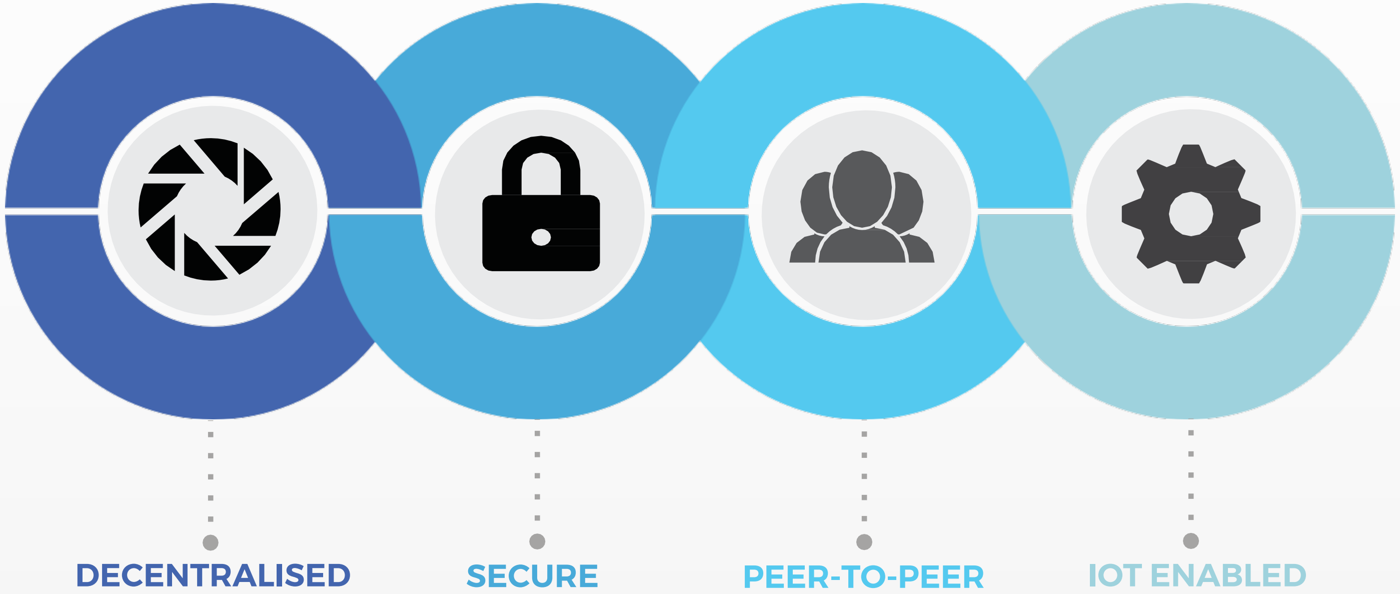
Autonomous Vehicle Management

Peer-to-peer system for self-driving cars based on Streembit™



COMMUNICATION PLATFORM FOR HUMANS AND MACHINES

Why work with us? Why invest in Streembit™?

> **“As our data is then held in proprietary silos, out of sight to us, we lose out on the benefits we could realise if we had direct control over this data, and chose when and with whom to share it”**
>
> Tim Berners-Lee

We pointed out more than a year ago that one of the most concerning issues of our age is that Google, Amazon, and Microsoft own their users' data. In recent news reports, Tim Berners-Lee, the inventor of the worldwide web, voiced his concerns about the personal data of users http://bit.ly/2mywlAs.

We have been arguing for a longtime that a peer-to-peer and blockchain based system is a viable solution for the Internet-of-Things. It seems that IBM agrees with this technology view and invested US$ 200 million to create such a solution http://bit.ly/2dDb0QS. Unlike IBM, we have already a working decentralised IoT software.

WHICH PROBLEMS DOES STREEMBIT SOLVE FOR AUTONOMOUS VEHICLES?

Our decentralized peer-to-peer solution can address problems, and save money for autonomous vehicle management in several areas

Cybersecurity
In 2020, organizations are expected to spend $101.6 billion on cybersecurity

Cost of software
Client-server solutions are becoming increasingly more expensive

Real-time data management

Scalability
Expensive using a client-server topology

Availability & booking management

Authentication and access control

Identity management
Who are the operators and users?

Publishing device and customer information

Contract management
Blockchain & smart contracts

Audit activities
Comply with legislation and law enforcement requirements

Corporate image
Respect privacy

Problem No. 1 - Cybersecurity

Cybersecurity is not just an IT issue anymore. Digital networks are critical to businesses and national security. In 2020, organizations are expected to spend $101.6 billion (http://bit.ly/2lIvnmh) on cybersecurity.

