블록체인과 인공지능

이흥노

Heung-No Lee (Publication/facebook ID)

https://infonet.gist.ac.kr

July 19th 2018

Blockchain and AI Workshop

일 시	2018년 7월 19일(목) 15:50 ~ 19:30
장 소	고려대학교 미디어관 12층 크림슨홀
주 최	(사) 한국정보통신설비학회, OSA DC
주 관	고려대학교 암호화폐연구센터

참가비 무료(음료, 식사 제공) / 주차비 무료

한국정보통신설비학회 OSA

| 프로그램 |

시 간	강 연 제 목	발표자(소속)
15:30~15:50	등 록	
15:50~16:00	인사말	이상진 원장 (고려대 정보보호대학원)
16:00~16:30	Blockchain and AI	이흥노 교수 (GIST)
16:30~17:00	Blockchain and Bigdata	차상균 교수 (서울대)
17:00~17:30	AI Boosts Profits	Nikolay Lysenko (OSA DC)
17:30~18:00	Applied AI in Retail	Oleksii Potapenko (OSA DC)
18:00~19:30	식사 및 네트워킹	

※ 경품추첨에서 뽑힌 참가자에게 암호화폐 제공

| 행사장 안내 |

고려대학교 미디어관 12층 크림슨홀 (6호선 안암역 2번 출구)

블록체인과 AI

블록체인이란 무엇인가?

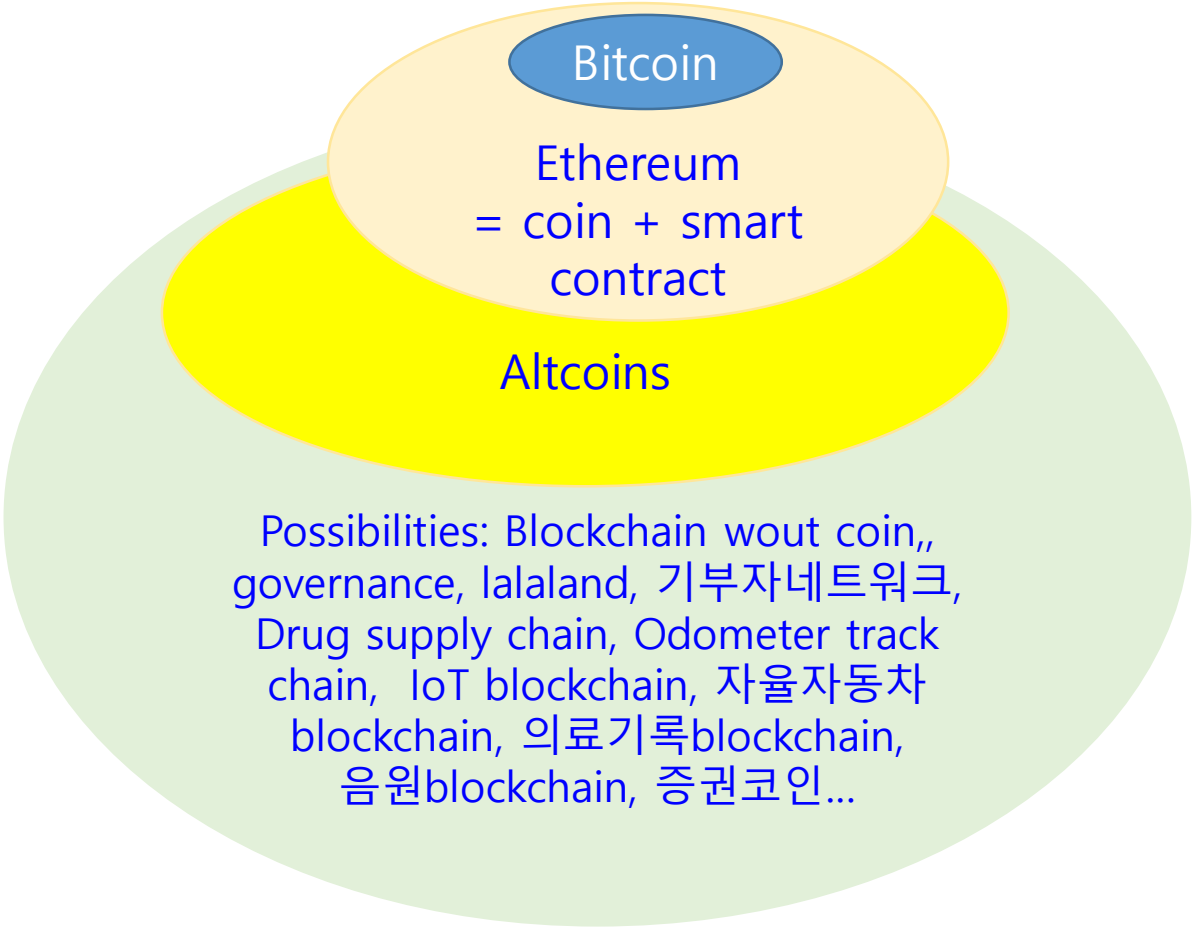
AI란 무엇인가?

둘을 합치면 어떤 세상을 만들 수 있나?

Zug 시

- 인구 3만명
- 취리히에서 기차로 1시간 거리
- 기업 친화 정책으로 가장 못 사는 도시가 가장 부자 도시로 탈바꿈 (15년)
- 새로운 암호화폐 기술의 50%가 이 도시에서 개발되었다고 함.

블록체인 암호화폐 응용



Priority

1. 시장 검증 여부
2. 논문 여부
3. 코트 오더, 법 제정 여부
4. 화이트 페이퍼 여부
5. Github 코드 공개 여부
6. 신문 및 아티클

Proliferation of ideas, BUT

- Be careful
  - 98% of ICOs done in 2017/2018 did not fulfill their obligations!
- Non blockchain solutions…
  - IOTA with Tangle
  - Hashgraph
- Private blockchains…
  - No coin, no mining, …
  - Consortium of companies in competition, building trust among them using blockchain.

블록체인은 서버 망

- 거래내역을 순서대로 그때 그때 바로 바로 기록한 원장.
- 기록 내용, 순전 무결하게 보존하는 기술.

- 원장에 무엇을 기록하나?
  - 코인거래 (Bitcoin, Tokens, …)→ 암호화폐
  - 중요한 내용 → 공공기록소
  - 컴퓨터 코드 및 실행 → 계약 실행 컴퓨터

- 블록체인은 분산컴퓨터 서버 네트워크
  - 컴퓨터는 다양한 App을 돌릴 수 있으므로, 다양한 역할 수행 가능

- 탈 중앙화 : Intermediary → 십시일반 역할하자!
- 화폐로 Incentivize하자!
  - 분산 협력, 분산 신뢰, 글로벌경제, coin economy의 탄생!

Blockchain Core (프로그램)

Network of peers

- Node registration, get-address, give-address
- Full node or light node

Wallet for TX generations

- Make private and public keys, address, store UTXOs, make TX, put signature, announce it to the neighbor, check to see if the TX is included in the blockchain.

Miners guard the blockchain

- Data: Genesis block + regular blocks, one block every 10 min, block-size 1Mbyte,
- Protocol: consensus, block header, difficulty level adjustment, …
- Mining: Get the longest chain, validate it and all transactions within it, get transactions from mempool and form a block, run SHA repeatedly until you hit a good hash, put the proof into the block header, and attach the proofed block to the longest chain, and make announcement ASAP.

