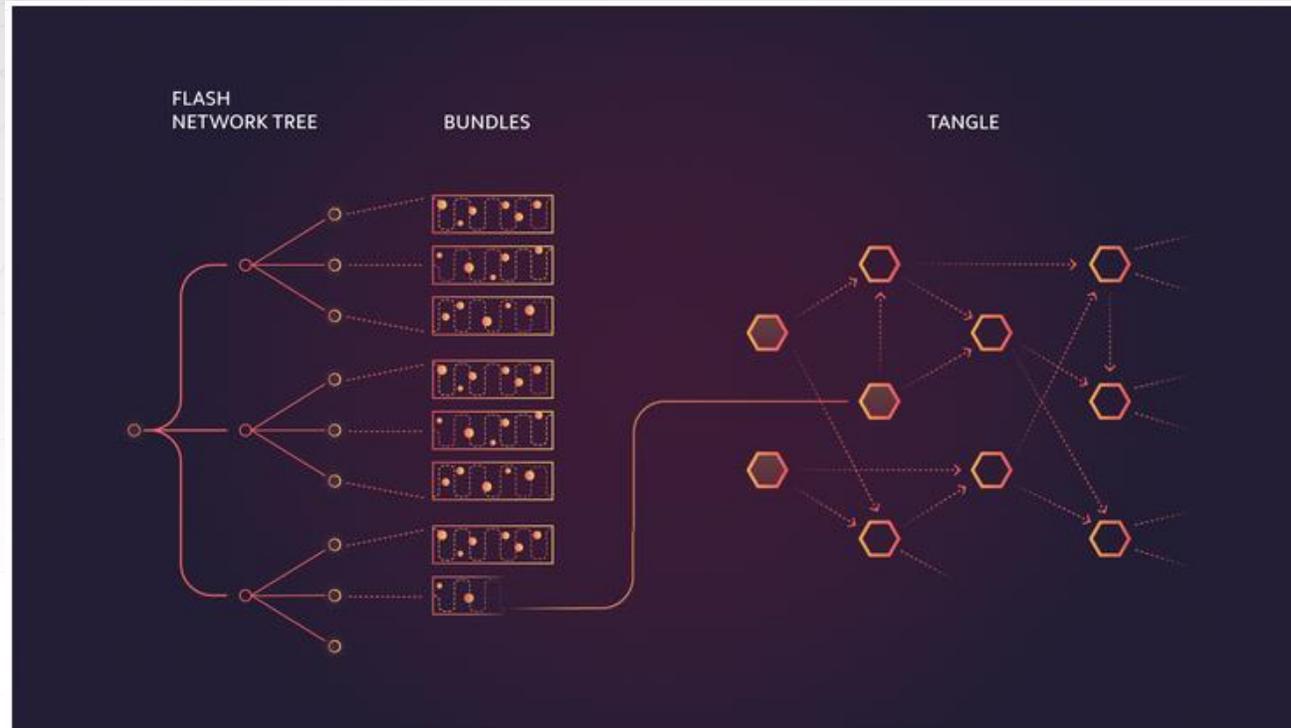
- 원장의 데이터가 영구적으로 접근 가능하고 보관되어야 하는 특정한 어플리케이션(예, 투명 검사(transparent audit) 지원
- 모든 탱글 히스토리와 데이터를 영구적으로 보관 (2017년 기준 약 30GB)
- 현 진행 상황: 알파 테스트



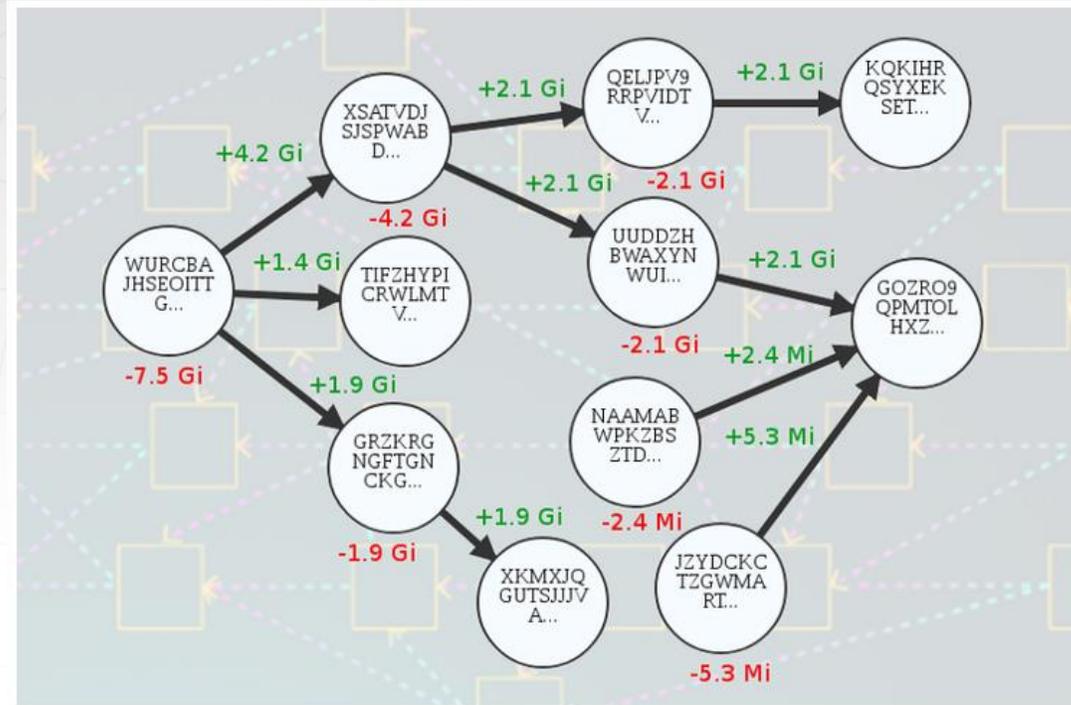
- 사물 인터넷을 구성할 디바이스들을 위해 "스냅샷"(snapshotting) 사용
- 전체 원장이 너무 많은 저장공간을 차지하면 "스냅샷"을 통해 가장 최근의 부분만 유지 가능
- IoT 디바이스가 저장할 수 있게끔 원장(ledger) 데이터베이스를 아주 작게 만들어줌
- 동일 주소에서 동일 주소로 보내어진 여러 개의 트랜잭션을 하나의 레코드로 묶어서 처리
- 현 진행 상황: 개발(2017. 8 ~) 중 & Test



