지능화된 스마트 계약: 탈중앙 AI 시스템

산디 라마디카*, 이경현**
*부경대학교 정보보호학협동과정
**부경대학교 IT 융합응용공학과
e-mail : sandika@pukyong.ac.kr; khrhee@pknu.ac.kr

AI on Smart Contract: The Decentralized AI System

Sandi Rahmadika*, Kyung-Hyune Rhee**
* Interdisciplinary Program of Information Security, Graduate School PKNU
** Department of IT Convergence and Application Engineering
Pukyong National University, Republic of Korea

Abstract

Blockchain is emerging to be the topic of conversation because of the technology behind it, whilst Artificial Intelligence (AI) is a technology that can change our future. Therefore, research in combining these two topics has been widely discussed lately. This idea can be realized by increasing the capability of smart contracts. A simple algorithm of AI can be directly applied in the future smart contract since the current state of smart contract does not satisfy the application of AI. By looking at this opportunity, we conduct a study about AI on smart contract to realize the decentralized AI that brings benefits to users. Possible use cases AI smart contract are outlined.

1. Introduction

Blockchain, the technology behind smart contracts, and AI are expeditiously converging presently. The blockchain technology arguably is an ingenious invention, the brainchild of a user or group known by the pseudonym, Satoshi Nakamoto [1]. Whilst, the smart contracts are all the rage in the blockchain world these days. Some pundits claim this will produce an entirely new paradigm that forever changes how the parties write contracts and conduct business. Therefore, it has been applied in various fields of science.

Blockchain smart contract removes trade or service agreement from the realm of static documents that require human management. Smart contracts transform into automation tools that manage complex transaction in the decentralized system. In 2015, Ethereum appeared to the public which adding Turing-Complete smart contracts to the blockchain. Ethereum performs more complex computations and it manages more response compared to Bitcoin. However, it is not self-evolving codes. Simply, Ethereum is a collection of purely rule-based and recursive programs [2].

A recent study conducted by Kiffer et al. [3] showed that the diversity of the smart contract is direct or near copies of other contracts. Moreover, the smart contract's ecosystem has a considerable lack of diversity, since it is reuse code extensively, as well as there are few creators against the number of overall contracts. However, the concern is about to change since there are various approaches to solving the aforementioned issues. By combining AI and blockchain within the smart contract provide a solution. Without improving the capability of a smart contract, it is difficult to be applied to real-world applications.

```
Starting Balance in the contract = Take Money From A.
Update Starting Balance = Take Money From B.
Record outcome of the bet as per received signal.
If ( Outcome = 'Team A wins' ) { Send Money To A }
Else { Send Money To B }
```

Fig. 1. A simple logic of a smart contract

In this paper, we present the current state of AI smart contracts (benefits and the issues), which running AI on the blockchain ecosystem. The existing platform is also elaborated. We provide an outline of why we need it, how it is achieved, and what does it offer for the future.

2. The Current State of Smart Contract

The existing smart contracts such as Ethereum smart contract can only perform simple smart contract computations, it cannot satisfy the

application of real-world AI. Due to smart contract exists on the blockchain, the parties can program the codes that self-executes without the third party involvement as shown in Fig. 1.

However, the issue with traditional contracts that deal with the points below has been solved.

1. Execution is active. If both parties agree with conditions, the smart contract will run the codes without interference.
2. The data record is available since the history of a transaction is recorded in the blockchain system.
3. The smart contract is efficient. It is executed within seconds.
4. Low fee. It gets rid of paperwork and third-party involvement [4].
5. It removes user error. Smart contract eliminates user facilitation by reducing user error and fraud.

3. AI Enabled Blockchain Smart Contracts

The research on a combination of Artificial Intelligence and blockchain into a coherent idea is warmly discussed today. AI on smart contract integration and innovation may provide a more resilient and efficient path for a decentralized system which is interactive for the parties [5].

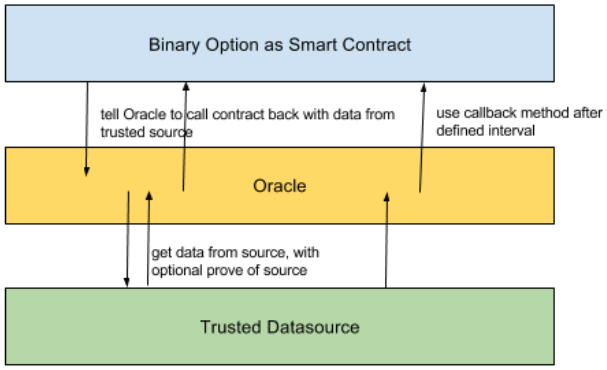

Fig. 2. AI as Oracle to control smart contract outcome

AI as shown in Figure 2 can be used for decision making while the blockchain as its nature is an auditable tamper-proof mechanism for the input, neural net states, and the output. It allows the system to audit the AI processes. Finally, the decision is based on the AI view of events.

