Decentralized Consent Management Platform for Monetization of Energy Data

FH Hagenberg, 2023
Michael Zauner

Presentation: Bachelor Project

"Energy Community" from **https://energiegemeinschaften.gv.at/**

Introduction

- Extension to the eCommunity Platform project (since 2nd semester)
- **Goal:** share and sell energy data between members of the platform
- **Requirements:**
  - find sharing partners
  - make an agreement about the energy data
  - secure storage of the agreements
  - payment for the energy data
- **Conclusion:** Decentralized Consent Management Platform on a private Blockchain with payments in a cryptocurrency

Definitions

Definition - Consent

Permission for something to happen or agreement to do something. The consent may be given for processing personal information, financial agreements, marketing purposes and many more.

Definition - Consent Management Platform

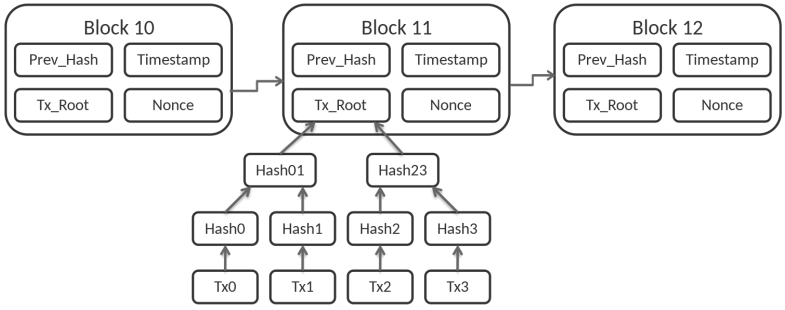
is a technology to obtain the legal consents from users to process their personal data, typically through cookies and terms and conditions.

- Collection: collect the consent from the user
- Storage: store the given consent according to use-case
- Usage: make usage of the consent transparent

Blockchain

Definition: Blockchain

A blockchain is a decentralized digital ledger that records transactions across multiple computers. Each block contains a unique cryptographic code linking it to the previous block, creating a secure and transparent chain of information that cannot be altered retroactively.



System Design

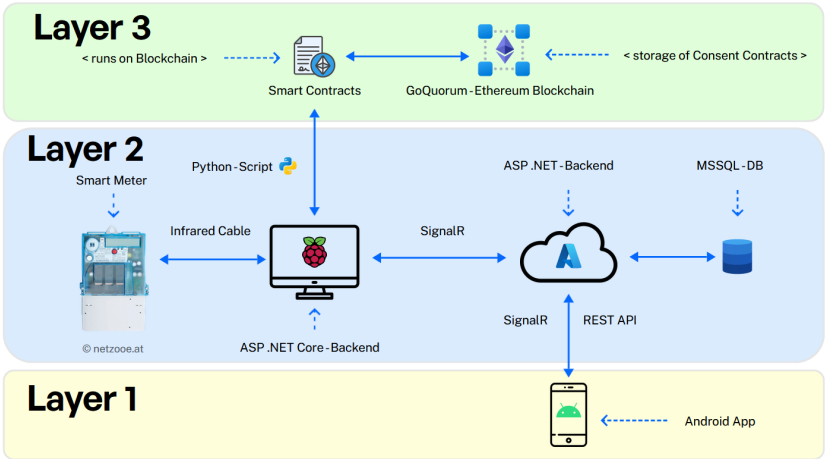
Consent Contract

Contract between two parties about the consent of one's energy data.

Parameters:

- **ProposerId**: want the consent from the consenter
- **ConsenterId**: gives the consent to the proposer
- **TimespanEnergyData**: timespan of the energy data
- **ValidityOfContract**: validity date of the contract
- **DataUsage**: usage of the energy data
- **TotalPrice**: price of the energy data

3-Layer Technical Architecture



SignalR: realtime communication (Remote Procedure Calls)

Implementation

Layer 3 - Blockchain

- GoQuorum Blockchain - fork of Ethereum
- QBFT - Consensus: Quorum Byzantine Fault Tolerance (Proof of Authority)
  - Validators: validate and process transactions
  - Members: can only create transactions but cannot validate them
- Cryptocurrency is Ether - ETH (only valid in this private network)
- Peer Discovery via Static Nodes hosted on a cloud

Layer 3 - Smart Contracts

- written in Solidity programming language
- compiled as EVM bytecode and deployed to an address (e.g: 0x1aE0EA34a72D944...)
- interaction with Python (Web3py - library)

ConsentContract
defines a consent contract between two involved parties with all necessary parameters.

- deposit(): send ETH to the contract
- withdraw(): transfer ETH from the contract
- revoke(): revoke the given contract
- ...

ConsentContractFactory
used as the factory for consent contracts. Deploys the base contract's and manages it's addresses inside an array.

- create(): deploys a ConsentContract
- getContracts(): returns contract for an user
- ...

Layer 2 - Cloud & Local

Cloud

- ASP .NET Backend, hosted on Azure
- SignalR Connection Hub
- Blockchain Controller: communication to the Raspberry Pi's Blockchain node
  - getAccountBalance(): returns the balance in ETH
  - createConsentContract(): creates new consent contract
  - getContracts(): returns the contracts for an user

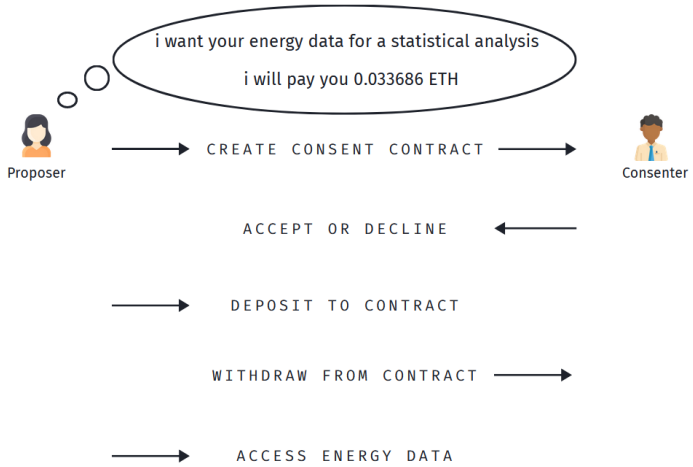
Local - Raspberry Pi

- ASP .NET Core Backend
- SignalR Listener and GoQuorum Blockchain node
- reveices SignalR calls and executes Smart Contract functions

Layer 1 - Android

- search for members (stored in MSSQL DB on Azure)
- blockchain dashboard (account balance & contracts)
- consent management actions (accept, reject, revoke and manage consents)
- once a contract is active, energy data is synced directly to the Android device (in RoomDB)

Layer 1 - Android



Android - Demo

Summary

Conclusion - Is the blockchain technology suiteable for a CMP?

- In short Yes, due to the immutability of the consent contracts and the participants may not need to trust a central authority
- Down side (Ethereum): transaction may take some time to be validated (10s Block Time)

Outlook

- Different Payment methods: Bank transfer, PayPal, BTC, ...
- Visualization of Energy Data: chart diagrams
- Export to other format: csv, db inserts, ...