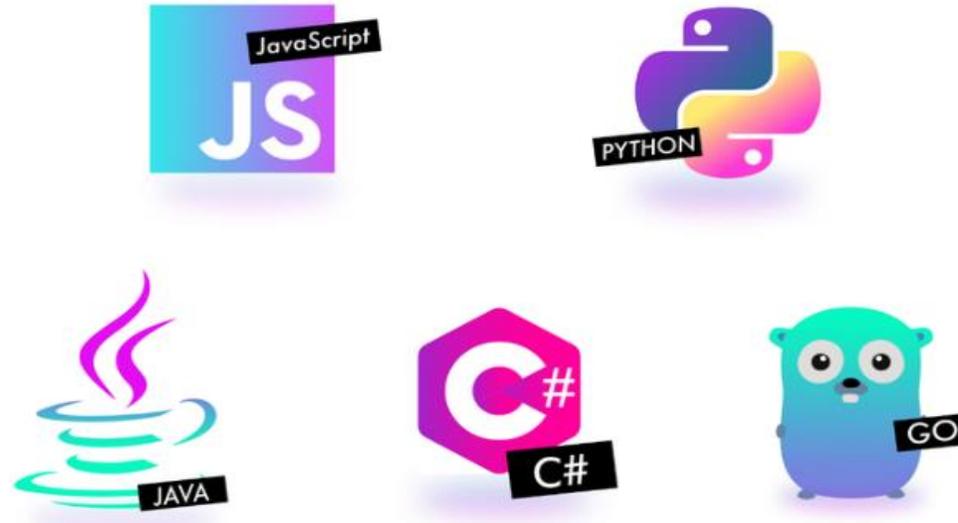
- Offline Transactions = Partitioning
- 탱글을 통해 사용자의 디바이스 집단이 메인 네트워크에 자유자재로 분리/통합 가능
- 비동기적인 사물 인터넷 환경(항상 네트워크에 연결 x)에 아주 중요한 필수 요소
 - ❖ IoT 디바이스(GW, Sensor Node, Drone, Smart Phone)의 Full Node화 필수
- 오프라인 환경에서도 내부 통신 프로토콜 (ZigBee, 블루투스 LE 등등)을 통해 안전한 데이터 전송 및 거래 가능
- 현재 개발 중



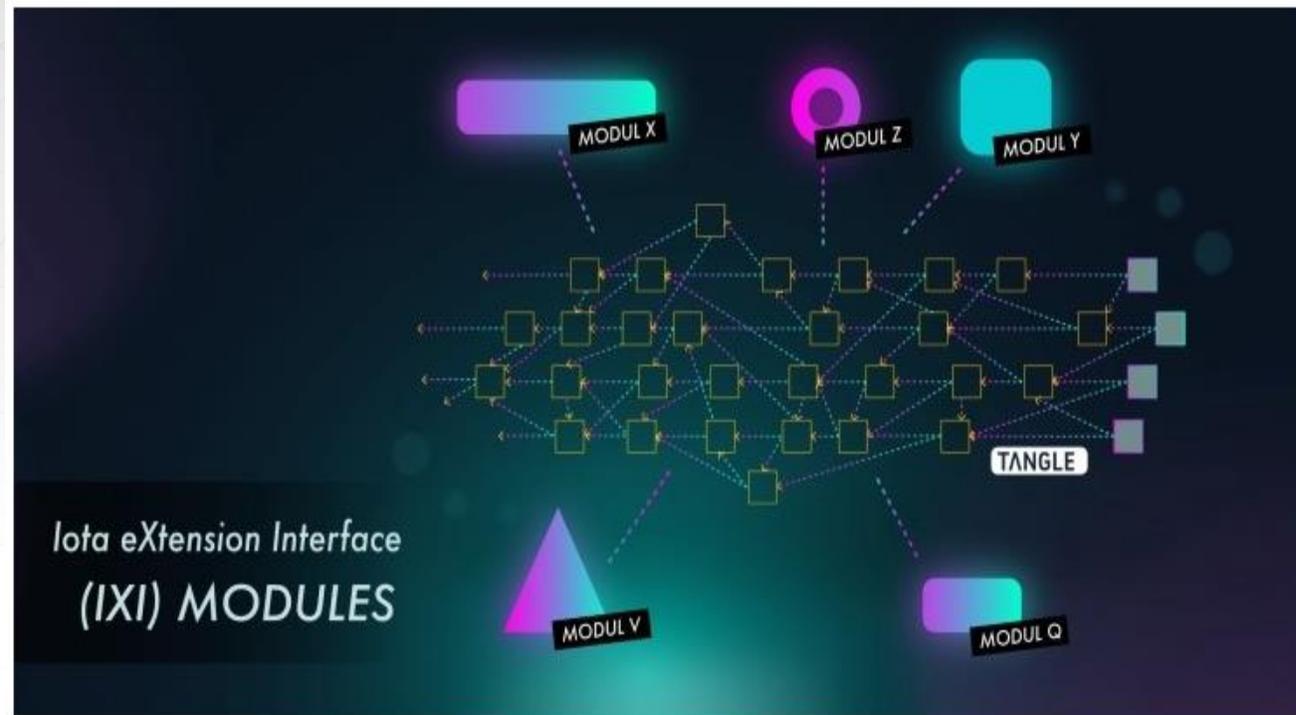
- 높은 처리량의 거래들을 신속하게 처리하는 양방향성 **off-Tangle** 지불 채널
- 비트코인의 라이트닝(Lightning) 네트워크나 이더리움의 레이든(Raiden) 네트워크와 유사
- 각각의 거래가 승인되는 것을 기다리지 않고, **거래자들끼리 빈번한 거래** 가능
- **IOTA 네트워크에 단 두 거래만이 발생** : 플래시 채널의 첫번째/마지막 거래
- 두 사용자 사이에 토큰 스트리밍이 필요한 특정한 사용 사례에 적용
- **현 진행 상황: 베타 테스트**



