

AIMS 2018, June 4 - 5, Munich, Germany

Leveraging Smart Contracts for Automatic SLA Compensation – The Case of NFV Environments

Eder John Scheid, Burkhard Stiller

*Department of Informatics IFI, Communication Systems Group CSG,
University of Zürich UZH
{scheid, stiller}@ifi.uzh.ch*



**Universität
Zürich^{UZH}**

Motivation
Background
Approach
Conclusions



Introduction

- ❑ What is an **Service Level Agreement (SLA)**?
 - Contract between a Service Provider (SP) and a client
 - Describes requirements that must be met
 - SLAs do not determine how a service is to be delivered
- ❑ Examples:
 - Web server must have 99.99% of **Availability** (uptime)
 - Database server **throughput** ≥ 1 Mbps
 - VoIP **latency** ≤ 50 ms

If an SLA is not met → **SLA violation**

Motivation

- ❑ Typically, SPs and clients **do not trust** each other
 - Service must be monitored
 - Support of the SLA violation claim (client)
 - Evidence of SLA compliance (SP)
 - Monitored data must be trusted by both parties

- ❑ SPs must **compensate** the client according to the SLA, if a validation occurred
 - Penalty described in the SLA
 - Monetary penalties or credits on next service period
 - *E.g.:* 10% money back or 10% deducted from next bill

Current Compensation Process (Example)

- ❑ Example: Amazon Compute SLA
 1. Client opens a formal case in the AWS Support Center
 2. Submit a claim with “SLA Credit Request” in the subject line
 3. Inform **dates** and **times** of **each unavailability incident**, and **the affected services** (instances or volumes)
 4. Send request **logs** (replacing or removing **sensitive information**) that document the errors and that corroborate the claimed outage



Evaluation of Current Process

- ❑ If the request is confirmed by the responsible team
 - Compensation is paid (in the form of credits)
 - Next billing cycle (1 month)

- ❑ If one party fails to provide necessary information or the team does not acknowledge the claim
 - Compensation is not paid

- ❑ Process is manual, complex, and prone to errors

Blockchains

- ❑ Blockchain (BC) characteristics
 - Append-only decentralized ledger
 - Data is replicated and agreed upon by all participants
 - Each block is cryptographically linked to previous block
 - Hard to tamper with
 - ❑ Smart Contract (SC) characteristics
 - Executable code
 - Runs on a given blockchain
 - Executes immutable agreements between parties
 - No third-party intervention
 - BCs automatically executes the contract
- Blockchain-based SCs may help to manage SLAs

Combining Compensation and Blockchains

- ❑ **Guarantee** of contract enforcement
 - SP will receive the fee for the service
 - Client will receive the compensation in case of violation

- ❑ **Immutability** of the data
 - SLA terms will not change
 - Monitored data will not change
 - Data can be trusted by both parties

- ❑ **Compensation process may be well simplified!**

Derived Research Questions (RQ)