Most cybersecurity attacks are possible because the server components of the client-server architecture have inherent flaws that expose the business to risk.

To paralyze millions of users, all that the attacker would have to do is concentrate their attacking power on the centralized servers or cloud services.

The emergence of autonomous vehicles increases cybersecurity risks for operators. The number of connected cars will grow by the millions. All self-driving vehicles would be offline following a successful DDoS attack.

THE SOLUTION

A DDoS attack on a decentralized, peer-to-peer network wouldn’t be effective – no wonder the decentralized, peer-to-peer Bitcoin has not experienced a network outage since the inception of the network.

Autonomous vehicle operators can mitigate cybersecurity risk much more effectively using peer-to-peer software in the autonomous vehicles use case.

Problem No. 2 - Cost of software

Businesses today rely on client-server solutions. Conventional client-server solutions are becoming increasingly more expensive.

The horde of engineers required to develop and maintain their back-end systems adds even more cost.

To address scalability and high availability requirements, the business must deploy load balancers and cluster servers, even when using the cloud.

Client-server architecture becomes even a bigger issue when considering connected vehicles and devices.

THE SOLUTION

Peer-to-peer software can radically reduce the infrastructure cost of businesses.

We estimate using Streembit could reduce the operators’ server costs by around 95% in the case of autonomous vehicle information management.

Problem No. 3 - Real-time data management

Real-time data management is essential for connected self-driving vehicles, but not easy to achieve.

Server components of the client-server topology introduce a single point of failure risk in real-time device communication.

Real-time data transfer and device control must be secure and efficient – both are challenging tasks.

THE SOLUTION

In a peer-to-peer system, the real-time data transfer is between the nodes, and nothing needs to be channeled through a server.

Our existing peer-to-peer software can achieve more robust, resilient, secure, and efficient real-time data management in machine-to-machine and human-to-machine communication.

Problem No. 4 - Scalability

Not only is scalability incredibly expensive using a client-server topology, it is also a technical challenge. There will be millions of self-driving cars in the not too distant future.

Scalability is likely the most visible problem in conventional client-server based systems. More customers require more servers.

Large server farms create many problems (e.g. security and cost) for any business.

THE SOLUTION

One of the biggest strengths of a peer-to-peer Internet-of-Things network is the capability to manage a large number of devices without exponentially increasing the cost.

We have a data model and network design that can grow to 1.28 billion devices within seconds, all without increasing the cost. This remarkable result is achieved using a simple Kademlia DHT distributed storage.

This is not possible with a client-server architecture. We can solve the problem of scalability for autonomous vehicles.

Problem No. 5 - Availability & booking management

Autonomous vehicles will be shared by users through a pay per trip business model. However, this business model requires the management of availability information and booking.

The availability information must be published, and users must have quick and reliable access to it.

To reflect such information changes across the system in real time is a difficult task. Data security and integrity must be maintained throughout the process.

THE SOLUTION

Using our peer-to-peer distributed storage and communication system we can manage all of this efficiently, and with relatively little cost.

Problem No. 6 - Authentication and access control

A robust authentication and access control management system must be rolled out for autonomous vehicles.

The data of autonomous vehicles will be harvested in an automated fashion, but who will have access to that data? What functions can a human or another machine execute on the IoT connected vehicle?

Is the data being forwarded by the IoT device, or compromised at all on its way to the end-user, never mind whether or not it was sent by the actual device and not in fact by an imposter?

THE SOLUTION

We argue that authentication and access control can be managed on a peer-to-peer network with much less risk and resources compared to a client-server architecture.

We understand IoT security and are experts in the field. We are one of the main players in the W3C WoT(Web-of-Things) standardisation process, and can implement a robust authentication and access control system for autonomous vehicles.

Problem No. 7 - Identity management

Autonomous vehicles will be owned and operated by businesses, most likely by dealers. The dealers will sell the places in the car to their customers.

The business model for this will require precise and dynamic identity management. Customers will want to know, and verify, who operates the vehicles. Likewise, dealers must be able to identify the customers.

Using conventional client-server topology this would require web systems, relational databases, interfacing with certification authority (CA) information, load balancers, clusters, and of course hundreds of software engineers, database experts and system administrators.

THE SOLUTION

Using Streembit and the peer-to-peer approach, we can offer a more robust, secure, significantly simpler, and cheaper identity management solution that is secured by strong PPKI certificates for all parties involved.

Problem No. 8 - Publishing device and customer information

Self-driving vehicles that wish to sell their spaces must make certain information available to both their customers and authorities. Information like safety certificates, details about their owners and operators, as well as insurance policy certificates.

Customers and authorities must be able to validate and verify this published information.