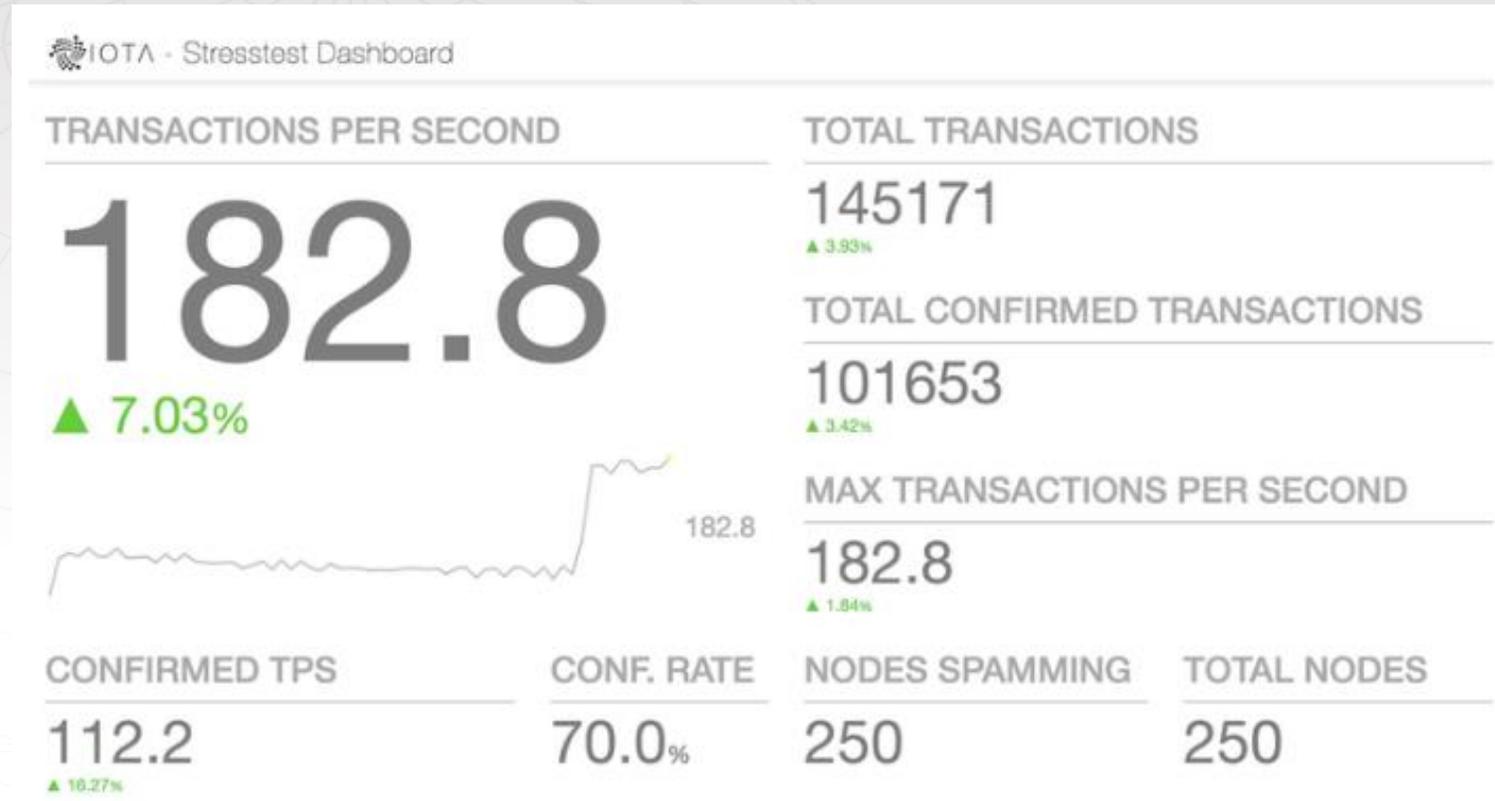
- 가장 큰 보안 문제들은 대부분 주소 재사용에서 기인
- IOTA는 결정적인(deterministic) 주소 생성을 사용하여 코인을 받을 때마다 새로운 주소로 수신
- 사용 시, 이 주소들을 하나의 페이먼트로 통합(모든 주소들의 연계 증명) 필요
- 추후 해결 과제(Update 예정) : University College London의 IOTA팀에서 개발 중



구현 언어	현 황	비 고
• JavaScript	Done	현재 운영 중
• Java	Done, Stresstest 예정	현재 운영 중
• C++	In early port stage	IoT 디바이스에 Java VM이 설치될 필요가 없고, 실시간으로 기계 코드로 컴파일되기 때문에 IoT에 더 적합
• Rust	Early development	사물 인터넷을 위한 가장 촉망되고 빠른 언어들 중 하나
• Go	Early development	구글 개발 언어



- IXI : IOTA eXtension Interface
- 아이오타 플랫폼 모듈러 역할
- 목적에 최대한 적합하게끔 각각의 요소를 하나의 어플리케이션으로 제작
- 기능들 중 하나만 사용할 때 각각의 기능에 오버헤드를 유발하지 않고서 프로토콜의 활용을 자유자재로 조정 가능



- 현재 1000 TPS를 목표로 하는 더 큰 스트레스 테스트를 준비하는 과정



The screenshot shows a blog post header with navigation links (HOME, ANNOUNCEMENTS, VISION, RESEARCH & DEVELOPMENT, ECOSYSTEM, WELCOME TO THE IOTA FOUNDATION!, IOTA.ORG) and a search icon. The author is David Sonstebø, Founder of IOTA, with a 'Follow' button. The title is 'IOTA Ecosystem Fund (\$10 million)'. Below the title is a large graphic with the text 'IOTA ECOSYSTEM FUND \$10.000.000'.

Every great open source project has a great ecosystem surrounding it, in many ways it is the defining characteristic that separates a mediocre project from a great one. A thriving ecosystem is a prerequisite for long term success. In that spirit we are very happy to announce the 'IOTA Ecosystem Fund', which is valued north of \$10,000,000. This fund is entirely dedicated towards fostering growth of IOTA through incentivizing participation in expanding and shaping the ecosystem.

- 아이오타 생태계 개발을 위한 계획 중 하나
- 커뮤니티 멤버와 파트너들과 함께 아이오타의 이해와 인식/관심을 높이기 위한 프로젝트, IXI 모듈 연구, 프로토타입, 그리고 사용 사례 개발을 위해 1천만 달러 이상의 자금 조달
- 자금 지원 요청 : <https://blog.iota.org/iota-ecosystem-fund-2-million-f6ade6a4d8ba>

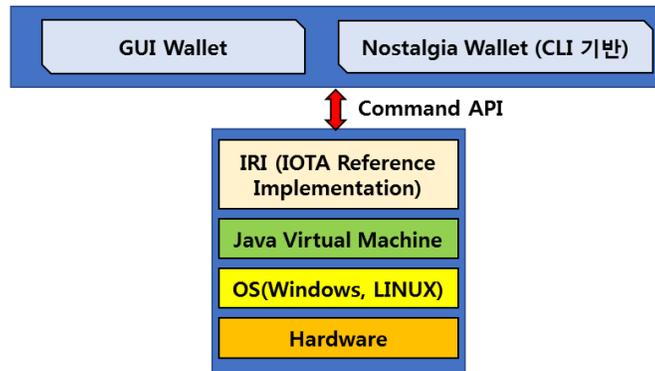


Tangle Install부터 트랜잭션 Confirm까지



● Full Node

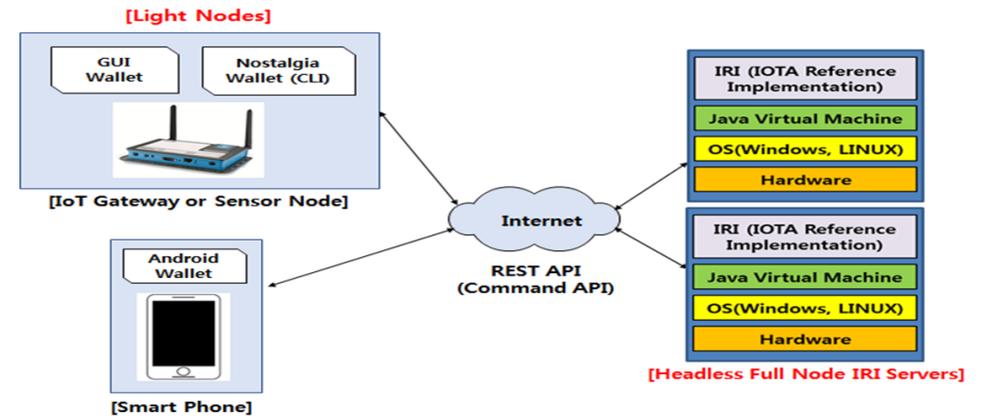
- ❖ Java VM 필요
- ❖ Local에 IOTA 코어(IRI, IOTA Reference Implementation) 설치
- ❖ GUI Wallet or Nostalgia Wallet(CLI 방식)을 통해 IRI 연동
- ❖ Static IP 필요
- ❖ Neighbors 필요