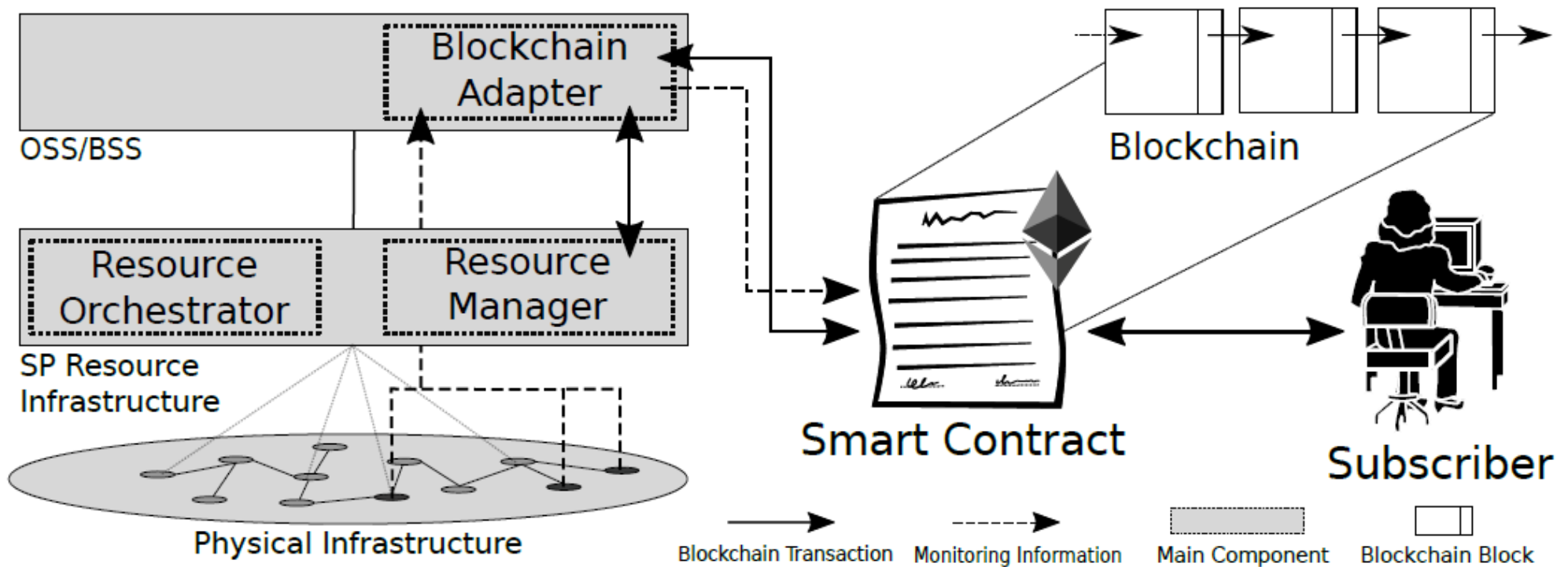
1. How **long** does it take to detect an SLA violation and pay the compensation to the subscriber using SCs?
2. How **complex**, regarding human-computer interaction, is the approach proposed compared to existing solutions?
3. How to **monitor** the terms of the SLA and resources, while providing trust in the data monitored to all involved parties?

BC-based Compensation Approach

- ❑ Translate SLAs into SCs
 - Based on SLA text applicable to measurable data
- ❑ Automatically manage
 - Measurement data persistence in blockchain
 - Compensation payment
 - Subscription payment
 - Trusted SLA monitoring
- ❑ Client and SP interaction performed using the SC
- ❑ Relies on a Turing-complete language
 - Implement of many compensation functions possible
 - Solidity language → Ethereum blockchain