Implementing a verifiable information management system - that allows for large scale and dynamic real time data updates - using the conventional client-server topology would be a very resource consuming task.

THE SOLUTION

We can make any information available to a worldwide audience using the Streembit peer-to-peer network.

Problem No. 9 - Legal contract management

Operation of autonomous vehicles will require legal contract management. Contracts that include, but are not limited to, selling insurance policies as well as selling places in the vehicle.

Such transactions require a comprehensive legal framework that ensures the implementation can be used in various jurisdictions worldwide, and complies with local regulatory requirements

To design a system like this using conventional technologies would require tremendous infrastructure and engineering resources.

THE SOLUTION

We believe that the legal contract management of autonomous vehicles can be dramatically simplified with smart contracts and blockchain technologies.

Problem No. 10 - Audit activities

For regulatory and law enforcement compliance as well as insurance management reasons, the activity of vehicles and customers must be audited. Multiple actors must have access to the information on demand and upon request.

This access must be configurable, secure, and shouldn’t compromise the privacy of the users. This is an enormously expensive and complex task using conventional client-server architecture and web based systems.

THE SOLUTION

Using a peer-to-peer topology, the auditing activities can be radically simplified and secured. Businesses can delegate most information management aspects of activity auditing to the peer-to-peer system, while retaining the capability of accessing the information when it is needed. The vehicles and customers could share their audit information with all relevant parties directly peer-to-peer without going through the company infrastructure. At the same time, the business can pull all activity related information from the P2P network.

Problem No. 11 - Corporate image

The younger generation is concerned about privacy as well as ethical business practices. This will force businesses to turn away from the conventional, centralized, client-server software solutions.

A social conscience and ethical behavior strategy is surfacing, particularly in ‘western’ societies where people are becoming more reluctant to trust their private and personal data to commercial third parties.

The same is true for communications, thus the rise of many more encryption-based mobile applications. Although the majority of these still rely on the centralized server model.

THE SOLUTION

Only peer-to-peer software can adequately address such privacy and ethical issues. Businesses can project an ethical and user-friendly image to the world by using a peer-to-peer solution. An increasing number of computer users and businesses are interested in blockchain and peer-to-peer software for this very reason.

REINVENTING THE AUTOMOTIVE INDUSTRY WITH THE BLOCKCHAIN

Rapid integration of new entities.

SCALE

Operates without servers

EFFICIENT

Data is secured with PPKI cryptography

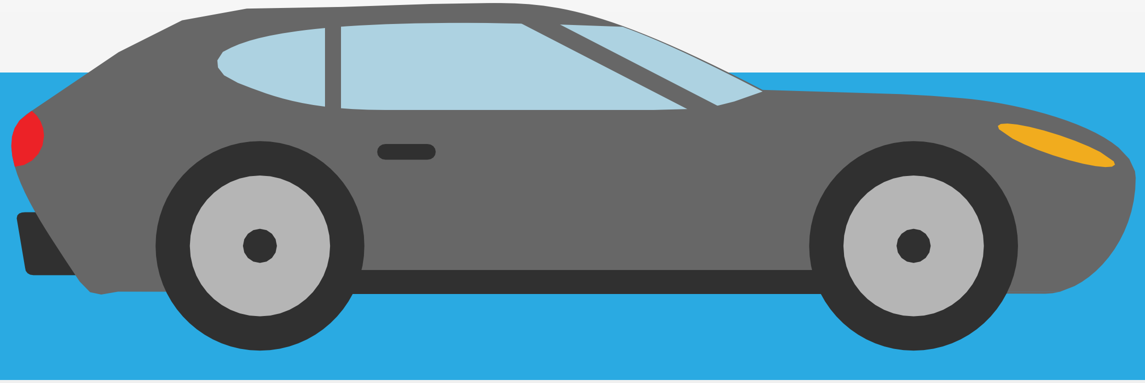
SECURE

Resilient to DDoS attacks

RESILIENT

Minimal infrastructure cost

ECONOMICAL



STREEMBIT VALUE PROPOSITION

- **P2P communications platform** allowing anyone, anywhere in the world to send secure content and conduct transactions across multiple channels without any requirement for personal information