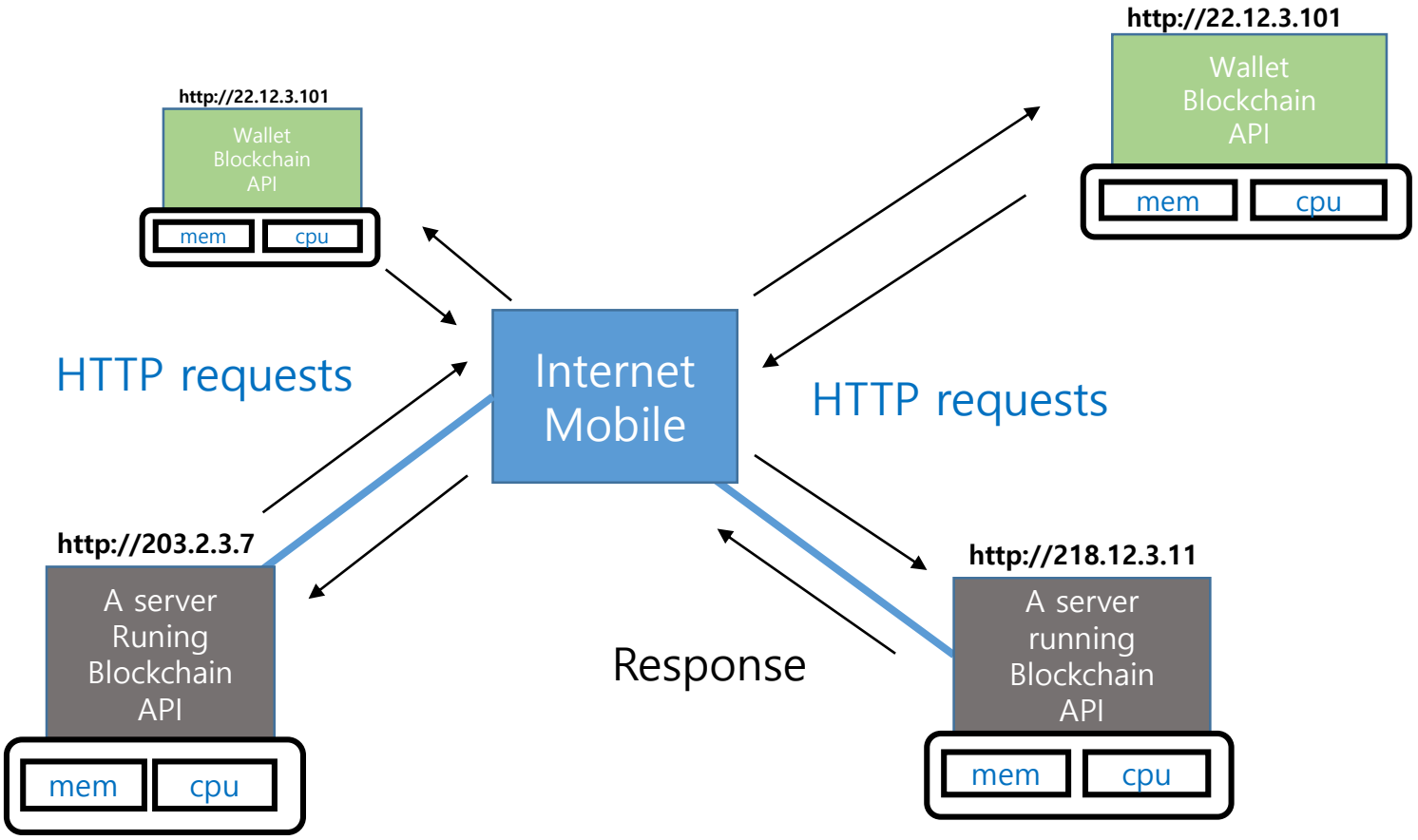
Web server interface

- Communication among the wallets and the miners

Program

- **C++, Python, Go, Java, Flask, http**
- **Download and run, then you have a blockchain server.**

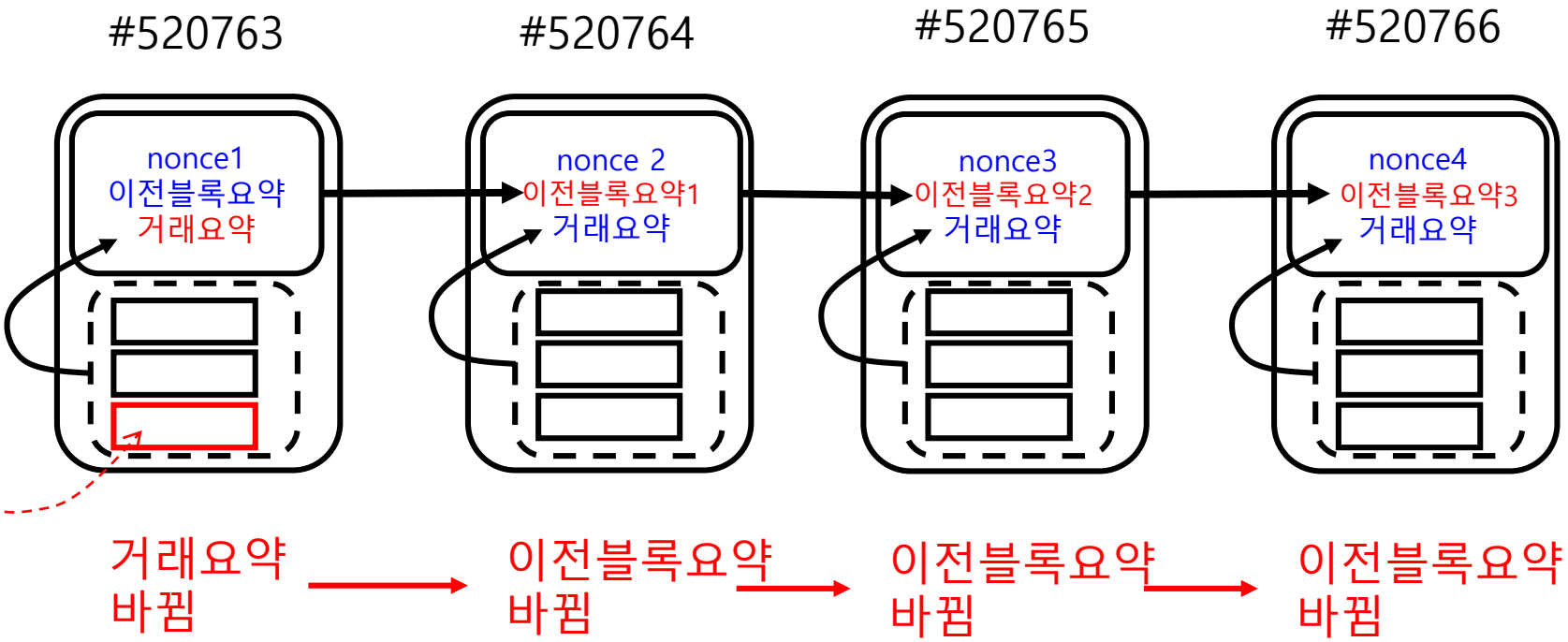
누구든지 Blockchain.core를 다운, 설치 및 구동 하면 참여



Python, Pycharm, Flask, Postman

위변조시 바로 들통나는 파일

- 아래 빨간색으로 표시된 거래에 기록된 내용을 누군가 임의로 내용을 바꿀 때 생기는 일은?



위변조, 큰 네트워크에서는 힘들다!

- 하나의 블록에 작업증명을 붙이는데 걸리는 시간은?
  - 채굴기 하나로 하면 평균 16년 정도 걸린다.
  - 그러나, 8백만대의 채굴기가 10분간 동시에 채굴할 때, 그 중에 문제를 푸는데 성공한 채굴기가 평균적으로 한 대 나온다.
- 즉 각 블록에 기록된 Nonce값은 8백만대의 채굴기가 모두 동시에 Work를 했다는 증거다.
- 이런 Proof-of-work를 혼자 하려고 하면?
  - 한 블록도 혼자 하기는 어렵다. 16년.
- 그러므로 블록체인 내용을 안 들키며 바꾸지 못 한다. 공격자는 소수라는 가정 하에.