[전용 Wallet을 가지고 있는 Full Node 구성도]

● Light Node (with Headless Full Node)

- ❖ Wallet을 이용한 원격 구축
- ❖ Local에 Wallet(GUI/Nostalgia/Android) 설치
- ❖ 원격으로 IOTA 코어가 설치된 외부 Headless IRI Server 연동
 - ✓ Headless Full Node IRI : GUI Wallet이 포함되지 않은 Full Node. 원격에서 여러 Wallet이 동시에 접속 가능
- ❖ Java VM 필요 x



[Headless Full Node IRI와 Light Node(Wallet 만 탑재) 간의 구성도]



● Full Node(Headless) IRI 다운로드 및 실행

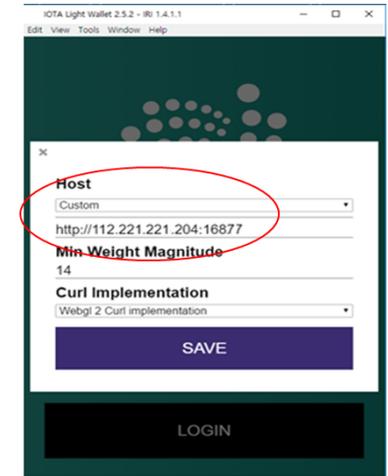
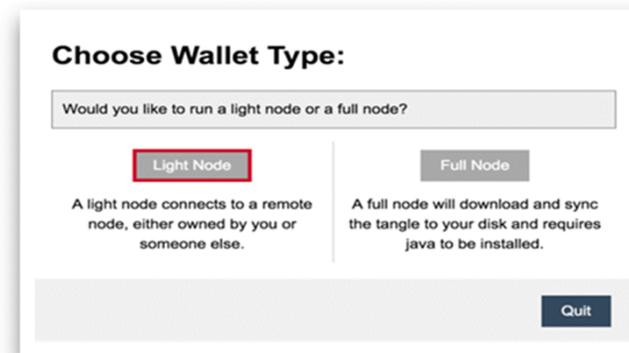
- ❖ 실행환경 : 64bit Linux, Windows, MacOS, 64bit **java 8u66 이상** (www.oracle.com)
- ❖ 다운로드 링크 : <https://github.com/iotaedger/iri/releases>
- ❖ 파일명 : iri-1.4.1.2.jar

```
java -jar iri-1.4.1.1.jar -p 14265 -n "udp://NeighborIP:14600  
tcp://NeighborIP:15600"
```

- p : http 명령을 수행하는 포트번호
- u : udp 포트, 설정하지 않을 시 기본포트는 14600
- t : tcp 포트, 설정하지 않을 시 기본포트는 15600
- d : debug 모드
- remote : 원격접속을 허용
- n : Neighbor의 IP address

● Light Wallet 다운로드 및 설치

- ❖ 다운로드 링크 : <https://github.com/iotaedger/wallet/releases>
- ❖ 파일명
 - ✓ iota-2.5.4.x86_64.rpm : Redhat, CentOS, openSUSE 용
 - ✓ IOTA.Wallet-2.5.4.dmg : MacOS 용
 - ✓ IOTA.Wallet.Setup.2.5.4.exe : Windows 용
 - ✓ iota_2.5.4_amd64.deb : Debian, Ubuntu 용
- ❖ Windows용 (IOTA.Wallet.Setup.2.5.4.exe) 실행
 - ✓ Wallet Type을 Light Node로 설정



- ✓ Node Configuration – HOST는 Custom – Headless Full Node 주소 입력



- This is a list of public IOTA nodes that you can use with your Light Wallet. All addresses listed on this site are dedicated 24/7 nodes hosted by volunteers from the IOTA community.

Iota Nodes
HOME ADD NODE EDIT NODE CONTACT

Open Directory of Public IOTA Nodes

This is a list of public IOTA nodes that you can use with your Light Wallet. All addresses listed on this site are dedicated 24/7 nodes hosted by volunteers from the IOTA community. We are not affiliated with The IOTA Foundation, just enthusiastic about its future.

As the lists on iota.dance/nodes and iotalad.org are listed publicly, I have added them here for convenience. If you host a node and would like it listed here, please [submit your info](#).

The table is sorted by its 'online' status (and then by its 'id' in the database). If you wish to perform your own multi-column sort, just hold the [Shift] key and click the next column header.

online	online%	synced	synced%	offline	offline%	total
101	69.18%	57	56.44%	45	30.82%	146

