NRC: a decentralized platform for Human-Robot Communication

Chen Min, PhD*
NEO Robotics
Singapore
`mchen.x91@gmail.com`

Xie Shudong, PhD†
NEO Robotics ‡
Singapore
`purplebamboot@gmail.com`

Chen Liyuan, Msc
NEO Robotics
Singapore
`colacly@gmail.com`

Abstract

More and more robots are coming into human's daily life, *e.g.*, autonomous driving car and household robot. Unlike traditional robots in the factory, robots that share the same workspace with humans have to (i) gather information on humans' physical state and mental state; and (ii) take actions to achieve their own objectives. Currently, most robots rely purely on onboard sensors to gather information, such as lidar and camera. However, those sensors might fail due to weather or lighting conditions, which might result in fatal accidents. This paper introduces NRC, a decentralized platform built on NEO blockchain for trust-free human-robot communication. With NRC, the human and the robot are able to broadcast their information on the blockchain, and receive the information from other agents for their decision making. Compared with onboard sensors, NRC can provides additional information for the robot that can not be achieved by any sensors available. For example, with NRC, the robot will be able to know the intention of humans. Compared to the traditional communication protocols, the blockchain based NRC provides serveral adavantages: (i) it reduces the cost of trust, *i.e.*, the human and the robot can trust the information they received is correct. This is handled automatically by the smart contracts without any extra effort. (ii) the NRC token gives incentive for the human to share their information to the robots, *i.e.*, the human gets paid instantly when his/her information is used by a robot. As a proof of concept, we test NRC in the scenario of autonomous driving, where we demonstrate the adavantages that NRC provides. Note that NRC is general and not limit to autonomous driving. It can be potentially applied on any robots that share their workspace with humans.

1 Introduction

In the past decades, dramatic prograss has been made in the field of robotics Thrun et al. (2005); Siciliano and Khatib (2016). Robots are moving from factories, where robots have their own workspace, into people's daily life, where robots share their workspace with humans (Fig. 1). There is an urgent need for developing robotic systems that can work closely with human without hurting human or disturbing human's working flow Goodrich and Schultz (2007); Broz (2008).

Unlike industrial robots, robot that working closely with human has to reason over human's physical state and mental state; and plan its own actions accordingly.

---

*Expected to graduate in Aug 2018

†Expected to graduate in Dec 2017

‡NEO Robotics is the name of our team. The objective of our team is to use blockchain technology to improve robots' capabilities and safety when working with humans.

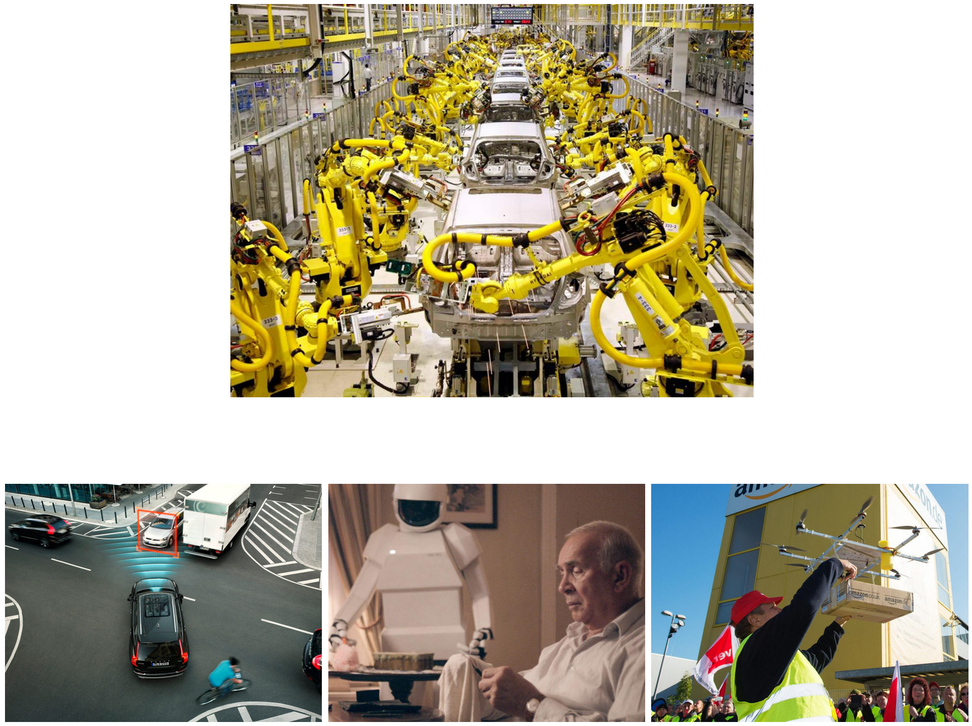

Figure 1: Top: Robots have their own workspace. Bottom: Robots share their workspace with humans.

