

SOLIDITY IN THE CLOUD

LEVERAGING THE BLOCKCHAIN AND
SMART CONTRACTS FOR CLOUD
GOVERNANCE

Roberto Reale @ Viduo

OUR AGENDA

1. Going Trustless
2. Pacta Sunt Servanda
3. Three Governance Scenarios
4. And Beyond



GOING TRUSTLESS

BLOCKCHAIN

- No central authority in control
- No need to trust your counterpart to perform their obligations or properly record transactional data
- Game Theory is used to model incentives
- Cryptography guarantees security as well as privacy

PACTA SUNT SERVANDA

A smart contract is a computerized transaction protocol that executes the terms of a contract.

— Nick Szabo, Smart Contracts, 1994

SMART CONTRACTS

- The blockchain acts as a Virtual Machine
- Cryptographically stored
- Operate autonomously
- Typically, have a long lifetime

Solidity is a contract-oriented, high-level language for implementing smart contracts over the Ethereum Virtual Machine

```
helloworld.sol x JS 1_initial_migration.js
1  pragma solidity ^0.4.22;
2
3  contract helloWorld {
4
5      function PrintHelloWorld () public pure returns (string)
6      {
7          return 'Hello World !';
8      }
9
10 }
```

THREE GOVERNANCE SCENARIOS

Blockchain Ecosystem

OpenStack

Identity

Keystone

Certificate Authority

Barbican

Node Ledger Storage

Cinder / Swift

Stack Management

Heat

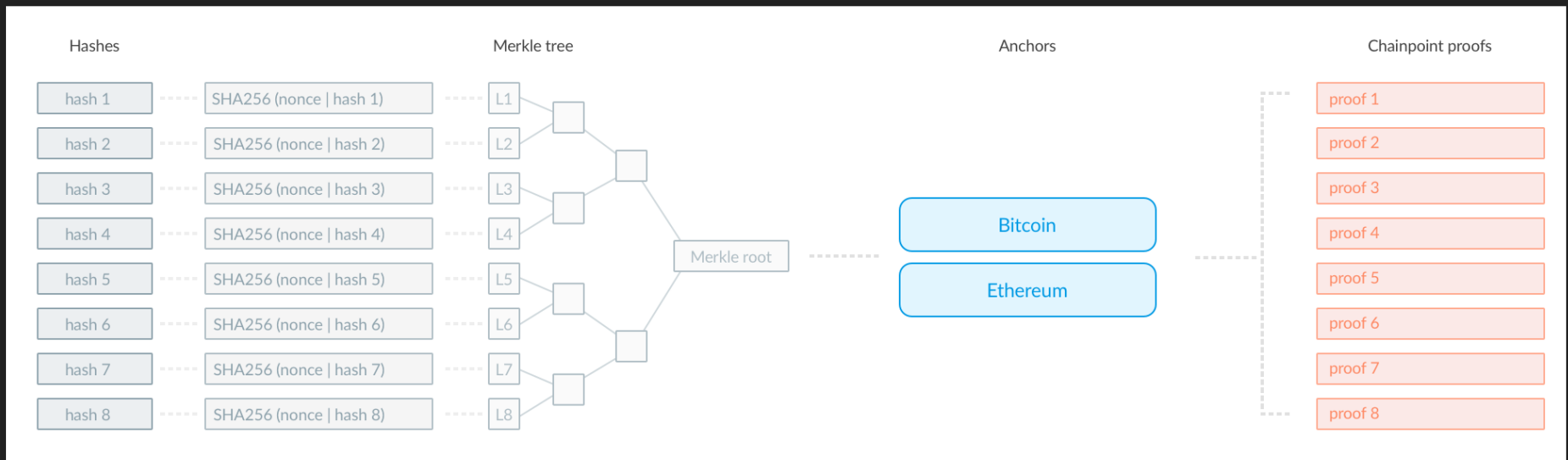
DNS

Designate

Adapted from [Blockchain and OpenStack - Building Trusted Chains](#)