다양한 Applications

- 화폐: 신뢰하고 쓰면 화폐다.
- 공공기록: 언제 어디서나 열람 가능한 위변조가 방지된 기록장은 쓸데가 많다.
- 계약: 법률가, 보험가, 행정가의 개입없이 smart contract로 계약 맺고, 계약사항 집행 및 정산 가능
- 주목 받는 블록체인 use cases (Killer App은???)
  - Pharmaceutical supply chain
  - Track vehicle odometer and data chain
  - International aid chain
  - Tracking government complain

불완전한 블록체인 문제

- 전기소모량, 한 국가(Iceland)보다 많다!
- 스마트 컨트렉트 사고!
- 채굴기업 등장, *Re-centralization* 문제 대두!
- 써 먹기 불편하다!
  - 느리다, 용량이 작다, 가맹점이 많지 않다.
- 현행법과 마찰!
- 화폐 거래/데이터/네트워킹/서버기술– 각종 해킹공격의 대상
- 채굴자원 공유시장 탄생 – 소규모 체인은 신뢰할 수 없다. 왜? 공격이 쉬우므로.

블록체인/암호화폐 가능성

- 4차 산업혁명의 핵심 철학과 괘를 같이한다.
  - 개방, 공유, 협력, 신뢰, 혁신, 집단지성

- 모든 것들이 연결되고, 상호협력하여 하나의 기능을 한다.
  - Things 들간 유기적 연결: 암호화폐 보상, 하나의 공통된 목표 달성을 위해 협력
  - 자동차와 자동차간의 협력
  - 드론과 드론 간의 협력
  - 센서와 센서 간의 협력
  - 소비자와 공급자간 협력

- 인공지능은 독립노드들의 연결이다.

2018년 현재

인공지능은 어떤 것들을 잘 할 수 있나?

블록체인과 결합하면 어떤 세상을 만들 수 있을까?

두뇌와 인류문명

45억년 전 지구의 탄생

20만년 전 Homo Sapiens(지혜로운 인간) 출현

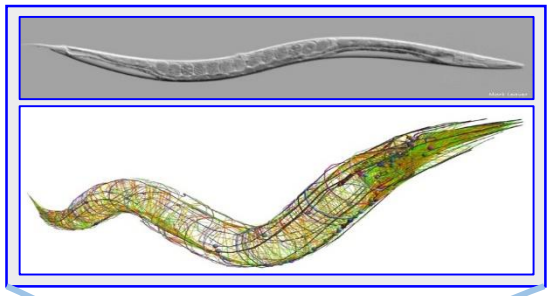
BC 3,000년 문명의 시작

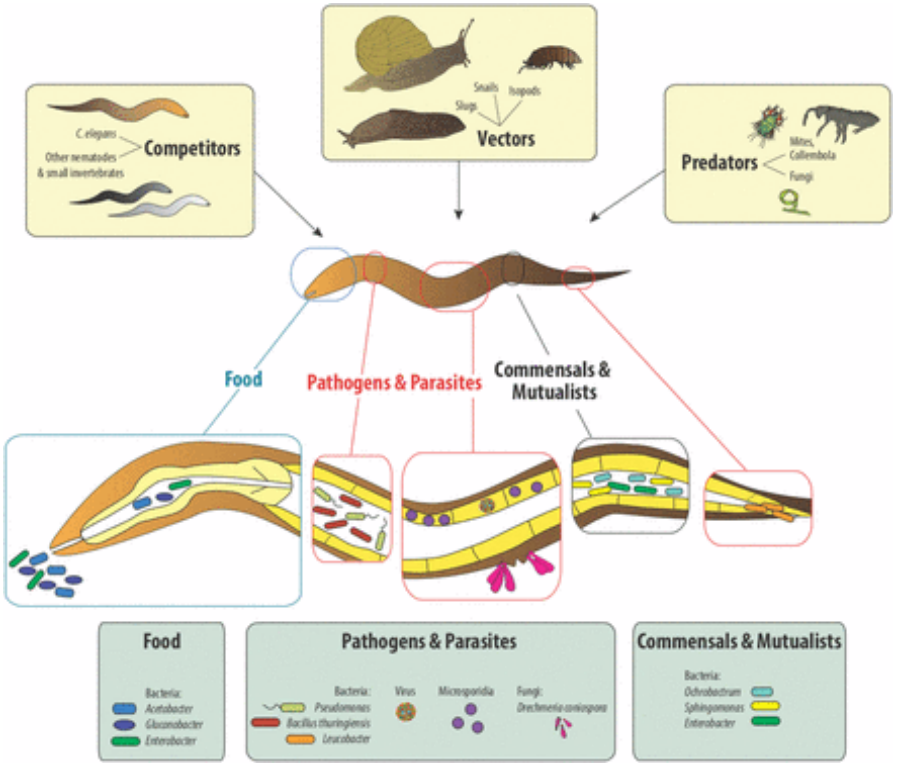
AD 1세기 지구상의 인구는 1억, 평균 수명 20세

두뇌와 협력으로 이루어낸 기적!

두뇌??? 뉴론의 연결
"센싱→ 상황판단→ 액션 → 보상" 연결의 특화
특화된 연결이 특정 기능의 수행을 잘할 수 있게 함

C elegans

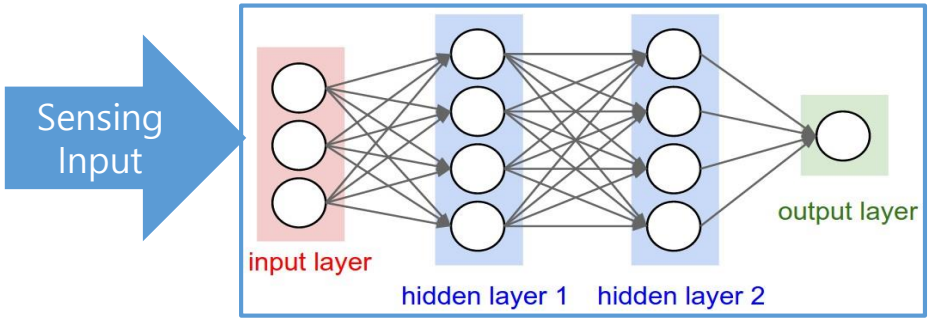




지능이란?

- 뇌는 센싱을 통해, 상황을 판단하고, 행동의사를 결정한다.
- 세상은 인간의 결정에 반응하고
- 인간은 세상의 반응을 통한 학습을 통해 의사결정 능력을 고도화 한다.
- **시의 적절하게 *잘 내릴 수 있는* 의사결정능력을 지능이라 한다.**

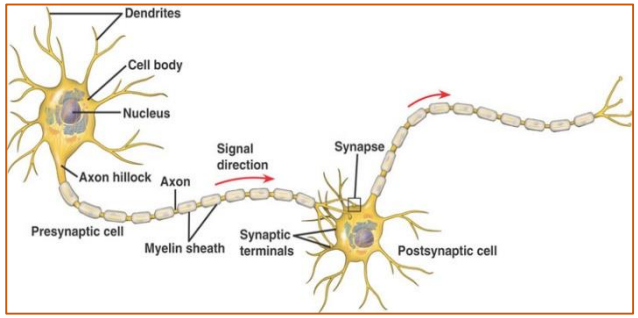
Artificial Neural Network 과 RL 강화학습 (인공지능)

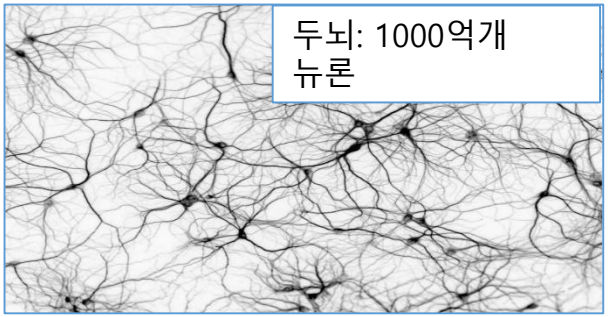


학습: 많은 수의 Sensing 샘플 사용, Network 연결 결정

Classification : Sensing Input, 상황판단, 결과 제시

보상 통한 강화 학습으로 스스로 성장 가능 (판단 세분화)