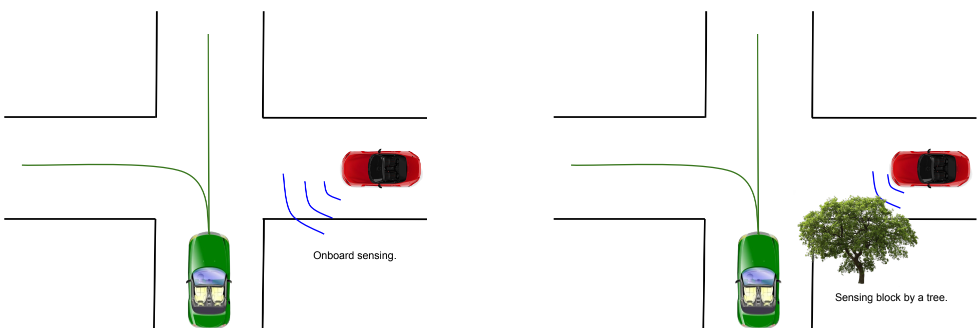

Figure 2: Left column: Autonomous car (red) navigating through an unsignalized intersection, with another human driven car (green) around. Right column: The onboard sensors might fail due to unexpected obstacles, *e.g.*, trees around the road.

Consider an autonomous driving example in Fig. 2 (left column). The autonomous car tries to navigate through an unsignalized intersection while interacting with another human driver on road. Although it is a trival task for human drivers, it turns out to be extremely difficult for a robot car to perform well in such scenario Cunningham et al. (2015). In order to be safe and efficient, the robot car needs to know the positions of nearby human driven cars and the paths that human drivers are following.

Nowadays, most robots rely purely on onboard sensors, *e.g.*, lidar and camera *etc*, to gather information from the environment Siciliano and Khatib (2016); Thrun et al. (2005). Onboard sensors provides only limited information for the robot due to the following reasons.

- Onboard can not read humans' mental state, *e.g.*, the sensors will not be able to tell which direction the huma driver is going (Fig. 2, left column).
- Onboard sensors can fail due to unexpected weather conditions or obstacles, *e.g.*, the sensors is blocked by a tree in the autonomous driving task (Fig. 2, right column).

In this paper, we introduce NRC, a dApp based on NEO blockchain that enables trust-free human-robot communication. With NRC, (i) the robot can get extra information by communicate with the human directly, *e.g.*, the human can convey his/her intent to the robot through the NRC dApp; (ii) the information on the blockchain is guaranteed to be trustable, and the whole system is more robust to server failures due to the decentralized nature of blockchain technology; (iii) the NRC token provides incentives for the human to use the dApp and willing the share the correct information with the robot, *i.e.*, the human will receive certain amount of tokens as reward once his/her information is used by a robot and the information is proven to be correct.

Previous works have been working on protocols for robot-robot communications Yang et al. (2004); Torrent-Moreno et al. (2009); Biswas et al. (2006); McLurkin and Smith (2004). However, none of those protocols can deal with scenarios when human is in the loop. Unlike robot-robot communication, human and robot have different lauguages and they might not understand each other. In addition, humans tends to not share their information with robot for privacy reasons. NRC addresses these two issues by providing intuitive interfaces that are easier for both the human and the robot to understand, and the NRC token gives incentives for humans to share the correct information with the robot.

We tested NRC on the autonomous driving task in simulation as a proof of concept. The preliminary results showed that by applying the NRC blockchain, the autonomous car was able to know other cars positions beforehand, and plan its own actions accordingly to avoid accident.

We believe that robots will become more and more popular in people's daily life, and NRC provides a general solution for human-robot information sharing. Note that, although we demonstrated NRC on the autonomous driving task, NRC is much more general and it can be potentially applied on any robots that share their workspace with humans, *e.g.*, service robots in restaurants or hospitals.

2 Background

2.1 Traditional ways of robot information gathering

Most robots today rely on onboard sensors to gather information from the environment Siciliano and Khatib (2016), including lidar, camera and GPS *etc*. The onboard sensors often work well when the environment is static or well regulated. For example, the robots working in the factories have a well regulated environment, which people are not allowed to go in. However, when robots come into people's daily life, the onboard sensors can fail due to various reasons. For example, none of the sensors available can read humans' mental state, which is crucial for autonomous drving task in Fig. 2. In addition, the lidar or camera can be easily blocked by obstacles or affected by whether conditions Xharde et al. (2006); Levin (2015); Ali (2017).