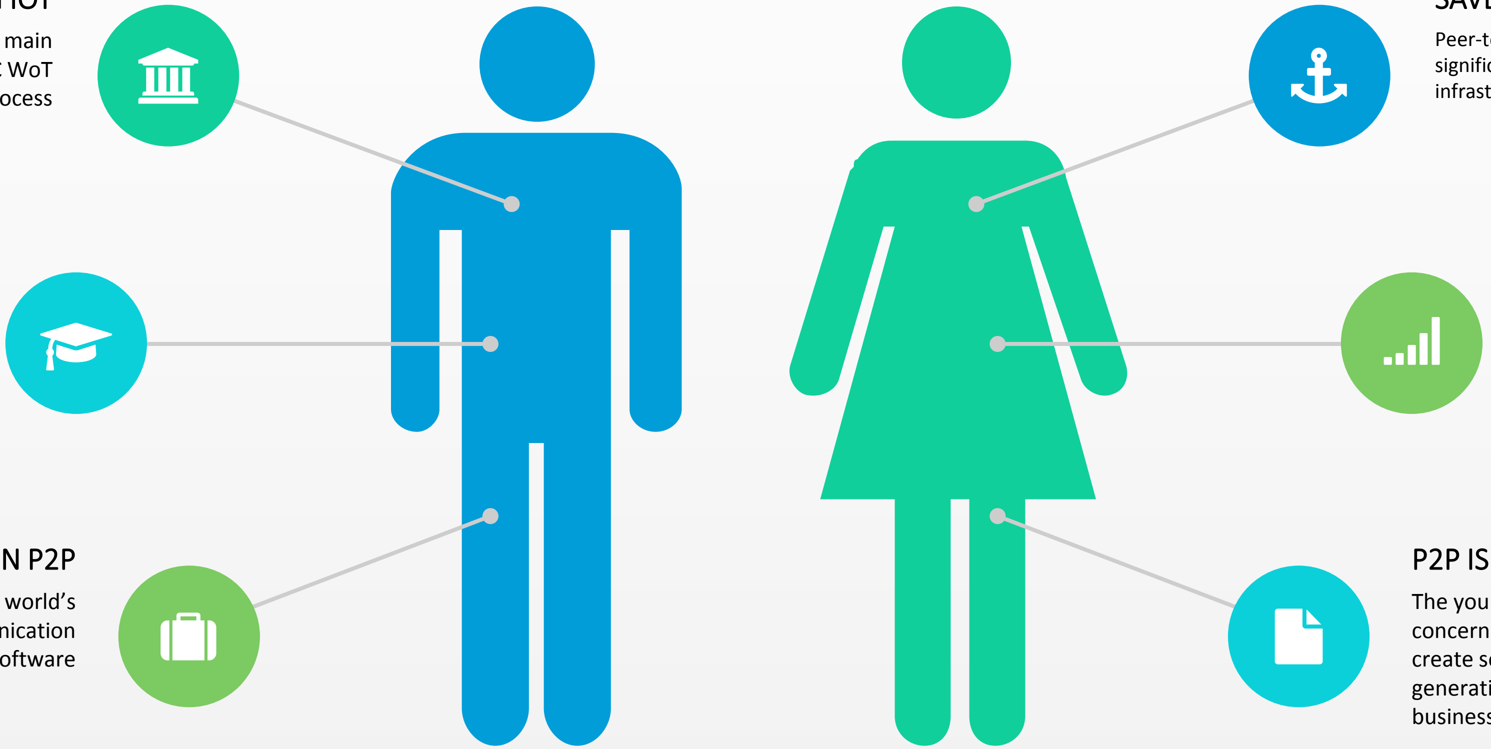
- Eliminate ‘**reliance on a middleman**’ infrastructure to enable rapid and cost-efficient scalability – moving away from the client-server model and it’s associated costs (storage, load balancers, etc)

- Delivers **step-change in security principles for IoT** and secure messaging via a decentralised model. A product of cutting edge research and expertise in the Web Of Things and W3C

- Provision of **new business models and services** running on the Streembit network, linking the communication process to contractual services

- **Community driven and Open Source**. There is no corporation in the Streembit ecosystem that manages users data. Unlike users of Amazon AWS or Microsoft Azure, the users of Streembit cannot be monitored by any service providers

Why work with us? Why invest in Streembit™?



EXPERTISE IN IOT

We are one of the main contributors in the W3C WoT standardization process

EXPERTISE IN SECURITY

We define the W3C WoT security standards

EXPERTISE IN P2P

We've developed the world's first P2P communication software

SAVE MONEY

Peer-to-peer software can significantly reduce the IT infrastructure cost

GLOBAL POTENTIAL

Our novel software solves problems for human users and machines worldwide.

P2P IS THE FUTURE

The younger generation is concerned about privacy. We create software for the younger generation and forward thinking businesses.

ABOUT US

STREEMBIT

Decentralized, peer-to-peer, secure communication system for humans and machines

Home Page

https://streembit.github.io/
http://www.zovolt.com/

Telphone

(+44) 07557 126881

E-mail

tzpardi@streembit.com

Social Media

www.twitter.com/streembit
www.facebook.com/streembit/
https://uk.linkedin.com/in/tibor-z-pardi-b406a780