CORE®

BLOCKCHAIN AS AN ENABLER FOR THE DECENTRALIZED INTERNET OF THINGS

Kenneth Chu Sam

19. April 2016
COREtechmonitor | Blogpost

Key Facts

- With a growing number of interconnected smart devices in the market, the Internet of Things (IoT) is bound to become a reality
- Security is still a critical requirement that IoT must fulfill before it can gain widespread acceptance
- Blockchain based solutions can be used to address some of the key security challenges faced in IoT ecosystems

Report

INTRODUCTION

The evolving technological landscape has increased the available means for individual devices to collect, store, process and transmit data, also augmenting their capability to interact with their environments. Internet of Things (IoT) is the name given to the result of this new generation of interconnected devices and through it, a world of intelligent solutions has been envisioned, ranging from optimized garbage collection routes by detection of rubbish levels in containers, to remotely monitored pill cameras for patient diagnostics. However, a series of challenges still need to be overcome before IoT solutions can gain widespread acceptance and blockchain technology may present a viable approach to solve them.

In this article you will find out more about the idea of IoT, selected security challenges in IoT applications, and possible blockchain based solutions to address these issues.

IOT AND THE SMART CONNECTED FUTURE

Rising availability and accessibility of micro sensors, internet penetration rates and development of wireless connectivity (e.g. near field communication, LiFi) are making it possible to design devices that can collect a variety of data and interact with other elements in their environment. The notion of machine-to-machine interaction has existed since the late 60s: in 1968 the idea of devices communicating to provide the service we know today as caller ID was first conceived. However, most connected devices nowadays still act as stand-alones or are controlled by a central entity. IoT extends the impact of the interaction between devices to an entire network of objects to form a smart and decentralized ecosystem.

In the not-so-distant future we could expect our washing machines or other household appliances to monitor electricity prices to operate when fees are low, refrigerators to keep track of food expiry dates and initiate grocery orders, or maybe even toothbrushes and bathroom scales that measure our health and trigger doctor appointments when necessary.

The core concept of IoT, devices collecting and sharing information to allow (automatized) advanced decision-making, can be applied to a variety of scenarios, which together build the vision of a smart world.

Critical Requirement for IoT ecosystems: Security

While smart interconnected devices are already available in the market and are gaining traction, for IoT to develop into a mainstream reality there are still issues that need to be addressed. The ultimate IoT vision requires new devices being able to easily form a new ecosystem or join an existing one. These appliances will need to exchange information with each other and ideally perform transactions or execute predefined actions automatically. As the number of new devices that participate this network, the complexity of their interactions as well as the sensitivity of the exchanged data increases, security becomes one of the key challenges. Some of the basic issues revolve around identification and authorization, and can be summarized in three questions: is my communication partner really who he claims to be? Has the interaction between my communication partner and me been authorized? And how can we ensure the validity of transactions?

The traditional approach to solve these issues would require a central trusted third party to oversee or support the interaction between devices. For example, a certification authority would issue certificates and register public keys to assure the identity of an IoT participant, a central computer would act as an intermediary between parties, enforcing rules and routing communications or acting as a central bank, holding a central ledger where transactions between devices are recorded.

In the context of IoT, relying on a centralized solution has its drawbacks or may not always be applicable. A central entity through which all communications are routed can easily become the single point of failure or bottleneck of the entire network. Central databases recording transactions or identities become attractive targets for attacks aiming to manipulate the behavior of the network. Devices that spontaneously come in close proximity with each other and have the need to exchange information may not share a central node they know to trust and can confer with.

Blockchain based solutions

The issues faced by IoT systems have clear parallels to the challenges that blockchain, also named distributed ledger technology (DLT), was designed to tackle. Originally conceived as the cryptocurrency Bitcoin, DLT allows a network of computers that do not trust each other to perform transactions among themselves without the need of a trusted third party. A more detailed introduction about blockchain technology, can be found in the section “Blockchain in a nutshell” of our previous article “Blockchain – A brief introduction and guidelines for action”.

A number of applications using blockchain technology have been recently developed which could be used to solve the security challenges described above. ShoCard, for instance, proposes a digital identity service that relies on storing signed hashes of personal data on the blockchain. A trusted KYC checking company would then issue a signed certificate on the blockchain pointing to the user’s record entry also on the blockchain. To identify himself to a new party, the user would have to supply his public key and the raw identification information, as well as the location on the chain of the certificate and the hashed data. By calculating the hashes of the raw information presented, and comparing it with the hashes stored in the blockchain, the party receiving the information can be certain that the information provided by the user is identical to what was presented at the KYC-process. While created with the identification of people in mind, the concept