Beyond onboard sensors, robot can gather information from other agents by direct communication. Researches have developed protocols for vehicle to vehicle communication in the field of autonomous driving Yang et al. (2004); Torrent-Moreno et al. (2009); Biswas et al. (2006); Das et al. (2005).

However, most robot-X communication protocols suffer from two limitations: (1) There is no incentives for human to share their information with robot, and most people are not willing to due to privacy reasons. (2) It involves a third party, *e.g.*, the telecom companies, which makes the trust related fees too high. The telecom companies themselves are trying to make money from it as well, which makes the fee even higher.

2.2 Blockchain and smart contracts

A blockchain is a decentralized ledger that can record transactions between two parties in a verfiable and permanent way without the need for a third authority Swan (2015).

Bitcoin is the first public blockchain that serves the purpose of digital currency Nakamoto (2008). Few years later, Ethereum launched as the first blockchain with programmable and Turing complete smart contracts Wood (2014). Smart contracts allows developers to program on the blockchain. The smart contracts on the blockchain is public that anyone can inspect, and it will exectued deterministically to achieve certain goals in a way verifiable to any all involved third parties.

NEO is China's first publich blockchain, and it is considered to be a compelling alternative to Ethereum for smart contracts and distributed applications Zhang and Da (2017). NEO uses delegated

Byzantine Fault Tolerance (dBFT) for consensus Castro et al. (1999); Vukolić (2015), whereas Ethereum previously used Proof of Work POW (2017), and recently switched to a Proof of Stake model POS (2017). NEO's consensus model allows for a theoretical transaction throughput up to $10,0000$ tps. High transaction speed is critical for NRC, since it will most likely require real-time communication between many agents.

In addition, NEO supports multiple programming lauguages, such as C#, Java, C++, Python, *etc*. This makes it easier for developers to develop smart contract applications on NEO blockchain. NEO is rapidly growing its ecosystem with the help from the community groups, *e.g.*, City of Zion [4] and New Econo Lab [5]. We expect to see more and more advanced feature coming out from NEO platform in the near future.

Considering the various merits of NEO aforementioned, we decide to build NRC on NEO blockchain.

3 NRC for human-robot communication

One can view NRC as a blackbox for trustless human-robot communications. NRC provides the following advantages:

- The message on the blockchain can not be changed and can be trusted.
- The decentralized nature of the blockchain technology will make the whole system more robust to server failures.
- A reward scheme can be built upon the NRC token that provides incentives for human to share their information with the robot.
- The reward happens on the blockchain, which does not need any third-party companies. It provides several advantages, *e.g.*, the reward happens instant, there will be no fees (except for the possible transaction fees).

We believe that by applying the NRC blockchain technology, we can achieve seamless human-robot communications for better robot performance.

4 NRC token

NRC token plays an important role in the whole system. It has two major functionalities: (1) serves as the reward to human for sharing correct information with the robot. (2) serves as the penalty to human if they have been detected for sharing false information with the robot.

The amount of token supply, and the reward scheme has not been decided yet. We plan to do some surveys and user studies to figure out the best reward scheme.

5 Detecting false-positive and false-negative information

There is a possibility that the human intentionally shares the false-positive or false-negative information to the robot. In that case, the information might lead to robot accidents or poor robot performance. We need to come up with a way to detect those false-positive or false-negatie informations and give penalty to the human who sent them out.

In most cases, the robot that uses the information should be able to tell whether the information it received is true or not. However, the robot might make mistakes, *e.g.*, due to sensor failues or the robot itself is lying. Thus, we think there is no deterministic way to find out whether the human provides false information or not.

However, we can use the information from many robots to stochatically tell whether a human is lying or not. For example, if there are many more robots saying that a particular person provides false information to the robot, there is a high probability that the human indeed provides false information. Our NRC system will assign certain penalty to the human if the system thinks he is cheating. On the

[4] `https://cityofzion.io/`

[5] `https://github.com/NewEconoLab/Docs`

other hand, if one robot keeps on reporting other humans while those people have never been reported by other robots, there is a high probability that the robot is cheating. Our system will makes sure one person or one robot can only have one account, which can be achieved by the NEO blockchain easily. In this way, we can make sure the human or the robot will not cheat intentionally, since it will incur a high penalty.

We plan to implement this feature in the future.

6 Proof of concept

We demonstrated our idea in the autonomous driving car example in simulation Fig. 3. Please refer to our project github page for more details [6].