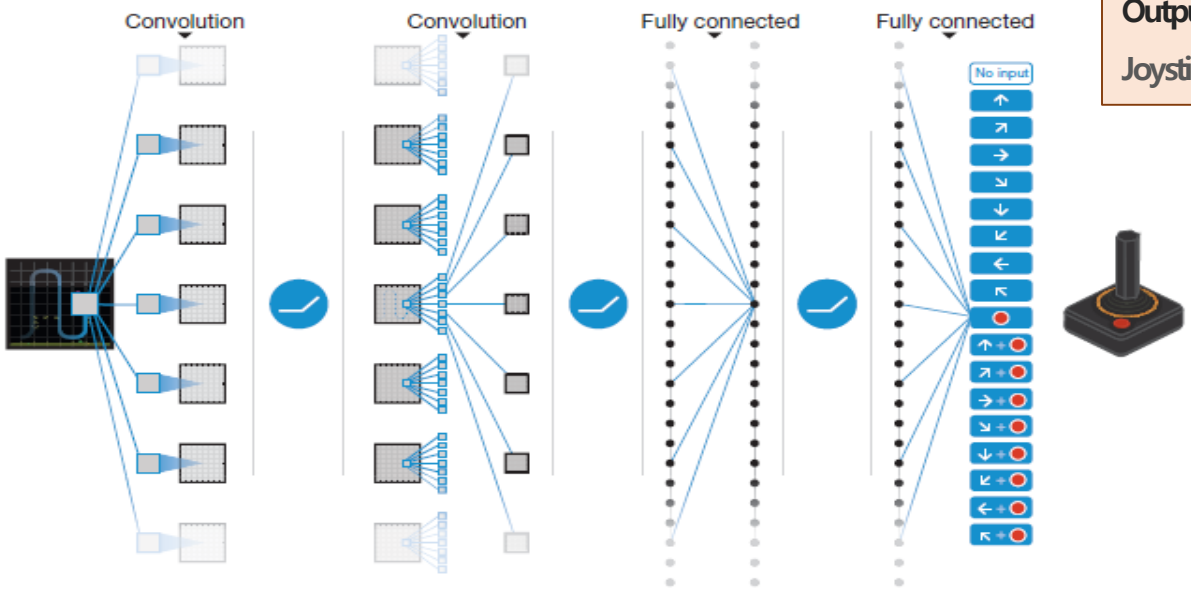
10

Deep Neural Network와 Reinforcement Learning,

숨겨진 패턴을 찾아내고, 전략적 계획을 수립한다.
강화학습을 통해 성장한다!

Sensing **상황인식** **Action**

Input : Screen

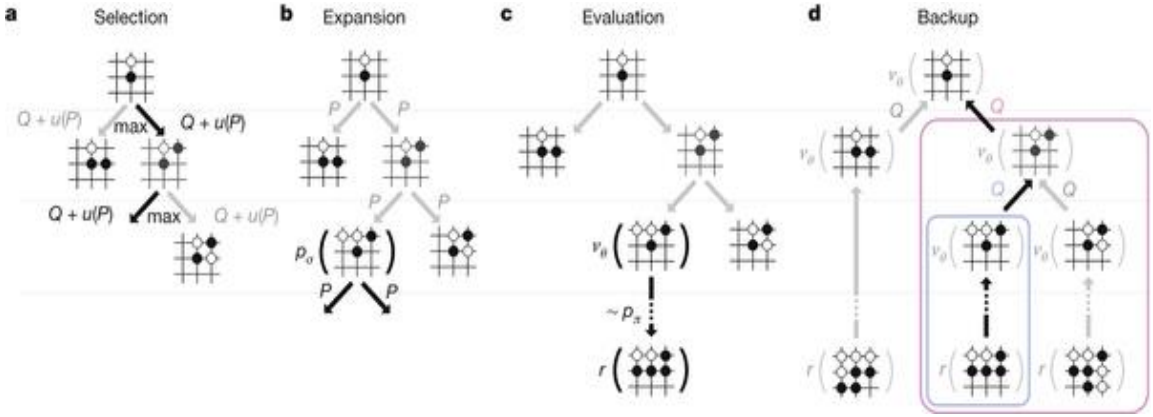


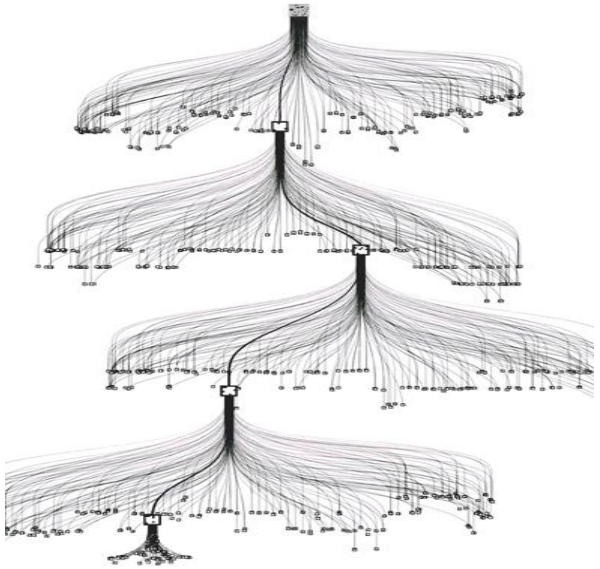
Output :
Joystick Action

11

경우의 수가 무수히 많은 문제를 넓고 깊게 보고 잘 푼다!

AlphaGo: Tree Search





12

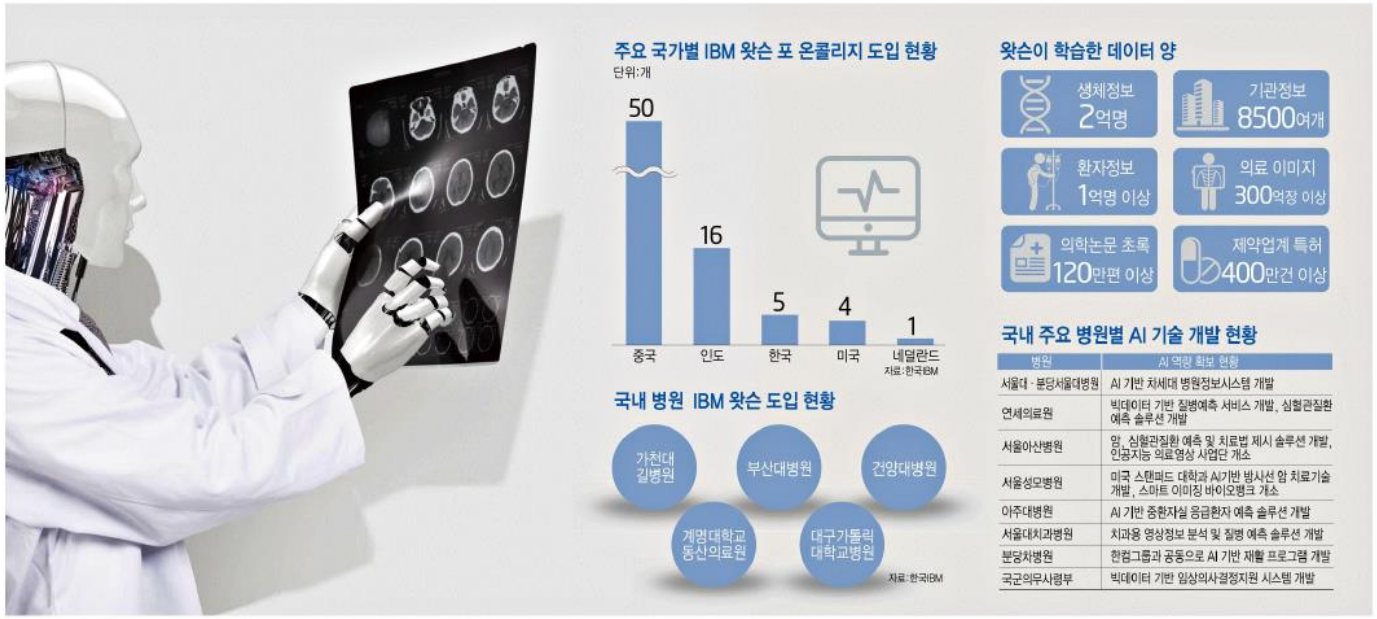
의사가 환자 상담, 진단, 처방에 쓸수 있는 시간 10분.