▶ Column Definitions

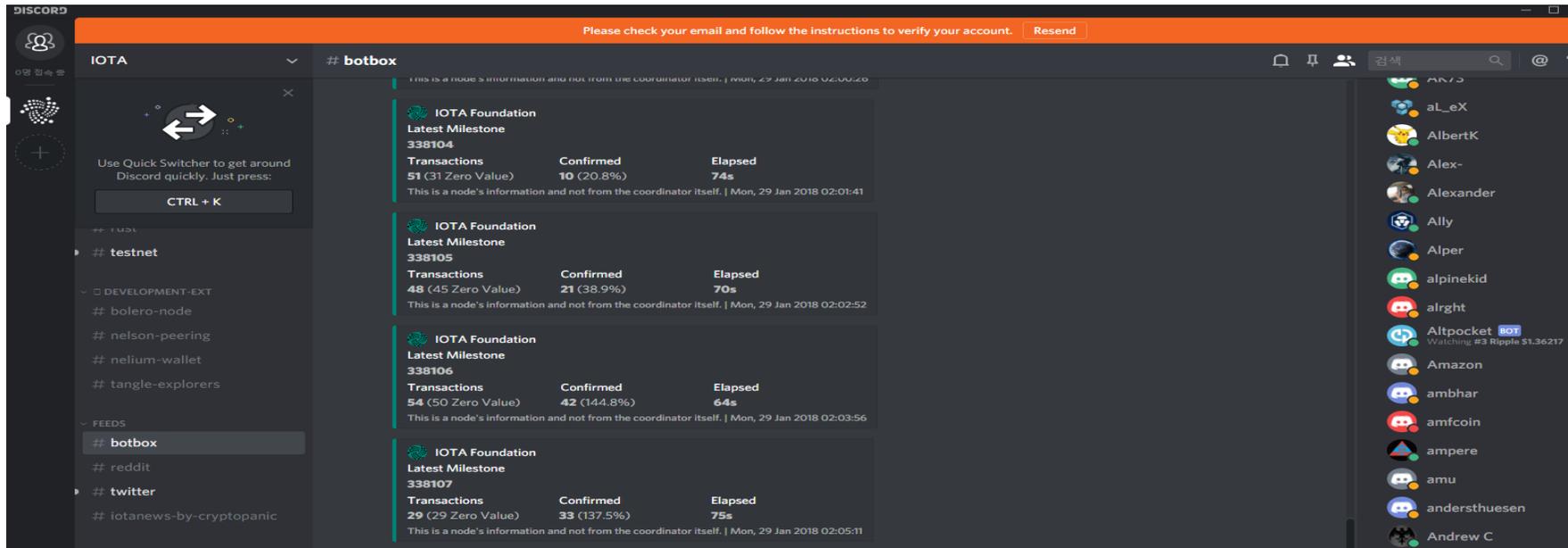
node ^	co...	st...	city ^	iri ver	on...	pr...	mem usage	index	latest	sy...	ne...	tips	updated ^
https://node.iotanode.host:443	US	NY	New York	1.4.1.7	Yes	8	67.5...	338,...	337,541	No	11	776	01-29-2018 12:03 AM
http://iota.pathin.net:14265	ES		Madrid	1.4.2.0	Yes	16	45.7...	338,...	338,000	Yes	6	62	01-29-2018 12:03 AM
http://node.davidsiota.com:443	DE		Kassel	1.4.2.0	Yes	8	79.9...	338,...	338,000	Yes	5	14	01-29-2018 12:03 AM
https://potato.iotalad.org:443	DE		Frankfurt	1.4.1.7	Yes	4	19.3...	337,...	337,541	No	9	5,306	01-29-2018 12:03 AM
https://durian.iotalad.org:443	SG		Singapore	1.4.1.7	Yes	4	84.0...	338,...	337,541	No	9	5,301	01-29-2018 12:03 AM
https://peanut.iotalad.org:443	US	GA	Atlanta	1.4.1.7	Yes	4	79.8...	338,...	337,541	No	10	5,288	01-29-2018 12:03 AM
https://tuna.iotalad.org:14265	JP		Tokyo	1.4.1.7	Yes	4	56.7...	338,...	337,541	No	8	5,317	01-29-2018 12:03 AM
https://turnip.iotalad.org:14265	UK		London	1.4.1.7	Yes	6	59.6...	338,...	337,541	No	10	5,229	01-29-2018 12:03 AM
http://173.249.18.180:14265	DE		Kassel	1.4.2.0	Yes	4	50.5...	338,...	338,000	Yes	8	12	01-29-2018 12:03 AM
https://iotanode.us:443	US	CA	Mtn View	1.4.1.7	Yes	6	44.0...	338,...	337,541	No	13	5,218	01-29-2018 12:03 AM
http://iotanode.party:14265	DE		Kassel	1.4.1.7	Yes	12	75.8...	338,...	337,541	No	21	2,114	01-29-2018 12:03 AM



● Full Node 구축 시 Neighbor 필요

❖ 원장 동기화(Milestone Sync.)

- ✓ Milestone : 1분마다 **Coordinator(IOTA 재단에서 운용)**가 Tx를 검증하여 포함
- ✓ It should be noted that the coordinator will be made optional to the network by Summer(2017), and then completely removed once the network is large enough.



[[#botbox](https://discordapp.com/channels/의)]

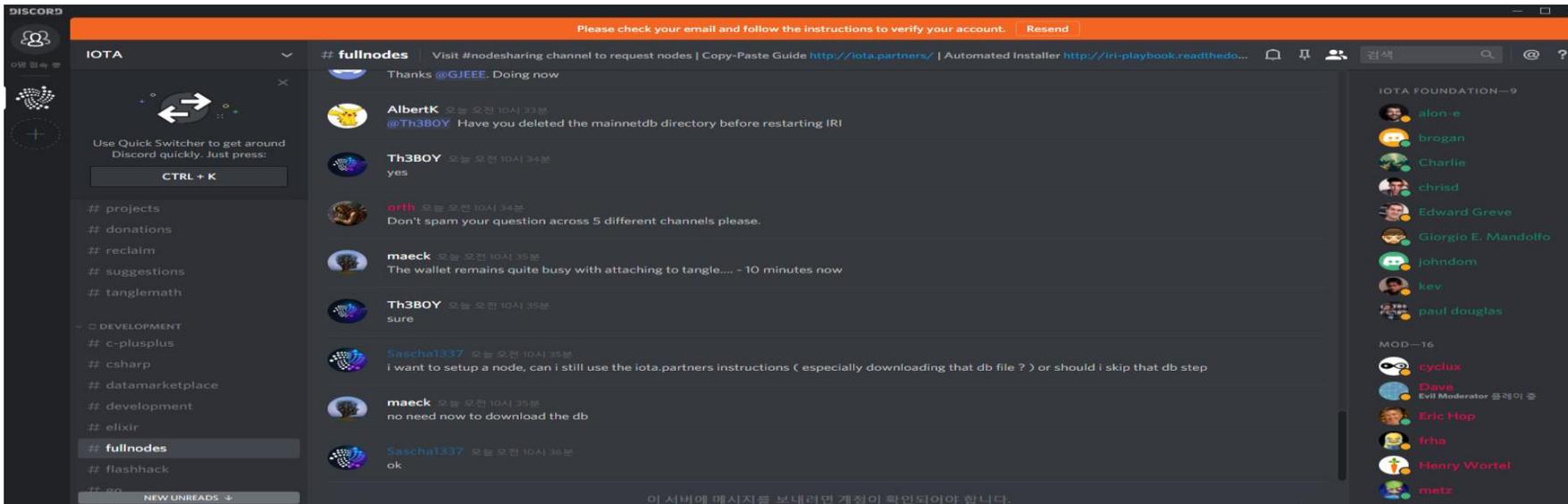
❖ 트랜잭션 Broadcasting

- ✓ 나의 Tx를 나의 Neighbor들로 Broadcast하고, 나의 Neighbor들은 각자의 Neighbor들로 Broadcast하여 전체 Tangle Network에 전파



Neighbor 검색 및 연결은 어떻게?

