Towards the Trusted Population-Based Optimization Systems

Hiroshi Sato
Department of Computer Science, National Defense Academy
1-10-20 Hashirimizu, Yokosuka, Kanagawa 239-8686, Japan

Masao Kubo
Department of Computer Science, National Defense Academy
1-10-20 Hashirimizu, Yokosuka, Kanagawa 239-8686, Japan
E-mail: hsato@nda.ac.jp, masaok@nda.ac.jp
https://www.nda.ac.jp/~hsato

Abstract

Following the development of evolutionary computation, various population-based optimization methods have been proposed. In these systems, optimization is achieved through the interactions of many individuals/particles/agents. However, when the system is implemented in a distributed environment, reliability becomes an issue. In such an environment, it may not be possible to trust others. There are numerous cases which we cannot guarantee trust, such as malfunction of distributed parts or failure to synchronize. Therefore, we have to make trust between distributed individuals/particles/agents. The record of past actions is usually a good tool for generating trust. This paper introduces the blockchain mechanism into the population-based optimization system to make a trust management system. By using blockchain, we can implement it without a central authority. In the system, all interactions are reviewed and get feedback, and the feedback is used to calculate the trust score.

Keywords: Trusted system, Blockchain, Surrogate Assisted Evolutionary Computation.

1. Introduction

So far, various population-based optimization methods have been devised. For example, Genetic Algorithm[1], Genetic Programming[2], Evolutionary Strategies[3], and Evolutionary Programming[4] are the pioneers in this field. Following the success of evolutionary computation, a lot of other population-based algorithms have been devised such as Particle Swarm Optimization[5], Ant Colony Optimization[6], Artificial Immune System[7]. In these systems, optimization is achieved through the interactions of many solution candidates. They are called individuals, particles, and agents. We use the word "individuals" to point a solution candidate from now on.

When the system is implemented in a distributed computational environment, reliability becomes an issue. In such an environment, it may not be possible to trust others. There are numerous cases which we cannot guarantee trust in individuals, such as malfunction of distributed component, failure to synchronize the information, or injection of malicious individual. Therefore, we have to make trust between distributed individuals. In these cases, the record of past actions is usually a good tool for generating trust.

This paper introduces the blockchain mechanism into the population-based optimization system to make a trust management system. We adopt evolutionary computation as a reference model. By using blockchain, we can implement it without a central authority. In the system, all interactions are reviewed and get feedback, and the feedback is used to calculate the trust score.

2. Blockchain

A blockchain[8] is a list of records, called blocks, linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Fig. 1 shows the example of usage blockchain in evolutionary computation.

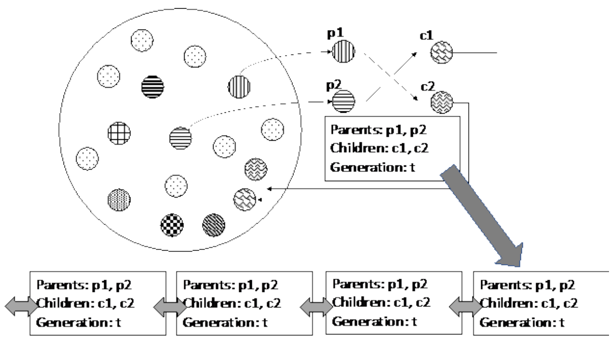

Fig. 1. The usage of blockchain in evolutionary computation.

When blockchains are used as a distributed ledger, they are usually managed by a peer-to-peer network and conform to protocols for inter-node communication and verification of new blocks. Once a block's data has been recorded, it cannot be changed retroactively without changing all subsequent blocks. For this reason, blockchain is considered secure by design and is an example of a decentralized computing system with high Byzantine fault tolerance. These make decentralized consensus a key concept in the blockchain. We use blockchain as a tool of maintaining trust.

Bitcoin[8] and Ethereum[9] are two of the most popular blockchains. While Bitcoin is a book of currency, Ethereum is a book of programs. In Ethereum, any computer program can be put on the ledger, which has attracted worldwide attention as it enables smart contracts, decentralized finance, and decentralized exchanges. Therefore, we focus on Ethereum in this study.

