Machinomy

Micropayments for the Internet of Things

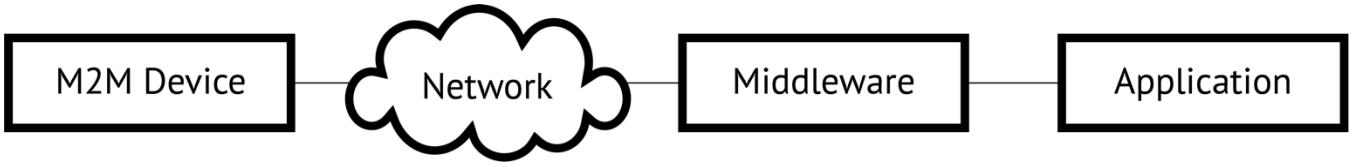
Coined by Kevin Ashton in 1999 Internet of things gains adoption as more smart things enter the market. An aquarium, a light bulb, an air conditioner, a toaster, and even a toothbrush become smarter. Current generation of the smart things heavily relies on cloud computing with its centralized architecture and security compromises. Machinomy is a platform for autonomous devices built on distributed communication and economic incentives. It allows a developer to easily build todays application in a safer and more reliable way as well as implement new scenarios such as paid machine-to-machine services.

Internet of Things in the Cloud

Idea on how connected devices change our life is ages old. Mark Wiser in a seminal paper “The Computer for the 21st Century” described a concept of ubiquitous computation, that run on low power devices connected to each other. From a user’s standpoint a group of the devices is a united computer blended into an environment. The paper was a success both in academic and industrial communities. Lack of ubiquitous wireless connectivity prevented the vision to be realized.

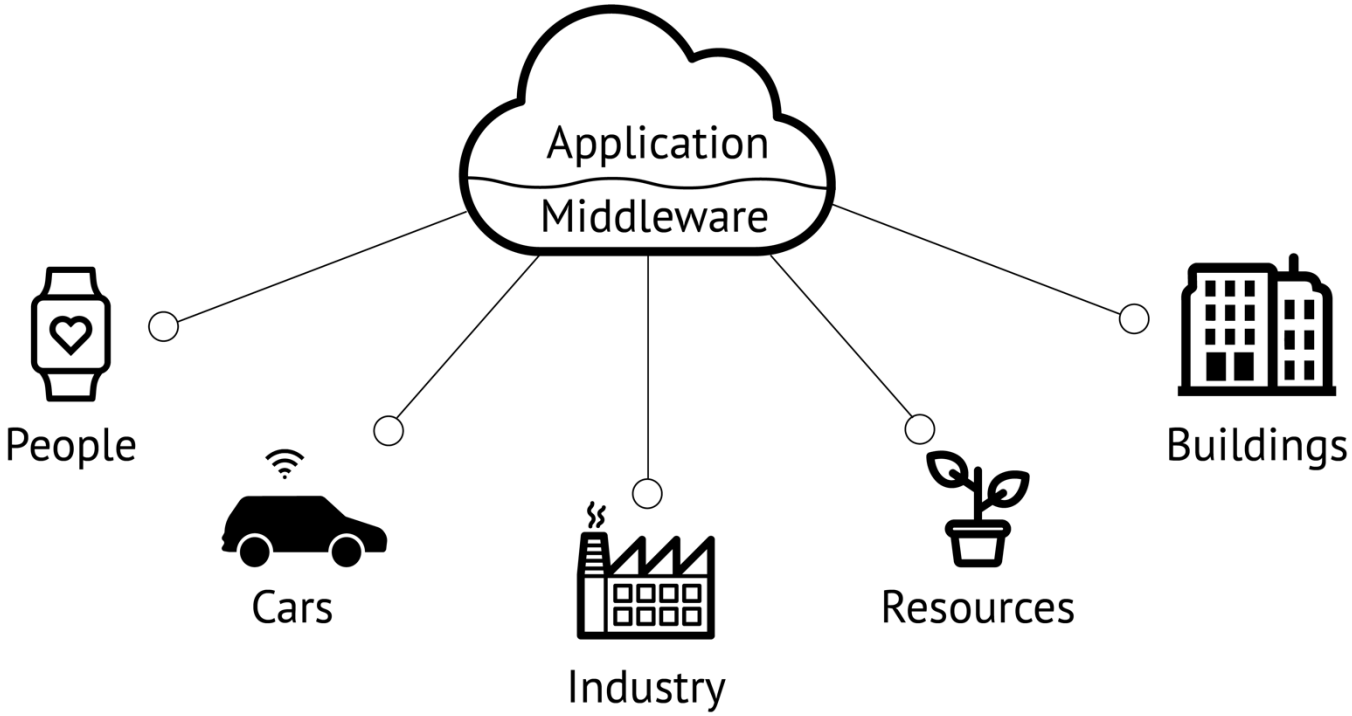
The closest approximation was so called M2M (machine-to-machine) systems. Here a lot of identical devices communicate to a central server via cellular network. The system lowered costs on remote control and monitoring. Contrary to the original vision it allowed devices communicate only to the