The value of AI in a smart contract can be interpreted to the where AI comes in. The thoroughly analysis is necessary in order to create and execute complex smart contracts to make them more effective. In this case, AI on smart contract can analyze predecessor negotiations to see how parties negotiated in the past and suggest the types of most likely decisions for the future.

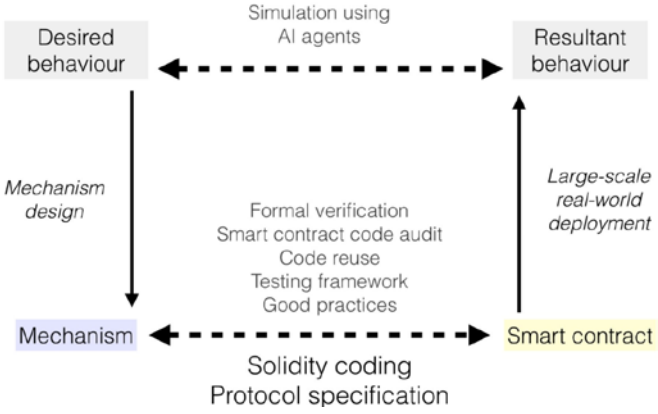

Fig. 3. AI agents / machine learning algorithm within smart contract to test the model

Smart contract for the economy such as market running on a blockchain can be understood as an incentive structure to encourage desirable parties behavior. The mechanism design is challenging to reach the desired output. There are possibilities for malicious users to try to attack the system. Thanks to Incentivai [6] platform as a tool which adapts machine learning to train AI agents that simulate how parties communicate with smart contracts and execute the code to deploy the contracts as shown in Figure 3.

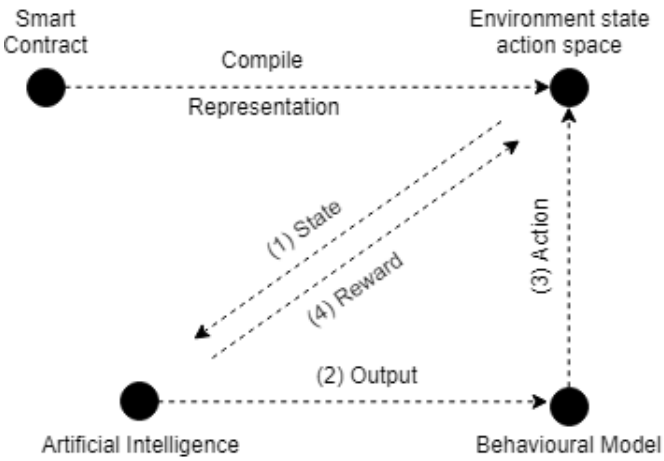

Fig. 4. The basic high-level structure of the model

The model in Figure 4 provides a way to represent smart contract structure design in the right framework which handles training of AI agents with an interpretable result. As the transition model towards the blockchain economy space, this could become a critical tool towards offering safer decentralized application (DApps) and validating incentives structures pre-launch. Intuitively, AI agents are trained to optimize the pre-defined objectives prior to simulating their interaction with real-world applications. Likewise, the model identifies the flaws design and fed back to provide iterative improvement.

Blockchain and AI developers have spawned several studies including the Cortex platform, AI Crypto, and to name a few. Specifically for Cortex, it is a decentralized AI platform that supports AI smart contract and AI execution. The developers enable to submit their models to the blockchain smart contract. The parties afterward can use the model by simply paying Cortex native token to the owner.

```
Prediction result (that Team A wins) = Infer prediction model
with Team A against Team B
If ( Prediction result > 0.80 )
       { send Money to bet Team A wins }
Else if ( Prediction result < 0.20 )
       { send Money to bet Team B wins }
Else { do nothing }
```

Fig. 5. The initial model of AI on smart contract

The model of AI on the Cortex smart contract with the basic prediction model can be seen in Figure 5. When the owner of the smart contract provides Team A and B, it will predict the winning percentage rate of Team A against Team B. The updated result is recorded to the blockchain, and it becomes an input for AI algorithm for the next prediction.