Ethereum is a platform for building decentralized applications and smart contracts, and the generic name of a related open-source software project being developed by the Ethereum Project. Ether is used as the internal currency required to use Ethereum. Ethereum is designed as a general-purpose computer and can run a virtual machine.

There are two consensus algorithms for Ethereum: one is for Proof of Work (POW), called “Ethash,” and the other is for Proof of Stake (POS), called “Casper.”

3. Trust in Evolutionary Computation with Blockchain

This paper concerns the reliability of each individual's information in distributed evolutionary computation. As noted in the chapter 1, the information may not be reliable in distributed environment for some reason. For example, when the computation is curried over the distributed machines, some machines may work differently from the rest by the failure or by malicious action. Moreover, the fitness information will be vague even in a single machine when the system uses a surrogate mechanism. Therefore, we have to estimate how the other individual can be trusted.

Let us assume individuals in evolutionary computation. An individual wants to know the fitness value of other individuals to produce good offspring. In usual evolutionary computation, the fitness value is assumed to be correct. However, we think distributed environment. In this case, the individual has to estimate the fitness through the record of other individuals’ actions. The individual has to decide which individual to trust. The fitness value provided by different individuals may differ. For instance, one may offer a quick answer at a lower quality while another may be slow but accurate.

While the individual will be confident of the validity of their previous interactions with the other individuals, they cannot rely on their knowledge to provide certainty in other individuals’ interactions. We can solve this problem by storing the verified feedback of the record of interaction on the blockchain. Such feedback can be accessed by any trust provider, which offers trust scores as a service. When we use blockchain, the information is available to all parties. This means that the information and trust scoring mechanisms have the following properties: Universal, Transparent, and Verifiable. As an added benefit, the integration of blockchain into the system enables the payment for resource access, including trust score estimation.

We take a quantitative approach to reason about trust, using the information which are built from the feedback of interaction between individuals. The trust calculation is done by direct experiences by aggregating individual feedback scores to form an overall individual opinion about the quality of interaction or reliability of other individuals. Sometimes, direct experience may not be possible when no interaction may have occurred between individuals. In this case, the individual would rely on third-person's information to infer information of other individuals.

4. System Architecture

Fig. 2 shows the architecture of our proposed system for evolutionary computation. This system is inspired Pal's work[10].

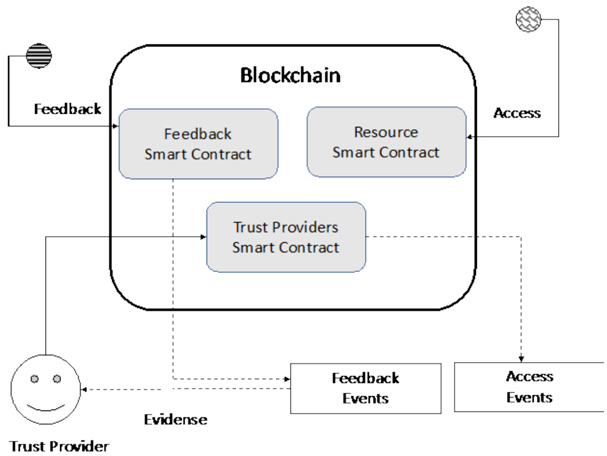

Fig. 2. The architecture of proposed blockchain platform for evolutionary computation.

There are three main components in this architecture, individuals, trust providers, and smart contracts. In the system, individuals can be both information providers and consumers. Individuals can store information, access a resource, deploy smart contracts, and communicate with one another. Trust providers maintain the trust scores. Smart contacts are collections of code and data used to execute agreements between two individuals and stored on a blockchain. We use three types of smart contracts:

- Resource smart contract: that handles access to a resource,
- Feedback smart contract: that handles the reviews submitted by the individuals,
- Trust provider's smart contract: that helps the trust providers to maintain trust scores.

The system is composed of a public blockchain that keeps track of all delegated access rights, consumer interactions, and consumer feedback that is directly linked to one consumer interaction.