- ❖ <https://iotatangle.slack.com/> 접속 → 2018년 1월 중에 discord (<https://discordapp.com/>)로 변경
 - ✓ iotatangle 커뮤니티의 일원으로 가입한 후, #nodesharing 채널에서 Neighbor로 추가할 노드(사람)를 검색
- ❖ 서로 Neighbor로 추가하려면 DM(Direct Message)로 고정 IP address/Port를 공유
- ❖ Neighbor 연결 수는 7~9개를 권장, Neighbor와는 UDP 및 TCP로 연결
- ❖ <https://forum.helloiota.com/Community/Node-Sharing> (최근에 추가)



[Neighbor Search : <https://discordapp.com/channels/>의 #fullnodes or #nodesharing]

(주의)

- 1) 불특정 다수에서 선택. 악의적 사용자 가능성
- 2) Neighbor는 24시간 Tangle Network에 연결 되어야 함
- 3) 최근에는 CPU/Memory 성능을 제시하면서 Neighbor 모집
- 4) Neighbor 역할을 충실히 못하면 Disconnect & Re-search 필요

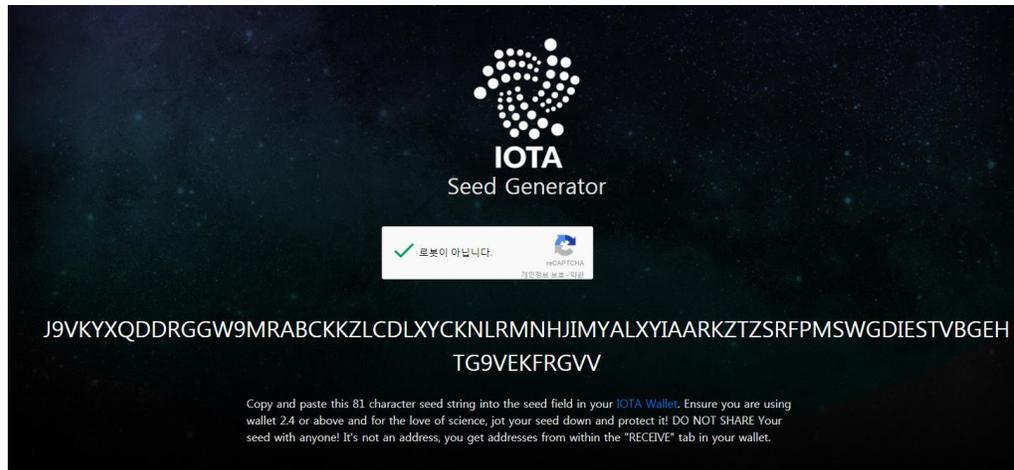


- 왜 IOTA Token(coin)을 구매해야 하나? → 현재 Tangle의 트랜잭션은 IOTA 거래 밖에 지원하지 않음
 - ❖ IOTA는 국내의 가상화폐 거래소(코인원)에서 구매 가능
 - ❖ 해외의 거래소(BitFinex, Binance)에서도 취급
 - ❖ 국내 거래소인(빗썸, 코인원 또는 코빗 등)에서 비트코인을 구입한 후, BitFinex 또는 Binace에 계정을 만들어 송금한 후, 이를 다시 IOTA로 환전하여 계정에 저장
 - ❖ 또한 개인의 Android Wallet/Light Wallet에 내려 받아 송금거래 가능
 - ❖ IOTA는 거래 단위가 Miota(1 Miota= 1,000,000 iota)로 거래가 되며, 현재 시점에는 약 Miota=0.5 USD 가치

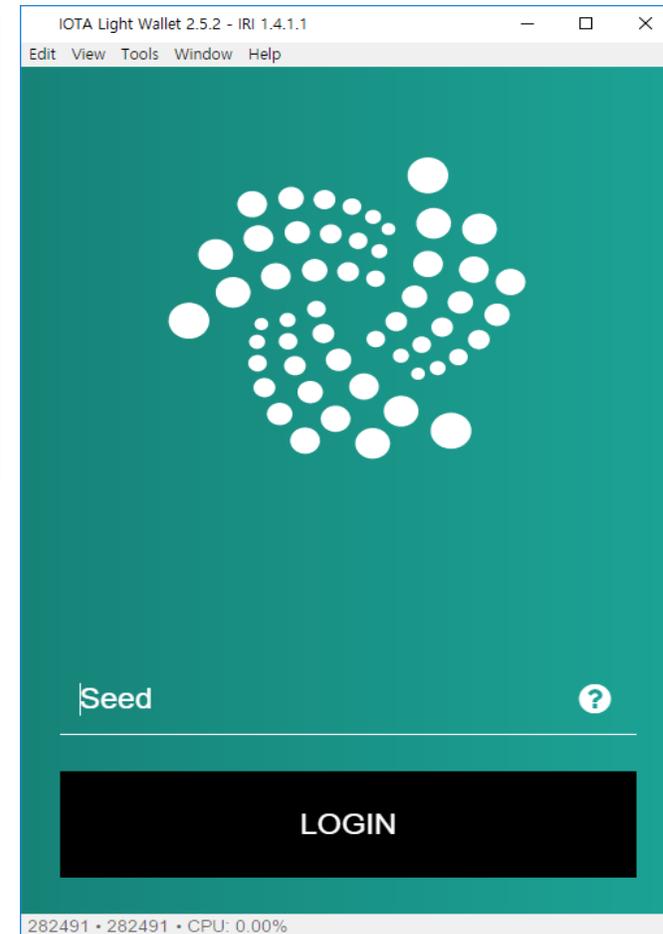


● Seed

- ❖ 로그인을 하기 위해 Seed 를 입력. Seed 는 대문자 A~Z 와 9로 81자를 생성
- ❖ Seed가 계정이며 IOTA가 귀속됨. Seed를 잊어버리면 IOTA를 찾을 수 없음
- ❖ Seed 생성 지원 Site
 - ✓ <http://iotaseed.co/> (Official IOTA - IOTA Seed Generator)