server. There were no direct device-to-device interactions. That limited applications to control and monitoring inside a single enterprise only.



In 1999 Kevin Ashton get the idea back into the discourse while working on radio frequency identification methods. He invented the name “Internet of Things”. The researcher proposed to attach sensor to every real life object so that computers could feel or sense what goes on in the real world. Technology developments in the 2000s turned the vision into a modern concept of smart machines connected to the Internet.

Cellular network, indoor wireless connectivity and low power computers became affordable enough to be embedded into everyday things. Server-side infrastructure got cheaper, familiar and itself turned into an everyday thing. Internet-related engineering practice evolved into an easy occupation. All of that drastically lowered the entry point to the industry. Boom of the smart things we are going to observe in the next few years.



The modern Internet of Things architecture is an evolution over M2M.

Heterogeneous devices communicate to a central server, also known as a cloud, via the Internet. The main difference point is using standard transport protocols between the device and the server. Now these are common internet protocols used everywhere else like HTTP, COAP, MQTT. Server side is too standardized all over. It is easier now to connect cloud services together thanks to a common communication and payments stack.

Centralization

Popularity of the web technologies put a monopoly on engineering approach to the architecture. Any problem is solved in client-server paradigm. Server stores data and performs a computation. Client handles user interface.

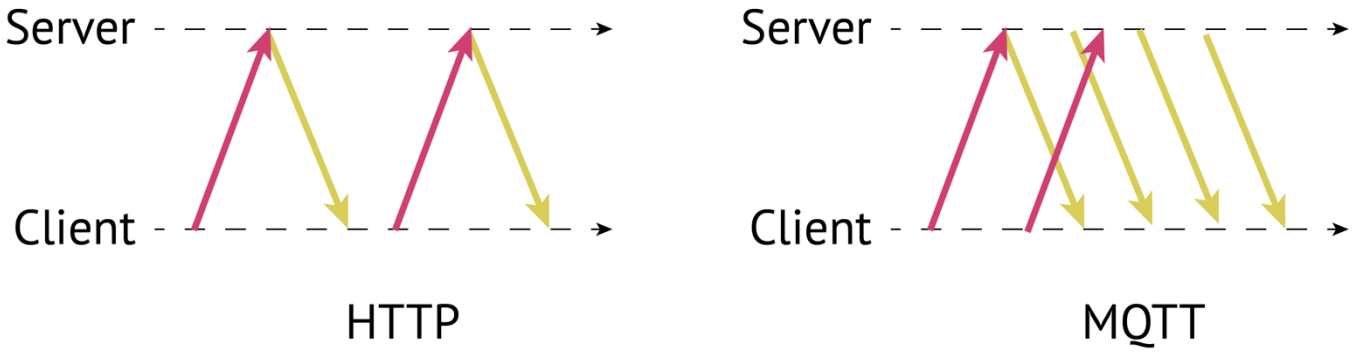
Solutions for IoT development work in that paradigm. A device sends raw data to the server and accepts a command. It is a client. The server analyzes the data and emits control signals.

Any software contains errors. Internet of Things today stores all the data from all the devices on the server. This is an obvious security threat, shown by Turkey, Filipino, and UAE breaches (1; 2; 3). In the worst case, a malefactor interrupts an industrial process, that leads to deaths and injuries. It is real brakes on your connected car could be remotely disabled (4).

