Decentralized Marketplaces for the Computing Continuum

Anthony Simonet-Boulogne, iExec, France
Nicolae Goga, University Politehnica of Bucharest, Romania
Ahmet Soylu, Oslo Metropolitan University, Norway
Dumitru Roman, SINTEF AS, Norway

Abstract

The concurrent increase of cloud computing usage by a majority of application providers combined with the advent of novel IoT, smart cities and mobility applications drive the need for new dynamic and distributed infrastructures. The added pressure on the network, the attention to the carbon footprint of IT services and recent privacy laws are additional motivations to augment the well-adopted public clouds with small data centers (or cloudlets) located closer to the users. This novel paradigm, often referred to as Computing Continuum, is expected to increase the performance of applications while reducing latency and data transfers. However, the Computing Continuum is not a mere evolution of cloud computing, and this paradigm brings unique challenges to the infrastructure. In this brief note, we argue about the need for decentralized resource marketplaces for the Computing Continuum, discuss key features of such marketplaces, and exemplify them with a blockchain-based use case.

Introduction

The Computing Continuum is inherently multi-party

To cover all possible use cases, territories and users the Computing Continuum has to integrate heterogeneous resources along the whole computing chain transparently, from gigantic data centers to in-network and edge devices. Because these resources belong to different providers, locations and administrative domains, the Computing Continuum is inherently multi-party.

Traditional cloud resource management becomes unsuitable on the Computing Continuum
Extensive research has investigated how to manage multi-party cloud infrastructures, including how to monitor servers, and how to place and migrate data and workload in a context where the resources are highly heterogeneous and the network is unreliable (Bertier 2014). Several infrastructure models have been proposed in the last decade, including centralized, hierarchical, and distributed. We argue, however, that while some of these models are physically distributed, they are all logically centralized, since their governance and control lie in the hand of one single entity.

Centralized resource management is impractical on the Computing Continuum

However, in the Computing Continuum centralization is at best sub-optimal, and it can even slow down its development and adoption; first, centralization creates a single point of failure which could impact all applications and users in a large territory; second, scaling centralized decision making (such as workload placement and scheduling algorithms) is not realistic, as it implies either that one actor must know and maintain the complete state of the infrastructure (e.g. the configuration of the servers and their load across many data centers) or that decisions are approximate and based on partial information; third, centralized control in the Computing Continuum implies that individual cloud providers hand over the control of parts of their infrastructure to a third party, which is an unrealistic expectation due to security and sovereignty concerns.

Key features for supporting resources, applications, and data on the Computing Continuum

Feature 1: Trust between all parties
Providers and consumers of computing resources, applications and data in the Computing Continuum must be able to trust each other at a level similar to the trust they have when using a public cloud, although they do not know who they are transacting with. In this context a blockchain-based approach can help set the rules of the infrastructure (e.g. no program can execute without a payment and vice-versa) and make sure they are enforced, without any trusted third party.

Feature 2: Ownership of data and code
Users of applications and data providers must be able to set rules on how their data can be used; similarly, application developers must have their intellectual property protected against theft. This protection role belongs to the platform which must ensure no one in the Computing Continuum (including the platform operators) can bypass or violate the rules that are set by the users.

Feature 3: Diversity of available resources
A platform for the Computing Continuum must offer a large variety of resources (e.g. servers, virtual machines, sensors, actuators, etc.) both in terms of hardware capabilities and location. This is supported by implementing appropriate standards, such as the Web of Things W3C standards.

Feature 4: Ease of accessing (joining/leaving) the market
The availability of diverse resources in the Computing Continuum is favored by the ease of accessing the marketplace, both in technical terms (with ready-to-use connectors for major computing and IoT vendors) and in administrative terms (buyers/sellers of resources only interact with the marketplace, no further contractual agreement is needed).

Feature 5: Fairness of the market
Prices are determined by market mechanism (offer and demand), they cannot be influenced by the operators of the marketplace or anyone else. Further, because the marketplace presents a single access point to several providers, it eliminates the risk of vendor lock-in.

Key enabling technologies for decentralized marketplaces for the Computing Continuum

Decentralized marketplaces represent an important evolution in the way cloud services (e.g. computing, networking, storage, sensing, etc.) are consumed and monetized. This is made possible by the combination of key enabling technologies:

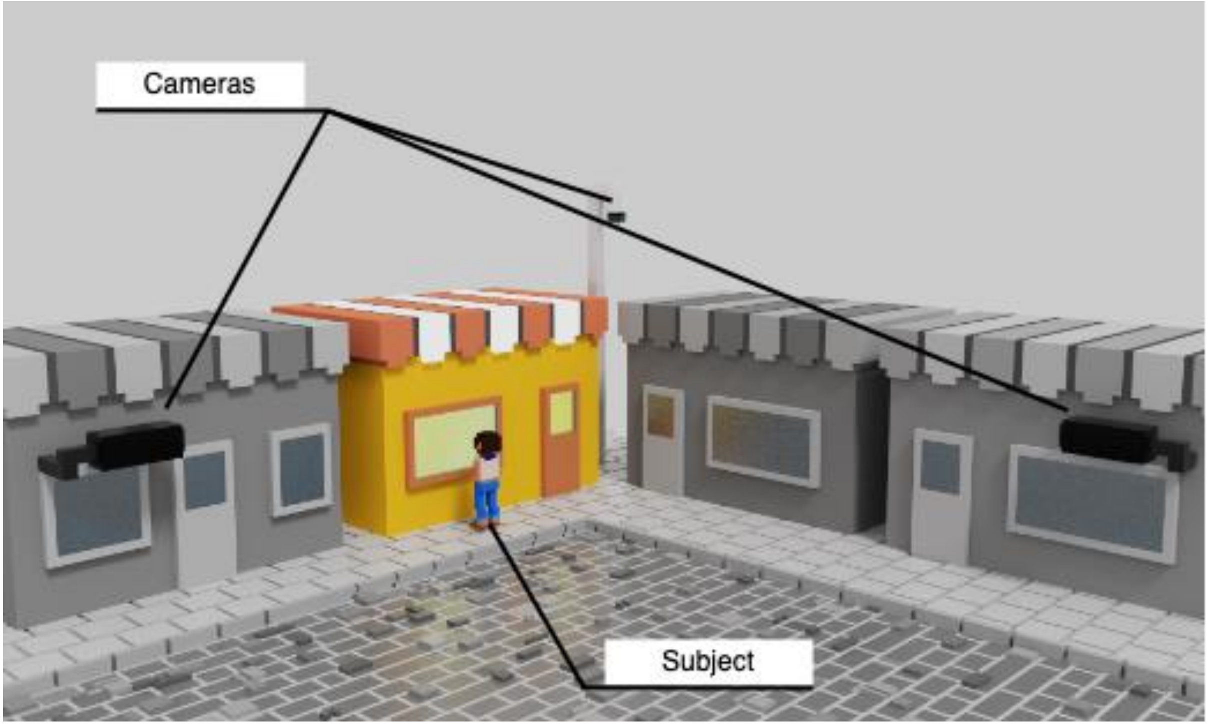
- Decentralized ledger technologies and smart contracts enable all parties in a deal to set immutable rules (e.g. price, which applications/users can access specific data or assets, etc.) and execute payment if and only if all the rules are satisfied.

- Software toolboxes such as the DataCloud toolbox (https://datacloud-project.github.io/toolbox).

- Trusted Execution Environments (TEE) such as the Intel SGX and ARM TrustZone technologies ensure that the off-chain parts of the marketplace (e.g. the middleware, the order book management system).

- Standards such as the W3C Web of things (https://www.w3.org/WoT).

Blockchain-based use case example



The domain of smart cities can offer a variety of relevant use cases (Simonet-Boulogne et al., 2022). Let us consider a concrete use case in the context of a smart city that could benefit from a decentralized marketplace to run a marketing application on the Computing Continuum with security, trust, and privacy. The goal of the application is to process video feeds captured by CCTV and public cameras in a busy commercial street to analyze the behavior of shoppers and wanderers. A traditional approach with one camera filming the entrance of a store from the inside could count the number of people coming into the store, how much time they spend inside the store or whether they made a purchase. By using a camera pointed at the store entrance from the outside, it would also be possible to infer the efficacy of the window display by measuring how much time walkers stop to look at it and how many of them enter the store. By adding even more cameras pointed at different store fronts and with multiple angles, it would even be possible to tell where shoppers are coming from and which other stores they visited before entering the store. This application would face several limitations that can be addressed natively with a decentralized marketplace for the Computing Continuum:

- The marketplace helps finding and provisioning cameras pointed at all the stores in a given area without contracting with the different people and organizations that operate them.
- Owners of such video cameras are incentivized to advertise them on the marketplace because it can easily bring additional revenue to them.
- The image processing code does not implement facial recognition: when detected, people are stored in memory only for a few minutes, in order to reconstruct their path; they are never linked to an identity, and the program deletes them after they leave the observed area. Each detected person is assigned a randomly generated identifier linked to a set of GPS coordinates and additional properties (e.g. light vs. warm clothes, empty hands vs. holding shopping bags, etc.).
- Privacy is ensured by the rules set on the blockchain: the marketplace only allows image processing applications that do not recognize or record faces; any other code will be rejected by the processing resources. The audit of such applications can be realized by a specialized

third party that satisfies regulatory requirements.
- The user of the marketing application is ensured to pay a fair price for the service because competition exists between the owners of video cameras and computing resources.

Summary

The Computing Continuum brings unique challenges to the infrastructure. Traditional resource management methods and techniques developed in the context of the cloud are insufficient. We argued in this brief note for the need for decentralized marketplaces for the Computing Continuum and introduced the key features they would need to support on the Computing Continuum: trust between all parties, ownership of data and code, diversity of available resources, ease of accessing (joining/leaving) the market, and fairness of the market. Furthermore, a blockchain-based approach may be a suitable implementation of such key features, and we exemplified the use of such a marketplace in a smart cities use case. Implementation of blockchain-based marketplaces for the Computing Continuum are currently being investigated in the DataCloud project (Roman et al, 2022).

Acknowledgements. This work received partial funding from the European Commission's Horizon 2020 projects DataCloud (Grant number 101016835) and enRichMyData (Grant number 101070284) and the NFR BigDataMine project (Grant number 309691).

References

Bertier, Marin, et al. "Beyond the clouds: How should next generation utility computing infrastructures be designed?." *Cloud Computing*. Springer, Cham, 2014. 325-345.

Roman, Dumitru, et al. "Big Data Pipelines on the Computing Continuum: Tapping the Dark Data." *Computer* 55.11 (2022): 74-84.

Simonet-Boulogne, Anthony, et al. "Toward blockchain-based fog and edge computing for privacy-preserving smart cities." *Frontiers in Sustainable Cities* (2022): 136.