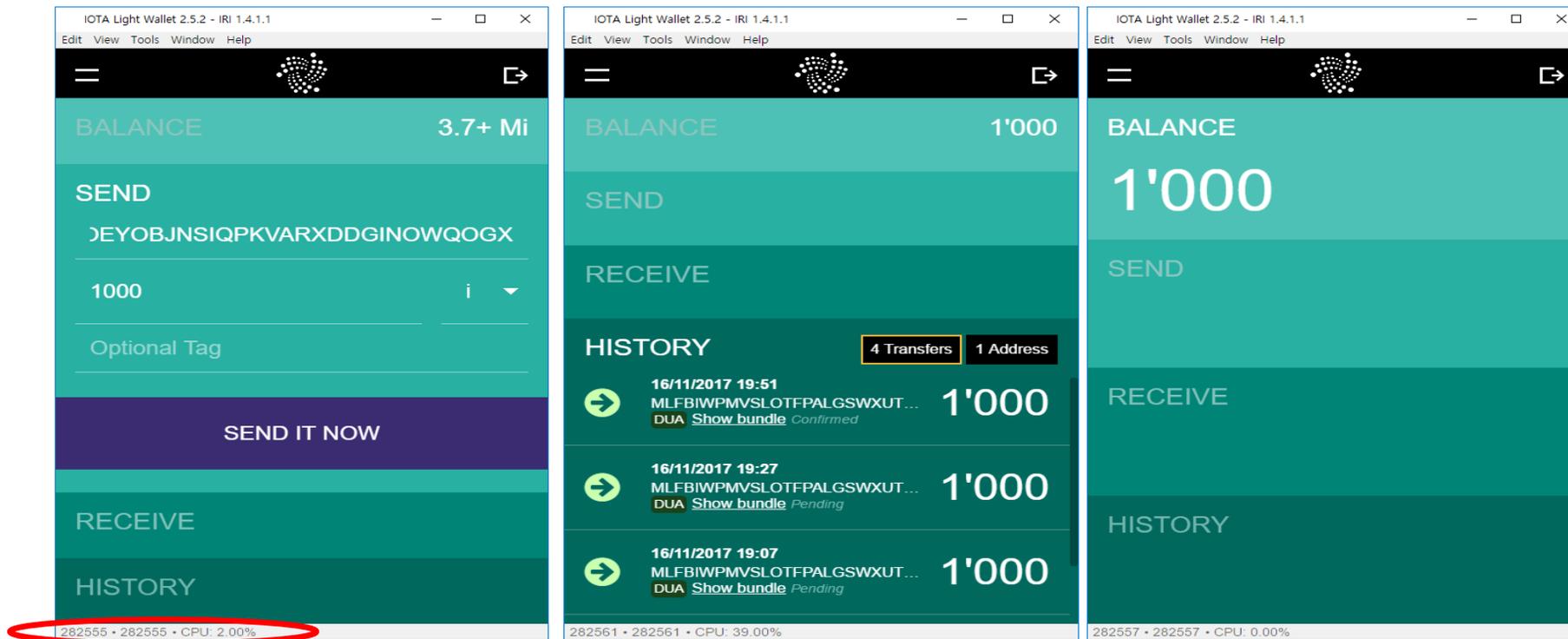
✓ <https://iotaseed.io/>





Transaction 절차

- ❖ IOTA 송신 : 다른 지갑에서 나의 지갑으로 1000 IOTA를 전송, SEND 메뉴에서 받을 지갑의 주소(나의 지갑)와 전송할 IOTA 수를 입력
- ❖ 트랜잭션 승인 과정 (HISTORY 화면) : 거래한 내역을 볼 수 있음. 거래가 시작되면 Pending 상태가 되고 Confirmed 상태가 되어야 거래가 완료된 것
- ❖ IOTA 수신 : 트랜잭션 승인 후, 내 지갑에서 1000 IOTA를 수신



[IOTA 송신]

[HISTORY]

[IOTA 수신]



The Tangle

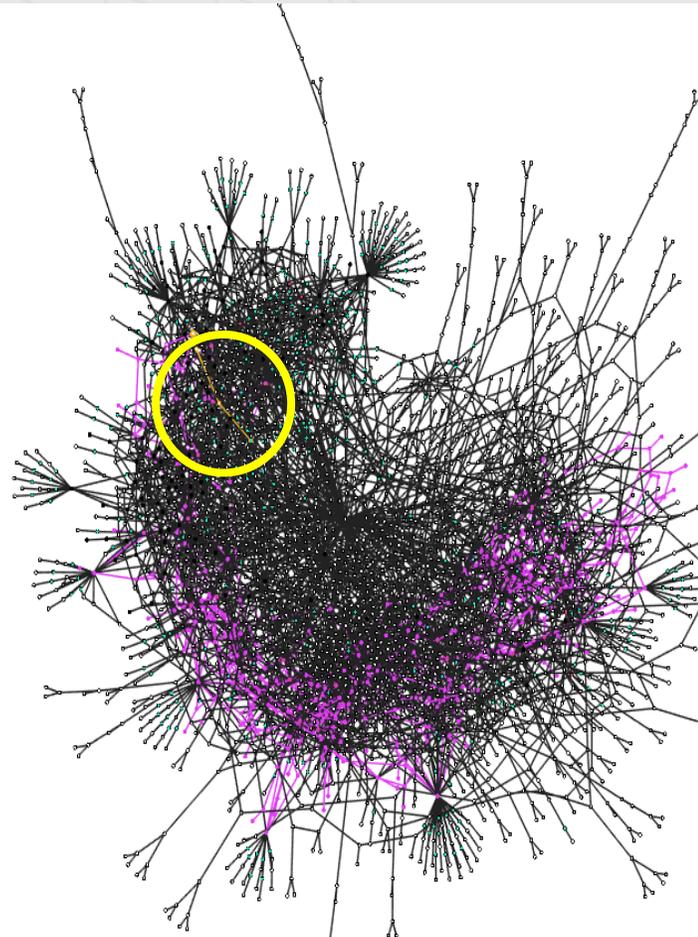
- tip
- milestone
- transaction
- confirmed

select a transaction to view

- confirmed by tx
- confirming tx

enter a tx hash

MJGYMGFBV9HJBTUKUCF



- remove floating tx
- limit to 4k nodes
- size by # of confms
- size by value
- lighten links

IOTA Light Wallet 2.5.4 - IRI 1.4.1.6

Edit View Tools Window Help

BALANCE 1 Mi

BUNDLE DETAILS

Hash: MJGYMGFBV9HJBTUKUCPPNCGFAMJWGYQM...

ZMWIX9KBECVDFQGDDIAL9ZJTFJFOHJPCGYG... 1 Mi

ASEOLGEWMMSV9ZTIHWDHAIQBRWUIVNFZ... -1 Mi

ASEOLGEWMMSV9ZTIHWDHAIQBRWUIVNFZCFX... 0

REBROADCAST

REATTACH

Persistence: Pending

10/01/2018 11:17

ZMWIX9KBECVDFQGDDIAL9ZJTFJ... -1 Mi

Show bundle Pending

323992 • 323992 • CPU: 7.00%

value: 1.00Mi
tx hash: MJGYMGFBV9HJBTUKUCPPNCGFAMJWGYQMNNJDMXAFEXGYSSJFXFDZLQGFVEHSIFBCAZROEMYVKKZZ9999

donate: XACMTQMWKHIJOUJYHTCXEKNBJZEGDMJFAKLIERACBYROLQCLIIWQZQKQWBOYUQFSUWWLVPAMGG9XMSDNRSUQZFC (0.000Mi)

tps: 0.75
nodes: 3134

Bundle Hash : MJGYMGFBV9HJBTUKUCPPNCGFAMJWGYQMNNJDMXAFEXGYSSJFXFDZLQGFVEHSIFBCAZROEMYVKKZZ9999



● IOTA Tangle 현황 분석

① Neighbor 노드 Search 및 추가가 용이하지 않음

- 현재의 IOTA Tangle은 다른 Node들과의 Neighbor 연결(가입 동의)을 통한 Private 형태로 운영
- IOTA는 신규 노드의 가입 및 동기화를 위해 7~9개의 Neighbor 연결을 권장
- 8개의 Neighbor 연결에 일주일 소요
- Neighbor 연결이 7~9개 정도로 제한되기에 적당한 수의 Neighbor를 이미 확보하고 있는 노드는 더 이상 Neighbor 추가를 허용하지 않으려 하는 경향이 있기 때문