BC-based Compensation Architecture

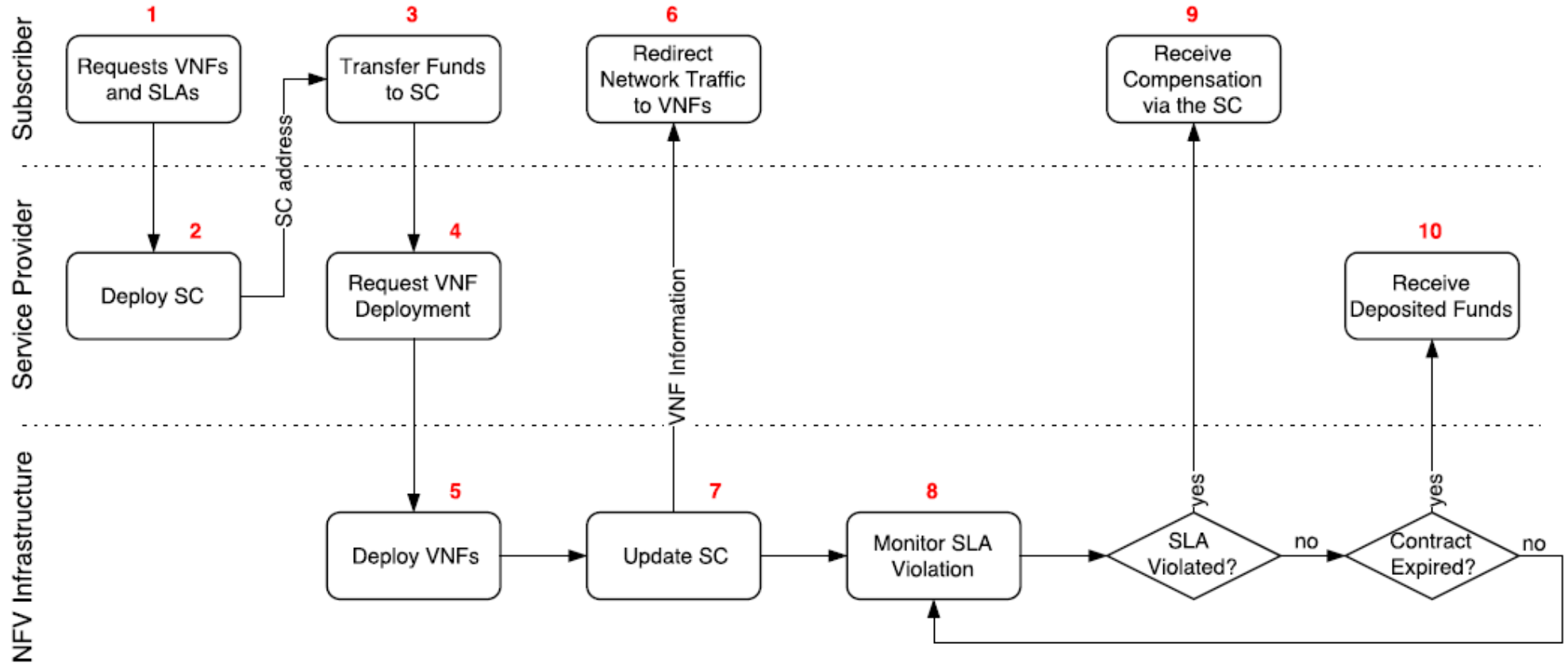


Proof-of-Concept: The NFV Case

- ❑ Network Function Virtualization (NFV)
 - Virtualize physical middleboxes
 - Host them on standard hardware
- ❑ Virtualized Network Functions (VNF)
 - Fast to deploy (virtual)
 - Easy to scale Horizontally/Vertically
- ❑ VNFaaS provider SLAs examples:
 - Single VNF (FW, DPI, Video Cache)
 - VNF throughput $\geq x$ Mbps
 - Chain of VNFs (FW $\rightarrow$ DPI, FW $\rightarrow$ Video Cache)
 - Packet loss $\leq x\%$

aaS: as-a-Service
FW: Firewall
DPI: Deep Packet Inspection

NFV Compensation Work Flow



Preliminary Conclusions

- ❑ Automatic payment of SLA compensations possible
 - Applying blockchain-based SCs
 - NFV case determined as a proof-of-concept
- ❑ SC-based solution helps to reduce or avoid
 - Managerial activities on SPs and clients side
 - Manual Interaction
 - Complexity
- ❑ Other SLA management tasks with potential benefits
 - SLA negotiation
 - SLA enforcement

Next Steps

- **Refinement** of payment procedure
 - Lock payment until end of contract?
 - Pay compensation when SLA violation is detected?} RQ1

- **Determination** of SC content
 - All SLAs?
 - Key SLA terms?} RQ2

- **Definition** of trusted monitoring approach} RQ3

- **Investigation** of the legal validity of the SC
 - Involving third-parties to solve disputes?

Thank You for Your Attention!



Questions?
scheid@ifi.uzh.ch