Decentralized authorization of access to energy data

Erwin Rooijakkers
September 18, 2017

1 INTRODUCTION

The Ethereum blockchain is an immutable, distributed ledger with a virtual machine [1]. Using peer-to-peer technology and cryptography no trusted third party is necessary to keep an "official" copy of the state of the Ethereum Virtual Machine (EVM). Code in so-called "smart contracts" can be executed and publicly verified. To change the state of the blockchain fees have to be paid in cryptocurrency (Ether). Querying the Ethereum blockchain is free and can be done by anyone with access to the ledger.

In Figure 1.1 obtained from [1] based on [2] the Ethereum blockchain is visualized. The Ethereum blockchain is a "chain" of "blocks" that is shared over every node in the network. Each block consists of a hash of the previous block, transactions (transferring the cryptocurrency Ether from one address to another) receipts (state changes) and state (the state of the EVM). To reach consensus on the state of the blockchain various algorithms can be used, the most famous ones being Proof of Work (PoW) and Proof of Stake (PoS). In PoW consensus is reached by the solution of a cryptographic puzzle, that takes computer power to solve. Because it takes so much computer power, the network can trust that the result was reached by consensus (it would take an attacker lots of computer power to built a longer chain). In PoS trust is reached because people who are invested in the network set aside their cryptocurrency to stake for receipts and transactions that have happened. Ethereum currently works with the former, but will switch to the latter sometime this year.

Within Alliander various projects (like Tippiq, HelloData, and GateKeeper) work on the use case of authorizing the access of energy data for P1-device to app, so that the consumer

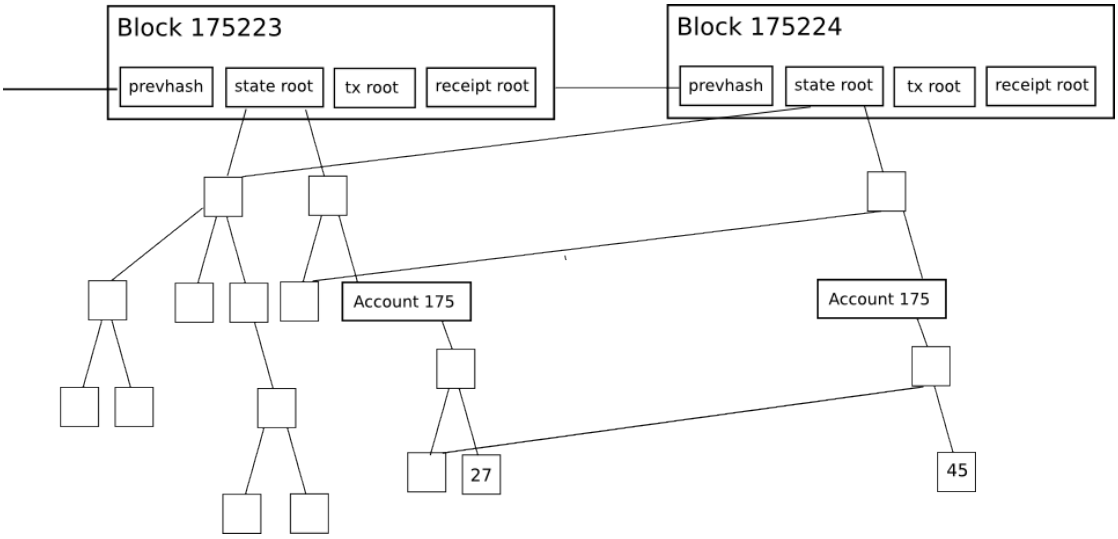

Figure 1.1: Ethereum blockchain stores three kinds of information: transactions, receipts, state.

is in control over his data. Because of the characteristics of the blockchain (immutability, decentralization, independence, automatic settlement), it might be beneficial to decentralize the authorization business logic on a public or private blockchain.

In this document a prototype of authorizing energy data on the Ethereum blockchain will be shown. Then the benefits and limitations will be discussed.