Interoperability

Common protocol is a prerequisite for a seamless communication between devices. Logical level, that is software, here is of more importance then physical one. Wireless protocols like Bluetooth, Wi-Fi, IEEE 802.15.4 provide usual TCP/IP to an application. Higher level protocols that work on top of TCP/IP match the paradigm. HTTP and its resource constrained brother COAP use “request-response” model. A client sends a request. A server sends back the response.

AMQP, MQTT, DDS use a “publish-subscribe” model. A client declares what it likes to receive after being connected to a server. The server dispatches or publishes updates to the interested clients.



Both communication models are important, as specifications for industrial applications show. One could not use them both simultaneously though. The protocols support just one model each. XMPP is suitable but too heavyweight for embedded applications.

Another problem appears when doing peer-to-peer interaction between the devices in comparison to device-cloud interaction. Use of the mentioned protocols in the setting lead to an obvious Denial of Service attack. Device identifier here is IP-address. A malefactor could send there garbage data and overloads the device up to its death.

Control

Client-server approach requires a client to always know how to connect to its cloud. DNS is used to match the cloud name and actual servers. It is easy to block. The more important problem you actually lease the name. Any delay from the cloud's owner leads to lost control over the device.

"Smart" part of the connected device is on the server, which is controlled by the vendor. Under some unfavorable conditions a device's owner lose control over her own property. It is either vendor bankruptcy (5) or intentional end of life (6).

Coupling of a device to its cloud and inability to make device-to-device communication sustainable leads to a walled garden IoT ecosystem per vendor. Devices in the same local network could be made interoperable. Devices that work through the cloud only are left alone.

Payments

Payments layer does not contribute to the Internet of Things now. The concept focuses on devices that neither pay nor accept payments by themselves. It would be a mistake however to consider economic relations and smart devices unrelated.

The Internet turned into what we know it to be today thanks to a payment layer built on top of traditional banking system. Easy payment from an ordinary user started boom in e-commerce. Easy payment for an infrastructure service like Amazon Web Service and Twilio gave rise to explosive growth of internet business. That allowed startups to trade CAPEX for OPEX and offload supporting operations to a 3rd party. Data analytics and low-level communication is an example of such an offloading in the cloud Internet of Things sphere.

Devices per se lack payments infrastructure. Bank infrastructure is inadequate for the application. Traditional payment mechanism essentially gives access to a bank account to a 3rd party. This is an obvious security threat. At the same time it is clear in one way or another payments belong to the open Internet of Things. Most of the meaningful use case scenarios depend on secure payment infrastructure. Due to reasons mentioned above they are quite impossible to implement today.

Distributed Internet of autonomous devices

Fundamental deficiency of the cloud Internet of Things makes it unsustainable in the next few years. Experts agree (2) the solution is a move to a distributed architecture. As much functions as possible should be moved to a network edge, to end devices. This significantly improves security of the system and opens up new use case scenarios. Movement for a distribution have just started. No platform out there could serve as a one stop shop for a distributed IoT developer. There is just a concept on what the platform includes (7; 8; 9).

Machinomy is a platform for autonomous devices based on distributed communication and economic incentives that allows a developer easily build secure and open IoT systems.

Open and closed Internet of Things

Internet of Things development path resembles the one for the big Internet (10). Now we are going through a stage of discovering a system is better be open. That means devices and software are interoperable with each other. The architecture is emergent. Closed system has a certain fixed architecture, and a predefined number of participants.

Communication

As shown above existing protocols do not fit the niche of distributed device communication. Machinomy provides a distributed communication protocol based on Tox. The protocol allows devices to communicate directly with no central server under any network conditions. It does not matter if the devices are in the same network or on separate continents. All the messages and metadata are encrypted. No malefactor can read a message, or infer its length, or find out a sender or a recipient. Audio, video and other streaming content are supported along with text messages. With that capabilities it is still low overhead and suitable for embedded applications. Protocol does not explicitly disclose IP address making Distributed Denial of Service attack harder to implement.