The smart contract handles reviews submitted by individuals in the system. It receives a review rating and ensures that the review is linked to interaction. It ensures that a submitted review has the following parts:

- Address of the individual that submits the review,
- Details of the interaction reviewed, and
- A review rating.

The correctness of the system can be verified by all individuals interacting with the public blockchain.

Trust provider is responsible for the trust scoring functions and making the output available to the individuals for some access fee. The trust provider complements its soundness by choosing a scoring mechanism and an evidence selection to implement.

The communication between the components of the system proceed as follows:

1. When an individual wants to check the information of other individuals, he asks the trust provider.
2. The trust provider retrieves a pre-computed score or performs an on-demand trust score calculation.
3. Once the resource has been used an event will be generated on the blockchain.
4. The trust provider will be notified of the new resource access since the event is broadcast on the public chain.
5. The trust providers will then update the feedback smart contract on the blockchain to update the feedback state.

6. If the individual is willing, they can leave feedback for that resource.

5. Conclusion

This paper proposed a framework for trust systems for evolutionary computation where the record of interactions backs up evidence. This paper introduces the blockchain mechanism into the population-based optimization system to make a trust management system. By using blockchain, we can implement it without a central authority. In the system, all interactions are reviewed and get feedback, and the feedback is used to calculate the trust score. We consider several scoring methods for this type of system and averaging approach is simple yet powerful. As future works, we will implement the framework using Ethereum, and a feasibility study should be conducted.

References

1. D. E. Goldberg, "Genetic Algorithms in Search, Optimization and Machine Learning", Addison-Wesley, 1989.
2. J. R. Koza, "Genetic Programming, On the Programming of Computers by Means of Natural Selection, MIT Press, 1992.
3. H. G. Beyer and H. P. Schwefel, "Evolution Strategies: A Comprehensive Introduction", Natural Computing, 1, pp.3 - 52, 2002.
4. D. B. Fogel, "Artificial Intelligence through Simulated Evolution", in Evolutionary Computation: The Fossil Record, IEEE, pp.227 - 296, 1998.
5. M. R. Bonyadi, Z. Michalewicz, "Particle swarm optimization for single objective continuous space problems: a review", Evolutionary Computation, Vol. 25 No. 1: pp. 1 - 54, 2017.
6. M. Dorigo, M. Birattari and T. Stutzle, "Ant colony optimization", IEEE Computational Intelligence Magazine, Vol. 1, No. 4, pp. 28 - 39, 2006.
7. D. Dasgupta (Ed.), "Artificial Immune Systems and Their Applications", Springer-Verlag, Inc. Berlin, 1999.
8. S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance", Computer Networks, Vol. 191, 108005, 2021.
9. Ethereum Project, https://ethereum.org/, (viewed on the 20th Dec. 2021).
10. S. Pal, A. Hill, T. Rabehaja, M. Hitchens, "A blockchain-based trust management framework with verifiable interactions", Computer Networks, Volume 200, 108506, 2021.

Authors Introduction

Dr. Hiroshi Sato

SHe is an Associate Professor of the Department of Computer Science at the National Defense Academy in Japan. He obtained a degree in Physics from Keio University in Japan and degrees of Master and Doctor of Engineering from Tokyo Institute of Technology in Japan. He was previously a Research Associate at the Department of Mathematics and Information Sciences at Osaka Prefecture University in Japan. His research interests include agent-based simulation, evolutionary computation, and artificial intelligence. Dr. Sato is a member of the Japanese Society for Artificial Intelligence (JSAI), Society of Instrument and Control Engineers (SICE), and The Institute of Electronics, Information and Communication Engineers. IEICE). He was the editor of IEICE and SICE.

Dr. Masao Kubo

He is Associate Professor of Department of Computer Science at National Defense Academy in Japan. He graduated from the precision engineering department, Hokkaido University, in 1991. He received his Ph.D. degree in Computer Science from the Hokkaido University in 1996 (multi-agent system). He had been the research assistant of the chaotic engineering Lab, Hokkaido university. He was a visiting research fellow of Intelligent Autonomous Lab, university of the west of England (2005). He is the associate professor of information system lab, Dep. of Computer Science, National Defense Academy, Japan. His research interest is Multi agent system.