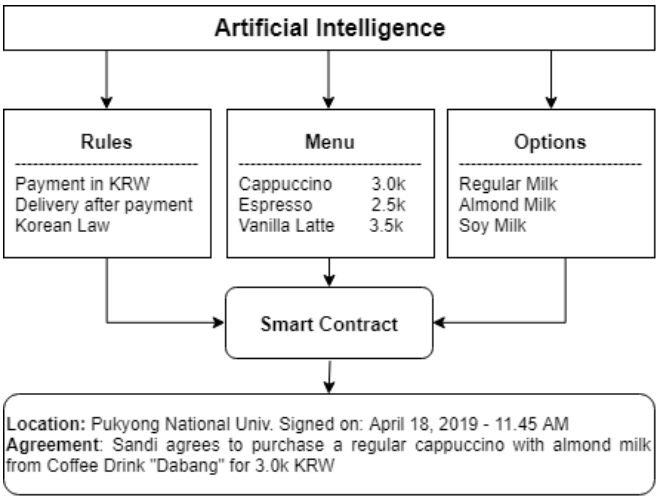

Fig. 6. AI smart contract for purchasing a coffee

A simple implementation of an AI smart contract in daily life is purchasing a cup of coffee as shown in Figure 6. Any basic Natural Language Understanding (NLU) engine today will be able to figure out from the first input that the customer is ordering a coffee. The AI then manages to ask all the questions needed to deploy the final deliverable. The AI gives the logic to the smart contract, which in turn generates a short and simple contract of the transaction in order to be stored in a blockchain record. The order within the smart contract is executed when the consumer has cryptographically signed the transaction created by the seller's smart contract.

The other form of combination AI and blockchain is the possibility to deploy machine and deep learning models with a serverless AI layer. For the parties who want to deploy, iterate, and scale their models on their own stack, the Algorithmia platform [7] provides the model deployment with the various kits. It allows the creators to put their work online and make it available to other developers through the API.

```
import Algorithmia
input = {
  "input_file": "data://path/to/file.mp4",
  "output_file": "data://save/data.json",
  "algorithm": "algo://deeplearning/IllustrationTagger/0.2.5"
}
client = Algorithmia.client('API KEY')
algo = client.algo('media/VideoMetadataExtraction/0.1.5')
print algo.pipe(input)

{
  "output_file": "data://save/data.json"
}
```

Fig. 7. The implementation of AI smart contract

In the case for videos over the internet, decentralized AI can be used as a computer vision and deep learning to search untagged video as shown in Figure 7. It is essential since the video can easily be modified to handle any video source by either downloading them directly from a remote source or by using the Data API to connect to the cloud account.

To do so, the creator simply pulled the video from YouTube or another source. The file format is examined before proceeding. Afterward, the video metadata extraction algorithm splits the videos into frames, then processes them in batches. The description and tags of the video for each frame are generated using image classification/extraction algorithms. After the process is done, timestamps are assigned to each extracted tag, allowing users to search across one or many videos for specific tags.

Finally, we can conclude that the AI on the smart contract must satisfy the following requirements:

1. Human accessibility. The contract made with AI algorithm on it should be easy to use.
2. Legal viability. The contract has to be structured in such a way that it serves as proof of acceptance of certain conditions which include the description of an offer, its acceptance, and many others.
3. Flexibility and control. The AI smart contract has to be open for management, adaptation, and renegotiation to realize the world business application.
4. Interactivity. AI smart contract has to encompass the entirety of a contract's life-cycle.

5. Oversight and analysis. The contract should be analyzable by AI agents, bettering user insights regarding their best course of action.

4. Conclusion

The development of AI and blockchain is so rapid that it brings goodness to human life. For AI to transact on their own, it has to be able to programmatically spend and earn a currency, without need to involve people in the process. It is an issue that blockchain solves in general. Blockchain smart contracts enable AIs to own and spend currency as autonomous economic agents. Furthermore, AI on smart contract allows every AI agent to write regular hash functions of their activity to a blockchain so that it is immutable and inspectable by the encryption keys.

Acknowledgment

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-0-00403) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation) and partially was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No.NRF-2018R1D1A1B07048944)

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Www.Bitcoin.Org*, p. 9, 2008.

[2] Z. Chen, W. Wang, X. Yan, and J. Tian, “Cortex-AI on Blockchain,” *Cortexlabs.Ai*.

[3] L. Kiffer, D. Levin, and A. Mislove, “Analyzing ethereum’s contract topology,” in *ACM SIGCOMM Internet Measurement Conference, IMC*, 2018.

[4] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, “CReam: A Smart Contract Enabled Collusion-Resistant e-Auction,” *IEEE Transactions on Information Forensics and Security*, 2018.

[5] M. Mylrea and S. N. G. Gourisetti, “Blockchain: A path to grid modernization and cyber resiliency,” in *2017 North American Power Symposium, NAPS 2017*, 2017.

[6] “Incentivai.” [Online]. Available: https://incentivai.co/product/. [Accessed: 12-Apr-2019].

[7] M. Kiser, “Introduction to Natural Language Processing (NLP) 2016 - Algorithmia,” *Algorithmia*, 2016.