인공지능은 2억명의 생체정보, 1억명의 환자정보, 300억장의 의료이미지 자료를 학습.

환자의 의료/생체정보를 분석, 가능한 진단 방법 제시

전자신문

2017년 04월 11일 화요일 004면 종합



AI 주치의 등장…의료혁신 脈 제대로 짚을까

◇세계 톱3 'AI 도입국', 의료 혁신 시작됐다

알파고가 불러온 AI 신드롬은 병원에서 IBM '왓슨'이 바통을 이어 받았다. 코그니티브(인지) 컴퓨팅 솔루션 왓슨은 빅데이터를 분석해서 자연어로 된 질문을 이해하고 답을 제시한다. 매일 쏟아지는 300여종의 의학저널, 200여종의 의학 교과서, 1500만쪽에 달하는 의료 정보를 학습해서 최적의 치료법을 제시한다. 암 진단·치료에 도움을 주는 '온콜로지' △유전자 분석에 초점을 맞춘 '지노믹스' △임상 시험을 돕는 '클리니컬 트라이얼 매칭' △연구개발(R&D)용 '라이프 사이언스' 등이 대표 솔루션이다.

2015년 국내에 첫선을 보인 왓슨 포 온콜로지는 지난해 9월 가천대 길병원을 시작으로 부산대병원, 건양대병원, 계명대 동산의료원, 대구 가톨릭대학병원, 중앙보훈병원 등 6개 병원이 도입했거나 도입할 예정이다. 세계 각국과 비교해서 도입 비율이 높다. 왓슨 포 온콜리지를 도입한 병원은 중국이 50곳으로 가장 많다. 인도가 마니팔 병원 그룹 내 16곳이 도입해 뒤를 이었다. 우리나라(5곳)는 3위다. 미국이 4개 병원, 태국·네팔·네덜란드가 각 1곳이다.

NN과 강화 학습법 개발로 인하여

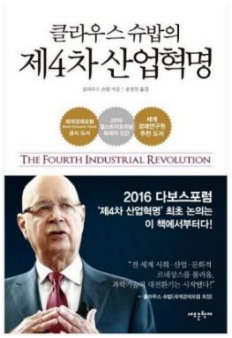
인공지능은

사람보다 잘 계산하고(Compute),
듣고(Listen),
보고(See),
사고하고(Cognitively Think),
맥락을 인지하고(Understand Context),

로봇은 말하고(Speak),
걷고(Walk),
뛰고(Run),
달리고(Ride),
날수 (Drone) 있게 되었다.

14

인공지능은 Cloud에 수집된 Big Data를 분석해서, 잘 안보이는 패턴을 찾아내고, 연결하여 숨겨진 가치를 찾아 낼 수 있다.



4th IR 는 Klaus Schwab 이 WEF 2016의 의제로 채택함
Schwab 혁신기술의 출현으로 급격하고 광범위한 사회, 경제구조의 변화 4th IR로 통칭 함.
Multistakeholder theory실천가, 공유, 개방, 혁신, 신뢰, 협력, 기업가정신 강조

4th IR 은 주요 시스템의 스마트 화를 의미함.
Factory를 예로 들어 보면, 모터, 밸브, 에너지 소스, 밸트, 로봇 등 사물이 구성 요소임.

- (*IoT*) 각 구성요소에 각종 디지털 센서를 부착하고 인터넷에 연결함.
- (*Digital twin*) 이때, 각 사물에 대한 디지털 트윈이 컴퓨터상에 생성됨.
- (*Optimization*) 컴퓨터 상에서 구성 부품을 연결하고, 실시간 모니터링, 시스템 최적화 가능.
- (*Big Data*) 각각의 사물로 부터, 역할 수행 및 상태 정보 데이터를 수집하고, 저장 가능.
- (*Prediction*) 과거로 부터 현재까지의 데이터 분석, 정확한 상황판단 및 미래예측 능력 제고.
- (*Value Creation*) 실시간 상황판단과 미래예측능력은 새로운 BM 창출을 가능케 함.

(확장) 위와 같은 개념을 연장 한 것이 바로, 스마트홈, 스마트스쿨, 스마트그리드, 스마트팜, 스마트빌딩, 스마트병원, 스마트도로, 스마트교통, 스마트시티가 됨.

29

스마트 시티

인간 과 사물이 모바일로 유기적으로 결합되며, 학습을 통해 도시의 문제를 파악하고 과학기술로 효율과 생산성을 제고하는 도시!