Identity Management

In a closed IoT system all the participants know and trust each other. It is clear who is responsible if anything goes wrong. The open Internet of Things states the trust problem in front of a developer. The device has to know if a vis-à-vis device can be trusted and who is responsible for a fault on its side. PKI solves a similar problem in human world. Certificate Authority issues a self-signed root certificate. It signs every certificate issued afterwards. If you trust the Certificate Authority, you trust all the certificates it signed. The technology is validated by almost 50 years of continuous evolution, but it is intended to answer the question “Who are you?”. We need to answer another question “Who do you belong to?”

Machinomy includes a device identification management system built on blockchain-based technology. Blockchain is a special append-only distributed database enforced by cryptography.

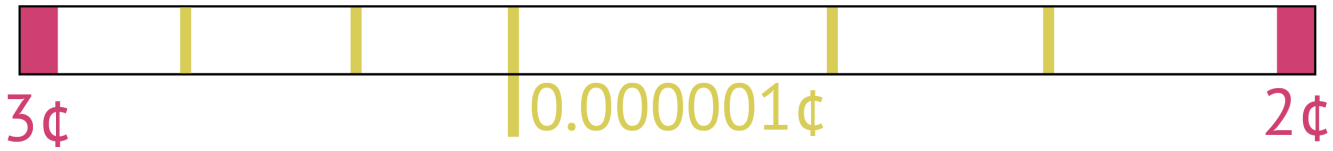
A device manufacturer and an owner play role as Certificate Authority and issue self-signed certificates. These sign chained facts of a device ownership transfer. Any change in the chain is signed by both parties. It is stamped by the blockchain for additional security.

Payments

In the Web payments are used in e-commerce as well as for purchasing of cloud services, that is computing power. Payments layer is based on the traditional banking infrastructure. For the reasons stated above, devices cannot use it without being hard pinned to the cloud.

Machinomy uses cryptocurrency for payments. It runs in a completely distributed fashion. It does not allow anyone to transfer money without the explicit order of the owner. In this respect, cryptocurrency is similar to cash. In addition to safety, cryptocurrency is a cheaper means of transferring money. Fee for a relatively large payment in cryptocurrency is a few cents compared to 30 cents for a bank transaction.

On top of this we have built a so-called payment channels, with a commission of about 5 cents per channel. This is a special type of money transfer extended in time. The channel can be opened for an arbitrarily long time. Inside the channel, you can make unlimited number of transactions, including microtransactions as low as 0.00000001 USD.



With micropayments a device buys extra computing power by itself. Thus, it is untied from the cloud and receives freedom to communicate with neighboring devices on an economic basis.

(Micro)payments mechanism is the most important thing in the whole system. Device identification management system and distributed communication are required for the payments layer to work.

Applications

Real Time Microinsurance

Microinsurance is an insurance for low income population. The segment earns less than $ 4 a day per person. The microinsurance is characterized by simplicity and low cost of the product. It is common in third world countries, but more and more penetrates the first world. Due to the simplicity of the product it is increasingly distributed via smartphones. In developing countries, large part of the population (12) is covered this way.

Micropayments enable real-time insurance. A user concludes a contract and terminates it any time, all through her smartphone. The insurer then withdraws the money per minute or larger quantum of time. Actual price depends on the user's activity and geography. That makes underwriting easier. Internet of Things sensors around the person make the microinsurance even more profitable as the cost of risk is precisely calculated.

Telematic Insurance

Auto insurance is available all over the world. An insurer calculates basic cost of the insurance based on social, demographic factors and a car's state. The next important factor, namely driving style, is accounted for via vehicle telematics. Traditionally a special device records that. Progressively a smartphone is used instead.

Insurance cost changes according to a road type, speed, time, and quality of driving. The driver observes the change in real time on the smartphone screen. However final payment is done at the end of a period. Usually, it is a month. Application of micropayments to the industry would turn it into real-time insurance, that could be turned on and off without costly red tape.

API Services

The main benefit of micropayments and Machinomy platform is that device buys the necessary service and communicates with the outside world all by itself. A manufacturer does not need to bind it to its own cloud, to be a gatekeeper between the device and a third-party service, which leads to savings in infrastructure.