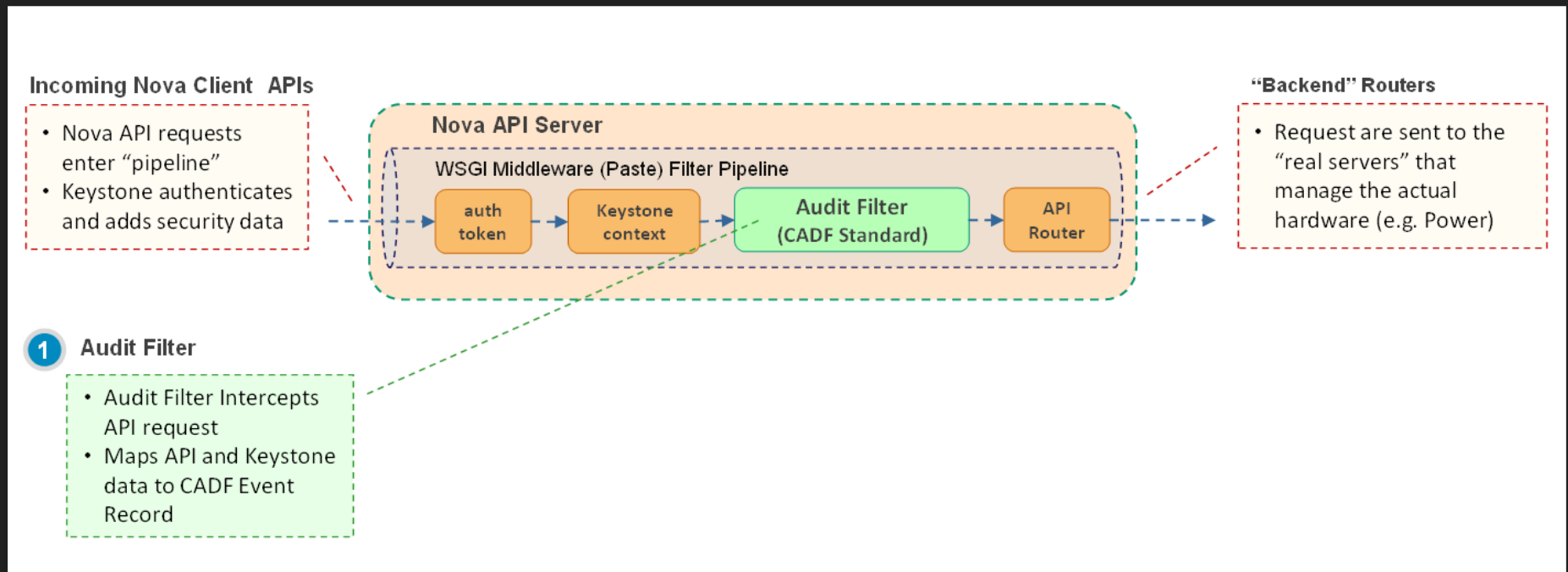
SCENARIO #1: IMMUTABLE AUDIT TRAIL

Chainpoint is an open standard for linking data to the blockchain to create a timestamp proof



Source: [Chainpoint.org](https://chainpoint.org)

The Keystone middleware library is able to audit API requests for each component of OpenStack



Source: [OpenStack.org](https://openstack.org)

Pros

Simplicity
Cost
effectiveness

Cons

Needs a trade-off between on- and
off-chain data in case of heavy
logging

SCENARIO #2: BILLING FOR CLOUD RESOURCES

Pros

Smart contracts are used to enforce payments
Fine control of resource consumption

Cons

VAT regulations for cryptocurrencies

SCENARIO #3: SMART GOVERNANCE

Using smart contracts to orchestrate the cloud by
calling the Heat API.

This is the most challenging scenario.

CAVEAT: Most blockchains (e.g., Ethereum) are designed to be entirely deterministic.

Hence making API calls from inside a smart contract (e.g., a Solidity program) is forbidden.

FIRST SOLUTION: We accept data inputs from more than one untrusted party and then execute the data-dependent action only after a number of them have provided the same answer.

INEFFICIENT

SECOND SOLUTION: We demonstrate that the data is genuine and untampered (auditable VMs, Trusted Execution Environments, ...).

Oracles (e.g., Oraclize) can act as data carriers,
building a reliable connection between APIs and the
smart contract

And we can build others.

Pros

Cons

Extremely powerful

Tricky to implement

AND BEYOND

BLOCKCHAIN INTEROPERABILITY (SIDECHAINS, COSMOS, AION, ...)

ZERO-KNOWLEDGE CRYPTOGRAPHY (ZCASH)

DECENTRALIZED AI-POWERED GOVERNANCE

THAT'S ALL, FOLKS (ALMOST)

Roberto Reale

- Mixed background (math, CS, economics, a touch of humanities)
- FOSS contributor
- Consultant for e-government
- Enthusiast of technology as an enabler for democracy

viduo.eu

Viduo is an open think tank based in Rome

- Digital democracy
- Privacy and data security/protection
- The Digital Single Market and EU funding
- Policymaker engagement
- Institutional and corporate communication

<https://reale.me/solidity-in-the-cloud-2018>