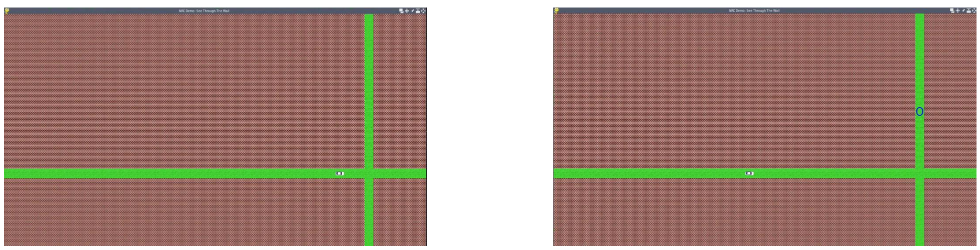

Figure 3: Left column: The autonomous car fails to detect the other car on the road due to onboard sensor failure. Right column: The autonomous car receives information on the other car through the NRC blockchain.

7 Roadmap

There are several milestones we want to achieve.

- Build a machine learning module to automatically detect human cheating or robot cheating.
- Fix the reward scheme through survey or user study.
- Scale up the NRC system to many robots and many human beings.

We do not have a fixed timeline yet, but we will fix that after we hear feedback from the NEO Dev competition committees.

[6] https://github.com/neo-robotics/NRC

References

Osman Ors Ali. 2017. RADAR, camera, LiDAR and V2X for autonomous cars. `https://blog.nxp.com/automotive/radar-camera-and-lidar-for-autonomous-cars`. (2017).

Subir Biswas, Raymond Tatchikou, and Francois Dion. 2006. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *IEEE communications magazine* 44, 1 (2006), 74–82.

Frank Broz. 2008. *Planning for human-robot interaction: representing time and human intention*. Ph.D. Dissertation. Carnegie Mellon University.

Miguel Castro, Barbara Liskov, et al. 1999. Practical Byzantine fault tolerance. In *OSDI*, Vol. 99. 173–186.

Alexander G Cunningham, Enric Galceran, Ryan M Eustice, and Edwin Olson. 2015. MPDM: Multipolicy decision-making in dynamic, uncertain environments for autonomous driving. In *Robotics and Automation (ICRA), 2015 IEEE International Conference on*. IEEE, 1670–1677.

S. M. Das, Y. C. Hu, C. S. G. Lee, and Yung-Hsiang Lu. 2005. An Efficient Group Communication Protocol for Mobile Robots. In *Proceedings of the 2005 IEEE International Conference on Robotics and Automation*. 87–92. `https://doi.org/10.1109/ROBOT.2005.1570101`

Michael A Goodrich and Alan C Schultz. 2007. Human-robot interaction: a survey. *Foundations and trends in human-computer interaction* 1, 3 (2007), 203–275.

Doron Levin. 2015. The cold, hard truth about autonomous vehicles and weather. `http://fortune.com/2015/02/02/autonomous-driving-bad-weather/`. (2015).

James McLurkin and Jennifer Smith. 2004. Distributed algorithms for dispersion in indoor environments using a swarm of autonomous mobile robots. In *in 7th International Symposium on Distributed Autonomous Robotic Systems (DARS*. Citeseer.

Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).

POS. 2017. Proof of Stake FAQ. `https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ`. (2017).

POW. 2017. Bitcoin Developer Guide: Proof of Work. `https://bitcoin.org/en/developer-guide#proof-of-work`. (2017).

Bruno Siciliano and Oussama Khatib. 2016. *Springer handbook of robotics*. Springer.

Melanie Swan. 2015. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Sebastian Thrun, Wolfram Burgard, and Dieter Fox. 2005. *Probabilistic robotics*. MIT press.

Marc Torrent-Moreno, Jens Mittag, Paolo Santi, and Hannes Hartenstein. 2009. Vehicle-to-vehicle communication: fair transmit power control for safety-critical information. *IEEE Transactions on Vehicular Technology* 58, 7 (2009), 3684–3703.

Marko Vukolić. 2015. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security*. Springer, 112–125.

Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper* 151 (2014).

R. Xharde, B. Long, and D. Forbes. 2006. Accuracy and Limitations of Airborne LiDAR Surveys in Coastal Environments. In *2006 IEEE International Symposium on Geoscience and Remote Sensing*. 2412–2415. `https://doi.org/10.1109/IGARSS.2006.625`

Xue Yang, L Liu, Nitin H Vaidya, and Feng Zhao. 2004. A vehicle-to-vehicle communication protocol for cooperative collision warning. In *Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on*. IEEE, 114–123.

Erik Zhang and Hongfei Da. 2017. NEO White Paper. `http://docs.neo.org/en-us/index.html`. (2017).