② 트랜잭션 성공률이 낮음

- pending 상태의 트랜잭션은 "confirmed" 상태로 변경되어야 트랜잭션 처리 완료
- 본 시험 결과, 트랜잭션의 약 40% 정도가 실패
- 이 경우, 트랜잭션을 계속 reattach해야 하며, reattach시 confirm 확률은 높아짐(트랜잭션 승인에 reattach 과정을 포함해 평균 20분 이상 소요)
- reattach를 하지 않으면 영구적으로 pending으로 남음
- pending 상태에서 거래를 하게 되면 이중거래(Double Spending)로 거부됨
- 나의 트랜잭션이 승인되려면, 다른 노드에서 발생한 트랜잭션 처리 과정에서 특정 알고리즘(MCMC)을 통해 나의 트랜잭션이 선택/승인되어야 함 → 네트워크에서 발생하는 트랜잭션 수가 적어 승인 시간이 지연되는 것으로 판단

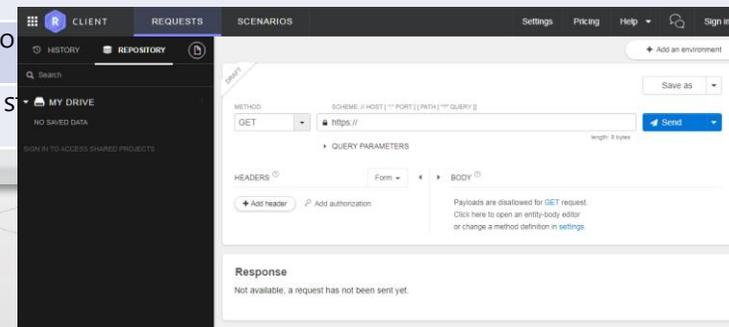
③ IOTA 시험 결과 정리

- 사물인터넷 환경에서 IOTA를 적용하여 서비스에 대한 가상화폐 결제 방식은 IOTA의 여러 차별화된 장점이 있는 반면에,
- IOTA가 현재 베타 버전임을 고려하여 시스템 운영의 안정성 및 기능 확장 등의 완성도를 좀 더 지켜보고 적용 필요



API Command	Description
getNodeInfo	Returns Information about your node
getNeighbors	Return the set of neighbors you are connected with, as well as their activity count. The Activity counter is reset after restarting IRI.
addNeighbors	Add a list of neighbors to your node
removeNeighbors	Removes a list of neighbors to your node
getTips	Returns the list of tips.
findTransactions	Find the transactions which match the specified input and return
getTrytes	Returns the raw transaction data (trytes) of a specific transaction
getInclusionStates	Get the inclusion states of a set of transaction
getBalances	Similar to getInclusionStates
getTransactionToApprove	Tip selection which returns trunkTransaction and branchTransaction. The input value is depth, which basically determines how many bundles to go back to for finding the transactions to approve
attachToTangle	Attaches the specified transactions (trytes) to the Tangle by doing Proof of Work
interruptAttachingToTangle	Interrupts and completely aborts the attachToTangle process
broadcastTransaction	Broadcast a list of transactions to attachToTangle
storeTransactions	Store transactions into the local store to attachToTangle

chrome-extension://restlet_client.html 가능





● IOTA Tangle 기술 분석(IRI Release 1.4.1.1, 현재 Beta 버전)

❖ (데스크탑 PC 기반) Tangle 환경 구축/트랜잭션 처리 가능 확인(Full Node / Light Node)

- ✓ Tangle에서 현재 지원하는 모든 기능 시험 및 확인 완료

❖ (Raspberry Pi-3 기반) Tangle 플랫폼 설치 및 시험(Full Node / Light Node)

- ✓ IoT 게이트웨이/센서 노드에서 주로 사용하는 Raspberry Pi-3 환경에서의 구동 가능 여부 시험

✓ (Full Node) Raspberry Pi-3에서 IRI 1.4.1.1 버전 구동 실패

- 현재의 IRI는 ARM64 계열 지원 불가
- iri-1.4.1.1.jar 에 arm64 용 librocksdbjni.so 부재

✓ (Light Node) Raspberry Pi-3에 Wallet 설치 가능(원격의 Headless Full Node를 통해 트랜잭션 가능 확인)





IOTA Index

We aim to list all useful IOTA websites.
If you feel we have missed somewhere please [let us know](#).

You can buy IOTA on Binance:
Save fees in your first month with our [Binance referral link](#).

[Follow](#)



IOT Price Index
USD -0.91% ▼

\$ 1.09

OFFICIAL SITES <ul style="list-style-type: none">Official SiteOfficial ForumOfficial BlogDiscordDeveloper HubGitHub	WALLETS <ul style="list-style-type: none">GUI WalletMobile Wallet	TOOLS/SERVICES <ul style="list-style-type: none">Tangle MonitorIOTA NodesIOTA.coolTangle VisualizerChatangle	FORUM <ul style="list-style-type: none">Hello IOTA
BUY IOTA <ul style="list-style-type: none">BitfinexBinanceYDXbit520CoinSpot	TUTORIALS <ul style="list-style-type: none">IOTA SupportIOTA.PartnersIOTA Guide/FAQDeveloper TutorialsUK Crypto Guide	EXPLORERS <ul style="list-style-type: none">IOTASear.chThe Tangle.orgTangleBossIOTA.coolCodebuffetExplorerIOTA Balance	NEWS & BLOGS <ul style="list-style-type: none">Tangle BlogIOTA.newsSteemit ArticlesUntangled Blog
MARKET DATA <ul style="list-style-type: none">IOTA PricesCoin Market CapIOTA MarketCryptowatchTrading View	INTERNATIONAL <ul style="list-style-type: none">IOTA BrasilIOTA JapanIOTA ChinaIOTA HispanoIBERIOTAIOTA ItalyIOTA KoreaIOTATangle.roIOTA TurkiyeIOTA DeutschlandIOTA Aotearoa	FAUCETS <ul style="list-style-type: none">IOTA Faucet.orgFaucet 2	SOCIAL MEDIA <ul style="list-style-type: none">TwitterRedditBitcointalkArea51
		DISTRIBUTION <ul style="list-style-type: none">Snapshot 02/04/17Snapshot 05/09/17	WIKIPEDIA <ul style="list-style-type: none">IOTA on Wikipedia
			WHITEPAPER <ul style="list-style-type: none">EnglishJapaneseChineseSpanish

감사합니다!