Third-party software services extend the capabilities of the device or take on the non-core functions. It is quite similar to Software as a Service (SaaS) model. The model has proven itself in a bigger human internet. Restrictions on the payment infrastructure restrict real-time billing and lead to monthly payment and billing thresholds: up to 100 requests per day 0.7 cents per query and 500 queries - 0.5 cents per query and so on. Micropayments through Machinomy platform tie the billing and payment in a flexible system adjusts the price depending on the complexity of requests, time, stress, and other factors.

Artificial Intelligence as a Service

Artificial Intelligence (AI) includes natural language processing, image and video tagging, predictions and analytics. Any good enough AI requires a lot of computing power, and does not quite fit the constrained environment of a device.

Weather

People get used to free weather forecast. It is not really free. It is subsidized through advertisement or paid clients. The forecast for a device, for example, a controller of an autonomous farm, could not be subsidized by an advertisement. It have to pay for the forecast. At the same time an owner of a weather station earns by selling the weather data to an aggregator.

Maps

Maps by itself are free if you use OpenStreetMaps. To draw a route, check the status of traffic jams, and get a location of landmarks requires money. Car giants enter into an agreement with the supplier of such information and

make it free for the car buyer. In a distributed Internet of things system, the car finds their own supplier of map services that meet the specified interface.

Autonomous vehicle

Just ten years ago, an autopilot in a car seemed to be a distant dream. Now it is a real. Autonomous vehicles and drones basically need maps and fuel. Geo services described in the previous section. Payments for a fuel could be made on behalf of the owner by a credit card, but it will require an appropriate acknowledgment by the bank rules. Human involvement greatly reduces the value of the autonomous device. Machinomy allows the device to ask its owner for a refill and provide regular report on spending. The device makes a decision to spend the money all by itself, freeing more time for the owner.

Autonomous appliance

IBM demonstrated a distributed Internet of Things on the example of a washing machine. It called the service engineer after breakage, and autonomously ordered a detergent. With the high cost of human labor it is cheaper to prevent damage. That is why a more realistic scenario is the washing machine periodically uploads data about their functioning to a predictive analytics service and purchases a forecast for the misbehavior. That gives the device a warning about a possible emergency break, after which it calls a service engineer.

Sharing Economy

An owner of real estate property, a car or a professional device does not always use them. She could use renting to reduce operating costs. Specialized renting marketplaces tie the owner to itself. It limits her opportunities to reach broader audience. A developer could unbundle the rental market. A marketplace like AirBnB remains a showcase. Machinomy provides an environment for the usage-based billing, insurance and transfer of ownership. A smart home controller accepts payment from the renter, and orders supplies and maintenance costs. Human attention is required only in complex, non-standard situations. This further reduces the costs of the owner.

Smart Refrigerator

An image of an intelligent refrigerator, which buys products on its own according to an owner's diet is the first to come to mind when talking about the Internet of things. As with fuel, the value is destroyed when a person has to confirm every payment. The platform allows the following scenario. The refrigerator monitors available products and their consumption. It transmits this information to an analytics service. The service responds with the preferred diet based on consumption, and recommendations on shopping list. The fridge then orders food online based on the shopping list.

References

1. [Online] https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/.

2. [Online] http://techcrunch.com/2016/04/06/how-to-deal-with-iot-challenges-through-abstraction/.

3. [Online] http://www.bankinfosecurity.com/qatar-national-bank-suffers-massive-breach-a-9068.

4. [Online] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

5. [Online] http://www.wsj.com/articles/ge-says-quirky-has-hurt-its-reputation-1449179311.

6. [Online] http://www.theinquirer.net/inquirer/news/2453441/revolv-users-revolt-as-googles-nest-bricks-smart-home-hub.

7. [Online] http://www.chainofthings.com.

8. [Online] http://www.ibm.com/services/us/gbs/thoughtleadership/internetofthings/.

9. [Online] http://m2m.digitalcurrencysumm.it.

10. [Online] http://radar.oreilly.com/2014/04/toward-an-open-internet-of-things.html.

11. [Online] http://www.wired.co.uk/news/archive/2016-04/22/philippines-data-breach-comelec-searchable-website.

12. [Online] http://techcrunch.com/2015/12/29/microinsurance-is-the-answer-to-the-insurance-industry.

13. [Online] http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies.

Sergey Ukustov
Konstantin Makarychev

http://machinomy.com/