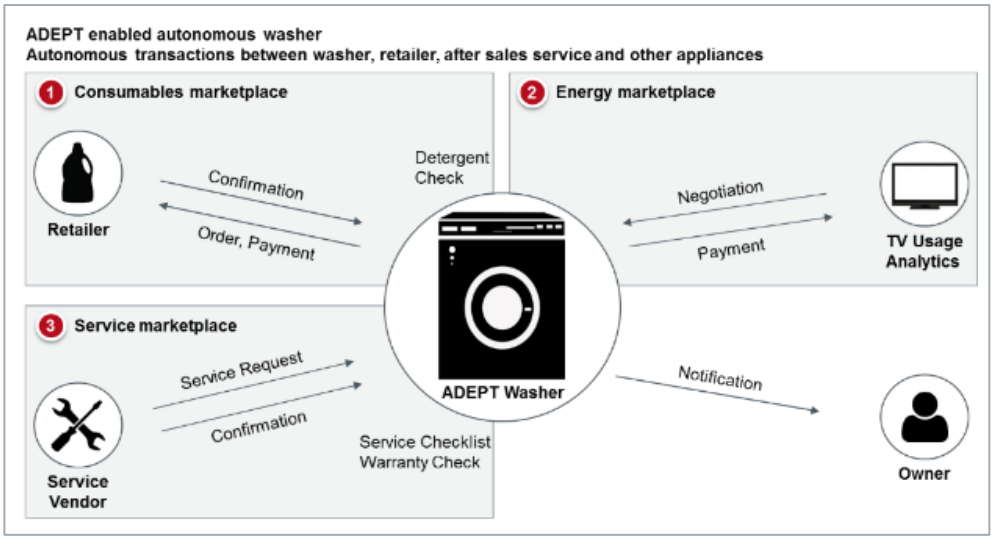

Figure 1: ADEPT enabled washer

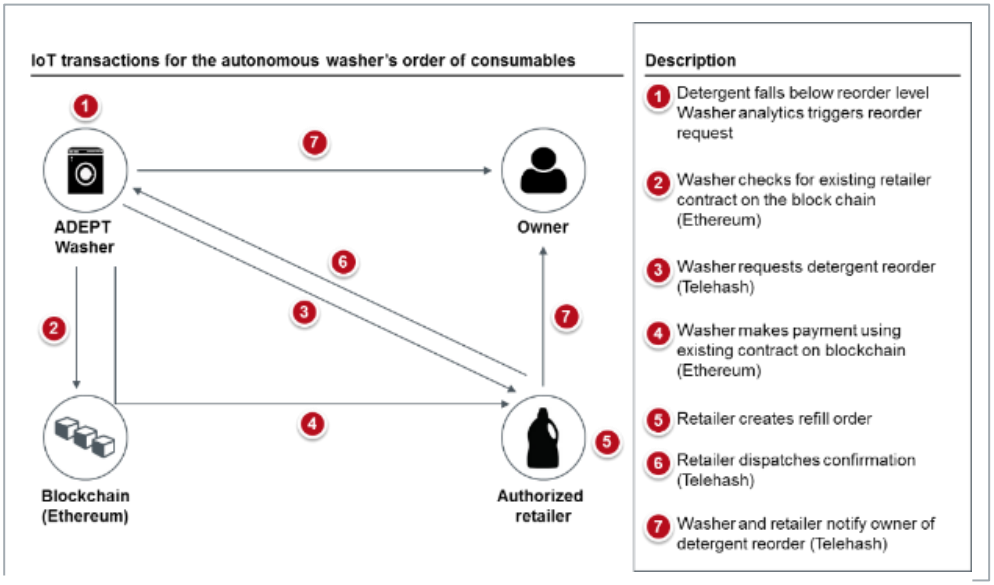

Figure 2: IoT transactions

behind ShoCard could also be applied to validate the identity of new devices in an IoT environment.

Smart contracts are a possible approach to implement and enforce rules in an IoT ecosystem. For example, the set of conditions that must be fulfilled for a specific action to be authorized can be modelled into the blockchain. If these conditions are met, the defined action is triggered at the corresponding devices. By using the blockchain based approach it is not necessary for devices participating in this action sequence to trust each other and an auditable record is produced in the process.

Due to the cryptocurrency Bitcoin being the origin of blockchain technology, applying blockchains to power transactions for IoT is probably the most evident use-case. IBM has jointly developed with Samsung Electronics a proof-of-concept for their Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT)

in which they describe a so-called “Economy of Things”, based on blockchain powered marketplaces for services, consumables or energy where connected devices can negotiate, order and pay for their needs autonomously. ADEPT’s solution approach requires three foundational functions: peer-to-peer messaging based on Telehash, distributed file sharing based on BitTorrent and autonomous device coordination relying on Ethereum. Combining these three protocols, ADEPT would allow devices to communicate, barter for resources and perform the necessary purchases without additional external intervention.

There are still significant challenges for IoT systems beyond the ones described in this article, both from the business as well as on the technical perspective. Nevertheless, it is safe to assume that in the near future, smart interconnected devices will play a much greater role in our lives. While blockchain itself is also a technology in its early stages, the benefits that it promises could strongly support the development of the IoT ecosystem. Companies exploring how IoT could affect their business should also evaluate how blockchain technology could be leveraged for the Internet of Things.

Sources

Use-cases
Libelium, 50 Sensor Applications for a Smarter World,
http://www.libelium.com/top_50_iot_sensor_applications_ranking

Smart contracts
Chih Cheng Liang, A Next-Generation Smart Contract and Decentralized Application Platform, 2016
https://github.com/ethereum/wiki/wiki/White-Paper

Rick Huckstep, What does the future hold for blockchain and insurance?, 2016
https://dailyfintech.com/2016/01/14/what-does-the-future-hold-for-blockchain-and-insurance/

Identity management
Ian Allison, ShoCard raises the bar for digital identity using blockchain, 2016
http://www.ibtimes.co.uk/shocard-technology-brings-digital-identity-cards-banking-ever-closer-1537548

Pete Rizzo, ShoCard's Quest to Secure Identity on the Blockchain, 2015
http://www.coindesk.com/shocards-quest-secure-identity-blockchain/

IoT marketplaces
IBM Institute for Business Value, Empowering the Edge, 2015
http://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf

Kenneth Chu Sam is a Transformation Associate at CORE. He has successfully completed both his bachelors and masters with focus on electrical engineering and information technology, specializing in biomedical technology at the Karlsruhe Institute of Technology. Prior to joining CORE, Kenneth acquired professional experience in the field of strategy development and international project management.

Mail: kenneth.chu-sam@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
www.coreinstitute.org
Phone: +49 30 16344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
www.coretransform.de
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
www.coretransform.ch
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
www.coretransform.co.uk
Phone: +44 203 319 0356
office@coretransform.co.uk