Sensors
신호습득

Situational Awarenesss
(신호 + 경험), 문제 파악

Actions
결정

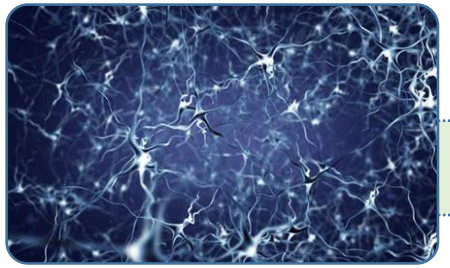
도시에 깔려진
각종센서를 통해

보고, 듣고, 냄새 맡고,
교통흐름을 모니터하고

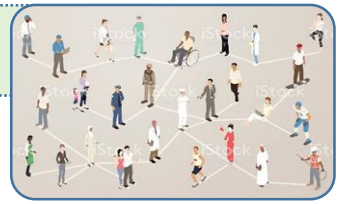
TV 와 인터넷 뉴스와
SNS 정보를 통해

시민의 반응을

센싱한다



World



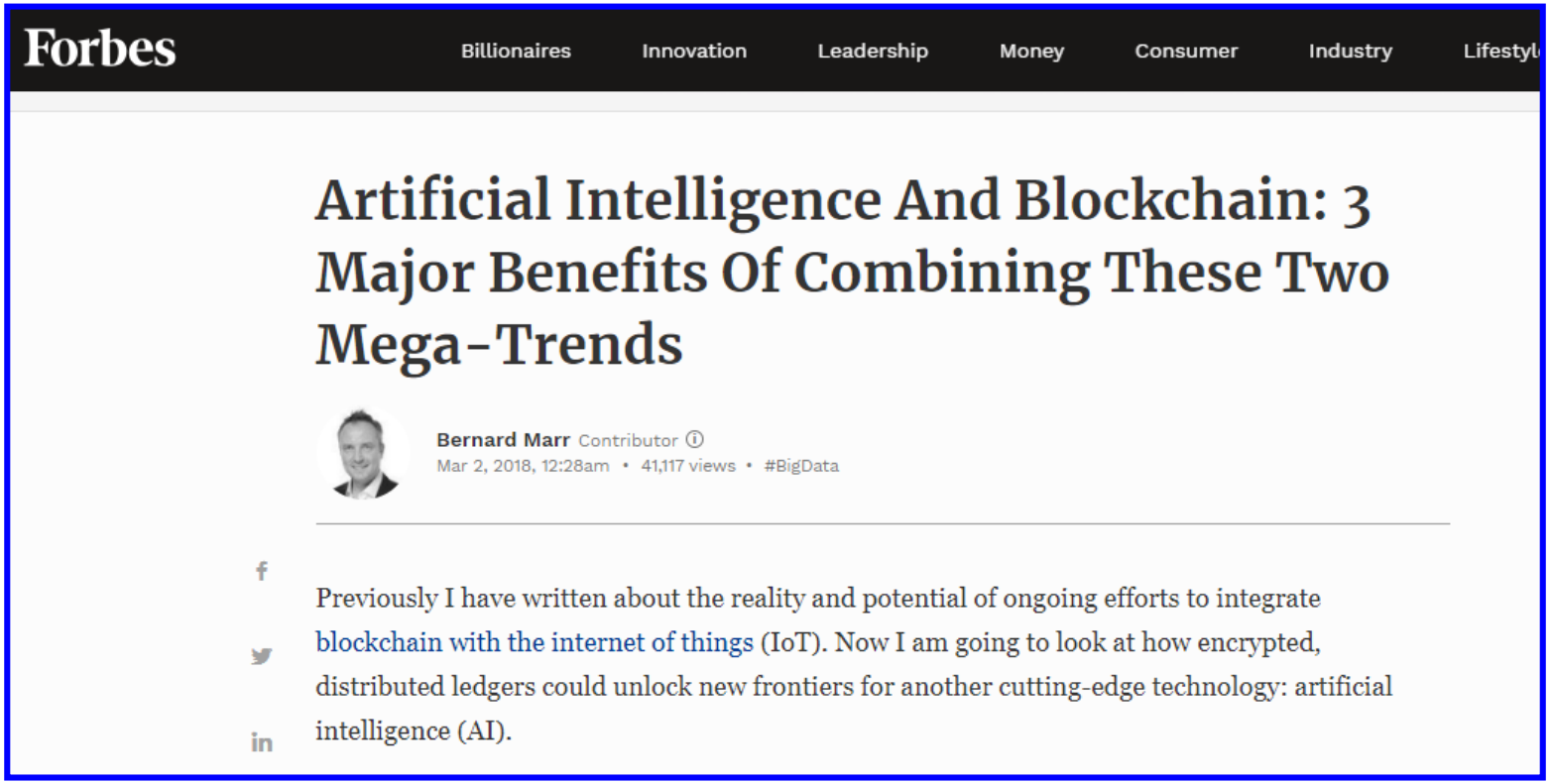
데이터를 요약
저장하고

교통신호등, 주차장소
표시, 온도조절,
에너지조절 등
제어하고

센서의 상태를 파악하여
교체하는 등 행동의사를

결정 한다

**사람(공급자, 사용자, 개발자, 교육자) 과 Things(각종센서와 제어장치),
무수히 많은 연결방법이 존재
암호화폐 보상체계로 사람과 Things들이 자발적으로 연결, 문제 해결**



Forbes

Billionaires Innovation Leadership Money Consumer Industry Lifestyl

Artificial Intelligence And Blockchain: 3 Major Benefits Of Combining These Two Mega-Trends

Bernard Marr Contributor ⓘ
Mar 2, 2018, 12:28am • 41,117 views • #BigData

Previously I have written about the reality and potential of ongoing efforts to integrate blockchain with the internet of things (IoT). Now I am going to look at how encrypted, distributed ledgers could unlock new frontiers for another cutting-edge technology: artificial intelligence (AI).

1. AI working with encrypted data
   - New AI algorithms will be developed capable of handling data while the data is still encrypted.
2. Blockchain can help us track, understand, and explain decisions made by AI
   - AI algorithms can be used to make decisions about whether financial transactions are confirmed or not.
3. AI can manage blockchains more efficiently than humans

스마트 콘트렉트로 탈중앙화한 인공지능, 개인 생체 및 메디칼 정보 수집, 데이터 토큰화

Blockchain And Artificial Intelligence: The Benefits Of Decentralized AI

March 24, 2018 By Jorn van Zwanenburg 1

Blockchain and Artificial Intelligence are two of the hottest technology trends right now. Even though the two technologies have highly different developing parties and applications, researchers have been **discussing and exploring** their combination, and they have **been found** to go extremely well together.

In the following article, I will discuss the basics of Artificial Intelligence, followed by the fields in which the two technologies exhibit highly promising convergent potentialities.

Decentralized AI with Smart Contracts

Decentralized AIs operate autonomously and in a decentralized way through smart contracts, without having a central party pulling the strings and making decisions.

Data protection

Blockchain gives the creation of fully secured databases which can be looked into by parties who have been approved to do so

Data monetization

Blockchain makes it possible for us to monetize the data we create through data marketplaces. By using blockchain technology, we can actually own our data and decide what to do with it.

인공지능 연구에는 개인의 생체 및 메디칼 정보 필수. 블록체인상의 정보제공으로 개인은 민감 정보 누출 걱정 없이 토큰화된 데이터 제공.

NEWS · 09 MARCH 2018

AI researchers embrace Bitcoin technology to share medical data

Blockchain could let people offer health records for research – without losing control over them.

Amy Maxmen

Researchers are developing AI algorithms to detect breast cancer in mammograms. BSIP/UIG/Getty

Goal: Train AI algorithms on the data they solicit using the blockchain systems

- Blockchain could let people offer health records for research without losing control over them.

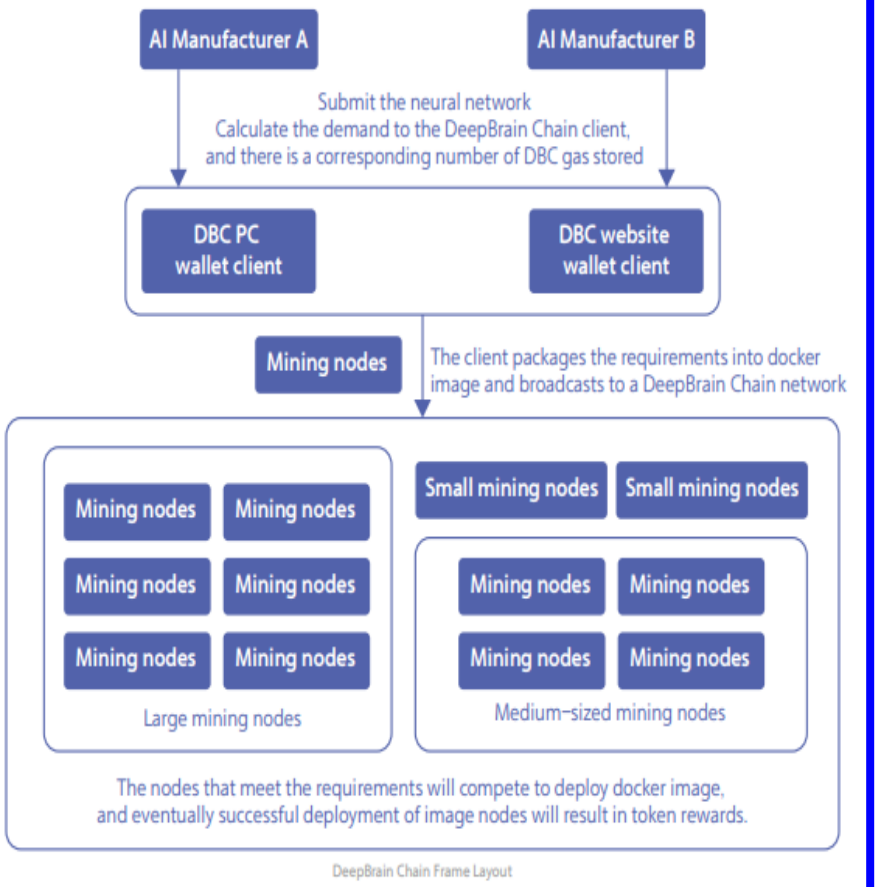
Artificial intelligence (AI) needs huge amount of data, but to access such sensitive medical information is limited due to privacy laws.

