Cube

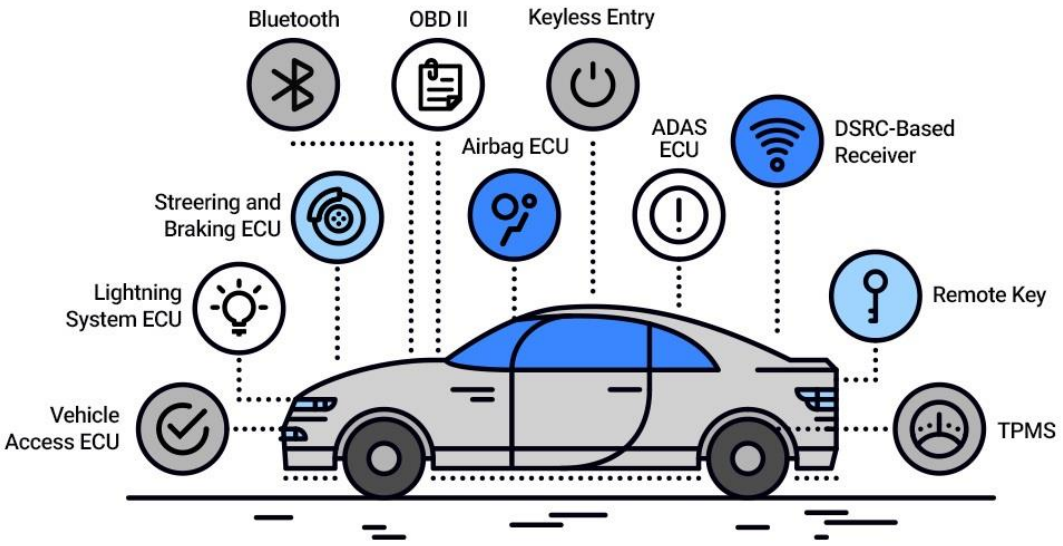
Autonomous Car Security Platform

Cube is the blockchain security platform for autonomous car. The key to Blockchain is that technology ensures trust. Cube uses block-chain technology to ensure the security of autonomous mobile networks.

These days, the car is a mass of software with over a million lines of code. Cars started to use more networks, and autonomous cars should depend on the network heavily for self driving. It uses network navigation route, traffic information, vehicle to vehicle information, and remote ECU upgrade.

This means that autonomous vehicles have a greater risk of being hacked. Perhaps no one has ever suffered from a hacking virus once or twice. However, if a self-propelled vehicle is hacked, it can be a huge risk.

Cube creates a security system that protects these autonomous vehicles from hacking. Unlike past methods that did not prevent hacking, we use blockchain technology. Applying blockchain is not a hack at all, unless you hack hundreds of thousands of computers at the same time. Cube uses blockchains, artificial intelligence, and Quantum Hash Cryptography technology.



The most hackable and exposed attack surface on an autonomous car

Blockchain Layer

Cube uses block-chain technology to ensure the security of autonomous mobile networks. But there are various difficulties in applying traditional blockchain technology to autonomous vehicle safety.

Blockchain instantiations suffers from high overhead and low scalability. Cube solves these limitations of traditional BC technology with hybrid BC.

In the operation of autonomous vehicles, many IOTs provide information to autonomous vehicles. The attacker seeks to gain access to the network between an autonomous car and IoT or traffic center, and manipulate the software binary with the goal of injecting malware into a large number of vehicles. In such instances, the hash of the infected binary differs from the hash included in the multisig transaction which is signed by the SW provider and the OEM. Thus, the vehicles can readily detect such an attack before installing the infected SW update. .

AI Deep Learning Layer

The second is AI Layer. So far, network security is a passive system that collects patches to prevent past hacking cases. Cube trains in supervisor mode in the past as a primary case, and construct a defense system against it by creating malicious attack scenarios that are likely to be made hundreds of millions of times. Cube's Intrusion Detection System using Deep Neural Network for Vehicle Network Security has two types, a discriminative deep architecture and a generative deep architecture, depending on how the architectures are exploited. After the pre-training, fine-tuning will be performed using the gradient descent method with the supervised learning. While Blockchain is used as a first and main security method, AI Deep Learning based security will guarantee the double defense system.

Quantum Hashing Cryptography Layer

Blockchain has improved security by using hashes appropriately. However, there is a growing concern that as the performance of computers grows rapidly, hash cryptography can become a limitation. Cube develops quantum cryptography to prevent malicious attacks against autonomous vehicles. This Quantum Cryptography will contribute not only to the autonomous drive, but also to the overall upgrade of the entire Blockchain technology.

Transparency Policy

Cube considers transparent operation important. Thus, Cube has established a policy for transparency as follows:

1) Cube is to receive a fair audit by recognised and credible accounting firms.

2) Cube shall publish monthly operational and half year financial reports to share the operational status of the company with its contributors.

3) When hiring new staff members, such as developers, Cube shall implement a validation process as well as thoroughly examining the candidates' portfolios and setting reward policies in accordance with their abilities.

4) The company's budget shall be tightly managed so that it will always be possible to operate and manage the company without additional funding for more than three years.

Contributor Protection Policy

To protect its contributors, Cube will be operated as follows:

1) The executive managers of Cube are bound by a lock-up system, which means they are not entitled to make token sales from the starting date of reservation sale for one year. The lock-up policy is intended to make sure the executive managers receive suitable rewards only after the company grows enough.

2) Cube shall strictly control the use of its budget to stably increase the value of Cube tokens. At least two-thirds of the beginning budget must remain after one year of funding. Using more than one-third of the beginning budget for any single event requires the approval of at least half of the board members.

Team

Team members can be divided into two categories. The first is the team for autonomous car communication part. Worldwide, autonomous vehicles were first created in 1995 by the computer engineering department at Carnegie Mellon University. Two members of that Carnegie Mellon Computer Engineering department, and other embedded developers are key members of Cube.

The second category is the blockchain development team. Two key developers are from Samsung Electronics. One was the project manager of the cloud development team at Samsung Electronics, and Geon H. Lee was the head of Samsung's one of major development teams, and brain related team members in KAIST.