2 AUTHORIZING ENERGY DATA ON THE BLOCKCHAIN

There are three entities at play when authorizing access to energy data:

1. A device (IoT-device that provides energy data)
2. Consumer (owner of a IoT-device)
3. App (service provider that wants to do something with energy data)

The consumer, app, and device need to have an address on the Ethereum blockchain (key pair). Because of the properties of blockchain addresses we can be sure that the actions are executed by the entities involved. A device can be claimed by a consumer. And a consumer can then give access to the app. Finally, a device can check if an app has access.

A smart contract that implements this logic is shown below in 3.

3 Prototype

```
pragma solidity ^0.4.10;


import "Mortal.sol";


contract SmartEnergyAuthorizations is Mortal {

  // Mapping from device to consumer
  mapping(address => address) claims;

  // Mapping from device to app to authorization flag
  mapping(address => mapping(address => bool)) authorizations;

  // Constructor
  function SmartEnergyAuthorizations() {
    owner = msg.sender;
  }

  function claimDevice(address consumer) {
    address device = msg.sender;
    claims[device] = consumer;
  }

  function authorize(address device, address app) {
    address consumer = msg.sender;

    require(claims[device] == consumer);

    authorizations[device][app] = true;
  }

  function revoke(address device, address app) {
    address consumer = msg.sender;

    require(claims[device] == consumer);

    authorizations[device][app] = false;
  }

  function isAuthorized(address app) constant returns (bool) {
    address device = msg.sender;

    // NOTE: Returns false when no entry for device, or for
    // device and app, exists in the ‘authorizations‘ mapping.
    return authorizations[device][app];
  }

}
```

It is possible to interact with the smart contract via the front-end deployed on `http://erooijak.simple-webhosting.eu`.

4 Discussion

- Performing the transactions (e.g., register device) costs money (gas fees on Ethereum blockchain). This means that the consumer and device have to pay. The IOTA Tangle

blockchain does not have this limitation [3]. It can also share energy data between IoT-devices in an encrypted manner.

- When a device changes owner the old authorizations are taken along to the new consumer. To fix this another data structure needs to be used, that can be iterated over and cleaned when switching ownership. For example an IterableMapping type.
- The list of devices for a consumer are not iterable. To provide a convenient user interface around the smart contract back-end these types of information needs to be queryable.
- A consumer cannot provide a granularity of access to a device (e.g., only part of the data of a device, like only realtime data but not the history). To fix this other data structures need to be used in the contract, like the IterableMapping mentioned above. Where also the capabilities of the device can be stored in.
- Scalability. If a lot of devices and authorizations are stored in the smart contracts it might lead to performance problems for large arrays.
- Authorization data is publicly available and inspectable. This needs to be solved by a proper anonymous identity management system like IRMA [4] or Sovrin [5], where only the attributes of an identity that are necessary (e.g., does a consumer live on the address of the device?) are available, in a non-identifiable manner.

5 Conclusion

Authorizing access to energy data on the Ethereum blockchain is doable. All the benefits of the blockchain become automatically available by doing this. The authorization data information cannot be tempered with. It provides an immutable audit trail for inspecting events.

There are some limitations like high transaction costs, limitations of the contracts, and identity management. A combination of IOTA, new data structures, and an identity management system (like IRMA [4] or Sovrin [5]) will help solve this.

I am convinced of the benefits of blockchain technology for energy data and hope to built a type of data authorization gateway backed by blockchain.

References

[1] V. Buterin. A next-generation smart contract and decentralized application platform. `https://github.com/ethereum/wiki/wiki/White-Paper`. Accessed 09-18-2017.

[2] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`. Accessed 09-18-2017.

[3] S. Popov. The tangle (version 0.6). https://iota.org/IOTA_Whitepaper.pdf. Accessed 09-18-2017.

[4] B. Jacobs. I reveal my attributes. https://www.irmacard.org/irma/. Accessed 09-18-2017.

[5] Sovrin Board of Trustees. Sovrin provisional trust framework. https://sovrin.org/wp-content/uploads/2017/06/SovrinProvisionalTrustFramework2017-03-22.pdf. Accessed 09-18-2017.