DEP – Future Management Challenges: Blockchain-based Management Services and Applications

Burkhard Stiller
Communication Systems Group CSG
Department of Informatics IfI
University of Zürich UZH
stiller@ifi.uzh.ch

With many thanks to Thomas Bocek, Sina Rafati, Bruno Rodrigues, Eder Scheid, David Hausheer

Universität Zürich[UZH]

Blockchains (Recall)
Services & Applications
Conclusions and Concerns

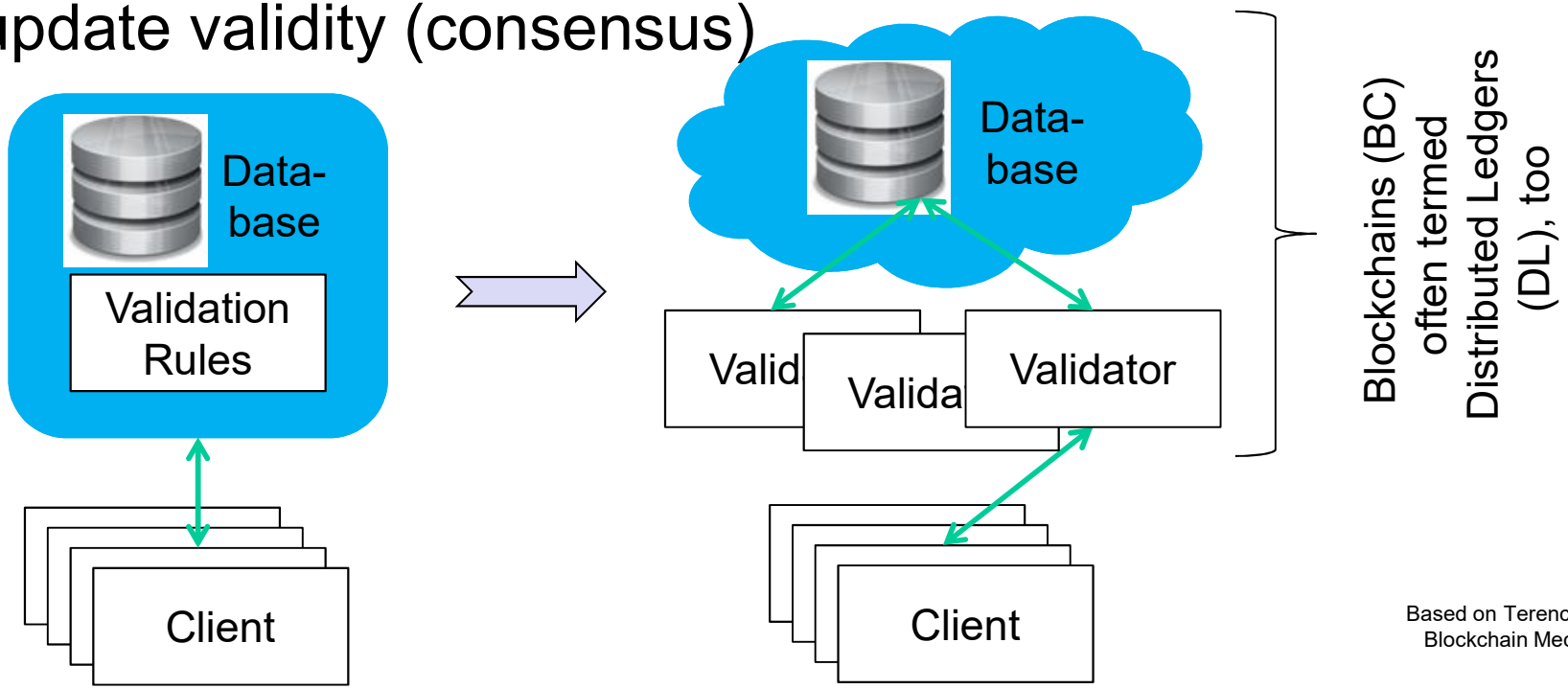
CSG
Communication Systems Group

ifi

Key Idea: “Replacing” (Central) Databases

- Blockchains (BC) replace clients’ access-protected writes to an authoritative database via validation rules by a distributed consensus of many validators
  - where the database’s state depends on majority agreement of update validity (consensus)

Reminder



Based on Terence Spies:
Blockchain Mechanics

Managing BC Networks: A Non-challenge

- There is no need to explicitly manage BC networks due to their networked P2P protocols applied and their fully distributed operations. That especially means:

Reminder

1. Blockchains ***do not*** have a relevant impact on general networking, however, “unreliable” networks do have an impact on the BC
   - Especially in case of longer outages
2. Blockchains ***do not*** have a relevant impact on Distributed Systems, however, the full decentralization is (very) costly (PoW) or still not secure (other Po”X”)
   - Especially (in case of PoW) BC-related energy demands

PoW: Proof-of-Work

Management Assumptions and Questions

- Under the assumption that someone likes blockchains being used as a mechanism for management tasks:
  - Many non-trusted stakeholders are involved
    - *E.g.*, competitive ISPs, but forced to cooperate across their domains
  - Volume/frequency of data required to be persisted (either events, suggestions, mandatory commands) remains small
    - *E.g.*, compression applied, hashing acceptable, storage off-chain
- Are then, *e.g.*,
  - BC-based, automated DDoS mitigation or
  - BC-based, automated SLA compensation or
  - BC-based, automated ISP-user contracting (set-up)

  possible?

Category
Security
Service
Business

Managament

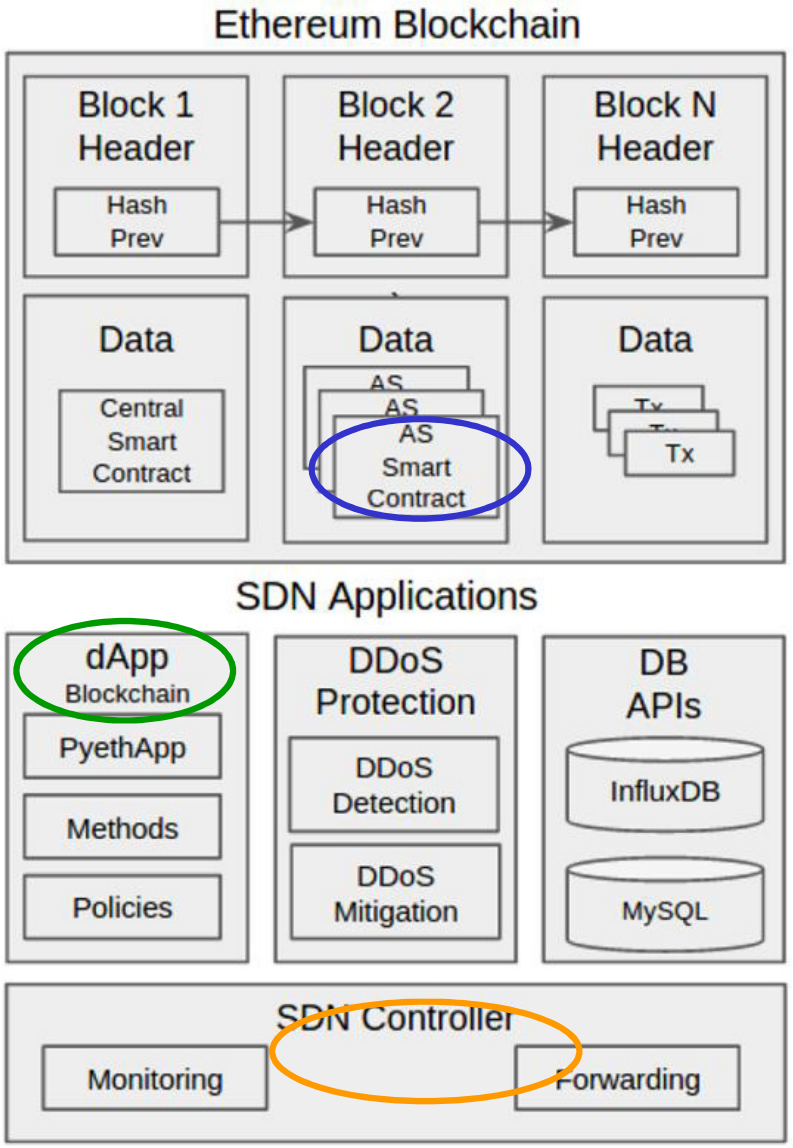
DDoS: Distributed Denial-of-Service; SLA: Service Level Agreement

Blockchain Signaling System (BloSS)

- DDoS defense systems are not capable of withstanding by themselves against large-scale attacks
  - Cooperative, multi-domain DDoS Defense is key
- Operations under the assumptions
    - ASes maintain a BC account, IP addresses known for ASes
    - ASes show a mechanism to retrieve IP addresses affected
  - ASes may request protection by submitting a transaction to their Smart Contract (SC) with a list of IP addresses
  - Requested ASes may accept or deny requests based on their security policies or SLAs
  - A transaction is completed when a log, showing actions, is submitted in response to a defense request