AI algorithm can be trained by the data set securely controlled in the blockchain based system.

Blockchain-based system for sharing health records

- MedRec
- Allows users to insert information into their health records, including data from wearable electronic devices such as Fitbits.

DeepBrainChain: 컴퓨팅 자원 공유, 컴퓨터 제공자, 데이터 제공자, AI startups을 Smart contract로 연결, 계약과 정산 담당



3.2.2 Mining node architecture

- 2012-2016: 100B USD invested on more than 5000 AI startups and large corps.
- No need for each company to build computing farm on their own.
- Use smart contracts between the AI companies, and Data providers, and computing equipment providers.

블록체인+인공지능 가능성

- **혁신기술에 의한 혁신 성장**
  - Cyber security initiatives → 블록체인 Police (거래질서확보)
  - 드론, 자율차, 로봇 → 로봇 Economy
  - 센서와 블록체인 → 코인 센서 지능화 Economy
  - 스마트교통과 블록체인 → 선진 교통질서 Economy
  - 미디어 컨텐츠 시장 선진화 → 코인 미디어 Economy
  - Data 컨텐츠 → Data 민주화 시장

- **인류 문화사적 진보**
  - 소득의 "공정"한 분배, 투명하고 효율적 행정,
  - 사회 양극화 해결에 기여
  - 인간 개개인 삶의 질 제고
  - 인류의 지속적이며 포용적 성장 추구
  - 더불어 같이 잘 사는 인류공동체

현실 비판

- GIGO: 좋은 데이터를 모을 수 없어서 인공지능 학습 못 시킨다.
- 현실문제는 게임과 달라서 상시 가변적이며 확실한 보상이 없다.
- 인공지능이 그렇게 잘 되면, 왜 내 컴퓨터는 원인도 모르게 느려지냐?

- 블록체인으로 데이터를 토큰화 하자.
  - 토큰을 발행하는 ICO하다가 규제에 걸리기 쉽다.
  - 토큰이 효율적인 집객 수단이 된 성공 사례가 없다.
- 스마트 컨트렉트 문제가 많고, New BM을 만든다는 보장이 없다!
- Oracle이 완벽하지 않아서 헛점이 된다!
- 토큰이 시장의 효율을 정말로 높인다는 증거가 어디있냐!
- 모든 것이 Blockchain안에서 돌지 않는 이상, 저작권 관리 문제, 불법 복제 문제를 때문에, 성공 할 수 없다.
- 규제를 바꿔야 성공하는데 우리나라 현실에선 절대 못 한다.

- 기술의 장밋빛 환상은 좋은 BM과 아무 연관이 없다.

미래방향 설정과 실행

- 바람직한 방향을 정하고 일하면 미래를 현실로 바꿀 수 있다.

- 그러나 그런 미래는 아직 오직 않았으니
- 글이나 그림으로서 설명 할 수는 있으나
- 실증해 보여줄 수는 없는 노릇

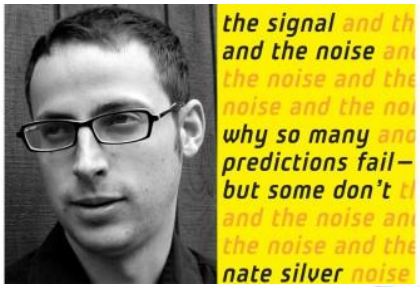
- 실현하기 위해서는 해야 할 일과
- 넘어서야 할 산과
- 열어제껴야 할 관문들이 많이 있다.

- 미래를 보는자는 소수, 현실주의자는 다수...

- 묵묵히 하나씩 만들어 보여주는 수 밖에는 답이 없다.

인공지능, Big Data ~ Bayes Theorem

융합(현재까지 정보, 새로운 정보) => 미래예측



- Nate Silver (1978 ~)
  - New York Times Best Seller
  - Poll Aggregation Blogger
  - Prediction Experts
  - Big Data = True + Noise, Predict Future?

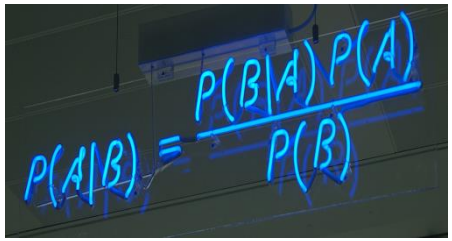
- Thomas Bayes(1701~1761)
  - Presbyterian minister
  - *Divine Benevolence*
  - *Later got interested in Probability*

인공지능은 여전히 단순한 Tool일 뿐!

어떻게 학습 시키지?

Neural Net의 구조와 깊이는?

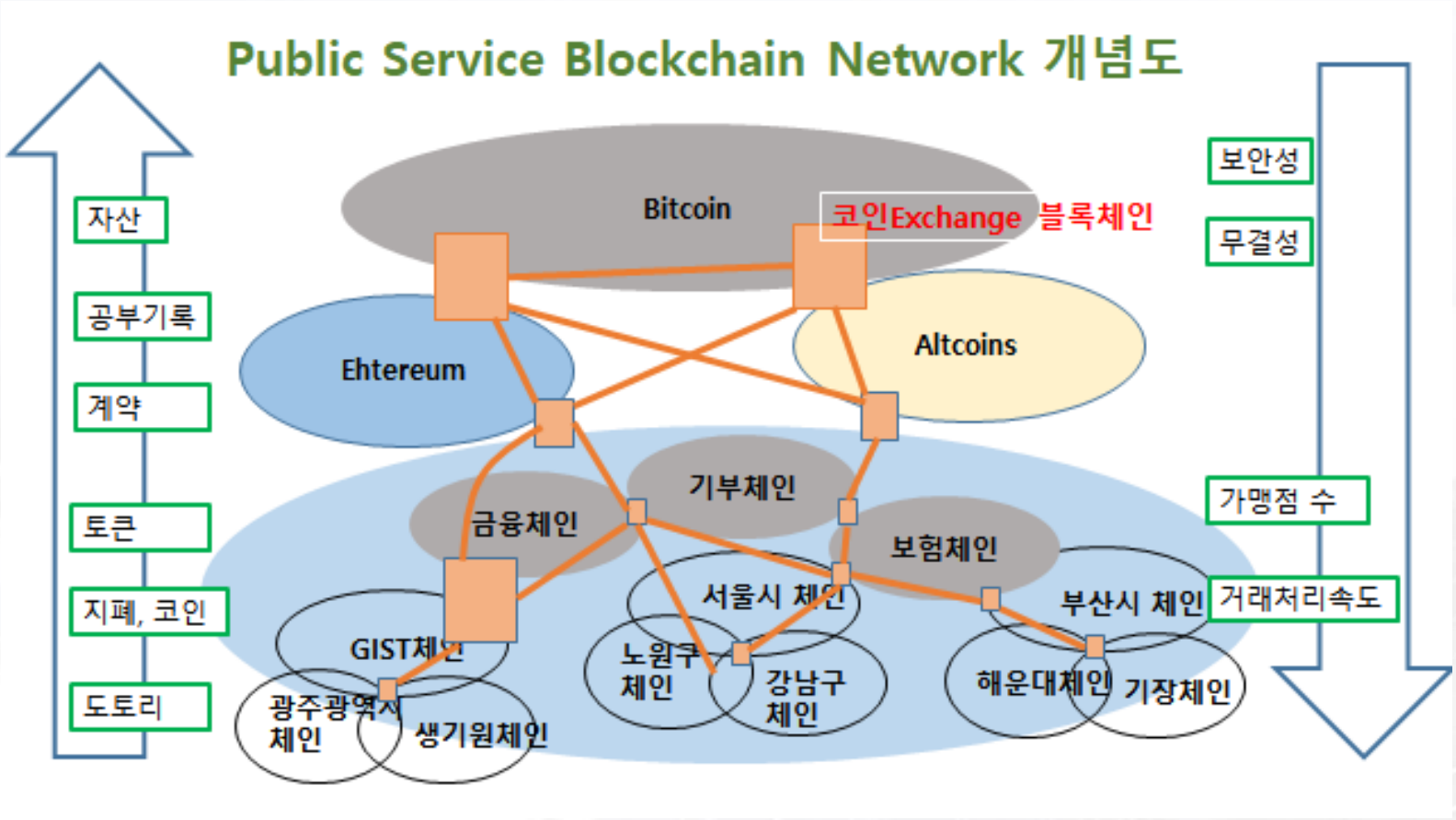
이때 인간 직관과 수학적 경험이 중요하게 작용함.