AS: Autonomous System

BloSS Architecture and Prototype

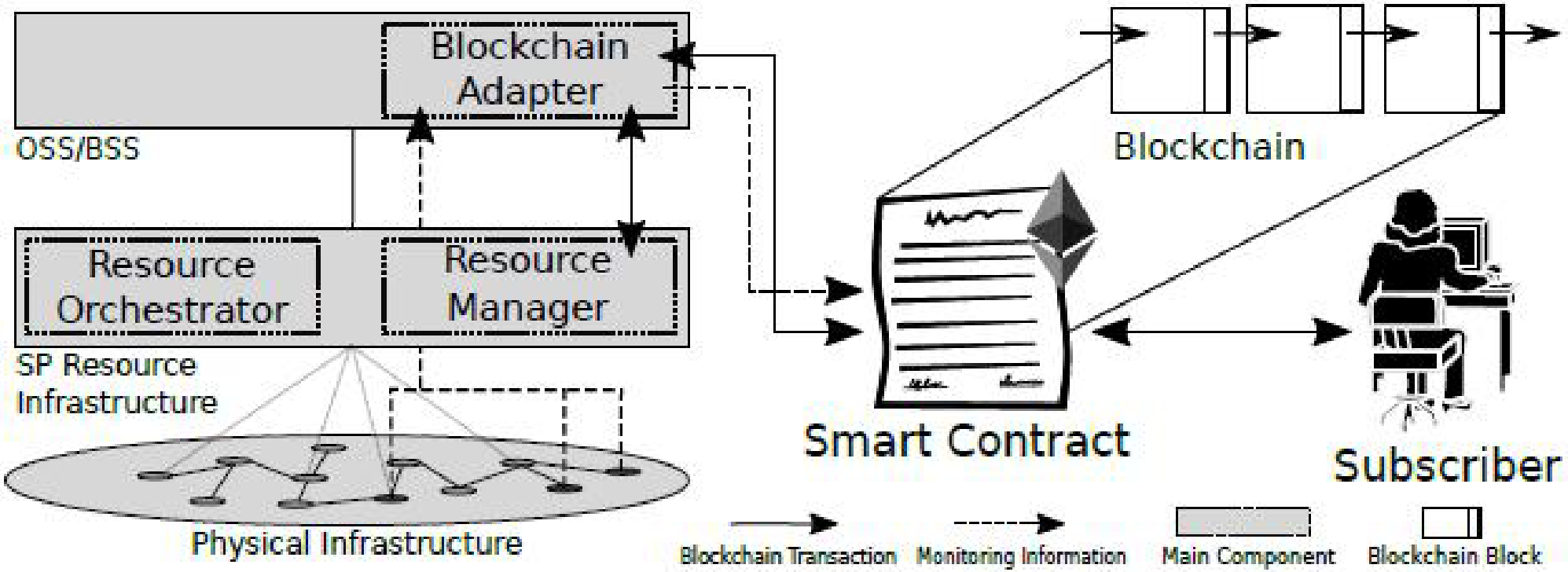


- 3 layers
  - SCs are deployed in Ethereum
  - Local dApp interfacing with the BC to report/retrieve addresses
  - Ryu SDN controller monitors or enforces rules in OpenFlow switches

- Prototype
  - Existing DDoS detection rules
  - AS SCs store addresses so that the entity that owns the contract performs an action required by other entities

BC-based, Automated SLA Compensation

- Management of SLA compensations is cumbersome and bureaucratic
  - Needed by customers, “feared” by providers (manual process)
  - Blockchain-based SCs potentially simplify this process



Conclusions and Concerns

3. Traditional Network&Service Management methods ***still do their job!*** *BCs* ***do not (yet)*** *revolutionize management*

- BC-based management tasks seem to be feasible
  - BloSS is cooperative among non-trusted stakeholders
    - "Private" BCs may provide a higher degree of privacy, but at the cost of transparency; at the same time at no need of a "costly" database operation
  - SLA compensation will minimize handling costs due to execution of SCs as soon as the agreed upon event(s) happen
- But concerns on BC-based management mechs remain
  - Efficiency gains in real operations need to be proven (still)
    - Transaction rates for BloSS and the compensation case are/may be "ok"

4. Long-term security management in BCs is key, unsolved

- Transparency vs. anonymity, performance vs. sustainability

Thank you for your attention.