블록체인 Police, 블록체인 기반 코인가치교환소 등 공공서비스 연구개발

이흥노 랩 연구주제

미국특허 가출원



기반 이론 연구: Error Correction Code기반 작업증명 기술, 거래 속도, 용량 제고 기술.

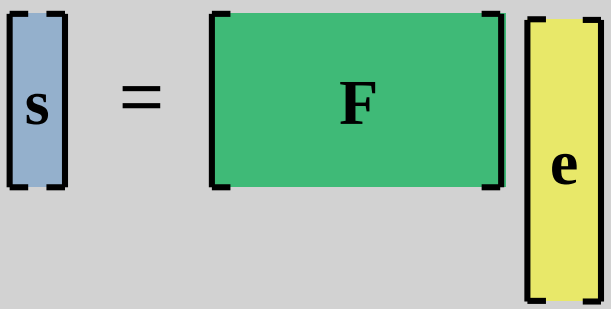
Blockchain Police: 인공지능 통한 불법 거래 추적, 차단 및 타격

HLee랩의 블록체인 연구주제

- 탈중앙화 Adaptive Mining 방법 개발
- 블록체인 해킹 수학적 Analysis
- 휴대폰에서 사용가능 한 개인 인증
- 인공지능 기반 이상거래 추적
- 계층 형 블록체인과 거래속도 다양화

Nakamoto와 C. Shannon이 만나면?

- ENC implies the encoder function, i.e., ENC takes the message vector **m** as the input and produces a codeword vector corresponding to it, e.g. **c** = ENC(**G**, **m**).
- DEC implies the decoding function; DEC takes an arbitrary vector **e** and returns a closest codeword $\hat{\mathbf{c}}$, i.e., $\hat{\mathbf{c}}$ = DEC(**F**, **e**).



$$\mathbf{s} \in GF(q)^{M\times 1}$$
$$\mathbf{F} \in GF(q)^{M\times N}$$
$$\mathbf{e} \in GF(q)^{N\times 1}$$

$$M < N$$

Decoder : Given **e**, find $\hat{\mathbf{c}} = Dec(\mathbf{F}, \mathbf{e})$

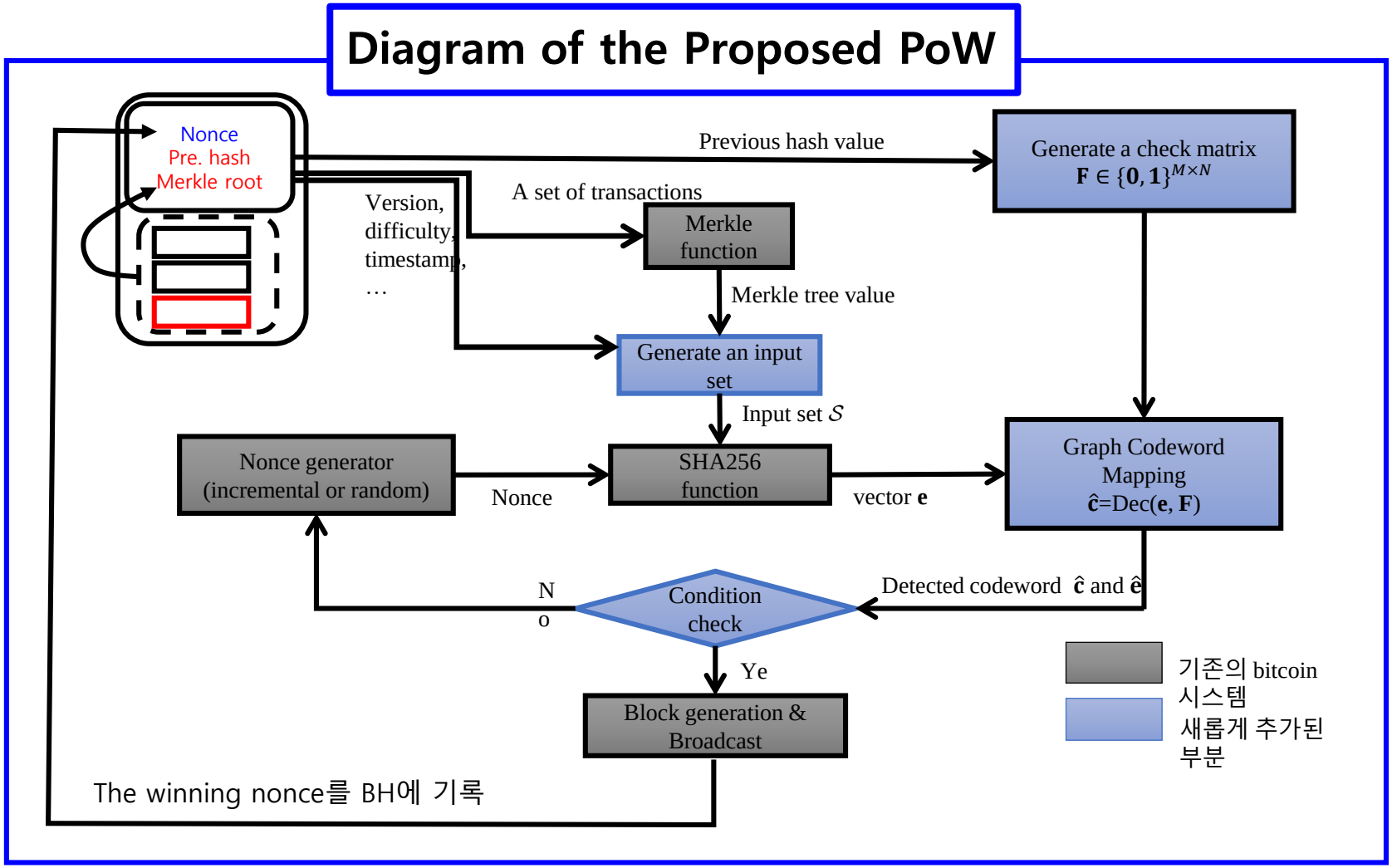
특허 출원 중: 새로운 암호화폐 PoW 생성, 증명, 검증 방식

특징: PoW 문제가 블록마다 변한다.

그러므로 채굴시장 독점이 어렵고,

무수히 많은 PoW를 만들어 낼 수 있으므로

안정된 블록체인을 무수히 많이 만들수 있다.



Blockchain과 AI 시사점

- 상상력과 혁신적 아이디어가 부족 할 뿐… 엄청난 기회!
- 체계적이고 지속적인 연구 통해 하나씩 풀어나가야!
- 혁신연구? 어렵다!
  - 삽질의 가능성, 전력투구 안 한다!
  - 장미 빛 미래와 현실의 차이를 실감하게 된다!
  - 코딩 하기도 어렵고, 된다고 하더니 잘 안되고, 어렵게 했더니 남들이 다 한거고, 힘들게 시스템 구축했더니 해킹 당하고, 평가장에서 망신당하고, …
- 미래는 예측하는 것이 아니고 바람직한 미래를 설정하고, 하나씩 만들어 가는 것.

감사합니다!